

NATIONAL INFRASTRUCTURE PROTECTION

EMERGING TECHNOLOGIES

APRIL 2012

Disclaimer:

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI or QinetiQ. The views and opinions contained within the technology maps are those of QinetiQ unless attributed to another source and shall not be used for advertising or product endorsement purposes.

Furthermore the information contained within this document was deemed accurate at the date of publishing but is expected to become outdated quickly (particularly in areas where research and development is occurring more rapidly).

To the fullest extent permitted by law, CPNI and QinetiQ accept no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances. Readers should be aware that they use the information contained within the technology maps at their own risk.

Contents

Contents	2
Introduction	3
This document	3
Technologies and techniques	3
Enhanced protection / Security compromise	3
Top 20 Critical security controls.....	4
QinetiQ's Technology map	4
Technology / Technique: Authentication Technologies	5
Technology / Technique: Behavioural / Gestural Analytics	8
Technology / Technique: Building and Environment Management Systems.....	11
Technology / Technique: Cloud Computing.....	14
Technology / Technique: Cloud Security.....	17
Technology / Technique: Future Collaboration Tools	20
Technology / Technique: Context-Aware Computing and Context-Enriched Services.....	23
Technology / Technique: Data Erasure	26
Technology / Technique: Data Recovery.....	29
Technology / Technique: Digital Trust Technologies	32
Technology / Technique: Emotion and Facial Recognition.....	35
Technology / Technique: Next Generation (Heuristic) Anti-Virus	38
Technology / Technique: High Security Wireless Communications for Civilian Use	41
Technology / Technique: Malware Detection.....	46
Technology / Technique: Cross Domain / Multi-level Security Solutions.....	50
Technology / Technique: Near Field Communication	53
Technology / Technique: Network Forensics.....	56
Technology / Technique: Future Protocols for Network Security	59
Technology / Technique: Next Generation Human Computer Interaction (HCI).....	62
Technology / Technique: Novel obscuration techniques for windows	65
Technology / Technique: Operating Systems Security	68
Technology / Technique: Protective Monitoring	71
Technology / Technique: Tamper Evident and Proof Seals for IT Equipment	77
Technology / Technique: The Future of Smart Meters for Home and Industry	80
Technology / Technique: Social Analytics	84
Technology / Technique: Supply Chain Integrity.....	87
Technology / Technique: Ultra-Mobile Computing Devices (including Smart Cameras).....	91
Technology / Technique: Virtualisation	94
Technology / Technique: Visualisation for network security.....	97
Technology / Technique: Web-based mail and Instant Messaging in business	100
Technology / Technique: Wireless Power	108
Technology / Technique: 'Big Data' - extreme information management	111
Annex A – Critical security controls.....	114

Introduction

The work presented in this document has been undertaken to increase awareness of technologies and techniques that may have an impact on the future protection of national infrastructure.

This document

This document is comprised of three-page summaries of technologies and techniques that are considered to be relevant to protective security.

The reader should be aware that this is not an advice document. The information is provided in order to stimulate interest and to promote further reading on subjects that may have future relevance to protective security. All of the technology pieces have been written and compiled for CPNI by the Technology Tracking and Forecasting Group at QinetiQ. As such, the reader should understand that all information is supplied by QinetiQ and any opinions, comments and forecasts, unless attributed to another source, are those of QinetiQ. It should be noted that all background research and summary production has been undertaken by QinetiQ on behalf of CPNI.

CPNI has commissioned this work in order to inform and to inspire a diverse audience working mainly within the UK national infrastructure. Each technology / technique piece has been written in a consistent format that has been designed to present, summarise and promote further investigation.

Technologies and techniques

This work covers technologies/techniques primarily within the Information Security discipline. All the technologies considered are already in existence and are at some stage of development, with a clear exploitation path.

Techniques have also been covered by this work. For this work a technique is defined as a way of using a given technology or collection of technologies, to achieve a desired outcome.

The summaries provide predicted maturity for each technology/technique at three, five and ten years from time of writing (2012).

Enhanced protection / Security compromise

The technologies and techniques covered in this work have been selected on the basis that they may:

- Offer an opportunity to enhance existing protective security measures.
- Present an opportunity to compromise protective security measures.
- Both of the above.

Topics have been selected by CPNI based on inputs from national infrastructure owners/operators and from other parts of UK Government. QinetiQ have also contributed to this list of topics.

The technologies/techniques list has been analysed to establish the most prominent topics – subsequently covered in this document.

It should be noted that the information provided is indicative. Also, the information provided, including lists of references, policy documents etc, is not exhaustive.

Top 20 Critical security controls

Most of the technologies/techniques covered within this document are cyber security related. Where possible, a technology/technique is linked to one or more of the SANS Top 20 Critical Security Controls (see Annex A). Within this document reference is made to Version 3.1 of the Critical Security Controls – the order of the controls may change in subsequent versions so it is important that this document is read with reference to Version 3.1.

The Top 20 CSC is a prioritised list of measures that organisations should implement in order to improve the security of computer systems and networks. The list, with full description, is published by SANS and can be found at www.sans.org/critical-security-controls/

QinetiQ's Technology map

QinetiQ's 'technology maps' are designed to be short but very informative briefs with forecast information covering technologies or related material such as technology trends. They are intended to provide the reader with a quick understanding of the readiness (maturity), capability and potential business impact of the topic they present.

With few exceptions, the technology maps presented in this work contain roadmaps that show the expected development of the technology, technique or trend over time. Many of the roadmaps show this development in three stages covering the 2 to 5, 6 to 9 and 10+ year timeframes from the time of writing. Where possible the roadmaps also show development in terms of maturity. In these cases a colour scale is used to indicate the gradual (or rapid) change in the subject's level of maturity.

<p>Technology / Technique: Authentication Technologies</p>	<p>Relevant to SANS Critical Control: 12, 15, 16</p>						
<p>Description</p> <p>Authentication is the process through which the identity of the user (human or computer) is established as being whom or what it claims to be. It is a means of verifying identity. Robust authentication is a key enabling component of many of the SANS Critical Security Controls, including ‘Controlled Access Based on the Need to Know’ and ‘Account Monitoring and Control’.</p> <p>Authentication technologies enable this process to be performed and include a wide range of products and services that implement methods far beyond that of traditional password-based authentication. These methods can be broadly split as follows:</p> <ul style="list-style-type: none"> • Knowledge-based authentication (KBA): This includes use of improved password methods and techniques that exploit things only known to the user (such as imagery or patterns). • Authentication tokens: Includes One-Time Password (OTP) hardware tokens and smart cards, which are held by the user. • Biometric authentication: This is based on the biological characteristics and/or behavioural traits that are known to be inherent to a particular user. <p>Quite often, two (or more) of the different classes shown above can be combined to provide ‘two-factor authentication’ or ‘multi-factor authentication’. Not relying on a single authentication factor is also known as ‘strong authentication’.</p>	<div style="text-align: center;"> <h2>Authentication Technologies Roadmap</h2> </div> <table border="1" style="width: 100%; text-align: center;"> <thead> <tr> <th style="width: 33%;">2 – 5 years</th> <th style="width: 33%;">6 - 9 years</th> <th style="width: 33%;">10+ years</th> </tr> </thead> <tbody> <tr> <td style="background-color: #ffffcc;"> <ul style="list-style-type: none"> • The use of static passwords will broadly be replaced or augmented by stronger forms of authentication that exploit two-factor and multi-factor authentication methods • There will be increasing moves toward the use of a single authentication credential to enable end users to access multiple applications. </td> <td style="background-color: #c8e6c9;"> <ul style="list-style-type: none"> • Mobile wireless authentication using mobile based tokens and proximity technologies are likely to become more prevalent. </td> <td style="background-color: #e0f7fa;"> <ul style="list-style-type: none"> • Use of adaptive, context-aware and versatile authentication techniques that can match to different use cases and to specific interactions. </td> </tr> </tbody> </table>	2 – 5 years	6 - 9 years	10+ years	<ul style="list-style-type: none"> • The use of static passwords will broadly be replaced or augmented by stronger forms of authentication that exploit two-factor and multi-factor authentication methods • There will be increasing moves toward the use of a single authentication credential to enable end users to access multiple applications. 	<ul style="list-style-type: none"> • Mobile wireless authentication using mobile based tokens and proximity technologies are likely to become more prevalent. 	<ul style="list-style-type: none"> • Use of adaptive, context-aware and versatile authentication techniques that can match to different use cases and to specific interactions.
2 – 5 years	6 - 9 years	10+ years					
<ul style="list-style-type: none"> • The use of static passwords will broadly be replaced or augmented by stronger forms of authentication that exploit two-factor and multi-factor authentication methods • There will be increasing moves toward the use of a single authentication credential to enable end users to access multiple applications. 	<ul style="list-style-type: none"> • Mobile wireless authentication using mobile based tokens and proximity technologies are likely to become more prevalent. 	<ul style="list-style-type: none"> • Use of adaptive, context-aware and versatile authentication techniques that can match to different use cases and to specific interactions. 					
<p>Relevant applications</p> <p>Authentication technologies are required almost anywhere where audited access control is required. This access could be to computer systems or end applications, or even to physical areas and buildings. Authentication technologies can also ensure sensitive information is bound to an individual and can also facilitate trust between multiple parties (people or systems) that want to work together. The type of envisaged application will dictate the authentication method(s) chosen.</p>							

General issues and challenges

A key challenge is assigning the most appropriate authentication type to the information, application or system. Of all the various types currently available, none can claim to be 100% secure and therefore the only current viable strategy for authenticating users is to resort to the defence in depth principle by mixing a number of authentication techniques. However, even the strongest of these can still be bypassed, for example, by session-hijack attacks. Particular issues have also been identified with leading OTP solutions, such as RSA's SecureID, where token seed records were compromised, resulting in a high-profile attack against Lockheed Martin's protected infrastructure. Interestingly, the CESG view (expressed at the 2011 CLAS Technical Conference) was that the wider impacts of this attack were somewhat less than suggested in the dramatic reporting of the initial incident.

Unfortunately, the choice of authentication solutions is complicated by other factors such as cost. The through-life costs for tokens/smart cards and biometrics are much higher since they must be physically issued, replaced and recovered on a user-by-user basis. It is a matter of ascertaining the risk present. High-risk systems will require stronger, multiple forms of authentication, as they can more robustly ascribe confidence to the user's digital identity as being who they claim to be.

The future challenge will be to find ways to improve and eventually replace the current strong authentication offerings, which are still prone to attack, with more flexible and adaptive authentication services.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

The IT analysis company Gartner provides a comprehensive taxonomy of authentication methods, which describes the distinct kinds of authentication methods under three canonical types: Knowledge (e.g. use of passwords) Tokens (e.g. a smart card) and Biometric characteristic (e.g. fingerprint).

Source: Allan, A. 'A Taxonomy of Authentication Methods Update', Gartner Research ID: G00213119. 25 May 2011.

In one of their recent hype cycle documents Gartner considers that authentication technologies will reach its 'plateau of productivity' in 2 to 5 years. To quote:

Some vendors are aggressively cutting the prices of traditional high-assurance authentication methods, such as hardware tokens, and many are offering lower-cost alternatives, such as phone-based and innovative KBA methods. These alternatives vary in the levels of assurance and accountability that they provide; thus, an enterprise can now more easily find the balance of cost and authentication strength appropriate to its needs.

1These dynamics mean that many enterprises will implement multiple new authentication methods during the next two to three years.

Source: Heiser, J. 'Hype Cycle for Governance, Risk and Compliance Technologies, 2011', Gartner ID: G00214721. 26 July 2011.

Various stories in the popular media have covered the attack on Lockheed Martin, through compromise of information related to the RSA SecureID OTP token. For example, BBC News states that:

...Experts believe that hackers who broke into RSA collected key information used to generate the tokens, allowing them to create fake ones which could then be used to attempt a breach of secure networks.

Source: 'Security Firm RSA offers to replace SecureID Tokens', BBC News Online. 7 June 2011.

Infiniti Research has released a market research that looks at the future market prospects and associated challenges for authentication technologies. The report covers different forms of two-factor authentication solutions such as USB Tokens, e-Signature, Subscriber Identity Module (SIM) USB Token, PC Soft Tokens, SMS Text Authentication, Display USB Token, and OTP Token. It also covers the hardware, software, and hybrid solutions or products.

Technavio's analysts forecast the Global Two-factor Authentication market to grow at a CAGR of 20.8 percent over the period 2010–2014. One of the key factors contributing to this market growth is the growing complexity of attacks and increasingly strict compliance regulations. The Global Two-factor Authentication market has also been witnessing growing adoption of phone-based authentication solutions and a preference for OTP authentication solutions. However, the high upfront cost of hardware tokens is negatively affecting the adoption of hardware tokens, which could pose a challenge to the growth of this market.

Source: 'Global Two-factor Authentication Market 2010-2014', Infiniti Research Limited. September 2011.

<p>Technology / Technique: Behavioural / Gestural Analytics</p>	<p>See also: Emotion and Facial Recognition, HCI and Video Analytics</p>
<p>Description</p> <p>This emerging field mainly supports video surveillance systems by enabling the detection of human and other object behaviours and analysing them within the context of their environment. It relies on sophisticated software algorithms that can include artificial intelligence and machine-learning techniques, to detect, classify and track objects from video imagery¹ and apply self-learning and pattern discovery to enable their behaviour and intent to be understood. This field is related to the areas of affective computing and emotion recognition as human gestures and behaviour can contribute toward indicating emotional state.</p> <p>¹ It can also be applied to thermal and audio sensor data.</p>	<p style="text-align: center;">Behavioural / Gestural Analytics Roadmap</p> <p style="text-align: center;">Present +3 years +5 years +10 years</p>
<p>Relevant applications:</p> <p>The technology has a wide range of applications. Its applications include crime prevention² supporting governments and operators of national infrastructure (for example to detect and analyse anomalous and suspicious behaviour in airports and other public places) to use in retailing (to monitor customer behaviour for security purposes and for market analysis). The technology also has applications in the area of entertainment, for example in casinos and for sports analysis and in video gaming.</p> <p>² Source: ‘Smart CCTV could track rioters’, BBC News, Technology, 23 August 2011. www.bbc.co.uk/news/technology-14629058</p>	<p>2 – 5 year forecast</p> <ul style="list-style-type: none"> • Individual behavioural analysis in use (indoor and outdoor environments) • Use of biometric features such as gait and facial recognition • Games (HCI) industry driving advances in software algorithms <p>6 - 9 year forecast</p> <ul style="list-style-type: none"> • Prototype systems capable of group behavioural analysis (indoor and outdoors) • Behavioural classification supported by extensive libraries <p>10+ year forecast</p> <ul style="list-style-type: none"> • Multi-modal systems using a suite of sensors • Detection of a wide range of behavioural indicators (including emotion) • Systems capable of reliably interpreting the behaviour and intent of groups in outdoor crowded spaces <p>Maturity ■ Proof of Concept/ Demonstrator ■ Prototype ■ Emerging/Niche ■ Mainstream</p>
<p>Technology Readiness and Maturity (forecasted arrival and accessibility)</p> <p>Within 2 - 5 years: We can expect to see improved software algorithms capable of analysing finer resolution body movements such as of the hands and fingers and that can cope with patterns of activities. These developments are likely to be driven by the games industry and the need to analyse the outputs of next generation motion sensing devices such as currently exemplified by Microsoft’s Kinect. We can also expect to see early adoption of systems where the emphasis is more on individuals than</p>	

groups (in indoor and outdoor settings) that use biometric features such as gait and facial recognition.

Within 6 - 9 years: In this time period we can expect behavioural/gestural analytics systems to have advanced to a state where prototype systems will be able to interpret group behaviour and therefore detect behaviour and intent in small groups of people (indoors and outdoors). We can also expect to see extensive libraries becoming available for classification.

10+ years: In the longer term, we can expect a multi-modal capability exploiting a range of sensors that will include audio as well as video cameras. These will enable the detection of numerous attributes such as posture, gaze direction, tone of voice and other indicators of emotion that will be supported by sophisticated software that can fuse this data, classify it and reliably interpret the behaviour and intent of groups of people in outdoor crowded spaces.

General issues and challenges

The key challenge confronting researchers in this field is being able to reliably classify human activities in order to identify anomalous and suspicious behaviour from video image sequences. The modelling and classification of these activities is a difficult exercise due to the random and complex nature of human movement. Although there has been some progress in this area through partitioning human motion into discrete states and then classifying them appropriately.

For early adopters the key issues will be cost and the frequency of false alarm rates (particularly when used in public spaces). The technology is dependent on a suite of high-resolution cameras that will be able to operate in all-weather environments and that will be able to provide the pixel resolution required to enable the reliable classification of body positions and movements. It is also dependent on appropriate computer hardware (servers and databases) and sophisticated software algorithms that can identify human behaviours and gestures from body positions and movement in the context of their environment. There is the possibility that cost will reduce once a broader range of commercial-oriented applications materialise.

There is currently a lack of libraries available for matching observed behaviours with those known and classified. These libraries will need to be extensive and should cover variations in behaviour due to context, the environment, culture and other relevant variables.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

The field of behavioural/gestural analytics has appeared on Gartner's Hype Cycle for the first time. To quote:

The initial adoption of behavioural/gestural software algorithms will be for only comprehensive surveillance systems capable of capturing from a field-of-view perspective full-body behavioural/gestural and movement recognition that includes facial recognition.

While the software is maturing, the cost of implementing, cameras, sensors and behind-the-scenes pattern matching will likely limit this type of solution to select hot spots of activity.

Source 1: Prentice S., Fenn J.: 'Hype Cycle for Human Computer Interaction, 2011', Gartner Research ID: G00215631. 28 July 2011.

A survey by the US company Raytheon provides a current overview of behaviour analysis in video surveillance applications. To quote:

The main purpose of this survey is to look at current developments and capabilities of visual surveillance systems and assess the feasibility and challenges of using a

visual surveillance system to automatically detect abnormal behaviour, detect hostile intent, and identify human subject.

The survey highlights the lack of research and current challenges regarding classification which were raised above:

An automated visual surveillance system generally requires a reliable combination of image processing and artificial intelligence techniques. Image processing techniques are used to provide low-level image features. Artificial intelligence techniques are used to provide expert decisions. Extensive research has been reported on low level image processing techniques such as object detection, recognition, and tracking; however, relatively few researches has been reported on reliable classification and understanding of human activities from the video image sequences.

Source 2: Ko T.: 'A Survey on Behaviour Analysis in Video Surveillance Applications' InTechWeb.org. See: www.intechopen.com/source/pdfs/13689/InTech-A_survey_on_behavior_analysis_in_video_surveillance_applications.pdf. February 2011.

Standards and policy (Government and non-Government)

There are no known standards at the current time. It is possible that the first standards will evolve as a result of libraries of common gestures and behaviours becoming available. There are currently a number of US military evaluation and pilot studies underway but it is too early for any form of policy.

QinetiQ comment

A primary driver for behavioural analytics is the need to support personnel who must monitor a large number of CCTV screens. The ability of automated support to cue operators to suspicious events could improve monitoring ability. Poor performance though is likely to increase operator workload and cause him/her to miss significant events. The evolutionary development of behavioural analytic technology is strongly tied to progress with the development of behaviour analysis schemes in general. Part of the challenge lies in having reliable and clear descriptions of suspicious behaviour that are unambiguous enough that they can be articulated to a machine detection system. The reality is that suspicious behaviour is context-sensitive and often easily confused with other benign behaviours. It is relatively easy to detect gross behaviours in people or vehicles such as violating prohibited zones and crossing trip wires, but more problematic to classify behaviours where no such constraint boundaries exist. Many behaviours of interest can rely upon detecting subtleties of body language (e.g. suggesting hesitation or anxiety when approaching security checks). Ultimately, people are required in the loop to make judgements about behaviour in many public settings and infer intentions. The capability to date has concentrated upon analysis of visual material, but audio is underutilised and offers the potential for cuing visual aids towards areas where suspicious or criminal activity may be occurring.

The market driver for this technology is likely to be Human-Computer Interaction (HCI). HCI solutions are likely to augment normal imaging cameras (e.g. Microsoft Kinect has a range sensor) and be aimed at co-operative users. The challenge will be extending methods designed for co-operative HCI to detect subtle gestures/behaviours recognition at a distance, in cluttered environments, using existing CCTV infrastructure.

Technology / Technique: Building and Environment Management Systems

Description

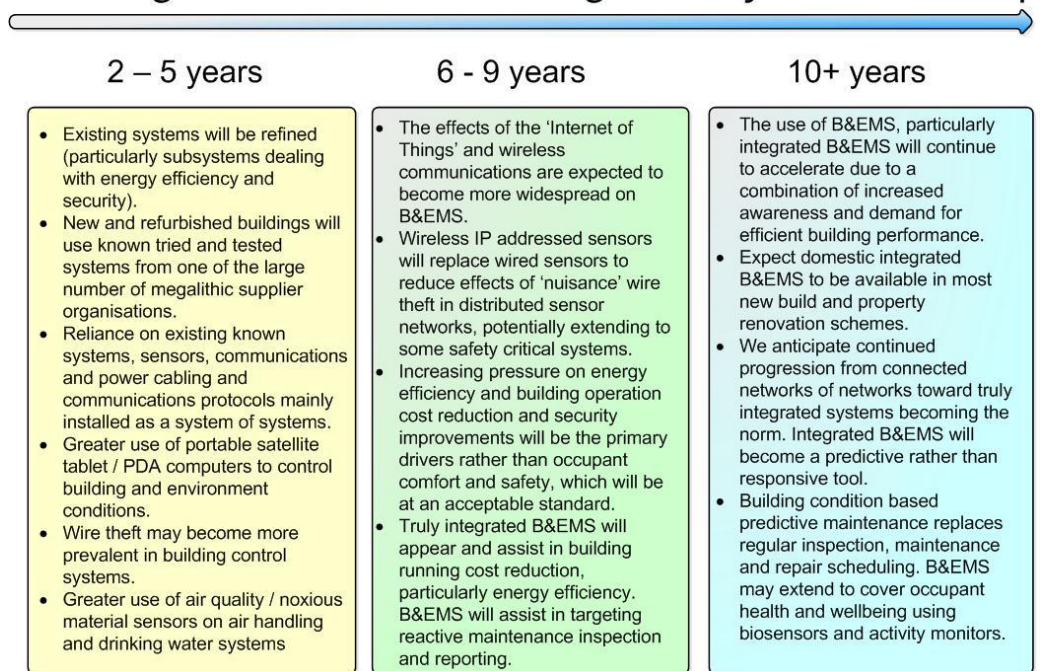
Building and Environment Management Systems (B&EMS) exist at some level of sophistication in most occupied and unoccupied commercial, civil and government buildings plus a growing number of domestic buildings. B&EMS are distributed control systems often deployed as systems of subsystems. Typically, the control system is based around a number of computerized networks of electronic sensors and actuators designed to monitor and automatically control some or all of the 'building operation' functional systems. Such systems range from office lighting to automatic number plate recognition and access control - these are distinct from systems controlling processes conducted in the building, for example robotic assembly lines/automated bottle filling.

Relevant applications

Most building automation networks consist of a primary and a secondary bus to connect high-level controllers specialised for building automation or alternatively programmable logic controllers. These collect and process information provided by operators and sensors, sensor networks or external data sources, and effect changes as required. The B&EMS can control a range of sub-systems including:

- Occupant comfort, work and convenience (lighting, air conditioning/environment control, window blinds/photo-chromics, elevators/escalators, power grids, water, vending, toilets, telephones, internet, distributed TV/visual information boards/screens, local area networks, networked printers/scanners/photocopiers, network management and security firewalls, public address/announcement system).
- Central plant (chilled water, hot water, fire main, effluent, UPS, energy harvesting).
- Safety and security systems (smoke detectors, temperature rate of rise fire detectors, carbon monoxide/dioxide detectors, event alarm and announcement systems, emergency lighting), CCTV network, building access control/perimeter breach/unauthorised entry detection, automated connections to law enforcement and emergency services etc.
- Other sub-systems that are uncommon in UK built environment include seismic detectors and links to meteorological and natural threat monitoring systems.

Building and Environment Management Systems Roadmap



General issues and challenges

The degree of human intervention or reliance on computer aided or computer controlled decision making in individual B&ES subsystem components ranges from 'none', for example temperature triggered water sprinklers to 'high', for example monitored CCTV with target recognition algorithms. Systems are frequently designed to take account of building occupancy to minimise energy consumption, these are based on predicted need (e.g. office opening) or occupant detection (e.g. passive infrared motion sensor and automatic stairwell lighting). The B&ES are usually a number of discrete networks of networked sensors, servers and data terminals each controlled by an automating algorithm with supervisor monitoring and manual override. Truly integrated B&EMS are not known of at present, but common communication protocols are available and should enable integration. Considered as a simplified analogue to help predict the evolution of B&ES, vehicles have had similar networked systems of discrete monitoring and automatic control subsystems for some time. These have evolved more rapidly and are moving toward highly integrated systems including Health and Usage Monitoring Systems (HUMS) and techniques such as 'condition based maintenance' (CBM) probably close to implementation. One common problem highlighted in current HUMS and CBM development is how to best interpret the significant volume of information delivered by the sensors to enable good decision making – this could be a larger problem for larger systems such as buildings or larger complexes such as shopping arcades or 'Malls'.

The key threats from use of B&EMS arise from a combination of factors including; their distributed topology, automation of decision-making, their reliance on networked human input and supervisory nodes sensors and effectors, their connection to the internet and the importance to personal health of the building systems that they control. Attacks on a B&EMS can cause the building to become uncomfortable or uninhabitable and/or vulnerable to a range of additional threats from physical invasion. Examples of physical invasion could include the introduction of obscurants, water- or air- borne poisons. An attack could be designed in order to cause confusion, disorientation and/or to mislead emergency response services, security personnel. Such attacks could be used cause panic amongst building occupants. In a number of dramatisations buildings are attacked by first disabling some safety critical and security systems, typically effected remotely through a vulnerable data link and then by controlling the building environment control system introducing a noxious substance (nucleotide, chemical or biological agent). Albeit a fictional example is given, this type of attack could be viable for moderately sophisticated adversaries either now or in the future and may be appealing given the success afforded to attackers in films.

The increased use of wireless technology for sensor and command system elements to help defeat nuisance wire theft will increase the number of nodes susceptible to attack through TEMPEST or cyber attacks on B&EMS. More resilient cryptographic and data security standards may need to be introduced to the protocols used in IP and wireless communications.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

TSB funded Modern Built environment knowledge transfer network and discussion forum :- www.mbektn.co.uk/

The Fires: How a Computer Formula, Big Ideas, and the Best of Intentions Burned Down New York City and Determined the Future of Cities, Joe Flood (Riverhead Books (27 May 2010) ISBN 1594488983.

Building Energy Management Systems: An Application to Heating, Natural Ventilation, Lighting and Occupant Satisfaction, Geoff Levermore Taylor and Francis; 2 edition (18 May 2000) ISBN 0419261400.

Example provider of system of system B&EMS www.clearview-communications.com/index.html

Standards and policy (Government and non-Government)

ISO/IEC standard numbers for building automation =14908, parts 1 to 4. 1 = Communication protocol, 2 = Twisted pair wire signaling technology, 3 = Power line signaling technology, 4 = IP compatibility technology.

BS5839-1:2002. Fire resistant, fire retardant and low smoke cable for use in buildings where systems need to remain operational

BS5839-8:1998, 2006. Voice alarm systems

BS5266-1:2005. Emergency lighting systems

BS7629-1:2008 Electric cables. Specification for 300/500 V fire resistant screened cables having low emission of smoke and corrosive gases when affected by fire. Multicore and multipair cables.

QinetiQ comment

As B&EMS become more sophisticated with wider deployment of sensors and increased network connectivity, they will become more susceptible to a variety of threats and the mitigation of this risk will prove extremely challenging - therefore also potentially expensive.

<p>Technology / Technique: Cloud Computing</p>	<p>See also: Cloud Security</p>
<p>Description</p> <p>Cloud Computing is the latest in a long line of heavily marketed, ‘revolutionary’, computing paradigms. Few commentators appear to agree on what the term actually means; Cloud Computing Journal asked 21 ‘expert’ commentators for their definition¹ and unsurprisingly they got 21 different answers. The most popular theory for the origin of the term is that engineers draw the internet (or the external network) as a cloud on network diagrams. Cloud Computing seems to be largely a marketing term that encompasses a number of existing technologies and service offerings.</p> <p>Gartner defines cloud computing as a style of computing in which massively scalable IT-enabled capabilities are delivered 1as a service1 to external customers using internet technologies.²</p> <p>The main components of Cloud Computing are generally considered to be:</p> <ul style="list-style-type: none"> • Infrastructure as a Service (IaaS) – provides an environment that can host a complete operating system image for a customer; • Platform as a Service (PaaS) – where computational resources are provided via a platform upon which applications and services can be developed and hosted; • Software as a Service (SaaS) – the provision of software functionality that is owned, delivered and managed remotely by one or more providers. <p>Some of the benefits Cloud Computing can purportedly bring to organisations include reduced costs, more flexibility, greater automation (that will free-up internal resources) and greater mobility for users (employees can access information from anywhere).</p> <p>¹ cloudcomputing.sys-con.com/node/612375</p> <p>² <i>Gartner IT Glossary. Retrieved on 4 May, 2012 from: www.gartner.com/it-glossary/cloud-computing/</i></p>	<p style="text-align: center;">Cloud Computing Technology Roadmap</p> <p>The diagram illustrates the maturity of three cloud computing models over time. A horizontal timeline at the top marks 'Present', '+3 years', '+5 years', and '+10 years'. Three horizontal bars represent the models: Platform as a Service (top), Infrastructure as a Service (middle), and Software as a Service (bottom). Each bar is divided into segments representing maturity levels: Proof of Concept/Demonstrator (orange), Prototype (yellow), Emerging/Niche (green), and Mainstream (blue). Platform as a Service reaches the Mainstream stage around +3 years. Infrastructure as a Service reaches the Mainstream stage around +5 years. Software as a Service reaches the Mainstream stage around +10 years.</p> <p>Maturity ■ Proof of Concept/Demonstrator ■ Prototype ■ Emerging/Niche ■ Mainstream</p>

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 - 5 years: Cloud computing is already mainstream. Some concerns about trust and security remain, and are one of the main arguments against its uptake. Provision of private clouds is still immature.

Within 6 - 9 years: Private clouds become mainstream and become the dominant way of organising and managing data-centres.

10+ years: More advanced concepts such as 'Cloudbursting' (increase or decrease service capacity on demand) and Virtual Private Cloud Computing (where a part of a public cloud is isolated into an environment for use by a single entity or group) are likely to see adoption in this timeframe.

General issues and Challenges

There are potential drawbacks in exploiting Cloud Computing. These include issues over privacy, security, reliability and vendor lock-in (given the lack of open standards). During the next few years, it is quite likely that more media coverage expressing concern for the Cloud Computing model could hinder growth. Most of these concerns will be regarding security and loss of control over data. Nevertheless the overall outlook is promising as highlighted in a global forecast of the cloud computing market to 2015 by the US market research company MarketsandMarkets (M&M):

While interoperability and data security issues may hinder market growth, the future of cloud computing seems promising with IT giants such as IBM, Google, Microsoft, and Salesforce.com actively developing new solutions to address existing issues.

The global cloud computing market is expected to grow from \$37.8 billion in 2010 to \$121.1 billion in 2015 at a compound annual growth rate (CAGR) of 26.2% from 2010 to 2015. SaaS is the largest segment of the cloud computing services market, accounting for 73% of the market's revenues 2010. The major SaaS-providers include Adobe Web Connect, Google Mail, Cisco WebEx, and Yahoo Mail. Content, communications, and collaboration (CCC) accounts for about 30% of the SaaS market revenues.

Source: 'Cloud Computing Market - Global Forecast (2010 -2015)', MarketsandMarkets, www.marketsandmarkets.com/Market-Reports/cloud-computing-234.html. October 2010.

The well-known analyst company Gartner has given considerable attention to cloud security concerns:

The relative security of the cloud computing style, compared to classic approaches that do not employ a service-delivery and shared-service approach, remains a major concern. User polls consistently indicate that security is the most significant inhibitor to the use of cloud computing. The primary challenge is the lack of best practices, including control standards, for cloud security assessment. The secondary challenge is the relative non-transparency of commercial cloud service providers.

Source: Mitchell Smith D.: 'Hype Cycle for Cloud Computing, 2011', Gartner Research ID: G00214915. 27 July 2011.

Information sources, Supporting extracts and quotations (websites, forums, publications etc.)

European Commission, Expert Group Report: 'The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010'. Jan 2010. See: cordis.europa.eu/fp7/ict/ssai/events-20100126-cloud-computing_en.html

Object Management Group: Cloud Computing Standards: Building a Multi-View Specification. See: www.omg.org/news/meetings/GOV-WS/css/css-pdf/OMG.pdf

Standards and policy (Government and non-Government)

There are currently very few standards for Cloud Computing. The PaaS platforms are largely proprietary (or at least unique to the platform); this means that an application that is written for one provider's platform cannot easily be moved to another platform. There are now some platform independent abstraction layers, such as libcloud. IaaS models are a little better served because the applications are written to run on the hosted operating system, which is usually Linux or Windows. However, when the additional services of the IaaS provider are used (e.g. storage, user authentication etc.) the interfaces to these services are not standardised and this provides a means of locking the customer in to the platform. Some service interfaces are starting to emerge as de-facto standards because multiple providers are providing duplicates of the market leading platforms (e.g., a number of providers offer the Amazon Web Service interfaces).

The UK Government plans to create a countrywide cloud infrastructure known as 'G-Cloud'. It is planned that the beta phase of a single web domain for Whitehall will be implemented in 2012, according to the executive director of digital at the Cabinet Office.

Source: Laja S.: 'G-Cloud boss expects framework ready by Christmas', ZDNet, www.zdnet.co.uk/news/networking/2011/10/07/g-cloud-boss-expects-framework-ready-by-Christmas-40094133/7 Oct 2011.

QinetiQ comment

Like all hyped offerings from the ICT sector cloud computing is starting to suffer a backlash as some become disillusioned about its ability to deliver as promised. Unfortunately cloud computing has been affected by what many in the business call 'cloudwashing'. Cloudwashing is the purposeful and sometimes deceptive attempt by a vendor to re-brand a service or old product by associating it with 'the cloud'. Furthermore cloud computing has also been affected by security concerns. The truth is that cloud computing is still in its infancy in many sectors, although it has very strong penetration in e-commerce and social media. Some of the underpinning tools are mature but the market is still evolving rapidly. Many cloud technologies and concepts will start to see mainstream adoption in the next two to five years but it is unlikely that cloud computing will fully mature within this timeframe. Although not perfect, the professional security administration provided by cloud operators is often better than the capabilities of the customer organisation, providing an improvement for those that lack strong in-house security skills.

<p>Technology / Technique: Cloud Security</p>	<p>See also: Cloud Computing</p>						
<p>Description</p> <p>Security has long been blamed for holding back the wider adoption of cloud computing [1]. With its touted efficiency savings through economies of scale, and increased 'consumerism' of resources, cloud computing makes a lot of sense. However, cloud security is still immature and much still needs to be done on standardisation, particularly with regard to terminology, comparison matrices and incident data.</p> <p>A number of initiatives are underway, which cumulatively, may help to address current concerns. Suppliers are beginning to develop genuine, tailored cloud security technologies, to appeal to risk conscious consumers. Security experts are working more coherently, in drawing up best practice guidance, checklists, education and awareness literature and standards. More widely, the UK Government has recently stated that Cyber Security is its top priority [2]. As such, it is one of the few areas receiving heavy Government investment. Recent statements from the Head of GCHG about the threat posed by Foreign Intelligence Services (FIS), and London hosting the October 2011 Cyberspace Security Conference support these aspirations.</p>	<div style="text-align: center;"> <h3>Cloud Security Roadmap</h3> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 33%; text-align: center;">2 – 5 years</th> <th style="width: 33%; text-align: center;">6 - 9 years</th> <th style="width: 33%; text-align: center;">10+ years</th> </tr> </thead> <tbody> <tr> <td style="background-color: #ffffcc; padding: 5px;"> <ul style="list-style-type: none"> The increased impact of cloud security incidents, plus the increased likelihood of attack, cause a dramatic shift in market demand for cloud security. Within 3 years there will be a competing range of solutions from providers, employing divergent techniques and business models to tackle cloud security. </td> <td style="background-color: #c8e6c9; padding: 5px;"> <ul style="list-style-type: none"> The most successful cloud security mechanisms will have pulled away as market leaders. Successful providers will draw on the right combination of technique and business model, combined with several years of credible track record. </td> <td style="background-color: #e0f7fa; padding: 5px;"> <ul style="list-style-type: none"> The threat to cyber security (including cloud) continues to increase, with providers continuously innovating to keep up the defences against new attacks. With greater maturity in trusted cloud solutions, and continuing budgetary pressures, sensitive data is now stored in clouds. </td> </tr> </tbody> </table>	2 – 5 years	6 - 9 years	10+ years	<ul style="list-style-type: none"> The increased impact of cloud security incidents, plus the increased likelihood of attack, cause a dramatic shift in market demand for cloud security. Within 3 years there will be a competing range of solutions from providers, employing divergent techniques and business models to tackle cloud security. 	<ul style="list-style-type: none"> The most successful cloud security mechanisms will have pulled away as market leaders. Successful providers will draw on the right combination of technique and business model, combined with several years of credible track record. 	<ul style="list-style-type: none"> The threat to cyber security (including cloud) continues to increase, with providers continuously innovating to keep up the defences against new attacks. With greater maturity in trusted cloud solutions, and continuing budgetary pressures, sensitive data is now stored in clouds.
2 – 5 years	6 - 9 years	10+ years					
<ul style="list-style-type: none"> The increased impact of cloud security incidents, plus the increased likelihood of attack, cause a dramatic shift in market demand for cloud security. Within 3 years there will be a competing range of solutions from providers, employing divergent techniques and business models to tackle cloud security. 	<ul style="list-style-type: none"> The most successful cloud security mechanisms will have pulled away as market leaders. Successful providers will draw on the right combination of technique and business model, combined with several years of credible track record. 	<ul style="list-style-type: none"> The threat to cyber security (including cloud) continues to increase, with providers continuously innovating to keep up the defences against new attacks. With greater maturity in trusted cloud solutions, and continuing budgetary pressures, sensitive data is now stored in clouds. 					
<p>Although cloud computing is perceived as dynamic, flexible and cost efficient, gaining security specific funding in commercial markets may still prove challenging. This is because the impact of the financial crisis means that (despite the rhetoric, the concerns of security experts and intelligence agencies and the potential for legislation) business continues to see security as a prohibitive overhead.</p> <p>Aspects of cloud security have relevance to the following critical security controls within the SANS Critical Security Controls for Effective Cyber Defence document – ‘Application Software Security’ and ‘Boundary Defence’.</p>							
<p>General Issues and Challenges</p> <p>Cloud security is in a catch 22 situation; risk adverse consumers will not move to the cloud until security has matured, and providers are reluctant to develop security offerings until they see interest from consumers. This stalemate is starting to shift, with the early innovators (primarily web security companies) such as Trend Micro [3], McAfee [4] and senior information security experts pushing for better solutions in cloud security. Broadly, those organisations that have current cloud consumers are those that do not regard security as a priority and are satisfied with the existing offerings, or believe the cost savings is worth the trade-off. This tends to be</p>							

organisations with a strong appetite for risk, such as innovators, start-ups, or SMEs focussed on the economies of scale associated with out-sourcing. Some larger organisations are using cloud services for part of their operations, allowing low-risk data to be processed in the cloud, while keeping the higher risk systems in house. While there are 'low-hanging fruit' in this bracket for cloud suppliers to target, there is 'no business need' to develop mature cloud security offerings. However, once this set of consumers has been saturated, cloud suppliers will look to the next group that can be enticed to the cloud, i.e. those that have so far resisted the move, due to security concerns.

The other scenario that will drive the development of cloud security is if an incident of sufficient gravity occurs resulting in mainstream media attention. A likely consequence will be that the current trend to move to the cloud will stutter, and confidence in cloud security will be crucial in remedying the situation. Even at the time of writing, there is enough back chatter about incidents taking place to start causing concern [5]. In one published story, the Foreign Commonwealth Office (FCO) was targeted by a significant but unsuccessful phishing attack. The email was described as sophisticated and malicious [6].

We are already starting to see substantial mainstream media coverage of cyber security concerns. In an unprecedented move, Ian Lobban, the Head of GCHQ, recently made a public statement that cyber attacks on the UK are at 'disturbing' levels [7]. Government computers, along with defence, technology and engineering firms' designs have been targeted, with China and Russia thought to be amongst the worst culprits [8]. The impact of this statement should not be underestimated. If organisations do not start taking cyber security seriously, it seems likely that the Government will move closer to forcing them to do so, presumably through more regulation.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

Gartner's 'Hype Cycle for Cloud Security, 2011' examines technologies and standards that improve the security and reliability of the cloud computing model, as well as trusted application and security services that are delivered by cloud service providers. To quote their key finding:

Over the past several years, concern over cloud computing security, and its impact on regulatory compliance, has consistently ranked as the most common reason for avoiding further use of this style of computing. Improving attack resistance, enhancing reliability and increasing the risk transparency remain crucial to widespread enterprise use of cloud computing. Perhaps somewhat surprisingly, the cloud delivery model is being used to deliver a growing number of security-critical tasks. For example, several different forms of secure delivery platforms, used to share highly proprietary or regulated data, are based on public cloud models. A growing variety of security services are also being delivered from the cloud, some intended to improve the robustness of the enterprise, and some intended to improve the attack resistance of other cloud-based services.

Source: Heiser J., Cearley D.W.: 'Hype Cycle for Cloud Security, 2011', Gartner Research ID: G00214151. 28 July 2011.

The following refer to references used in the rest of this document:

[1] Asford W.: 'Securing the cloud is much like securing the enterprise', Computer Weekly, 11 April 2011, www.computerweekly.com/Articles/2011/04/11/246299/Securing-the-cloud-is-much-like-securing-the-enterprise-says-industry.htm

[2] 'London hosts Cyberspace Security Conference', BBC News, 1 Nov 2011, www.bbc.co.uk/news/technology-15533786

[3] 'Trend Micro Cloud Security', uk.trendmicro.com/uk/about/cloud/

[4] 'McAfee Cloud Security', www.mcafee.com/uk/solutions/cloud-security/cloud-security.aspx

[5] 'McAfee reveals cyberattacks against 72 organisations', ZDNet, 3 Aug 2011, www.zdnet.co.uk/news/security-threats/2011/08/03/mcafee-reveals-cyberattacks-against-72-organisations-40093605/

[6] 'Attacks on UK Cabinet Office systems', 31 Oct 2011, www.fco.gov.uk/en/global-issues/london-conference-cyberspace/cyber-crime/case-studies/cyber-attacks-cabo

[7] Meikle J.: 'Cyber-attacks on UK at disturbing levels, warns GCHQ chief', Guardian, 31 Oct 2011, www.guardian.co.uk/technology/2011/oct/31/cyber-attacks-uk-disturbing-gchq

[8] 'GCHQ Chief reports 'disturbing' cyber-attacks on UK', BBC News, 31 Oct 2011, www.bbc.co.uk/news/uk-15516959

Standards and policy (Government and non-Government)

CESG, the National Technical Authority for Information Assurance, are beginning to circulate guidance on cloud security (although it is not formally released, at the time of writing) – particularly 'Advice for Impact Level 2 – Public Cloud' and 'Advice for Impact Level 3 – Public and Private Cloud'. CESG have also standardised on using the US National Institute of Standards and Technology (NIST) definitions for cloud services.

Other relevant standards and policy sources:

- Cloud Security Alliance (CSA) website, <https://cloudsecurityalliance.org/>
- European Network and Information Security Agency (ENISA). www.enisa.europa.eu/

QinetiQ comment

Cloud security remains an immature domain, but is developing quickly. Many key issues are still being identified. Organisations have sprung up in the last 12 - 24 months to deal with these concerns - the front runners of these are gaining momentum. Standards and policy are being driven by working groups, looking to achieve best practice and advise on the 'tweaking' of existing documentation, rather than to create new elements. Currently cloud security is a self-governing entity, driven by market forces and consumer demand. Cost savings will continue to drive consumers to the cloud. Security concerns will encourage better offerings of cloud 'security-as-a-service'.

<p>Technology / Technique: Future Collaboration Tools</p>	<p>See also: Future social networking tools</p>						
<p>Description</p> <p>Collaboration is an activity undertaken by humans who are co-operating with one another to achieve a common goal. This activity is dependent on these individuals being able to share and exchange information. The so-called ‘collaboration technologies and tools’ supporting and enabling this activity are largely based on computer software that exploits communications technologies for messaging and content sharing.</p> <p>The challenge for technologies supporting collaborative working is to create working environments and tools such that humans can comfortably share information and collaborate, regardless of the time zone difference or the geographical distance separating them.</p> <p>A broad continuum of technologies and vendors has risen to the collaboration challenge, claiming to tackle it from the personal to the enterprise level. Over the next decade the following areas are expected to grow and provide the medium through which most individuals and groups will conduct collaborative activities:</p>	<div style="text-align: center;"> <h3>Future Collaboration Tools Roadmap</h3> </div> <table border="1" style="width: 100%; text-align: center;"> <thead> <tr> <th style="width: 33%;">2 – 5 years</th> <th style="width: 33%;">6 - 9 years</th> <th style="width: 33%;">10+ years</th> </tr> </thead> <tbody> <tr> <td style="background-color: #ffffcc;"> <ul style="list-style-type: none"> • The use of social networking tools for business collaboration will increase • Social networking services will increasingly replace e-mail for interpersonal communications and collaboration activities • Growth in Web conferencing and Telepresence for group collaboration </td> <td style="background-color: #ccffcc;"> <ul style="list-style-type: none"> • HD Video comes to dominate most collaboration interactions • Mobile devices such as smartphones and tablets will start to become the focus for most collaborative activities </td> <td style="background-color: #ccffff;"> <ul style="list-style-type: none"> • Likelihood of immersive collaboration for static users through exploiting virtual reality • Mobile collaboration will become pervasive </td> </tr> </tbody> </table>	2 – 5 years	6 - 9 years	10+ years	<ul style="list-style-type: none"> • The use of social networking tools for business collaboration will increase • Social networking services will increasingly replace e-mail for interpersonal communications and collaboration activities • Growth in Web conferencing and Telepresence for group collaboration 	<ul style="list-style-type: none"> • HD Video comes to dominate most collaboration interactions • Mobile devices such as smartphones and tablets will start to become the focus for most collaborative activities 	<ul style="list-style-type: none"> • Likelihood of immersive collaboration for static users through exploiting virtual reality • Mobile collaboration will become pervasive
2 – 5 years	6 - 9 years	10+ years					
<ul style="list-style-type: none"> • The use of social networking tools for business collaboration will increase • Social networking services will increasingly replace e-mail for interpersonal communications and collaboration activities • Growth in Web conferencing and Telepresence for group collaboration 	<ul style="list-style-type: none"> • HD Video comes to dominate most collaboration interactions • Mobile devices such as smartphones and tablets will start to become the focus for most collaborative activities 	<ul style="list-style-type: none"> • Likelihood of immersive collaboration for static users through exploiting virtual reality • Mobile collaboration will become pervasive 					
<ul style="list-style-type: none"> • Social software and networking: See: Future social networking tools • Web conferencing and telepresence: Enable collaboration and interactions, the former can use video conferencing but the latter extends this to more immersive environments and use of high definition video. • Enterprise collaboration tools and suites: One-stop shops purported to cover most or all of an organisation’s collaboration needs – that can include facilities such as social networking tools and web conferencing as mentioned above but also a raft of other functions such as real-time document management tools, mobile collaboration applications and cloud-based services. • Collaborative virtual environments: Immersive environments that could impact in the longer term. 							

Relevant applications

The use of collaboration tools is pervasive and they are of relevance to almost all applications where groups or individuals need to collaborate.

General issues and Challenges

One of the most important challenges for any organisation is procuring the right collaboration solution for their business. First and foremost, procurement of a collaboration solution for any organisation requires explicit knowledge of what the product is intended to achieve. Moreover the processes the product is intended to support need to be identified, be they group maintenance processes such as communication and scheduling, or wider organisational functions. Also the information and control flows require consideration since the implementation of collaboration software may change working practices.

The need for security within collaborative systems is vital and a major issue. To date security concerns have restricted collaboration expansion. Mechanisms need to be in place that control access to content and applications and that protect the user from malicious software. Enterprise-wide collaboration systems have many components whose functionality can be scattered over an organisation. This can pose numerous security issues. Firewalls, for example, can act to block ports used by many collaboration tools to exchange information over a local area network. The latest breed of collaboration tools such as the enterprise collaboration suites, are mostly built around a portal, which provides a Single Sign-On (SSO) facility. The SSO removes the need for users to repeatedly login to each area accessed, instead a single process authenticates the user for all the underlying applications.

Information sources, Supporting extracts and quotations (websites, forums, publications etc.)

The Ovum analyst group have produced a report entitled 'Enterprise Collaboration 2011/2012', which examines the enterprise collaboration landscape and the key vendors in some detail. To quote: *The document-centric world of enterprise collaboration is changing to encompass a broader range of interactive mechanisms. Real-time communication technologies, such as voice and video, are starting to merge with traditional collaboration technologies, and the result is a high-tech, wide awake workplace that is full of new possibilities.*

Source: Edwards R. et al.: 'Enterprise Collaboration 2011/2012', Ovum. July 2011.

Gartner's 'Hype Cycle for Unified Communications and Collaboration, 2011' covers many emerging supporting and enabling technologies and includes forecasts for areas such as presence, conferencing and messaging.

Source: Johnson G.: 'Hype Cycle for Unified Communications and Collaboration, 2011', Gartner Research ID: G00215510. 2 August 2011.

The Markets and Markets analyst company predict considerable growth for the team collaboration and web conferencing market:

The global team collaboration and web conferencing market is expected to reach \$19.97 billion by the year 2015, registering a CAGR [Compound Annual Growth rate] of 10.4%. The main forces driving the market are conferencing and collaboration to enhance productivity of businesses as well as employees.

Source: Global Team Collaboration Software & Audio, Video, Web Conferencing Solutions Market (2009 - 2015), Markets and Markets, May 2011.

CollaborateCom – an International Conference on Collaborative Computing: Networking, Applications and Worksharing. This forum involves academic and industrial

researchers, practitioners, and students interested in collaborative networking, technology and systems, and applications.

See: CollaborateCom 2011, collaboratecom.org/2011/

Standards and policy (Government and non-Government)

Standards exist for many of the technologies supporting collaboration (e.g. there are video conferencing standards and a raft of internet/communication standards supporting collaboration tools) but much standardisation work is still required. For example, Web conferencing technologies are not standardized, which has been a significant factor in the lack of interoperability, transparency, platform dependence, security issues, cost and market segmentation in this area. The need for organisations to link disparate communications and collaboration technologies is likely to drive the adoption of XMPP as a common standard during the next few years.

No specific UK Government policy or guidance could be found for the use of collaboration tools.

QinetiQ comment

Collaboration technologies and tools are numerous and an in-depth report would be required to cover them all to a sufficient level of detail such that comparisons and assessments can be made.

The collaboration technology landscape has changed considerably over the last decade particularly due to social software and the recognition of its value to the enterprise. The social software and networking element is likely to be the most unpredictable. It is possible that a slew of new, 'free' collaboration support sites will appear in the 2 to 5 year timeframe, sweeping up several of the features that current tools offer (scheduling meetings, finding geo-co-located friends, raising awareness in a cause, sharing intelligence on) and supported by advertising and data sales, that could result in a highly disruptive capability. Governments should be getting very concerned about crowd-sourced intelligence. There is a real possibility someone will find a way for people to build the social dynamics of Facebook into a site that organises passionate citizens into co-ordinated protestors.

It is also worth noting that collaboration, especially involving teams of people, is best performed when the members of the team are co-located and face-to-face meetings are possible. There are currently no tools or technologies that can emulate all the nuances present in a face-to-face meeting. In the next two decades, it is likely that advanced communication and display technologies will be able to support distributed virtual reality such that realistic 3D virtual meeting places could become viable spaces for collaboration. The use of collaborative virtual environments and Tele-immersion for group collaboration will then become more likely. Tele-immersion is a combination of collaborative virtual reality and audio/video conferencing technology. These technologies elevate the level of presence by providing realistic settings for virtual face-to-face meetings.

Technology / Technique: Context-Aware Computing and Context-Enriched Services

Description

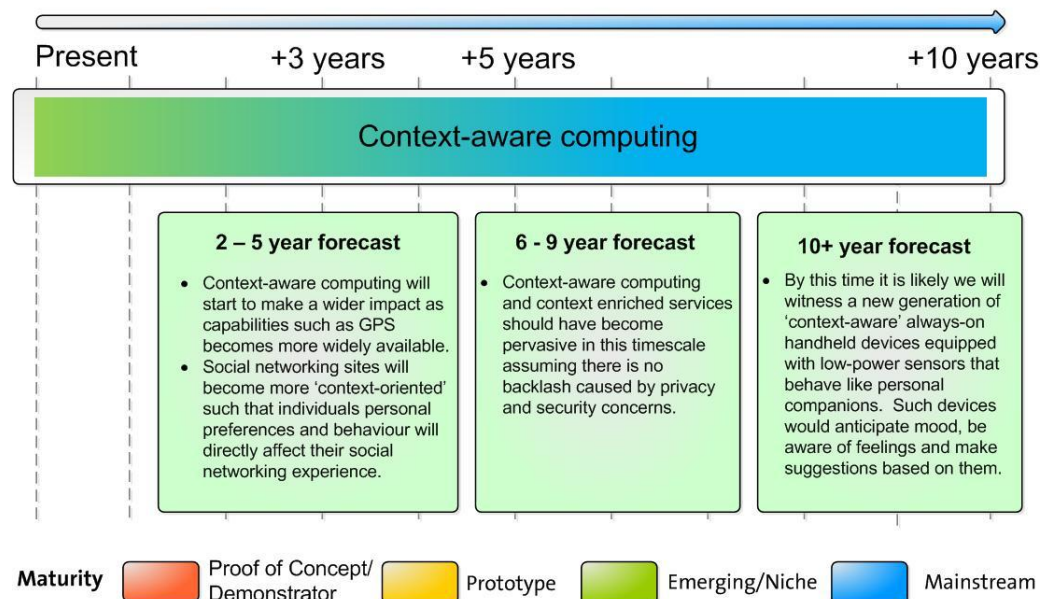
Context-aware computing and the services that it can provide concerns the delivery of personalised information to the user which is based on their identity and preferences and that can be instigated by where they are (location and environment) as well as the time of day and what they are doing. At the current time it is mostly aimed at supporting mobile users and therefore is particularly applicable to mobile devices such as smartphones.

This capability is still in its infancy but some analysts expect context aware computing to be making a big impact in the next two to five years. It is expected that context awareness will be as influential to mobile consumer services and relationships as search engines are to the Web (see Source 1 below).

Currently we are witnessing the evolution of a number of disparate technologies that are contributing toward context-aware computing. At the core of these are the location-sensing technologies which include GPS, Wi-Fi and network-supported cellular. Yet it also includes areas such as natural language understanding and machine learning.

Apple's Siri application for the iPhone 4S is a good example of the current state-of-the-art. This is a context-aware personal assistant that uses a natural language user interface to answer questions and make recommendations.

Context-Aware Computing Roadmap



Gartner estimate that by 2015, 50% of mobile phones will be GPS-enabled.

Lapkin A.: 'Hype Cycle for Context Aware Computing, 2011', Gartner Research ID number: G00213793. 28th July 2011.

Relevant applications

Applications in the near term to include digital personal assistants, e-Business (particularly customer relationship management), T.V. and media advertising.

General issues and Challenges

Although there are many benefits expected from the broad adoption of context aware computing and context-enriched services there are concerns where this technology might lead. Of particular concern are the threats to privacy and security. Source 2 listed below raises the issue of what context based information aggregation will do to personal privacy. To quote:

The mainstreaming of context-aware computing between now and 2015 will be driven by four data aggregators [named as Apple, Nokia, Microsoft and Google] that are collecting personally identifiable transactional information on hundreds of millions of people...By 2015, these four context providers will continuously track the 'daily journeys and digital habits' of 10% of the developed world's population... An intense amount of analytics is going on already with this information.... Tools will move beyond tracking where you've been to predicting what you'll do next.

It will therefore be possible not only to track where individuals have been (on-line and in the physical world) but also what they are likely to do next and where they are likely to go. Contextual information could help businesses decide what products or services an individual is most likely to be interested in purchasing but there is a host of other un-related potential applications.

A detailed examination of the issues of context-aware systems identified four common research issues which included 'privacy protection' (as referred to above) along with 'Architecture Style', 'Performance & Scalability' and 'Historical Context Data and User Behaviour' (see Source 3 below).

Information sources, Supporting extracts and quotations (websites, forums, publications etc.)

This article looks to the future when context-aware computing could make gadgets smarter.

Source 1: Ganapati G.: 'How Context-Aware Computing Will Make Gadgets Smarter', Wired Gadget Lab. www.wired.com/gadgetlab/2010/09/context-aware-computing/

The following research paper examines issues in context-aware systems.

Source 2: Lee S., Park S., Sang-goo L.: 'A Study on Issues in Context-Aware Systems Based on a Survey and Service Scenarios', 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing. 2009.

IT analyst firm Ovum predicts that context-aware computing is set to improve business processes. To quote:

Context is not only about online status. It can also provide information on actual location, readiness and willingness to accept a communication, and the current preferred medium. Presence details are relevant for numerous types of communication mechanisms including Instant Messaging (IM), landline telephones, mobile phones, IP phones, and email. The mobile environment is where context could initially be of more interest, and combining IM presence details with the ability to identify a user's location could lead to new and innovative services.

Source 3: 'CIO Agenda', Ref Code: OI00001-015 Ovum, 25 November 2010.

Standards and policy (Government and non-Government)

The likely delivery of context-aware services will be through Web Services and through the use of international standards such as the IP Multimedia Subsystem (IMS) architectural framework. It is envisaged that context-enriched software services will have the modularity and accessibility of Service Oriented Architectures (SOA) and use SOA-related standards.

There are no known Government policies covering context-aware computing and services.

QinetiQ comment

Context-aware computing is currently experiencing considerable hype that is more of a positive nature than one of caution with regard to the problems it could cause. Nevertheless, context-aware applications and services have already demonstrated business benefits and once the supporting and enabling technologies are mature are set to become a pervasive influence in our lives.

<p>Technology / Technique: Data Erasure</p>	<p>Relevant to SANS Critical Control: 17</p>						
<p>Description</p> <p>Data Erasure is a software-based method of overwriting data. Data erasure destroys all electronic data residing on a hard disk drive or other digital media. Permanent data erasure goes beyond basic file deletion commands, which only remove direct pointers to data disk sectors and make data recovery possible with common software tools. Unlike degaussing and physical destruction, which render the storage media unusable, data erasure removes all information while leaving the disk operable for reuse [1].</p> <p>There are a number of different methods for data erasure. Each follows the same principle of overwriting data but characters, and the number of times the data is overwritten, are both varied to provide different levels of assurance. The most straightforward method is to overwrite the data with zeros (the character '0'). This can be done cheaply and effectively by a number of programs, including straightforward commands in DOS or LINUX. Several U.S. Department of Defence (DoD) standards exist that require data to be overwritten with a combination of zeros, ones and random bytes and between 1 and 7 passes to meet different requirements.</p> <p>Bruce Schneier's algorithm [8] overwrites the file with zeros on the first pass, then ones, and then 5 further passes of cryptographically random bits. Bits are the zeros and ones used in binary code – 8 bits are used to define a byte, which equates to one character –not all combinations of bits equate to a readable character. Peter Gutmann's algorithm [9] is considered the strongest method, and uses 35 overwrite passes.</p>	<div style="text-align: center;"> <h3>Data Erasure Roadmap</h3> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 33%; text-align: center;">2 – 5 years</th> <th style="width: 33%; text-align: center;">6 - 9 years</th> <th style="width: 33%; text-align: center;">10+ years</th> </tr> </thead> <tbody> <tr> <td style="background-color: #ffffcc; padding: 10px;"> <ul style="list-style-type: none"> • Requirements for data protection and privacy will continue to increase the need for secure data destruction. • The desire to save costs and help the environment will encourage asset owners to look at data erasure that enables reuse, over physical destruction. </td> <td style="background-color: #c8e6c9; padding: 10px;"> <ul style="list-style-type: none"> • Cloud computing presents challenges to robust data erasure processes, with concerns around security for cloud tenants that exit the cloud leaving 'footprints' of sensitive data behind. </td> <td style="background-color: #e0f2f1; padding: 10px;"> <ul style="list-style-type: none"> • Data erasure will remain a fundamental part of the data lifecycle. • New technologies for storage will lead to new challenges, and uncertainties around how corresponding commensurate data erasure processes are devised, implemented and audited. </td> </tr> </tbody> </table>	2 – 5 years	6 - 9 years	10+ years	<ul style="list-style-type: none"> • Requirements for data protection and privacy will continue to increase the need for secure data destruction. • The desire to save costs and help the environment will encourage asset owners to look at data erasure that enables reuse, over physical destruction. 	<ul style="list-style-type: none"> • Cloud computing presents challenges to robust data erasure processes, with concerns around security for cloud tenants that exit the cloud leaving 'footprints' of sensitive data behind. 	<ul style="list-style-type: none"> • Data erasure will remain a fundamental part of the data lifecycle. • New technologies for storage will lead to new challenges, and uncertainties around how corresponding commensurate data erasure processes are devised, implemented and audited.
2 – 5 years	6 - 9 years	10+ years					
<ul style="list-style-type: none"> • Requirements for data protection and privacy will continue to increase the need for secure data destruction. • The desire to save costs and help the environment will encourage asset owners to look at data erasure that enables reuse, over physical destruction. 	<ul style="list-style-type: none"> • Cloud computing presents challenges to robust data erasure processes, with concerns around security for cloud tenants that exit the cloud leaving 'footprints' of sensitive data behind. 	<ul style="list-style-type: none"> • Data erasure will remain a fundamental part of the data lifecycle. • New technologies for storage will lead to new challenges, and uncertainties around how corresponding commensurate data erasure processes are devised, implemented and audited. 					
<p>Relevant applications</p> <p>Data erasure is part of the data lifecycle for sensitive data. For as long as there is a need to store sensitive data there will be a need to permanently erase data from electronic devices as they are upgraded or disposed of [2]. Rapid technological change such as different types of storage media and different ways of building storage infrastructure mean that data erasure techniques will continue to evolve to meet demand. Theft and loss of computers, laptops, devices and removable media are a common source of data breaches [3] for which the UK Information Commissioner's Office (ICO) and other prosecutors are increasingly pursuing [4].</p>							

General Issues and Challenges

Challenges for data erasure include new types of media such as flash based Solid State Drives (SSD) [5] which has proved harder than anticipated. The design of SSD means that the devices wear out faster if the same blocks are written and rewritten, so the Flash Transition Layer (FTL) responsible for managing the read and write commands to the drive, balances the load across the drive by delaying some of the erase commands. This leads to unpredictable behaviour, with research consistently showing that data can be recovered even when the drive has reported it is erased.

Large logical volumes such as cloud infrastructures present their own problems for ensuring that files are truly deleted. Cloud services are based on a cost efficient business model, offering standard services to multiple users taking advantage of the economies of scale. They need a secure, cost-effective option for reusing enterprise storage systems without rebuilding them. Organisations using the environment may have a requirement that the storage be wiped, for example to demonstrate compliance to the Payment Card Industry Data Security Standard (PCI DSS). Blancco, a leading data erasure provider, has this year launched a product to meet this demand [6].

Advances in data preservation technologies such as Microsoft's registered patents for Erasure Resilient Coding (ERC) [7] also highlight the dilemma between scenarios which require data resilience verses data erasure needs.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

The following information sources relate to references in this document:

- [1] 'Description of Data Erasure', Wikipedia, en.wikipedia.org/wiki/Data_erasure
- [2] 'Why Erase Data?', Data Erasure', 2008, www.dataerasure.com/why_erase_data.php
- [3] 'NASA sold computers with sensitive data, report says', Reuters, 7 Dec 2010, www.reuters.com/article/2010/12/07/us-nasa-computers-idUSTRE6B66UG20101207
- [4] 'Afghanistan military secrets sold for £18.87 on eBay after army officer dumped laptop in a skip', Daily Mail, 11 Nov 2010, www.dailymail.co.uk/news/article-1328667/Afghanistan-military-secrets-sold-eBay-army-officer-dumped-laptop.html
- [5] 'Flash-based solid-state drives nearly impossible to erase', InfoWorld, 22 Feb 2011, www.infoworld.com/t/solid-state-drives/flash-based-solid-state-drives-nearly-impossible-erase-263
- [6] 'Blancco Offers Solution for Cloud Computing Need for Erasure in Live Storage Environments', Cloud News Daily, 22 June 2011, cloudnewsdaily.com/2011/06/blancco-offers-solution-for-cloud-computing-need-for-erasure-in-live-storage-environments/
- [7] Patent application title: DISTRIBUTED DATA STORAGE USING ERASURE RESILIENT CODING, www.faqs.org/patents/app/20080313241#ixzz1d7lf22uf
- [8] Schneier B. : 'Applied Cryptography: Protocols, Algorithms, and Source Code in C', John Wiley & Sons Inc., 1996 (ISBN 978-0471128458)
- [9] Gutmann P.: 'Secure Deletion of Data from Magnetic and Solid-State Memory', See www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html, 1996.

Standards and policy (Government and non-Government)

Standards (such as the Security Policy Framework (SPF)) and regulations (such as the Data Protection Act (DPA)) which require organisations to protect personal and sensitive data, require organisations to conduct secure data erasure when required.

A number of standards exist to assure the validity of overwriting software. As a minimum, data should be erased to MOD approved/CESG Baseline Standard as described in HMG Infosec Standard No: 5. Key requirements for data erasure include the number of times the data is overwritten and verification that the data has been overwritten.

An international trade association for companies providing global information destruction services exists: National Association for Information Destruction.

QinetiQ comment

Data erasure is a mature capability for which there will always be a requirement, so long as sensitive data is stored on digital media. Destruction of sensitive data once it is no longer needed, or copied to another location, is a core tenet of information security. Standards for the levels of verification required for different classifications of data are well established, and can be applied to different architectures and types of media. While developments in technology will require continual evolution of the capability, the core principles remain unchanged and are here to stay.

<p>Technology / Technique: Data Recovery</p>	<p>See also: Data Erasure</p>	<p>Relevant to SANS Critical Control: 17</p>
<p>Description</p> <p>Data Recovery is the process of salvaging data from damaged, failed, corrupted, or deleted data storage devices/components using hardware or software methods when the data cannot be accessed normally.</p> <p>Storage devices/components include hard-disk drives, solid-state drives, USB devices, tapes, floppy disks, CDs, DVDs, SIM cards or any other type of device/component that can hold data in any form.</p> <p>Data Recovery techniques may be required in cases of both physical and logical damage. Physical damage of a storage device/component may prevent data from being accessed (e.g. damaged circuitry or mechanics). Logical damage to data on a storage device/component may allow data to be read but it fails to be understood (e.g. corrupted or deleted data). Typical data recovery scenarios and possible data recovery options are:</p> <ul style="list-style-type: none"> • Physical damage of a storage device/component: <ul style="list-style-type: none"> ○ Mechanical failure It may be possible to repair the damaged mechanism (e.g. hard disk drive mechanics) using donor parts from other devices/components and access the data through normal methods. ○ Circuitry failure It may be possible to repair or replace the damaged circuitry (e.g. USB connectors) and access the data through normal methods. • Logical damage to data on a storage device/component: <ul style="list-style-type: none"> ○ Corrupted data It may be possible to read some or all of the corrupted data using hardware or software data recovery tools. ○ Deleted data Deleted data is often not erased immediately, only the reference to the location of the data is deleted. Therefore, the space occupied by some or all of the data may be accessible by hardware or software data recovery tools to restore some or all of the original data. 	<div style="text-align: center;"> <h2>Data Recovery Roadmap</h2> </div> <div style="display: flex; justify-content: space-around;"> <div data-bbox="1205 491 1646 842" style="border: 1px solid black; padding: 5px; background-color: #ffffcc;"> <p style="text-align: center;">2 – 5 years</p> <ul style="list-style-type: none"> • Data recovery techniques will become increasingly challenging as proprietary data storage methods become more sophisticated and the complexity of the associated components/ devices increases. • Use of online data recovery services allow remote methods to assist a user to recover data but they are limited in what they can achieve. </div> <div data-bbox="1668 491 2110 842" style="border: 1px solid black; padding: 5px; background-color: #ccffcc;"> <p style="text-align: center;">6 - 9 years</p> <ul style="list-style-type: none"> • The maturation of cloud computing and prevalent use of cloud services with online backup features may result in fewer catastrophic data loss scenarios for those components/ devices, which connect to such a service. • Data recovery techniques continue to be more complex and specialist as the type and number of data storage devices/ components grows. </div> </div>	

Relevant applications

Data recovery is broadly used where data is lost and requires salvaging.

General Issues and Challenges

The majority of users may only employ standard software based data recovery techniques to recover important deleted or corrupted files. However, law enforcement may use advanced software and hardware techniques to recover illegal files, perhaps for intelligence gathering or for prosecution. The resource and skill required varies and the following gives an overview of the issues and challenges with the most common methods used today.

• Standard software based techniques:

- Usually can only restore data that has not yet been overwritten.
- Uses software techniques to locate and join data.
- Does not work on a physically damaged device/component e.g. physically damaged USB device that could not be read.
- Inexpensive software products available off the shelf.
- Examples: Undelete Pro, EasyRecovery, Norton Utilities etc.

• Advanced software and hardware based techniques:

- Can sometimes restore data that has been overwritten by examining previous 'layers' of data:
 - Depending on the type of storage technology, clues to previous data stored may remain (polarity for magnetic devices/components, charge for electrical devices/components etc.).
- Uses complex software and hardware techniques to locate, join and interpret data.
- Can sometimes work on a physically damaged device/component e.g. a physically broken part of a hard-disk drive platter.
- Expensive software and hardware combinations sometimes requiring specialised microscopes which can be very expensive.
- Examples:
 - Scanning Probe Microscopy (SPM) for hard-disk drives – a magnetic tip attached to a flexible cantilever which is placed close to the surface to be analysed where it interacts with the stray field emanating from the sample to produce a topographic view of the surface which can be analysed and interpreted.
 - Magnetic Force Microscopy (MFM) for hard-disk drives – similar to SPM however by also monitoring the position of the cantilever caused by the magnetic force by using an optical interferometer, detailed magnetisation patterns with high resolution which can be analysed and interpreted.
 - Chip reading of flash drives – physically remove a flash memory chip from a printed circuit board and read the data with a memory chip programmer or reader which can be analysed and interpreted.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

The following source examines forensic data recovery from flash memory, it suggests:...*a low level approach for the forensic examination of flash memories and describes three low-level data acquisition methods for making full memory copies of flash memory devices.*

Source 1: Small Scale Digital Device Forensics Journal Vol. 1, No. 1, June 2007.

This source reports on techniques and tools for recovering and analysing data from volatile memory paper, it covers:

...*the theory behind volatile memory analysis, including why it is important, what kinds of data can be recovered, and the potential pitfalls of this type of analysis, as well as techniques for recovering and analysing volatile data and currently available toolkits that have been developed for this purpose.*

Source 2: Amari K. et al.: 'Techniques and Tools for Recovering and Analysing Data from Volatile Memory', SANS Institute InfoSec Reading Room, www.sans.org/reading_room/whitepapers/forensics/techniques-tools-recovering-analyzing-data-volatile-memory_33049, 26 March 2009.

This source examines techniques in computer forensics from a data recovery perspective.

Source 3: Battula B.P. et al.: 'Techniques in Computer Forensics: A Recovery Perspective', International Journal of Security (IJS), Volume (3) : Issue (2), www.cscjournals.org/csc/manuscript/Journals/IJS/volume3/Issue2/IJS-13.pdf

Standards and policy (Government and non-Government)

There are no formal standards and policy regarding data recovery, however there are policies which relate to secure sanitisation i.e. methods to prevent data recovery. CESG, the UK National Technical Authority for Information Assurance (IA), publish various policy documents to selected members of the CESG community. These policies provide guidance on assessing risk, securing assets and assuring the confidentiality, integrity and availability of computer systems and data. IA Standard 5 (Secure Sanitisation) is one policy document that is intended to cover the protection of sensitive information but it also outlines possible data recovery methods.

Other non-UK governments have similar policies relating to secure sanitisation but the most influential is the US National Institute of Standards and Technology (NIST) Special Publication 800-88 (Guidelines for Media Sanitization) which describes practical sanitisation methods for most types of data storage components/devices.

QinetiQ comment

QinetiQ can confirm that the majority of data loss situations are recoverable. QinetiQ and other organisations have successfully recovered data even when there has been severe environmental or physical damage to a component/device. Most commonly, a hard-disk drive has stopped functioning and in most cases, the data can be retrieved using a combination of technical specialists and bespoke software. As the number, type and storage capacity of data storage components/devices increases, it is estimated that data recovery techniques will continue to be in demand.

Backup strategies which utilise the benefits of cloud services (where data is copied to more than one location that is physically and environmentally controlled to reduce the risk of data loss) are likely to reduce the number of instances where data recovery techniques are required. However, where these types of services are not used, consideration should be given to the type of data storage device used and how easily data can be recovered should it be required.

<p>Technology / Technique: Digital Trust Technologies</p>	<p>Relevant to SANS Critical Control: 11, 13, 15</p>						
<p>Description</p> <p>Supporting secure digital services used for sensitive interactions requires an underlying trust between parties. Digital trust technologies provide a range of services to help build this trust. The topic includes assurance that the parties are who they claim to be and also that the interaction is protected.</p> <p>This area is dependent on a number of technologies discussed in this paragraph. Web-browsers are the prevalent interface for accessing digital services and use a number of techniques to build trust, using either add-ons or core technology. Anti-phishing tools prevent or highlight to the user that the name of the Web site they are visiting is unexpected. The use of https (which itself utilises Transport Layer Security (TLS), also known as Secure Sockets layer (SSL)), provides the user of the Web browser with reliable information about the server (e.g. name), but anecdotally this is rarely inspected by users. Whilst anti-phishing tries to ensure the correct Web site name is used, Domain Name System Security Extensions (DNSSEC) enhances DNS to ensure the translation to internet Protocol (IP) address is correct. Https is supported by all major Web browsers and provides a tunnel for the secure transfer of information, though if mis-configured the protection is only an illusion. Stronger protection is afforded by use of Virtual Private Networks (VPNs) and by the HMG PRIME framework. Identification of a user to Web services is provided in a number of ways including passwords, secure tokens (e.g. RSA SecureID) and federated identifies (e.g. OpenID).</p>	<div style="text-align: center;"> <h2>Digital Trust Technologies Roadmap</h2> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 33%; text-align: center;">2 – 5 years</th> <th style="width: 33%; text-align: center;">6 - 9 years</th> <th style="width: 33%; text-align: center;">10+ years</th> </tr> </thead> <tbody> <tr> <td style="vertical-align: top; padding: 5px;"> <ul style="list-style-type: none"> Secure tokens will be exploited but will move from company specific solutions to more general services. This is likely to fuel deployment of federated identity schemes like OpenID. General usage remains for low value transactions as the identity is only asserted with low assurance. US federal government adopts technologies and approaches developed under their National Strategy for Trusted Identities in Cyberspace (NSTIC) programme. </td> <td style="vertical-align: top; padding: 5px;"> <ul style="list-style-type: none"> Adoption of US NSTIC approach outside of the US. UK Government backed identity enrolment scheme provides higher confidence in digital identity, which together with improvement in secure computing allows for greater trust in identities and services. </td> <td style="vertical-align: top; padding: 5px;"> <ul style="list-style-type: none"> Secure computing matures sufficiently to allow high value trusted services on Commercial Off The Shelf (COTS) platforms, this is coupled with a high assurance identity token which can be used across a range of services. </td> </tr> </tbody> </table>	2 – 5 years	6 - 9 years	10+ years	<ul style="list-style-type: none"> Secure tokens will be exploited but will move from company specific solutions to more general services. This is likely to fuel deployment of federated identity schemes like OpenID. General usage remains for low value transactions as the identity is only asserted with low assurance. US federal government adopts technologies and approaches developed under their National Strategy for Trusted Identities in Cyberspace (NSTIC) programme. 	<ul style="list-style-type: none"> Adoption of US NSTIC approach outside of the US. UK Government backed identity enrolment scheme provides higher confidence in digital identity, which together with improvement in secure computing allows for greater trust in identities and services. 	<ul style="list-style-type: none"> Secure computing matures sufficiently to allow high value trusted services on Commercial Off The Shelf (COTS) platforms, this is coupled with a high assurance identity token which can be used across a range of services.
2 – 5 years	6 - 9 years	10+ years					
<ul style="list-style-type: none"> Secure tokens will be exploited but will move from company specific solutions to more general services. This is likely to fuel deployment of federated identity schemes like OpenID. General usage remains for low value transactions as the identity is only asserted with low assurance. US federal government adopts technologies and approaches developed under their National Strategy for Trusted Identities in Cyberspace (NSTIC) programme. 	<ul style="list-style-type: none"> Adoption of US NSTIC approach outside of the US. UK Government backed identity enrolment scheme provides higher confidence in digital identity, which together with improvement in secure computing allows for greater trust in identities and services. 	<ul style="list-style-type: none"> Secure computing matures sufficiently to allow high value trusted services on Commercial Off The Shelf (COTS) platforms, this is coupled with a high assurance identity token which can be used across a range of services. 					
<p>Relevant applications</p> <p>These will include high value or sensitive interactions. For instance, accessing financial details from banks or other institutions; interactions with government services such as tax returns; and supporting trusted e-commerce services.</p>							

General issues and Challenges

Wide spread adoption of DNSSEC has encountered political and technical obstacles. With a concept of a root of trust associated with a domain that signs all the sub domains it is difficult for various governments, organisations and companies to decide who that should be.

As stated in 'Trusted Identities in Cyberspace' (Source 7 below) the use of trusted identities is coupled to secure software systems, the assurance of both needs to grow together. Approaches for cryptographic trusted identity (e.g. X.509 certificates) are known today but it is practical scalable schemes, and their implementation, that is the real challenge.

The supporting registrations/enrolment necessary for an identity scheme that is scalable and robust, is an issue for widespread uptake of secure identities.

The need for common trust points is much easier in a closed community; it becomes more difficult across organisations and with the public.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

The following publications were used in development of this forecast:

Source 1: Technology Strategy Board: Ensuring trust in digital services. www.innovateuk.org/_assets/0511/tsb_trustedservicesdirectory520.pdf

Source 2: Trust in the digital age: survey analysis. www.guardian.co.uk/digital-trust/trust-in-the-digital-age-survey-analysis

Source 3: Cyber Trust and Crime Prevention: A Synthesis of the State-of-the-Art Science Reviews. Whilst the technology review is now dated the approach and philosophic view of trust and identity usage remains useful. www.bis.gov.uk/files/file15270.pdf

Source 4: Security Usability Fundamentals. Discussions on security usability covering observations on why the technology may be good. Highlights that because the actual user does not understand the technology, this means the technology cannot deliver the expected assurance. Page 25 covers SSL. static.googleusercontent.com/external_content/untrusted_dlcp/research.google.com/en//pubs/archive/32872.pdf

Source 5: Hackers break SSL encryption used by millions of sites. www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/

Source 6: (US) National Strategy for Trusted Identities in Cyberspace. The home web site for the US initiative to develop trusted identities (principally for US use). www.nist.gov/nstic/

Source 7: Trusted Identities in Cyberspace. A recent article covering the complexity of trying to establish trusted identities, especially in a commercial and national or global context. [dx.doi.org/10.1109/MIC.2012.15](https://doi.org/10.1109/MIC.2012.15)

Source 8: OpenID. openid.net/

Standards and policy (Government and non-Government)

[1] Information Assurance (IA) Manual V. *1Use of IPSec in Government System – Implementation Standards1*. Issue 3.0, October 2007. Available from CESG.

[2] PRIME Framework: Specification Guide. Issue 1.2, May 2011. Available from CESG.

QinetiQ comment

The technical aspects of trusted identities will be simpler to solve than the wider legal, liability, and privacy aspects. These aspects are easier to solve in small-closed groups (e.g. companies or departments) rather than in a public, national or global context. The use and implementation of trusted identities is coupled in order to secure software and computers. The maturity of both will evolve together.

Technology / Technique: Emotion and Facial Recognition

Description

Emotion and Facial Recognition have some commonality yet are two separate fields that are in different states of maturity.

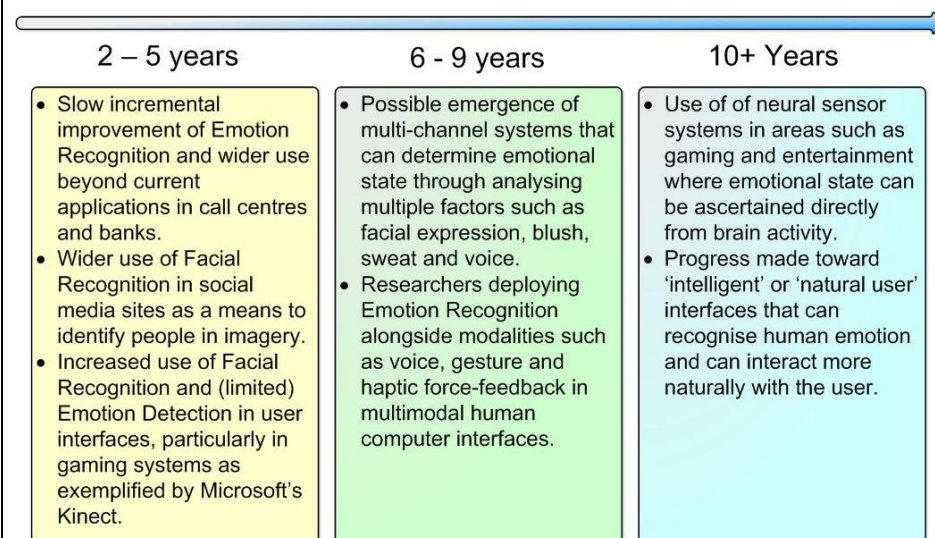
Facial Recognition is a form of biometrics that can be used to identify people. Computer Facial Recognition Systems take either a digital image or video frame of an individual's face and analyse selected features in order to compare them with those held in a database. More recently, this field has been exploited alongside gesture recognition in advanced user interfaces, particularly for consumer entertainment.

Emotion recognition falls within the field of 'Affective Computing', which researches the recognition of human emotion by machines and the means through which machines can understand emotion and express it. Over the last few years, it has become clear that numerous applications could benefit from a computer being able to process human emotions. At the forefront of these is emotion detection in call centres where troublesome callers can be routed to a supervisor; in advertising to ascertain people's responses to new products; and in security products.

The emotional state of the user can be assessed through the examination of a number of indicators, such as the tone of speech, facial signs and movements of the body. There is now a considerable body of research covering all these approaches where it has been shown that emotions are intricately linked to other functions such as attention, memory and decision making¹. Finally, it is worth noting that recent work has attempted to try to assess emotional state through measuring brain activity (see information sources below).

¹Sebe N et al.: 'Multimodal Emotion Recognition'
staff.science.uva.nl/~nicu/publications/emotion_chapter.pdf June 2004.

Facial and Emotion Recognition Roadmap



General issues and Challenges

Unlike Facial Recognition the field of Emotion Recognition and processing is in an immature state and faces many challenges. Emotional state is hard to measure and current systems using facial expression analysis or voice analysis are rudimentary despite claims to the contrary. For example, researchers at the University of Amsterdam used a Facial Recognition system to try to decipher the emotion behind the enigmatic smile of the 'Mona Lisa'. Their program exploits a number of machine learning and statistical algorithms and a database of 'neutral' expressions as the standard for comparisons to determine the probabilities for various emotions. In the case of the Mona Lisa it was concluded that the subject was 83% happy, 9% disgusted, 6% fearful and 2% angry.

A potential security threat lies in the use of facial recognition being used to tag individuals faces in images in public domains such as social networking sites (see source on Facebook facial recognition below). Besides Facebook's automatic tag suggestion feature, facial recognition is also being used by Apple's iPhoto and Google's Picasa.

Current research challenges (gleaned from MIT Media Lab's Affective Computing Group) include: 1) the creation of novel wearable sensors and new machine learning algorithms that can jointly analyse multimodal channels of information (i.e. a combination of input channels that could include factors such as brow furrowing, blush and sweat); 2) the creation of new techniques to assess frustration, stress and mood indirectly through natural interaction and conversation.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

The use of facial recognition by Facebook has caused some privacy concerns and does open up the possibility of interesting applications as well as threats to personal security. With regard to Facebook's automatic image tagging service (which comes as default) the following extract from an article in PCWorld clearly outlines the possibilities:

...as far as we know, the company is not going any farther with its current technology than suggesting that you tag people you are already friends with in newly uploaded photos. But could Facebook ever identify people you're not friends with and suggest that you become friends with them? 'Absolutely, it would be easy to do. All that data would be on that server farm. Technically, it's totally possible to expand that,' says Applied Recognition's Ganong.

It's not hard to imagine Facebook's 'Suggest photos of me to friends' privacy setting becoming 'Suggest photos of me to friends of friends' and then 'Suggest photos of me to others--essentially allowing you to take photos of strangers on the street and request a friendship.'

Source: Geuss M.: 'Facebook Facial Recognition: Its Quiet Rise and Dangerous Future - New facial recognition technology used to identify your friends in photos could have some interesting applications--and some scary possibilities', www.pcworld.com/article/226228/facebook_facial_recognition_its_quiet_rise_and_dangerous_future.html, 27 April 2011.

Most of the seminal work in the field of emotion detection has been conducted by Prof Rosalin Picard who leads MIT Media Lab's Affective Computing Group. See: affect.media.mit.edu/index.php. This group is researching techniques that enable computers to assess human states such as frustration, stress and mood and appropriately modify their response to improve human computer interaction.

A number of companies (such as Nemesysco, Nice Systems and Verint Systems) are currently offering emotion detection solutions. For example, the Israeli company

'Nemesysco' (www.nemesysco.com/) offers a number of voice analysis products and psychological evaluators that support a number of different types of applications. These include lie detection, emotion detection, security voice analysis for access control and voice risk assessment.

The BBC recently reported on technology developed by Neurofocus (see: www.neurofocus.com) that is reported to measure 'Emotional response, attentiveness and memory function'. This technology uses Electroencephalogram or EEG sensors that scan the individual's brain activity in order to measure their reaction to consumer products and advertising. Professor Nilli Lavie, from the Institute of Cognitive Neuroscience at University College London is quoted as saying: '*Neural marketing is becoming a hot topic in the marketing and scientific communities. In general, the approach can be very productive and may potentially reveal information about the consumer's brain that would otherwise be hard to obtain*'. Source: Walton D.: 'Can brain scan help companies sell more?' BBC News 17 March 2010. news.bbc.co.uk/1/hi/sci/tech/8569087.stm

Standards and policy (Government and non-Government)

There are no current standards in place although the World Wide Web Consortium (W3C) has released a working draft proposal for an Emotion Markup Language (EmotionML). EmotionML or EML is intended to be the standard mechanism for data to be annotated with human emotions. The W3C envisages three main application areas for EML:

- To annotate information streams, such as speech or video, with tags describing related emotions;
- To provide a standard output format for emotion recognition software or sensors;
- To provide a framework for systems to process and reason about human emotions.

Source: www.w3.org/2005/Incubator/emotion/XGR-emotionml-20081120/

<p>Technology / Technique: Next Generation (Heuristic) Anti-Virus</p>	<p>See also: Malware Detection</p>	<p>Relevant to SANS Critical Control: 5</p>						
<p>Description</p> <p>Most modern Anti-Virus Software (AV) has a heuristic element. This checks for behaviours that suggest malware activity, rather than previously-seen elements of malware noticed in code. This is, in part, to counter the use of polymorphic malware techniques, where no two instances of a given piece of code are exactly the same.</p> <p>This heuristic analysis is an essential part of the technology type - it means that, as well as observing currently known malware attack types, it also has a certain degree of ability to notice attacks that attempt to bypass known signatures, by highlighting software activity indicative of malware - for example, a PDF document should not normally attempt to connect silently to the internet.</p> <p>No profound step-changes in anti-virus heuristics are foreseen - most development seems incremental.</p>	<div style="text-align: center;"> <h2>Next Generation Heuristic Anti-Virus Roadmap</h2> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 33%; text-align: center;">2 – 5 years</th> <th style="width: 33%; text-align: center;">6 - 9 years</th> <th style="width: 33%; text-align: center;">10+ years</th> </tr> </thead> <tbody> <tr> <td style="background-color: #ffffcc; padding: 10px; vertical-align: top;"> <ul style="list-style-type: none"> Heuristics in commercial products standardise on monitoring behaviour, rather than doing wildcard searches through the code. Heuristics increase in capability and prominence in community/open source projects. Increasing processing power puts heuristics in AV in the mobile space. </td> <td style="background-color: #ccffcc; padding: 10px; vertical-align: top;"> <ul style="list-style-type: none"> New and more complex heuristic methods are introduced, taking advantage of increasing processing power. These may increasingly use more advanced assessment techniques, including concepts from artificial intelligence and machine learning. This will keep the playing field level as malware developers also adapt. </td> <td style="background-color: #ccffff; padding: 10px; vertical-align: top;"> <ul style="list-style-type: none"> The battle continues between AV vendors and virus writers. Other technologies and security methods (including, but not limited to, standardised code signing, role-based access control and trusted computing) continue to support AV products. </td> </tr> </tbody> </table>		2 – 5 years	6 - 9 years	10+ years	<ul style="list-style-type: none"> Heuristics in commercial products standardise on monitoring behaviour, rather than doing wildcard searches through the code. Heuristics increase in capability and prominence in community/open source projects. Increasing processing power puts heuristics in AV in the mobile space. 	<ul style="list-style-type: none"> New and more complex heuristic methods are introduced, taking advantage of increasing processing power. These may increasingly use more advanced assessment techniques, including concepts from artificial intelligence and machine learning. This will keep the playing field level as malware developers also adapt. 	<ul style="list-style-type: none"> The battle continues between AV vendors and virus writers. Other technologies and security methods (including, but not limited to, standardised code signing, role-based access control and trusted computing) continue to support AV products.
2 – 5 years	6 - 9 years	10+ years						
<ul style="list-style-type: none"> Heuristics in commercial products standardise on monitoring behaviour, rather than doing wildcard searches through the code. Heuristics increase in capability and prominence in community/open source projects. Increasing processing power puts heuristics in AV in the mobile space. 	<ul style="list-style-type: none"> New and more complex heuristic methods are introduced, taking advantage of increasing processing power. These may increasingly use more advanced assessment techniques, including concepts from artificial intelligence and machine learning. This will keep the playing field level as malware developers also adapt. 	<ul style="list-style-type: none"> The battle continues between AV vendors and virus writers. Other technologies and security methods (including, but not limited to, standardised code signing, role-based access control and trusted computing) continue to support AV products. 						
<p>Relevant applications</p> <p>Most AV vendors provide some level of heuristic analysis already. For example, Sophos Anti-virus protection for Windows uses technologies it calls Host Intrusion Protection System (HIPS) to determine questionable behaviours prior to binary execution; McAfee, Symantec and Kaspersky, amongst others, have a similar capability, and each cites their own technology as the finest.</p>	<p>General issues and Challenges</p> <p>Most Anti-Virus software - aka AV software and more commonly referred to by AV vendors as Endpoint Protection software - already has a degree of heuristic analysis, allowing it to detect previously unseen malware (malicious software).</p> <p>However, the standard cycle of testing for a typical malware writer involves tweaking the code until it is invisible to known AV software by testing the code against a service such as virustotal.com, or a homegrown equivalent. This is true however good the next-generation heuristics are - they are shipped in the product, thus available for testing against.</p>							

As a result, even if there is a step-change in heuristic AV, all this will do is slow down the rate of release of new malware (unless the change is so perfect as to spot all possible malware, which is unlikely). The attackers will simply tweak their malware, until these improved techniques no longer notice their wares.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

The following publications were used in development of this forecast:

[1]. Sophos Endpoint Security and Control for Windows, *Sophos's HIPS technology uses the anti-virus engine to identify programs that will behave suspiciously before they execute. Behavioral Genotype® Protection scans for multiple specific behaviors and characteristics to proactively protect against zero-day malware. It detects new threats before code even begins to execute.*

Source: www.sophos.com/en-us/products/endpoint/endpoint-security-and-data-protection/components/anti-virus-protection/windows/medialibrary/PDFs/factsheets/sophossavwindowsdna.pdf

[2]. Norton internet Security 2010 with Reputation-based Security Technology Scores Perfect Threat Detection Rate, *Advanced new heuristic protection: STAR [Security Technology and Response] has introduced a new generation of heuristics to detect unknown malware files before they can run and cause damage. This advanced approach detects entirely new malware, spyware and adware strains without fingerprints, instead searching files for suspicious sequences of instructions typically used by malicious software.*

Source: www.symantec.com/about/news/release/article.jsp?prid=20091027_04

[3]. Symantec Granted Patent for Fundamental Antivirus Technology

Source: www.symantec.com/about/news/release/article.jsp?prid=20051214_01

[4]. Heuristic analysis in Kaspersky Lab 2011 products, *Heuristic analyser (or simply, a heuristic) is a technology of virus detection, which cannot be detected by Anti-virus databases. It allows detecting objects, which are suspected of being infected by unknown or new modification of known viruses. It allows detecting about 92% of new threats. This mechanism is quite effective and has very rarely false detections. Files which are found by heuristics analyser are considered to be suspicious.*

Source: support.kaspersky.com/faq/?qid=208281948

[5]. The McAfee Gateway Anti-Malware Engine Protecting Users from Emerging Malware Threats, *The McAfee anti-malware engine employs behavioral heuristics by combining rule-based and weight-based methodologies. This enables the module to estimate the functionality that a program may perform at runtime.*

Source: www.mcafee.com/uk/resources/white-papers/wp-gateway-anti-malware-engine.pdf

Standards and policy (Government and non-Government)

The HMG Security Policy Framework (MR39) requires that all Departments must develop an Anti-Virus Policy. ISO27002 states that the policy should as a minimum:

- a. identify and assess the risks from malicious code and services and mechanisms provided by their ICT systems by which malicious code could be introduced;
- b. identify the security controls that are employed to mitigate and manage these risks, including acceptable use of services and systems;

- c. identify associated Incident Reporting and Response plans and processes;
- d. identify business continuity and disaster recovery plans.

CESG Good Practice Guide Protection from Malicious Code (ref [cesg-bookstore/data/docs/ia-good-practice-guides/gpg7.pdf](https://www.cesg.gov.uk/bookstore/data/docs/ia-good-practice-guides/gpg7.pdf)) states:

Host AV software will scan files on access and scan the file system periodically or on demand, looking for suspicious files. If a suspicious file is identified, it should be quarantined and an alert should be raised. Host AV software is primarily signature-based (although some products have heuristic capability). It also states ... All external connections should include anti-virus solutions at the boundary to check both incoming and outgoing communications for the presence of malicious code. ... and in order to minimise the effects from detection deficiencies in individual anti-virus products Departments should use a different anti-virus product on the boundary protection system than that used on internal host systems.

QinetiQ comment

Heuristic AV is already a part of the market, and has been for a number of years. Although heuristics can be improved, the malware can also be improved in its methods for avoiding detection. Only by tailoring the heuristics to an individual's behaviour can the accuracy take a large step forward, but this is unlikely to become mainstream as it would require a great deal of training and the vast majority of users want a security system that 'just works'.

Other techniques, like white-listing of known safe executables, are complementary and help provide added layers of defence.

Technology / Technique: High Security Wireless Communications for Civilian Use

Description

Wireless communications for civilian use have become ubiquitous over the past decade or two. In the early days of analogue cellular systems, security was not provided. Hence it was possible for eavesdroppers to listen in to conversations with ease. A number of high profile instances of such eavesdropping raised the issue in the public’s awareness and forced mobile phone developers and service providers to provide robust security in GSM (Global System for Mobile Communications) and subsequent systems.

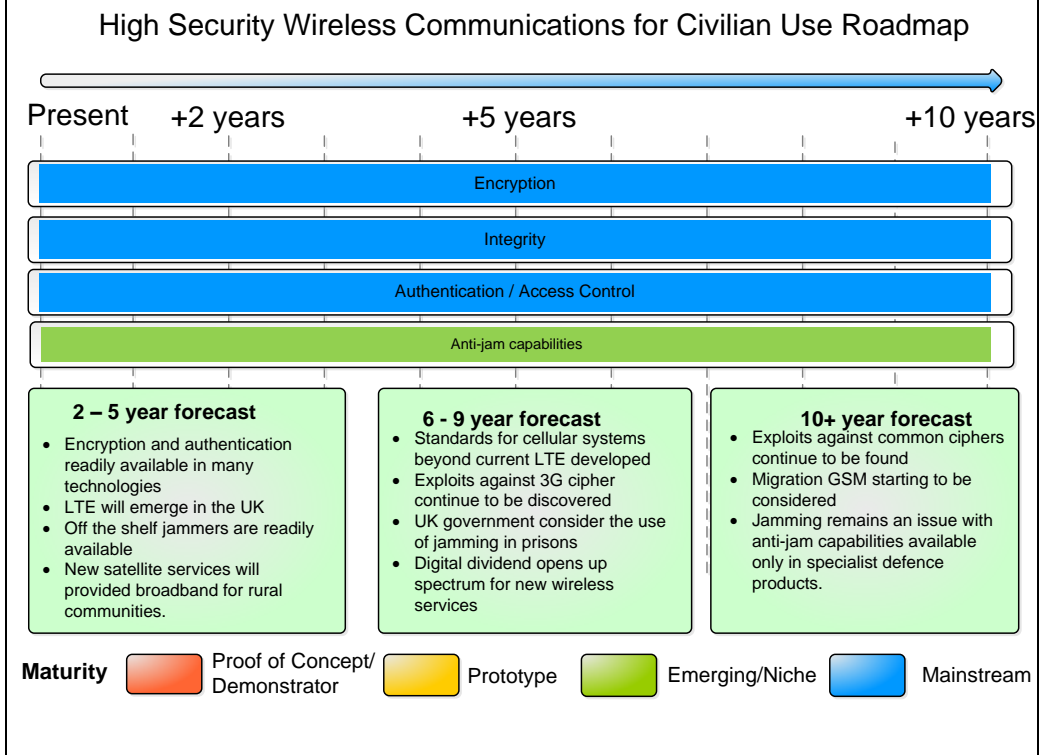
There are a plethora of modern wireless communications systems and technologies. For the majority of these, security of one form or another has been implemented. However, the robustness and capability of these varies.

When considering how secure a technology or solution is, we must consider a number of requirements, including:

- Confidentiality - prevent eavesdropping.
- Integrity - ensure that information has not be tampered with or changed in transit.
- Authentication/access control - ensure only valid users and devices can use the services.
- Availability - ensure that the services can be used when required.

In some applications, the actual information being communicated may not be particularly sensitive. However, validating sender identity and guaranteeing that the information has not been modified en-route, may be critical. Similarly, availability of the communications will be important, ensuring the communications channel is not blocked or jammed. Communications solutions will include a wide range of technologies and systems, including cellular services, satellite services (including those in low-Earth orbit (Iridium) and the newer high capacity broadband services), wireless local area network (LAN), point-to-point radio or meshed radio networks.

It should also be noted that security requirements may be met through characteristics of the communications system itself, or through appliqués or other system elements (e.g. external cryptographic devices or software). Further, whilst the communications services will provide some security capability, there are also security functions provided by the IT infrastructure. Often these capabilities will overlap (e.g. encryption). For instance, access control to the IT



system will be provided by the IT system, such as username/password challenges and two-factor authentication mechanisms (e.g. RSA SecurID Tokens). These latter capabilities are assumed out of scope of this forecast since they are properties of the attached IT system rather than the wireless communications services and technologies. Since this forecast covers civilian use, so-called 'high grade' evaluated security solutions aimed at defence and government customers are assumed not to be in scope. However, modern cryptographic solutions available to civilian customers can be very robust.

Relevant applications

There is a wide variety of relevant applications across all industrial sectors. Some applications that are considered important with respect to the national infrastructure include; voice and video communications; distributed control systems; Supervisory, Control and Data Acquisition (SCADA); telemetry; imaging systems (e.g. wireless CCTV). Distributed control systems and SCADA systems are used widely across many sectors, including utilities, manufacturing, environmental control systems and communications networks. The distinction between the control systems and SCADA systems are gradually being eroded through the availability of low latency communications. The security of SCADA has been a hot topic in recent years. Whilst attacks against SCADA installations may not have involved wireless communications directly, remote access facilitated by cellular and satellite systems will allow personnel to interact with SCADA systems from anywhere in the world. Consideration is needed as to whether this presents a significant new attack vector.

Wireless CCTV systems have been available for many years and are used in a variety of security and/or monitoring applications.

Remote access to enterprise networks has become more capable over the last few years with the rise of modern 3G cellular networks. These can give remote access from many locations in the world to office applications or any other networked enterprise capability, e.g. SCADA (see above).

Other emerging applications will increase demand for highly secure communications. In particular, mobile financial transactions (e.g. via near field communications (NFC) devices) and mobile banking will grow considerably in the coming years. The demand from consumers for robust security will not diminish, but will largely be met through the security solutions available in modern mobile phone networks.

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: Robust security is generally available in many wireless products and services. The next generation of cellular services Long Term Evolution (LTE) will gradually emerge in the UK from 2013 and grow over subsequent years. LTE brings with it a new encryption technology. However, jammers for a range of technologies and bands (e.g. GSM/3G, WiFi), are readily available. Wireless broadband from satellite brings more capable services to rural areas supporting greater remote working capabilities and providing an alternative bearer for many applications.

Within 6 – 9 years: Standards for cellular services beyond the current LTE technology will be developed. These will provide data rates in excess of 100 Mbps. Further exploits against the current 3G cipher will be developed, but will be difficult to develop into practical attacks. The UK government may consider using jamming technology in UK prisons, hence raising public awareness about jamming capabilities.

10+ years: In the longer term we can expect further attacks identified against ciphers and their implementation in modern wireless communications systems. This is

part of the continual process which helps evolve crypto capability. It is unlikely the vulnerability of GSM to spoof base stations will be addressed over this period. Operators and the UK government will start to look at the longevity of GSM and consider migration to 3G, LTE and beyond. However the installed base of GSM devices will be hard to migrate, including non-phone related applications. Vulnerability of wireless systems to jamming is likely to remain, with legislation ensuring jamming remains illegal. Anti-jam capabilities will likely remain the province of specialist defence systems.

General issues and challenges

- Encryption is available in many products. However, some products may use older or less secure implementations of encryption standards (e.g. WEP (Wired Equivalent Privacy) for wireless LAN implementations). Modern WiFi products implement the more robust WPA2 standard which provide an AES-based encryption algorithm with a maximum key length of 256 bits.
- A number of attacks have been shown against the ciphers used in GSM systems (A5/1 and A5/2). More recently (Source 2), attacks against the A5/3 Cipher for 3G (Kasumi) have been published. This showed an attack was possible against the cipher itself rather than an implementation. Whilst the paper shows that it is possible to recover a crypto key within two hours using a modest PC, the authors note that it may not be a practical attack against a real-world implementation in 3G systems;
- Availability of systems and services, and in particular resilience against intentional jamming, has not been high on the agenda with authorities, operators or solution developers. Legislation is only partially effective with jamming devices targeted at a number of technologies (WiFi, GSM, 3G etc.) readily available.
- Network spoofing attacks have been demonstrated for GSM systems (Source 3, Source 4). In these instances, a spoof base station under the control of an attacker can masquerade as a base station of a legitimate operator. This is because there is mutual authentication in GSM; the mobile authenticates itself to the network but not vice versa. This can be used to force the mobile to turn off encryption. Crucially this is not reported to the end-user in any way, hence they have no indication that encryption is not effective. Voice and data communications are vulnerable. This can also be used against 3G services by utilising the fact that the majority of 3G devices will fall back to GSM automatically if a 3G signal is not present. By jamming the 3G signal, the device will automatically connect to the spoof base station. Once this occurs, the same attack is possible as for the GSM device. Whilst this could be mitigated by removing the ability of phones to fall-back on 2G when 3G is not present (or denied), but many phones either do not have this option, or the users do not know it can be enabled.
- Recently, attacks have been described against the baseband processors in mobile devices. The attack is dependent upon the use of a rogue base station and allows the attacker to turn the mobile into a covert listening device amongst other things (Source 5).
- Always-on cellular packet data services (e.g. GPRS (General Packet Radio Service) and HSDPA (High-Speed Downlink Packet Access)) share capacity amongst the users. Hence availability and latency cannot be guaranteed and will be dependent upon the number of other active users within that cell. It is noted that these packet data services are becoming the norm for most cellular wireless data (as opposed to a dedicated data call), including remote access.
- Wireless CCTV – Many CCTV systems are not encrypted. This has led to so-called 1guerrilla artists¹ recording CCTV images and using them to make statements about the level of surveillance in the UK. More worryingly, there are reports of individuals hijacking imagery and broadcasting different images back to the security desks (Source 6).

Information sources, Supporting extracts and quotations (websites, forums, publications etc.)

The US Federal Bureau of Investigation (FBI) has recently acknowledged recent attacks on SCADA systems.

'We just had a circumstance where we had three cities, one of them a major city within the US, where you had several hackers that had made their way into SCADA systems within the city'.

Source 1: nakedsecurity Blog, FBI acknowledges more SCADA attacks, increases cyber budget, 13th December 2011 (nakedsecurity.sophos.com/2011/12/13/fbi-acknowledges-more-scada-attacks-increases-cyber-budget/).

Source 2: O Dunkelman, N Keller, and A Shamir, A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony, Jan 2010.

The GSM Association has responded to the spoof base station attacks:

The overall advice for GSM calls and fixed line calls is the same. Neither has ever offered a guarantee of secure communications. The great majority of users will make calls with no reason to fear that anyone might be listening. However users with especially high security requirements should consider adding extra, end to end security features over the top of both their fixed line calls and their mobile call.

Source 3: Forbes, Despite FCC 'Scare Tactics' Researcher Demos AT&T Eavesdropping, 31st July 2011 (www.forbes.com/sites/firewall/2010/07/31/despite-fcc-scare-tactics-researcher-demos-att-eavesdropping/).

Source 4: Forbes, Smartphone Data Vulnerable To Base Station Spoof Trick, 19th January 2011 (www.forbes.com/sites/andygreenberg/2011/01/19/smartphone-data-vulnerable-to-base-station-spoof-trick/)

Source 5: ReadWriteWeb, Baseband Hacking: A New Frontier for Smartphone Break-ins, 19th January 2011 (www.readwriteweb.com/archives/baseband_hacking_a_new_frontier_for_smartphone_break_ins.php)

Source 6: Newsweek Magazine, To Watch The Watchers, 9th Oct 2008 (www.thedailybeast.com/newsweek/2008/10/09/to-watch-the-watchers.html)

Standards and policy (Government and non-Government)

There are a wide number of encryption standards used in modern wireless communications systems. This includes:

- A5/3 Cipher (Kasumi) used in 3G;
- AES 256 used in many technologies including the latest cipher for LTE (Wireless LAN);
- WEP and WPA2 for 802.11.

Intentional jamming is illegal in the UK under Sections 8 and 68 of the Wireless Telegraphy Act 2006.

QinetiQ comment

Security for wireless technologies and systems for civilian use has been relatively robust for a number of years and is implemented in a wide range of technologies from cellular systems to satellite services and ad hoc meshed networks. However this has mainly focussed on authentication/access control (e.g. SIM cards) and encryption. Whilst there have been a number of attacks devised against the encryption algorithms and implementations, generally they are still considered relatively robust. However, other attacks are also possible that can render the encryption ineffective.

It is unlikely that civilian wireless communications technologies and services will have effective mitigations against jamming threats for the foreseeable future.

Technology / Technique: Malware Detection	Relevant to SANS Critical Control: 5														
<p>Description</p> <p>Malware detection is the set of techniques available to locate Malware, a cover-all term representing all trojans, adware, viruses, spyware, worms, and other malicious code; software intentionally designed to have an adverse effect on the system on which it is executed. Detection is typically performed at either network perimeter or on the desktop (or potentially on portable devices), but the ideal is to have both, each using different technologies.</p> <p>Traditional malware detection uses signature matching, but as the rate at which new malware emerges (hence signatures need updating), and as malware writers become ever more skilled at writing code that changes its form (polymorphic malware), this is becoming increasingly outmoded.</p> <p>2011 has seen a significant increase in both the diversity of malware types (Panda describe a daily average of 73,190 new samples of malware in early 2011), and an increasing proportion of trojans, intended to take control of the victim system. This latter trend also underpins topical discussion on Advanced Persistent Threats, where a Remote Access Trojan/RAT takes control of a system via some targeted means (such as selective phishing email/spearphishing).</p> <p>Malware detection is attempting to move toward more heuristic methods, specifically behaviour-based detection (isolating behaviours exhibited by malicious code), and anomaly-based detection (isolating unexpected and abnormal behaviour suggesting the presence of malicious code).</p>	<div data-bbox="1137 395 2136 1038" data-label="Figure"> <table border="1"> <caption>Malware Types from PandaLabs Q1 2011 Report</caption> <thead> <tr> <th>Malware Type</th> <th>Count</th> </tr> </thead> <tbody> <tr> <td>Trojan</td> <td>69,99</td> </tr> <tr> <td>Virus</td> <td>16,82</td> </tr> <tr> <td>Worm</td> <td>7,77</td> </tr> <tr> <td>Adware</td> <td>2,27</td> </tr> <tr> <td>Backdoor</td> <td>1,89</td> </tr> <tr> <td>Spyware</td> <td>0,08</td> </tr> </tbody> </table> </div> <p><i>Malware Types from PandaLabs Q1 2011 Report (see information sources).</i></p>	Malware Type	Count	Trojan	69,99	Virus	16,82	Worm	7,77	Adware	2,27	Backdoor	1,89	Spyware	0,08
Malware Type	Count														
Trojan	69,99														
Virus	16,82														
Worm	7,77														
Adware	2,27														
Backdoor	1,89														
Spyware	0,08														

Technology readiness and maturity (forecasted arrival and accessibility)

Within 2 – 5 years: Continued development of signature and heuristic-based detection methods

Within 6 – 9 years: Continued development of signature and heuristic-based detection methods, possibility of innovative mechanisms, increasing need on portable devices

10+ years: Continued development of signature and heuristic-based detection methods, possibility of innovative mechanisms, widespread need on portable devices

General issues and challenges

Malware is, and will continue to be a major issue, not simply in computer circles but right across the spectrum of business and Government – specifically, the targeted delivery of Remote Access Trojan, typically via phishing email, and potentially with state involvement/sponsorship (a cluster known generally as Advanced Persistent Threat/APT), is an increasing trend, and one which needs addressing. Also, the use of Stuxnet (widely regarded as a state involved/sponsored attack mechanism against the Iranian nuclear programme), and possibly the subsequent Duqu malware, suggests there is an increasing professionalism in malware production.

However, it is generally considered that more insidious widespread penetration of systems – the infection and covert control of systems ('bots'/'zombies', and their subsequent inclusion in a distributed command and control system (such as a 1botnet1 of appropriate size and subtlety) – is a more critical issue. There are numerous accusations of Nation-state involvement in intentional and focussed campaigns of attack for the purposes of industrial and state espionage, and offers a readily-deniable and effective mechanism for such attacks. Also, there is a burgeoning (and some claim overlapping) organised criminal involvement in such technologies.

Information sources, supporting extracts and quotations (Websites, Forums, Publications etc.)

The following publications were used in development of this advice:

Symantec emphasise that Duqu, although not Stuxnet-like in attacking SCADA systems directly, appears to be a precursor to such attack types - 1 *'Current analysis shows no code related to industrial control systems, exploits, or self-replication [but] The executables have been found in a limited number of organizations, including those involved in the manufacturing of industrial control systems'*. W32.Duqu: The Precursor to the Next Stuxnet ,

www.symantec.com/connect/w32_duqu_precursor_next_stuxnet

Information Assurance Tools Report - Malware, iac.dtic.mil/iatac/pdf/malicious_code.pdf

Symantec Granted Patent for Fundamental Antivirus Technology, www.symantec.com/about/news/release/article.jsp?prid=20051214_01

Simulating and optimising worm propagation algorithms, T. Vogt, web.lemuria.org/security/WormPropagation.pdf

Cryptovirology: Extortion-Based Security Threats and Countermeasures, A. Young, M. Yung, IEEE Symposium on Security & Privacy, pages 129-141, May 6-8, 1996.

Robert Slade's Guide to Computer Viruses, R. Slade, Springer-Verlag, 1994

The high proportion of Far Eastern infection is highlighted by Panda Labs - *In the ranking of the top 20 countries with the most infections, which was drawn from data generated by Panda ActiveScan, China, Thailand and Taiwan continue to occupy the first three places with infection rates of nearly 70 percent. Panda Labs 2011 Q1 Report*, press.pandasecurity.com/wp-content/uploads/2011/04/PandaLabs-Report-Q1-2011.pdf

Standards and policy (Government and non-Government)

The HMG Security Policy Framework (MR39) requires that all Departments must develop an Anti-Virus Policy.

ISO27002 states that the policy should as a minimum:

- a. identify and assess the risks from malicious code and services and mechanisms provided by their ICT systems by which malicious code could be introduced;
- b. identify the security controls that are employed to mitigate and manage these risks, including acceptable use of services and systems;
- c. identify associated Incident Reporting and Response plans and processes;
- d. identify business continuity and disaster recovery plans.

CESG Good Practice Guide *Protection from Malicious Code* (ref cesg-bookstore/data/docs/ia-good-practice-guides/gpg7.pdf) states:

Host AV software will scan files on access and scan the file system periodically or on demand, looking for suspicious files. If a suspicious file is identified, it should be quarantined and an alert should be raised. Host AV software is primarily signature-based (although some products have heuristic capability). It also states ... All external connections should include anti-virus solutions at the boundary to check both incoming and outgoing communications for the presence of malicious code. ... and In order to minimise the effects from detection deficiencies in individual anti-virus products Departments should use a different anti-virus product on the boundary protection system than that used on internal host systems.

QinetiQ comment

The increasing prevalence of Advanced Persistent Threats/APTs - where a Remote Access Trojan/RAT is delivered in a targeted manner, typically via spearphishing - has made Malware Detection an ever more critical technology. Although it is likely a sophisticated opponent will evade such detection, the higher the bar can be set, the better.

There are no 'magic bullets' to detecting all malware, so the key, at least given current technologies, is for an on-going 'arms race' of improvement in the signature-based and heuristic areas of malware detection - whenever a good defence technology is developed, the attackers will adapt, so there will need to be improvement and innovation in the arena. Signature-based detection is basic, but generally effective against older malware forms when kept current; behaviour-based and anomaly-based technologies are emerging, but can need more human intervention to handle false positives and other subtleties. There are also key issues regarding malware that need to be addressed at a human level, which do not relate solely to technology. For example, an attacker wishing to specifically target an organisation can easily infect a USB stick, leaving this e.g. in a car park, or give as a gift, to trick a curious user to insert into, and thus infect, their system. There must be effective technically-underpinned policy to limit the uncontrolled use of such items, and sufficient user education for them to know why such an action would be unwise. It is also worth mentioning that other technical disciplines, particularly intrusion detection/prevention systems (IDS/IPS), can offer the potential for detection, but these run similar issues (such as reliance on signatures) as the more dedicated techniques discussed.

The underlying malware is increasingly complex and ingenious – not least because increasing suspicion of nation-state, and/or criminal, involvement, moves the development of malware from the backroom into the paid, commercial development environment – and this means that static defences, relying on signature-based detection, are likely to be out-manoeuvred by those developing attack technologies. An attacker is unlikely to release a new piece of malware which has not been tested against a selection of current anti-malware technologies. Examples of the increasing complexity of malware include the development of polymorphic malware (see Slade in the references supplied below) - a series of techniques used to make instances of a given malware program to be functionally similar/identical, but to appear different when examined using signature matching; commonplace attacks using 1drive-by attacks¹, the automatic downloading/execution of malware simply through viewing a webpage on an unpatched web browser; and cryptovirology – the use of public key encryption techniques to evade detection and reverse engineering (see Young+Yung in the reference supplied below, as well as the Symantec analysis of Duqu).

<p>Technology / Technique: Cross Domain / Multi-level Security Solutions</p>	<p>Relevant to SANS Critical Controls: 5, 15</p>
<p>Description</p> <p>Cross Domain/Multi-level solutions are needed where a system that is permitted to contain data with a protective marking does not trust the security mechanism of a system that is permitted to hold data of a lower protective marking. Solutions are also needed where people who work at one security level need to access information generated and held at other security levels, either through convenient access to multiple systems or through information exchange.</p> <p>For lower protective markings, standard solutions generally suffice. For higher classifications, greater protection is needed.</p> <p>Multi-Level Access would enable someone at a single workstation to access different security levels. The challenge is to maintain the separation between logical systems on the same physical device (i.e. no information exchange enabled).</p> <p>A plausible solution could incorporate virtualised workstation products, thin client technology and thin client guards to limit exposure to attack.</p>	<p style="text-align: center;">Cross Domain/Multi-level Security Roadmap</p> <div style="display: flex; justify-content: space-around;"> <div data-bbox="1193 427 1637 887" style="background-color: #ffffcc; padding: 10px; border: 1px solid black;"> <p style="text-align: center;">2 – 5 years</p> <ul style="list-style-type: none"> • Some advances in multi-level information exchange for higher impact level information which include: <ul style="list-style-type: none"> ○ electronic exchange of documents between levels, but the types of document will be limited and may be subject to transformations that affect the ways they can be used. ○ limited messaging/email for conveying basic text messages from person to person. ○ arrangements that enable users to have effective access to different systems. </div> <div data-bbox="1637 427 2089 887" style="background-color: #ccffcc; padding: 10px; border: 1px solid black;"> <p style="text-align: center;">6 - 9 years</p> <ul style="list-style-type: none"> • Over time the position regarding multi-level access and information exchange is as likely to deteriorate as it is to improve, since every advance in IT will require a corresponding advance in Information Assurance technologies. • Improvements in CDS/MLS may result following users feedback of their experiences. This could create a 'virtuous cycle' in which the technologies become more widely accepted and enabling some advance. Conversely, broader acceptance could lead to added functionality to the available technologies, increasing their complexity and decreasing the degree of assurance that they behave correctly and are robust against attack. </div> </div>
<p>Multi-Level Information Exchange enables information to be exchanged between a 'Low' system and a 'High' system, subject to controls being applied to the information content. There are two challenges: (1) to provide controls that block 'unknown' attacks in imported data; (2) to remove hidden information from exported data and ensure that all visible information content has release approval.</p> <p>Relevant technologies include: deep content checking, data transformation and normalisation products; secure platforms for hosting the checkers; protocols and guard technologies to support interaction with the secure platforms; approved configurations for supporting labelling and review and approval processes.</p> <p>Successful implementation of cross domain/multi-level solutions has been 'just out of reach' for many years (with niche solutions intermittently delivered). Increasingly complex IT makes the goal ever more difficult to achieve as the opportunities for attack are greater the more complex the systems in which they operate. However, the demand for solutions has become significantly greater in recent years and significant UK effort is currently being brought to bear on the problem.</p>	

Relevant applications

Cross domain, multi-level solutions have widespread application within the defence and security. Three examples are given:

- Intelligence analysts need access to multiple security levels in order to retrieve and disseminate relevant information.
- Command and control for defence and security operations need information from diverse sources and instructions must be given to a range of people who lack clearance to use their highly classified systems. Access to different systems will be needed to enable collaborative activity with people who can only work with less protected systems.
- Some systems supporting national infrastructure (e.g. energy, finance etc.) are increasingly targeted by cyber attacks. Such connectivity may need the same sort of technologies that are required in defence and national/homeland security sectors.

General issues and challenges

Controlling the exchange of information with parties that are not entirely trusted affects the kind of information that can be exchanged and the way that people work with it. Optimising the security controls therefore requires a sound understanding of the business processes to be supported and how they are affected by the need for security protection. This understanding needs to evolve over time as products are trialled by users and refined in the light of that experience.

The market for security products of moderate strength and assurance is always likely to be more lucrative than the 'high end' market, which is likely to remain a niche requirement that is difficult to satisfy by commercial means alone. The challenge is to exploit the available commercial offerings as far as possible and enhance their overall effectiveness by using them intelligently in conjunction with each other and with a small number of simple, highly assured niche components.

Information sources, Supporting extracts and quotations (websites, forums, publications etc.)

A limited overview of multi-level security, that partially covers confidentiality concerns:

Source: www.centos.org/docs/5/html/Deployment_Guide-en-US/sec-mls-ov.html.

For integrity concerns see the following seminal paper:

Source: theory.stanford.edu/~ninghui/courses/Fall03/papers/clark_wilson.pdf.

Principles of supporting information exchange between levels are discussed in:

Source: books.google.co.uk/books?id=Vf3QzGSLlhUC&pg=PA129&lpg=PA129&dq=dbsy+qinetiq&source=bl&ots=T1NIK_csyg&sig=dbaFYKDYiW7MdGJEOO_bJqQ6h2A&hl=en&sa=X&ei=USnqTuDTKcWg8gOx-bH9CQ&ved=0CF0Q6AEwCA#v=onepage&q=dbsy%20qinetiq&f=false

VMware Press Release: 'CESG and VMware Deliver Trusted Platform for Hosting Multi-Level Environments':

Source: www.vmware.com/uk/company/news/releases/cesg-vmware_joint-statement14-09-11.html

Standards and policy (Government and non-Government)

Policy and standards for cross domain, multi-level security at higher impact levels are immature and currently limited to general indications of the degree of protection that security controls should aim to provide. Relevant HMG standards are:

HMG Information Assurance Standard number 1, 'Technical Risk Assessment' Parts 1 and 2. www.cesg.gov.uk/policy_technologies/policy/risk-tool.shtml

HMG Good Practice Guide number 12, *Use of Virtualisation Products for Data Separation: Managing the Security Risks*.

QinetiQ comment

Solutions enabling a multi-level access and information exchange capability are quite specialised. Nevertheless, there are a number of vendors (particularly from the US) who are offering so-called 'multi-level security' solutions. It is worth noting however, that when many of these 'solutions' are applied to higher levels of protective marking, issues arise concerning their readiness, particularly with respect to satisfying UK government policy and meeting the perceived levels of threat.

<p>Technology / Technique: Near Field Communication</p>	<p>Relevant to SANS Critical Control: 7</p>
<p>Description</p> <p>Near Field Communication (NFC) is a short-range high frequency wireless communication technology that is a derivation and subset of Radio Frequency Identification (RFID) technology. It enables the exchange of data and power between devices over short distances (usually around 4 cm, but no more than 20 cm when no amplification is applied). Typically, NFC occurs between a reader (usually a smartphone) and a target (which can be another reader or a microchip in an object, such as an interactive poster). If the device generates its own RF field it is called the 'active device', if it doesn't it is called a 'passive device'. Readers are usually the active device with their own built-in power supply, but at least one device must supply the power.</p> <p>The technology will take time to gain traction but is likely to become pervasive during the next five to ten years and volume shipments are expected in late 2011.</p> <p>Aspects of NFC have relevance to 'Wireless Device Control' within the SANS Critical Security Controls for Effective Cyber Defence document.</p>	<div style="text-align: center;"> <h3>Near Field Communication Roadmap</h3> </div>
<p>Relevant applications</p> <p>NFC has numerous applications although currently its most common application is to enable contactless payment with mobile smartphones. Other applications include:</p> <p>Access control – supporting authentication and providing access to secure areas;</p> <p>Information collection and exchange – information can be passed from reader to reader (e.g. by touching phones) and picked up from targets (tags) on objects (which might be marking particular locations);</p> <p>Marketing – Use in interactive posters e.g. one hundred locations in central London's busiest streets are to be equipped with digital advertising displays that include 72-inch HD screens and NFC.</p> <p>NFC is also expected to be used in areas such as transportation, social networking, point-of-sale loyalty and for improving user interaction with mobile devices.</p>	

General issues and challenges

There is currently a lot of hype and expectation set on NFC although there are still many issues and challenges to overcome which will slow adoption in the near term. For example there still needs to be agreement as to how all the parties involved, such as the handset makers, carriers and merchants, will share the revenues of the NFC ecosystem and exactly where sensitive data should be stored (e.g. whether it is on the SIM card or on the smartphone's embedded chip). To date, current deployments are on a trial basis and on a small scale (Source 2 below claims to have covered over 200 trials, pilots, tests and commercial NFC and related services in 54 countries).

Privacy and security will be major issues.

Security threats include:

- Eavesdropping (where an attacker can pick up transmitted data using an antenna);
- Data corruption (where an attacker can modify the data transmitted);
- Data modification (where the attacker manipulates the data but the receiving device believes it to be valid)
- Man in-in-the-middle attack (where for example, a party to one transaction inserts malware on the phone thereby infecting other phones that the original communicates with later).
- Loss of a handset that is not protected by an appropriate form of authentication.

The following is a good source covering security and NFC entitled 'Security in Near Field Communication (NFC)':
events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf

Information sources, Supporting extracts and quotations (websites, forums, publications etc.)

The analyst company Gartner predict that NFC as a means for making contactless payments will reach mainstream adoption in 5 to 10 years and expect to see companies deploying NFC services at the London 2012 Olympic Games. To quote:

Positive forces include major device vendors including NFC in their products from 2011, with volume shipments taking place from late 2011. A number of companies will try to demonstrate the service for the 2012 Olympic Games, making London a 'hot' place for deployments. However, these deployments and pilots are limited to one or two cities, and it is unclear whether various service providers will interoperate. The industry faces much confusion as to how the technology will evolve and what business models will be used.

Source 1: Fenn J., LeHong H.: 'Hype Cycle of Emerging Technology, 2011', Gartner Research ID: G00215650. 28 July 2011.

NFC World proclaims to be an international, independent and objective trade publication for those that design, supply, buy or use NFC-based products.

Source 2: www.nfcworld.com/

The NFC Forum (see standards and policy below)

Source 3: www.nfc-forum.org/aboutnfc

Nokia and the London School of Economics released a white paper entitled 'Near Field Communications; Privacy, Regulation and Business Models' in Oct 2011.

Source 4: www2.lse.ac.uk/management/documents/LSE-NokiaReport_14Oct2011.pdf

Standards and policy (Government and non-Government)


Although NFC was standardised in 2003 as ISO 18092 and as ECMA-340, more effort on standardisation is still required. The NFC Forum (see Source 4 above) which was formed by Nokia, Sony, and Royal Philips Electronics in 2004 now involves over 140 members and promotes the sharing, pairing, and transactions between NFC devices and develops and certifies device compliance with NFC standards.

Source 5 above examines the use of NFC in public transport applications and could inform future UK Government policy on the use of the technology in this sector.

QinetiQ comment

There has been growing impatience within the commercial sector for mobile phone companies to routinely embed NFC chips within handsets. Previous developments have used expansion cards to provide NFC capabilities for smart phones. One example is the Visa credit card initiative to embed NFC on microSD form factor cards (known as In2Pay) which can be inserted within mobile phone memory expansion slots and which has been rolled out via Akbank in Turkey for Blackberry users.

More recently high end smart phones have started integrating NFC technology directly into handsets. Significantly, the latest flagship Android phone, the Nexus S contains active NFC technology, while Apple have recently secured NFC patents on an 'electronic wallet' with speculation that the next generation of iPhone (v5) will incorporate NFC technology. However, if retailers are to invest in NFC payment technologies they need to be confident that smart phone users will be keen to pay for goods and services using their mobile phones. This may take time; the decision by Apple not to upgrade their iPhone 4GS with NFC may further delay that decision.

<p>Technology / Technique: Network Forensics</p>	<p>Relevant to SANS Critical Control: 10, 11</p>
<p>Description</p> <p>Network forensics has been defined as:</p> <p><i>The use of scientifically proved techniques to collect, fuse, identify, examine, correlate, analyse and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent or measured success of unauthorized activities meant to disrupt, corrupt and or compromise system components as well as providing information to assist in response to or recovery from these activities.</i></p> <p>Source: Palmer G.: <i>A road map for digital forensic research</i>, Digital Forensic Research Workshop, Utica, New York, 2001.</p> <p>Network Forensics is conducted using a variety of tools and systems such as Firewalls, Intrusion Detection Systems (IDS), Network Mapping Systems and Honeypots. These devices are placed at strategic points within a network and their output analysed along with data from log files in order to pinpoint anomalous behaviour. This activity is scrutinised to determine if it is indicative of a compromise of the network from an outside agent or breach of security policy from within the organisation itself. Such approaches are time consuming due to the sheer amount of data within a typical network and require a high-level knowledge of multiple technologies.</p> <p>Advances in Network Forensics Systems by security vendors [1], which collect data from multiple sources and provide a single point from which to analyse the data, together with Data Mining and Artificial Intelligence techniques allow for a degree of intelligent automated analysis. This will be refined and developed over the coming years as more organisations conduct research in this field [2] [3] leading to increased maturity in the field.</p>	

Technology readiness and maturity (forecasted arrival and accessibility)

Within 2 - 5 years: Dedicated Network Forensics Systems, tools and research will continue to develop and become more widely deployed, gradually centralising the task. The spotlight on cyber security and increased understanding of the value of digital assets and reliance on networks leads to increased investment in network forensics.

Within 6 - 9 years: Network Forensics Systems will become increasingly intelligent and configurable simplifying the processes involved in monitoring the network. They will be increasingly common place as organisations seek to protect their assets, identify attackers and prosecute culprits.

10+ years: Increasing use of Data Mining and Artificial Intelligence techniques will become more prevalent, reducing the data that must be examined by analysts. Large networks such as cloud infrastructures have sensors placed as standard as part of security-as-a-service offering.

General issues and challenges

The main issues and challenges with this field are as follows:

- Data Volume – The sheer volume of data moving around a typical computer network provides a major challenge within Network Forensics. Careful placement of any sensors and choice of data to analyse are essential to a successful deployment. This necessitates an accurate knowledge of network topologies which is dependent on sophisticated and reliable network mapping tools;
- New Technologies – With increased use of Cloud Infrastructures, Wireless Networks, Smart Phones and PDAs, any Network Forensic solution must be able to provide the same level of monitoring applied to the traditional computer network to these new technologies where they interface with the organization's network. This is a major challenge due to the rapidly changing capabilities of such technologies;
- Evidential Issues – The integrity of the data collected and the methods used must be ensured, particularly if it were ever to be used within a court of law;
- Privacy – Some data collected within a network may be of a personal nature. The handling of such data must reflect the various privacy and proper use regulations.
- Increased Threat – An increasing frequency of attacks from 'Hacktivists' such as Anonymous and LulzSec [4], as well as State sponsored intrusions [5] are leading to an increased awareness of the threat to digital assets, and a demand from organizations to improve network investigations and defences. [6]

Information sources, supporting extracts and quotations (Websites, Forums, Publications etc.)

[1] McAfee LEADS New Criteria for Next Generation IPS, Business Standard, 13/10/2011, www.business-standard.com/india/news/mcafee-leads-new-criteria-for-next-generation-ips/452433/

[2] Research on the clients of network forensics, Chongqing University (China), 13/03/2011, ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5764059&tag=1

[3] Network Forensics: Notions and Challenges. King Fahd University (Saudi Arabia), 2009, www.ccse.kfupm.edu.sa/~ahmadsm/research/almulhem09.pdf

[4] Nokia's developer network hacked, BBC News, 29/08/2011, www.bbc.co.uk/news/technology-14706810

[5] US names China and Russia as key cyber threats, SC Magazine, 04/11/2011, www.scmagazineuk.com/us-names-china-and-russia-as-key-cyber-threats/article/216007/

[6] Cyber attack tests for Olympic Games computer systems, BBC News, 10/10/2011, www.bbc.co.uk/news/technology-15244808

Standards and policy (Government and non-Government)

- HMG Security Policy Framework (SPF) provides requirements for security and risk management in government. It mandates the need for forensic readiness. www.cabinetoffice.gov.uk/resource-library/security-policy-framework
- The ACPO (Association of Chief Police Officers) Good Practice Guide for Computer-Based Electronic Evidence is the de-facto standard for gathering and processing digital evidence. www.cabinetoffice.gov.uk/resource-library/security-policy-framework

QinetiQ comment

Organisations depend upon networks, communications and the security of assets that are under their control. The aim of the UK Government Cyber Security Strategy is for the UK to be a prosperous place to conduct business in cyber space, and therefore the spotlight is on security. Network Forensics is a valuable reactive measure, post incident, to attempt to identify the perpetrator of an attack and gather the necessary information for a prosecution. This requires the correct sensors, technologies, people and process to be in place BEFORE an incident occurs (often known as forensic readiness). With increasing threats from hacktivism and State actors, the need for network forensics is pushing it from a back-office capability completed occasionally by a tech-savvy administrator, to a professional and essential service for the protection of organisations.

<p>Technology / Technique: Future Protocols for Network Security</p>	<p>Relevant to SANS Critical Control: 4, 13</p>
<p>Description</p> <p>Security is the degree of protection that an asset (either physical or virtual) has against loss, damage and other undesirable dangers. CESG break down security into three parts¹: Confidentiality, Integrity and Availability (sometimes referred to as the ‘CIA attributes’). Confidentiality is ‘<i>the property that information is not made available or disclosed to unauthorised individuals, entities, or processes</i>’. Integrity is ‘<i>the property of safeguarding the accuracy and completeness of assets</i>’. Availability is ‘<i>the property of being accessible and usable upon demand by an authorised entity</i>’.</p> <p>To manage the three properties of security, the concepts of Identity and Authentication are also important – ensuring that the other participant in the exchange is known and that they are allowed to access the information they are receiving. Without identity and authentication, a system cannot determine whether an exchange is allowable or not.</p> <p>Protocols, in the context of computer networks, are specifications and standards that define how two items of hardware or software will communicate so that they can understand each other for the transfer of data or instructions. Some of these protocols are intended to secure the communication, while others provide functionality (such as identity and authentication) that supports the securing of other network services.</p> <p>¹Note: The HMG InfoSec Standard Number One (IS1) is used to assess the technical risks to confidentiality, integrity and availability. See: www.platinumsquared.co.uk/IAStandardsPages/IS1part1.aspx</p>	<p style="text-align: center;">Future Protocols for Network Security Roadmap</p> <div style="display: flex; justify-content: space-around;"> <div data-bbox="1205 596 1496 1066" style="border: 1px solid black; padding: 5px; background-color: #ffffcc;"> <p style="text-align: center;">2 – 5 years</p> <ul style="list-style-type: none"> • Some Internet Engineering Task Force working groups will deliver their recommendations and improvements of public standards. • CESG’s PRIME Framework encryption interoperability standards should gain visibility in common products. • Devices that combine Quality of Service (QoS) and information routing with traffic encryption will become more prevalent. </div> <div data-bbox="1514 596 1805 1066" style="border: 1px solid black; padding: 5px; background-color: #ccffcc;"> <p style="text-align: center;">6 - 9 years</p> <ul style="list-style-type: none"> • Voice over IP systems will standardise on common security protocols, the most likely candidates include Secure Real Time Protocol and/or Datagram Transport Layer Security (DTLS), Multimedia Internet Keying (MIKEY) and Secure Communications Interoperability Protocol (SCIP). </div> <div data-bbox="1823 596 2114 1066" style="border: 1px solid black; padding: 5px; background-color: #ccffff;"> <p style="text-align: center;">10+ years</p> <ul style="list-style-type: none"> • Predicate encryption is used within some protocols (e.g. as part of database access), allowing for finer grained control of decryption based on time, location, user attributes or other factors. This improves security by reducing the necessity to over-share information. </div> </div>
<p>Relevant Applications:</p> <p>Network security protocols are relevant to all computer networks that contain information and functionality that must be protected against compromise of its CIA attributes. This includes those holding personal information, commercially sensitive information, or nationally sensitive information, as well as systems providing support to important capabilities and provision of essential services.</p>	

General Issues and Challenges

The commercial sector is already solving many of the network security problems for the lowest impact levels. Existing protocols (such as Hypertext Transfer Protocol Secure (HTTPS) for secured communication or Kerberos and Host Identification Protocol for authentication and access) as well as newer extensions (such as Domain Name System Security Extensions (DNSSEC) for record integrity checking and IPv6 with its integrated mandatory network-level security) are either already in extensive use or are being introduced on the internet. Groups such as the IETF also have on-going workgroups dedicated to creating standards for network security. Standard security protocols are being integrated with existing protocols where possible. Where appropriate, these technologies should be used for low cost of entry and high interoperability through standardisation.

Protocols that maintain the confidentiality and integrity of data on a network in-transit rely on cryptography and are often built into devices that are placed outside of most other infrastructure on the edges of the user's network. This interrupts the connection between the end-points, breaking important network management systems such as QoS and routing. To improve network management, crypto needs to be better integrated within other network devices and functionality. Without this integration, encryption degrades usability, system performance and the ability of administrators to appropriately manage their systems.

When there is a need to access values from a large set of data, it is sometimes the case that only partial access is required. For example, it may only be necessary to know that a value exists in a data set. In cases where the data is encrypted, it would be preferable not to completely decrypt this data to ensure that those who don't need access to the raw values cannot read them. This cannot be done with normal encryption protocols, but newer predicate encryption protocols allow queries to be created that can determine the existence of desired data within the encrypted data set without decrypting all of it. If this can be integrated into the protocols themselves then management can be improved by allowing minimal required access and security can be improved by sharing the minimal amount of data necessary.

Information sources, supporting extracts and quotations (Websites, Forums, Publications etc.)

Active IETF Working Groups Webpage.

Source 1: datatracker.ietf.org/wg/#SecurityArea

'While much of IT security is relatively mature (for example, network access control and vulnerability management), industry-specific technologies (such as consolidated logical/physical security systems and process control protection) are still evolving to address more modern [Operational Technology] platforms and software'.

Source 2: Young G.: 'Hype Cycle for Infrastructure Protection, 2011', Gartner Research ID: G00215771, 10 August 2011.

'...future network security can be effectively addressed on the lower-level by introducing an [application-level] identity packet for network protocols. ...This original work is aimed at providing another way of securing high speed network protocols...'

Source 3: Bernardo D.V.; Hoang D.B.: 'Future Networks, 2010', IEEE Computer Society. 2010.

Standards and policy (Government and non-Government)

The IETF is the main public body focusing on network security. Their Working Groups (WGs) are categorised according to topic, which includes the topic header 'Security Area' which lists active working groups in the field of network security (see source 1 above). Security aspects can also feature in the other WGs, such as the DNS

Extensions WG (including DNSSEC) and Host Identity Protocol WG for identity management and protection against spoofing, both of which are in the internet Area group.

Within UK Government, CESG are engaging with industry over the PRIME Framework for interoperability of networked cryptographic devices. Once this standard is widely used in manufactured devices then there will exist a range of devices that support a common set of interoperable protocols for use by organisations who wish to secure their communications. The previous major cryptography interoperability standard was HAIPE (High Assurance internet Protocol Encryptor) from the US National Security Agency.

QinetiQ comment

The majority of network security protocols focus on encryption to maintain confidentiality and integrity. Most cryptographic algorithms are not likely to undergo large changes in the coming years. Newer protocols may use more secure algorithms or larger keys, but these will generally be incremental improvements over the current state of the art. The main area of novel secure protocols is those that not only provide security in transit but also integrate with security at rest. These new protocols, in association with improved protocols for identity, will provide new ways to secure network communications and information on those networks and integrate identity and security more tightly within the business workflow.

In addition to network protocol developments, higher levels of assurance have requirements for key distribution methods that are still being researched and improved. The method in which this distribution is done is a separate issue from the protocols that use the keys and so has not been included here. Similarly, security can also be implemented outside the protocol space (within hardware and applications) and so can be important to enhancing the security of the network but is not included here. Both of these subjects should not be overlooked and are relevant and important to good network security.

Technology / Technique: Next Generation Human Computer Interaction (HCI)

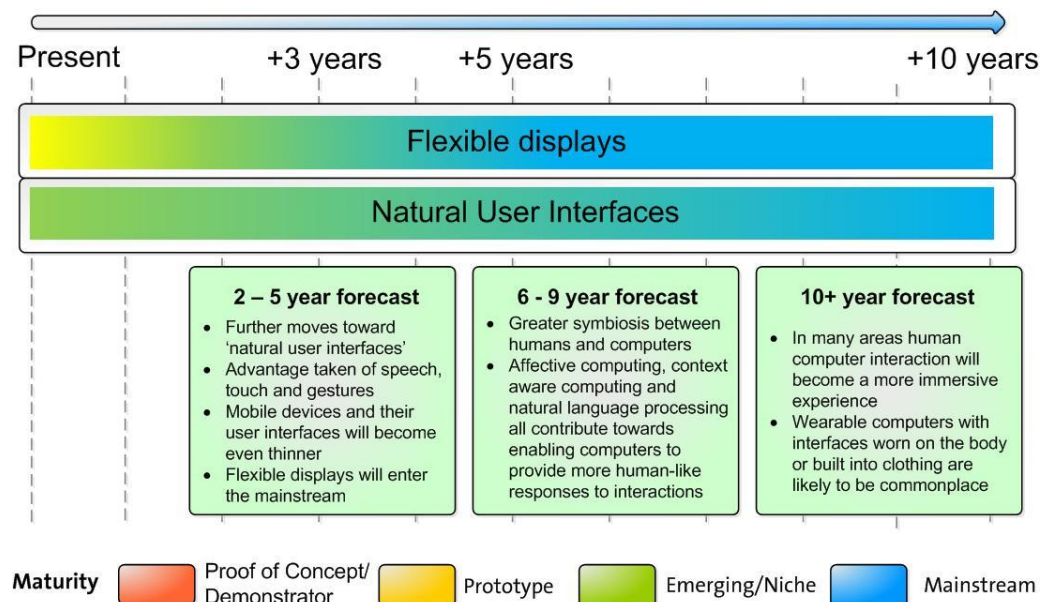
Description

There is no commonly used definition of the field of Human Computer Interaction (also known as HCI). However, a reasonable starting point could be: HCI is the study of the interaction between people and computers. The discipline is concerned with the design, evaluation and implementation of computer systems for human use, including both software and hardware.

A central theme in the field of HCI is that humans and computers work in fundamentally different ways, and understanding these differences is vital in ensuring harmonious interaction between them.

During the last few years there have been some major changes in the way humans work with computers driven in particular by consumer oriented devices such as the smartphone and media tablets with their multitouch interfaces and the entertainment industry with 3D technologies and devices such as Microsoft's Kinect motion sensor. Amongst the next generation of human computer interfaces we can expect to see flexible paper-like displays and also gesture recognition and emotion detection which will widen the gap further between the approach of easy-to-use consumer devices and the more complex and traditional approaches that are still adopted by many enterprise-oriented technology areas.

Human Computer Interaction Roadmap



Relevant applications

HCI occurs anywhere where humans are required to interact with a computer, through providing input (e.g. through the ubiquitous keyboard and mouse) or receiving output (e.g. through a visual display and audio headphones).

General issues and Challenges

HCI is a complex discipline. The key issue is that general theories of HCI must be based on an understanding of the body and mind of the human operator, which are in themselves a hugely complex subject about which much is still to learn. Additionally, the context of the specific interaction (such as the environment, the task at hand, and the characteristics of the individual user) will affect HCI. Each of these variables has a range of different (and sometimes not well understood) effects on human performance. Research that is thorough enough to be definitive concerning HCI is often prohibitively expensive, and so interaction design proceeds more often on an ad hoc basis, with cases of poor interfaces being common.

Information sources, Supporting extracts and quotations (websites, forums, publications etc.)

Gartner's 'Hype Cycle for Human Computer Interaction, 2011' highlights a number of trends and drivers for HCI research and development during the next few years. To quote:

The trends toward more-intuitive human-computer interfaces, which we saw develop slowly in 2010, have accelerated in 2011 with the rapid emergence of tablets and continued growth of sensor-enabled smartphones and gestural interfaces (that is, natural user interfaces) for gaming systems. The ease of use, intuitive (rather than intrusive) nature and innate discoverability of natural user interfaces (including touch, multitouch and gestural 3D movements) have clearly demonstrated that technology need not create a barrier between individuals (especially the 'nonexpert' user) and the myriad of devices that increasingly populate and influence the world around them.

Source 1: Prentice S., Fenn J.: 'Hype Cycle for Human Computer Interaction, 2011'. Gartner Research ID Number: G00215631, 28 July 2011.

The following quotation refers to the use of 'quantum dots' to create a paper thin flexible display:

1Television screens that can be rolled up and carried in a pocket are to become a reality using technology developed by British scientists. Researchers have developed a new form of light-emitting crystals, known as quantum dots, which can be used to produce ultra-thin televisions. The tiny crystals, which are 100,000 times smaller than the width of a human hair, can be printed onto flexible plastic sheets to produce a paper-thin display that can be easily carried around, or even onto wallpaper to create giant room-size screens. The scientists hope the first quantum dot televisions – like current flat-screen TVs, but with improved colour and thinner displays – will be available in shops by the end of next year. A flexible version is expected to take at least three years to reach the market.¹

Source 2: Gray R.: 'Forget 3D, here comes the QD TV' The Telegraph, www.telegraph.co.uk/technology/news/8948484/Forget-3D-here-comes-the-QD-TV.html, 14 December 2011.

When mention is made of future HCI many people recall the user interface in the Tom Cruise movie 'Minority Report'. The following source refers to technology that takes us a step nearer to this vision:

Forget the desktop environment with one or two screens. Oblong Industries' spatial operating system extends your workspace to every available screen in a room. With the latest developments, the technology is a frontrunner for the future of the user interface.

Source 3: Jablonski C.: "Minority Report' gestural computing pretty much here', ZDNet Emerging Tech., www.zdnet.com/blog/emergingtech/minority-report-gestural-computing-pretty-much-here/3050?tag=mantle_skin;content, 9 December 2011.

There are many conferences covering Human Computer Interaction. One of the largest is the HCI International Conference, which is held every two years.

Source 4: www.hcii2013.org/

Standards and policy (Government and non-Government)

Usability testing is an important factor when developing technologies to support and enable HCI. The International Standards Organisation (ISO) defines usability as 'The extent to which a product can be used by specified user to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use'. [ISO 9241, part 11, 1998]. This Standard, and the more recent ISO 13407, emphasise the need to measure usability in terms of the interaction between user and device (rather than simply seeing usability as a characteristic of the device itself).

To the author's knowledge usability, as developed in the HCI research tradition, does not feature in UK Government policy.

QinetiQ comment

Following a period of 'HCI lock-in' where for more than 20 years HCI has been almost exclusively through the QWERTY keyboard and mouse and visual presentation through the ubiquitous WIMP (Windows, Icons, Menu, Pointing) GUI (Graphical User Interface) a change is underway. As previously mentioned, this change is being driven by the consumer electronics industry, and mobile devices in particular. Nevertheless, at least for the desktop, the familiar windows, keyboard and mouse **will not be replaced** anytime soon despite recent media reports that 'minority report' style interfaces are '*pretty much here*' (see source 3 above).

As a final observation, it seems probable that flexible displays will first show benefits in applications that require toughness and resilience, rather than the ability to fold or roll completely away.

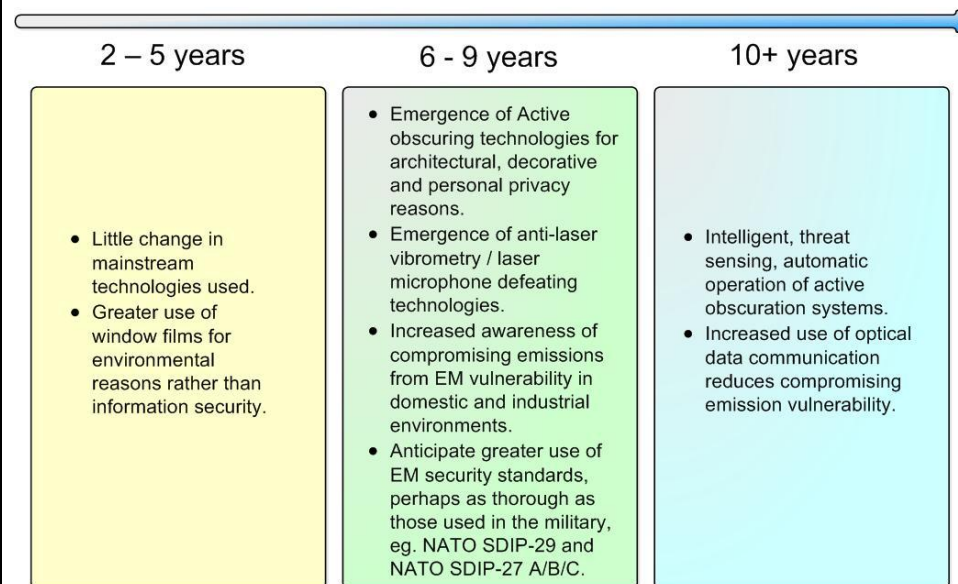
Technology / Technique: Novel obscuration techniques for windows

Description

Float glass windows provide a visually transparent and translucent physical barrier in a building/vehicle. To improve privacy while maintaining some of the other provisions a number of highly effective ‘compromise’ techniques exist for countering visual threats. Technologies include surface textures formed by embossing to obscure through light path distortion [1], or formed by etching or coarse abrasion, so called ‘frosting’, to obscure through scattering. Alternatively, an embossed or etched appliqué film can be adhered to the glass[2]. Dye colours, thin metal films and conductive ceramics (typically applied using a polymer substrate) can reduce translucence and in the case of metal films, increase reflectivity; different metals and ceramics and thicknesses provide different optical effects[3]. Adjustable/temporary techniques such as curtains and blinds (including in-glazing mini blinds) can also be effective[4]. More recent technologies include active privacy windows[5][6][7] that switch from transparent to opaque/translucent while prismatic[8] and micro-stripe[9] films can restrict viewable angles.

Glass is also partially transparent across much of the near infrared and microwave spectrum and so creates vulnerabilities to eavesdropping techniques such as laser microphones and Electro Magnetic (EM) emission monitoring (TEMPEST), electrically conductive window coatings can reduce these threats. To counter the EM/microwave threat, the window frame and seals also need to be treated too.

Novel Obscuration Techniques Roadmap



Technology readiness and maturity (forecasted arrival and accessibility)

Within 2 - 5 years: Continued use of existing passive visual optical obscuration and passive EM screening techniques is anticipated. Greater use of partially metallised or conductive ceramic translucent window treatments on vehicles, domestic buildings and other inhabited properties is also expected , in an attempt to reduce energy consumption.

Within 6 - 9 years: Greater use of active obscuration systems is expected. They become more widely available as technologies mature, popular understanding grows and the cost reduces. It is likely that decorative, modesty and architectural markets rather than information security will drive their increased use. We anticipate that in this timeframe the emergence of preferred techniques to reduce the efficacy of laser microphones and related laser vibrometry techniques as these threats become

cheaper and more widespread. Also expected is greater use of conductive window coatings and related methods to provide screened environments to a military INFOSEC standard, e.g. NATO SDIP-29 and NATO SDIP-27 A/B/C.

10+ years: In the longer term we can expect to see intelligent active obscuration systems that operate automatically when a threat is sensed. The increased use of optical computing and optical data transfer is likely to reduce the TEMPEST vulnerability.

General issues and challenges

The key commercial innovation in this field of increased optical privacy in glasses is the development of large area screens that switch from a highly transparent state to an opaque/translucent / reduced transparency state in a short period, typically milliseconds. Practicality requires a lifetime of many hundreds of thousands to millions of cycles while operating over a large range of temperatures and illumination conditions. There are several competing technologies/chemistries under development including electrochromic devices, reversible chemical deposition, suspended particle devices, micro-blinds and Liquid Crystal Devices (LCD). LCD systems are currently the most mature technology. In addition to providing visual privacy these systems will also significantly degrade the performance of laser microphones using target objects in the building. The common challenge confronting developers is the requirement for an optically transparent chemically stable electrical conductor. To date thin metal films and conductive ceramic materials are used, however large area grapheme [10] may provide an improvement in the 5 to 10 year timeframe.

Reducing the TEMPEST vulnerability of windows relies on visually transparent, highly electrically conducting, treatments on the glass and that a low resistivity gap-free electrical connection is maintained to the other parts of the EM screening the room. Two approaches are commonly used to achieve EM opacity and optical transparency; thin films of highly conductive metals and mesh/grids of fine highly conductive wires. When conductive enough to provide EM shielding, (e.g. <10 Ohm per square), metal films reduce visible translucence and can help reduce the performance of laser microphones exploiting objects in the building. The most conductive metals, silver and copper, are prone to atmospheric degradation causing darkening and increased resistivity. All thin metal films are very delicate and prone to scratches that significantly degrade their EM screening ability. A thin layer of indium doped tin oxide can slow the effects of atmospheric corrosion. Wire mesh/grids reduce transparency and translucency and are more cumbersome to install than thin conductive films. In conclusion, an environmentally robust highly conductive highly transparent and highly translucent material is not yet available.

Information sources, supporting extracts and quotations (Websites, Forums, Publications etc.)

The following sources are referred to in other parts of this document and provide a broad coverage of the topic, including links to industry and academia:

[1] www.pilkington.com/europe/uk+and+ireland/english/products/bp/bybenefit/decoration/textureglass/default.htm

[2] www.windowwallpaper.co.uk/

[3] www.lumar.com/en/Default.aspx

[4] www.vistamatic.com/uk/index.html

[5] electricglasswall.com/

[6] www.us.schott.com/architecture/english/products/smart-glass/magira-smart-view.html

[7] www.youtube.com/watch?v=RqWL2egaqYY

[8] solutions.3m.com/wps/portal/3M/en_US/Vikuiti1/BrandProducts/main/productliterature/prismfilms/

[9] solutions.3m.com/wps/portal/3M/en_US/SDP/Privacy_Filters/

[10] www.condmat.physics.manchester.ac.uk/research/graphene/

Standards and policy (Government and non-Government)

No standards are known that relate to visible privacy through windows, it is possible that a standard will arise as personal privacy has become a political issue. There are several standards relating to Electro Magnetic Inteference (EMI) screening and there are NATO specifications designed to prevent TEMPEST intrusions – NATO SDIP-29 and NATO SDIP-27 A/B/C.

QinetiQ comment

The available TEMPEST solutions tend to reflect EM energy. Tuneable optically transparent EM absorbing materials (Radar Absorbing Material (RAM)) could be used in buildings. Consideration is being given to techniques for reducing the effectiveness of laser microphones including passive sensor saturation/overload and noise inducement methods.

<p>Technology / Technique: Operating Systems Security</p>	<p>Relevant to SANS Critical Control: 3, 4</p>
<p>Description</p> <p>Operating Systems (OS) software provides the vital link between the computer hardware and end applications – managing a multitude of resources, and providing common interfaces for providers. Reliance on the integrity of the underlying operating system is an essential pre-requisite for a wide range of the 20 critical security controls identified by SANS, including ‘Application Software Security’ and ‘Controlled Use of Administrative Privileges’. The degree of trust that needs to be placed in the security and integrity of operating systems is fundamental in building robust computing platforms. This is equally applicable for the new computing form factors (such as tablets and smart phones), as it is for the traditional desktop environments.</p> <p>In the past, the concept of the secure operating system has involved bespoke development of locked-down hosts (for example, Trusted Solaris or Security Enhanced Linux). Now, many of the features previously seen on dedicated secure environments are being incorporated into mainstream operating system releases. Furthermore, the traditional ‘fat client’ OS is being joined in the market-place by much lighter client side environments, either fully provisioned via Terminal Services, or through a rudimentary client-OS, augmented by cloud-based applications.</p>	<div style="text-align: center;"> <h2>Operating Systems Security Roadmap</h2> </div> <div style="display: flex; justify-content: space-around; text-align: center;"> <div style="border: 1px solid black; padding: 5px; width: 30%;"> <p>2 – 5 years</p> <ul style="list-style-type: none"> • OS on mobile platforms, such as smart phones and tablets, will mature and attain greater breadth of capability; thus continuing the blur between the traditional PC and mobile environments. • A clear market will emerge for a dedicated “secure flavour” of a mobile OS. </div> <div style="border: 1px solid black; padding: 5px; width: 30%;"> <p>6 - 9 years</p> <ul style="list-style-type: none"> • The profusion of cloud-based technologies will dramatically reduce demand for ‘fat client’ operating systems in the commercial sector. • There will still be demand for traditional OS within government sectors, where the need to support legacy applications and the desire for host control over configurations persists. </div> <div style="border: 1px solid black; padding: 5px; width: 30%;"> <p>10+ years</p> <ul style="list-style-type: none"> • OS products from emerging markets will begin to strongly challenge those originating from the West, in the commercial market-place. </div> </div>
<p>Relevant applications</p> <p>An OS of some sort is needed wherever controlled interactions between computer hardware and end applications are required. This ranges from OS commercial usage, to bespoke control components for elements of SCADA.</p> <p>The level of security enforcing functionality required at the OS level is dependent on a myriad range of factors, including the complexity of the environment, the interfaces that need to be presented to external users or processes, the degree of trust that needs to be ascribed in the actions of the OS, and the level of security provided by supporting technical components, such as guards.</p>	

General issues and challenges

The trade-off between security and functionality is a vital consideration when assessing the robustness of OS implementations. The perception within industry is that tightly controlled OS platforms, such as Apple iOS and RIM Blackberry, are less susceptible to being seriously compromised through malware propagation, when compared with Microsoft Windows variants and open source releases. Part of this is due to the inherently tight integration between OS components (including drivers and interfaces) and the underlying hardware components on platforms such as the iPad – all aspects of which are under the complete control of the product manufacturer. This is even extended to the implementation of the concept of the ‘App Store’, which acts as a ‘gate-keeper’ undertaking thorough quality and security checks on all supported end application software, prior to release. In contrast, more general-purpose operating systems, such as Microsoft Windows and Google Android, support a much wider range of hardware form factors, component manufacturers and software developers, with corresponding greater market-share and cost benefits. However, this model has an impact on the tightness of the bindings between differing components, leaving more scope for malware exploitation. Microsoft is attempting to learn from previous implementation decisions, and many commentators saw Windows 7 as being a major step forwards. For the upcoming Windows 8, pundits suggest that features such as a built-in anti-virus solution, enhanced initial scans at boot time and additional checks on downloaded applications will all be included.

Most analysts agree that the future of operating systems in the commercial space will involve small end clients, with a much greater reliance on cloud-based technology to deliver the desired applications and services. In this context, the light-weight Google Chrome OS is seen as ‘the shape of things to come’. Interestingly, Google made the decision to only ship ‘Chromebooks’ with designated manufacturing partners (such as Samsung), instead of supporting as wide a range of hardware platforms as possible (which was the model used for Android). Google claim that Chrome OS will be the most secure consumer OS ever, relying heavily on the Trusted Platform Module to deliver trusted boot functionality and application sandboxing.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

The US National Security Agency (NSA) has developed and distributed configuration guidance for operating systems. These guides are currently being used throughout US government and by numerous entities as a security baseline for their systems.

Source 1: ‘Operating Systems’, NSA Website, www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml

The BBC reported that more than 26,000 people have downloaded an operating system which members of the Anonymous hacker group claim to have created. This purportedly comes outfitted with lots of website sniffing and security tools.

Source 2: ‘Anonymous operating system prompts security warnings’, BBC News. 15 March 2012. www.bbc.co.uk/news/technology-17381214

Google makes the distinction between the Android and Chrome OS development paths, implying that Chrome OS is a much more tailored, online offering:

1 Google Chrome OS is a new project, separate from Android. Android was designed from the beginning to work across a variety of devices... Google Chrome OS is being created for people who spend most of their time on the web, and is being designed to power computers ranging from small netbooks to full-size desktop systems.1

Source 3: ‘Introducing the Google Chrome OS’, The Official Google Blog, 7 July 2009.

Standards and policy (Government and non-Government)

CESG, the National Technical Authority for Information Assurance, provides policy relevant to operating systems security. Of particular relevance are the Government Assurance Pack (GAP) policy elements, produced for Windows XP, Vista and Windows 7. Here, CESG have worked closely with Microsoft to produce a 'best practice framework' for locking-down these operating systems, so that they can be used with confidence in 'high security environments'. Looking wider, a number of operating systems have been subjected to Common Criteria evaluation (including Solaris Trusted Extensions and Green Hills Integrity). However, the individual Targets of Evaluation (ToE) should always be closely scrutinised as to what aspects of the OS' functionality is in scope, as part of these assessments.

QinetiQ comment

Well-implemented OS security is vital in establishing confidence in the operation of computer systems. The traditional 'fat client' OS is being usurped in the market-place. For government, this will pose challenges when satisfying system requirements that do not conform to the wider demand for thin clients and cloud-based applications.

Technology / Technique: Protective Monitoring

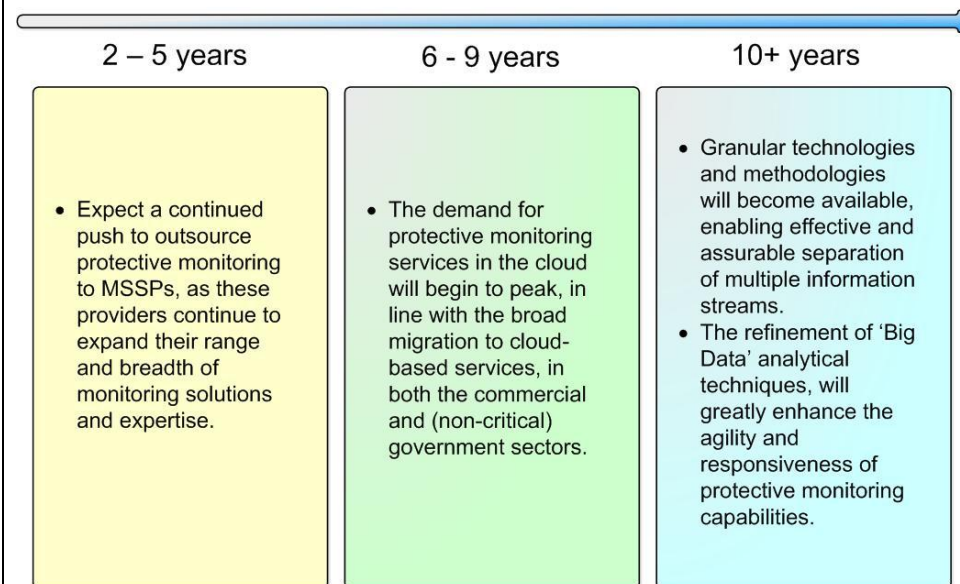
See also: Computer Network Defence

Relevant to SANS Critical Control: 14, 18

Description

Protective monitoring refers to applying the concepts of robust auditing, accounting and monitoring in a coherent way to deliver effective control and appropriate knowledge dissemination in relation to an organisation’s ICT assets and the information held by them. Effective monitoring will occur at multiple levels – ranging from monitoring the direct threats posed to the organisation (encapsulating network, system and business process aspects), to monitoring the architectural design utilised. Protective monitoring solutions have come a long way from an analyst manually trawling through lengthy event logs. There are now multitudes of enterprise-wide products that can refine multiple information sources, perform appropriate filtering and disseminate key findings to stakeholders in visually digestible formats. Such solutions are increasingly combining traditional signature-based tools with more agile anomaly-detection capabilities. The broad trend seems to be towards organisations outsourcing their entire protective monitoring capability to a Managed Security Service Provider (MSSP). MSSPs typically pool monitoring capability (including components such as loggers, knowledge bases and intrusion detection rule-sets) across a range of client systems, to provide 24-hour incident response services.

Protective Monitoring Roadmap



Relevant applications

Protective monitoring capabilities are essential for any scenario where the robustness, availability and performance of systems needs to be relied upon to deliver key organizational objectives. This covers a wide spectrum, ranging from commercial systems, to government applications and components of SCADA. With regard to outsourcing such capabilities, it is important to note that the consideration and decision making around 'risk management' issues will ultimately always need to reside with the direct customer, as they have the best understanding of the domain in which they operate, as well as their associated appetite for risk.

General issues and challenges

There is a risk that as protective monitoring capabilities become increasingly commoditized, such services are adopted for 'blind compliancy' purposes, rather than being implemented to deliver enhanced security responsiveness for the target environment. Defining a clear, unambiguous 'service description', detailing what activities are within scope as part of the capability, is a crucial step to undertake at the project's inception, regardless of whether services are out-sourced, or provided in-house. When considering the potential to enhance the responsiveness and intelligence exhibited by protective monitoring environments, there are difficult decisions around the extent to which information can be shared across systems in order to deliver over-arching improvement in analytical capability, whilst preserving data integrity (and client confidentiality, in the case of MSSPs). Accurate and auditable separation of the metadata gleaned to inform decision-making processes, from specific customer information, may assist in delivering an effective balance, in this context.

Going forwards, a key requirement within the commercial and government sectors will involve supporting protective monitoring of cloud-based infrastructures, augmenting traditional ICT deployed within customer sites. This will involve different approaches and tool-sets. It is clear that cloud-providers have inherent market advantages in offering rudimentary protective monitoring capabilities as a low-cost 1add-on1 to core cloud resource provisioning. However, the need for integrity and separation in the monitoring capability means that for many environments (especially those supporting the more sensitive deployments), it will remain appropriate to retain in depth protective monitoring expertise in-house, or engage a trusted MSSP.

Information sources, supporting extracts and quotations (Websites, Forums, Publications etc.)

Gartner's latest hype cycle for infrastructure services and outsourcing reports that:

The advent of 'big data' and the means to do something meaningful with it via pattern-based intelligent analytics combine with user demands for prevention-based services that go beyond remediation and drive tangible business value and on-going improvement.

Source 1: Addy R.: 'Hype Cycle for Infrastructure Services and Outsourcing, 2011', Gartner Research ID: G00215624. 29 July 2011.

Tier 3's white paper on e-Espionage describes the desire to move to 'Behavioural Anomaly Detection' (BAD) when monitoring networks, as opposed to more static, signature-based defences:

...many organisations with highly sensitive data choose technologies based on Behavioural Anomaly Detection (BAD) and Analysis for additional protection. These intelligent systems learn about the normal patterns of activity in the enterprise, detect those that are unusual, interpret them in context with other information, and alert IT security staff to investigate discernable threats... This is the key difference between rules-only security systems and those that add a layer of behavioural interpretation to the data they collect. They have the intelligence to detect, investigate and respond as it is happening, not afterwards when the damage is done.

Source 2: 'Woollacott P.: 'E-espionage: How Real is the Threat?', Tier-3, 2011.

The following source highlights issues concerning the physical location of data:

There are some indications that the follow-the-sun approach with which several providers operate is not always the best solution... Given the increasing need to store data in the country (or at least the region) of origin, clients are concerned that sensitive data is sent to countries with less protection. This can already be a problem regarding backup data centers in other regions, but it is an immediate issue when data is passed around on a daily basis.

Source 3: Casper C.: 'MarketScope for Managed Security Services in Europe', Gartner Research ID: G00219325, 24 October 2011.

Standards and policy (Government and non-Government)

CESG, the National Technical Authority for Information Assurance, provides clear policy on government protective monitoring, in the form of 'Good Practice Guide 13 (GPG13) – Protective Monitoring for HMG ICT Systems'. In particular, it defines 12 Protective Monitoring Controls (PMCs) (examples include 'Alerting Critical Events' and 'Accurate Time in Logs'), which should be applied against the target system. Protective monitoring capabilities also directly relate to a number of the crucial SANS Critical Security Controls, including 'Inventory of Authorized and Unauthorized Devices', 'Inventory of Authorized and Unauthorized Software' and 'Account Monitoring and Control'.

QinetiQ comment

Broad concerns over cyber security, combined with the requirement for increased enforcement (e.g. via policy elements) will ensure that robust protective monitoring capabilities will continue to be strongly in demand, in the decade ahead. The cost and service advantages gained through the outsourcing of such requirements to MSSPs is likely to result in continuing migration to third party provisioning, for all but the most sensitive of environments.

Technology / Technique: Quantum Cryptography

Description

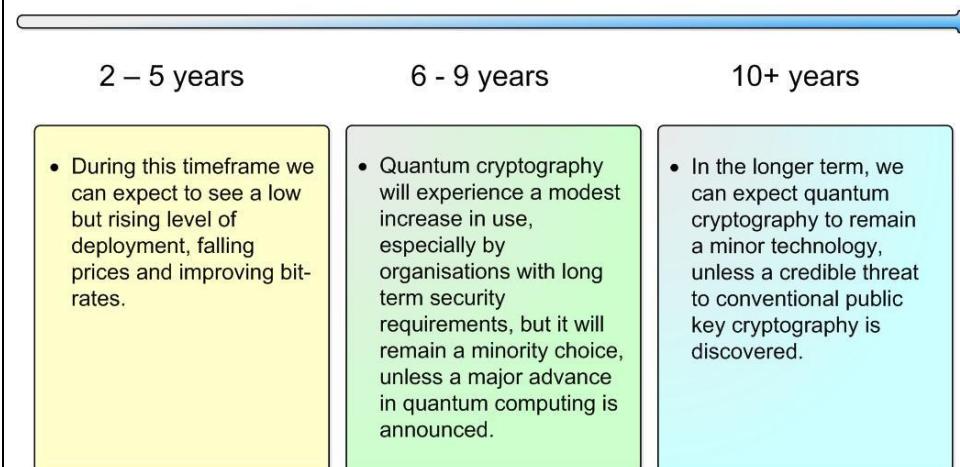
Quantum cryptography delivers encryption that is based on quantum physics principles and takes advantage of the particle-like nature of light. Each transmitted bit is encoded upon a single light particle (or photon).

Like traditional cryptography, quantum cryptography involves the exchange of coded messages that requires a key to decode them. In the case of quantum cryptography or quantum key distribution as it is sometimes referred to, quantum mechanics is involved in the generation of a shared secret key.

Any interference in the photons by a third party eavesdropping during transmission will disturb the transmission in a random and uncontrollable way and thus be detectable by the channel's users. The technology can be used in free space, but is more typically used over optical fibre.

There exists a proof of the security of an idealised implementation.

Quantum Cryptography Roadmap



Relevant applications

The technology provides an alternative to public key cryptography, which forms the basis of present day commercial and Government practice. If public key techniques became vulnerable, due to surprising advances in mathematics, or progress on quantum computing, there is a strong motivation to adopt quantum cryptography. Very cautious organisations have adopted it already, to mitigate against the risk of present day communications being decrypted in the future.

General issues and challenges

Quantum cryptography requires a direct optical connection between sender and receiver, so is limited to ranges of the order of 100 miles. The usable bit rate falls at longer ranges. It is possible to regenerate the signal by detecting the photons and resending at an intermediate point, but this must be a secure point – the physics precludes regeneration without ‘decoding’. Hacking attacks have been demonstrated on some commercial systems, exploiting various limitations and non-idealities (see Sources [1] and [2] below).

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

Quantum cryptography has undergone a transition from laboratory demonstrator to niche product, and is moving towards the technological and commercial mainstream. Recent research has shown that it is possible for attackers to eavesdrop on quantum key distribution.

Information Week highlight research presented in 'Nature Communications' where a team of researchers from Norway and Singapore had successfully conducted 'perfect eavesdropping' on a fully deployed quantum cryptography research system. They discovered they could use a laser to force the photon detectors in the quantum system to behave in a traditional manner, robbing the system of its ability to detect an intrusion. The research team hopes to build the 'perfect countermeasure' to this kind of attack and has shared its research with commercial quantum cryptography vendors.

The same article also provided insight of future developments to improve the current range limitations:

Commercial quantum cryptography key generation systems currently have a range of about 100 kilometres (62 miles), although the world record--achieved in the lab--is about 250 kilometres (155 miles). Currently, as distance increases, bit-rate decreases. The 'holy grail' in the future [sic] would be quantum repeaters, able to maintain bitrates over any distance.

Source 1: Schwartz M.J.: 'Eavesdropper steals Quantum Crypto Keys', InformationWeek, www.informationweek.com/news/security/vulnerabilities/231000312?pgno=1, 23 June 2011.

The following source also reports on the same research:

The peculiar properties of quantum mechanics allow two remote parties to communicate a private, secret key, which is protected from eavesdropping by the laws of physics. So-called quantum key distribution (QKD) implementations always rely on detectors to measure the relevant quantum property of single photons. Here we demonstrate experimentally that the detectors in two commercially available QKD systems can be fully remote-controlled using specially tailored bright illumination. This makes it possible to tracelessly acquire the full secret key; we propose an eavesdropping apparatus built from off-the-shelf components.

Source 2: Lydersen L. et al.: 'Hacking commercial quantum cryptography systems by tailored bright illumination' Nature Photonics 4, 686 - 689 (2010), www.nature.com/nphoton/journal/vaop/ncurrent/full/nphoton.2010.214.html, 29 August 2010.

The following source is a good overview of quantum cryptography.

Source 3: Mirza A.R., Petruccione F.: 'Quantum Technology: A next generation solution for secure communication' www.micssa.co.za/1.%20Papers%20-%20Day%201%2019%20July%202011/1-02B-3%20MICSSA%20Abdul%20Mirza%20paper.PDF 20 July 2011

Source 4: Trushechkin A.S., Volovich I.V.: 'On Standards and Specifications in Quantum Cryptography', adsabs.harvard.edu/abs/2005quant.ph..8035. 2005.

Source 5: Bernstein D.J. et al. (eds): 'Post-Quantum Cryptography', Springer, 2009, ISBN: 978-3-540-88701-0. pqcrypto.org/

Standards and policy (Government and non-Government)

None known yet. Discussion of what a standard would need to include may be found in source [4].

QinetiQ comment

Quantum Cryptography provides one of the possible responses to progress in quantum computing. Although commercially available, there is little sense in deploying it unless worried by the threat to conventional public key cryptography from quantum computing, or from unexpected breakthroughs in mathematics. Note that the non-ideal implementation of some commercial systems has led to successful hacking attacks against them, just as with conventional crypto equipment, details of implementation can undermine a valid algorithm. Before it can be trusted for the most critical applications, more experience will be needed to find and eliminate potential attack vectors in practical implementations. It is also important to note that there are other alternatives. Post-quantum cryptography is an active field of research, devoted to finding algorithms that are not susceptible to attack by quantum computers, see for example source [5].

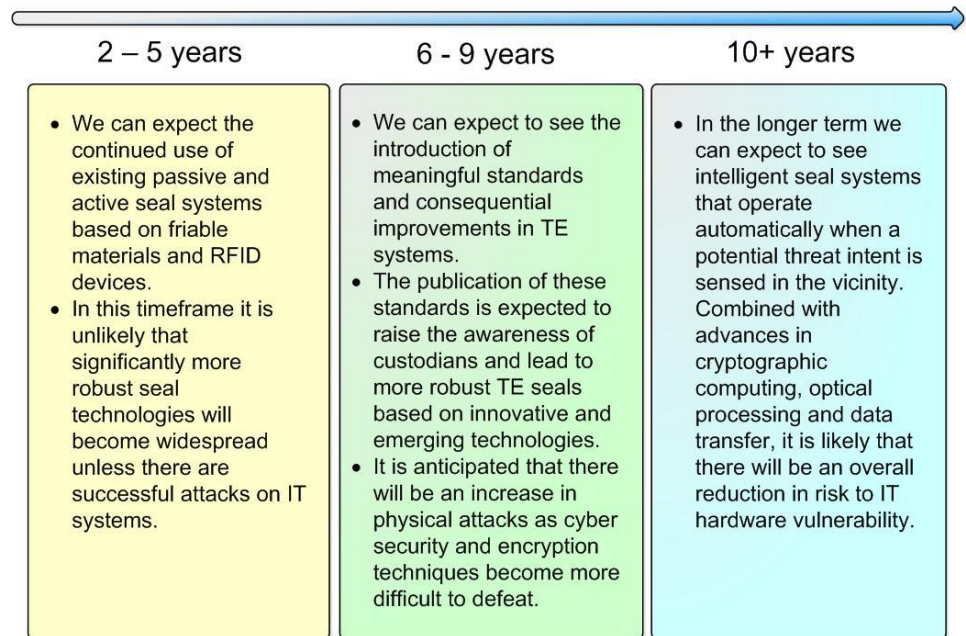
Technology / Technique: Tamper Evident and Proof Seals for IT Equipment

Relevant to SANS Critical Control: 1

Description

It is widely acknowledged that when challenged by a determined adversary that no equipment, including IT equipment is physically ‘tamper proof’ (see source 1 below). Even with multiple layers of protection such systems are vulnerable to physical attack of various forms; disassembly, micro-probing, drills, files, heating, solvents, etc. The best that can be achieved is an increase in the time to successfully complete the attack and/or to be aware that access to the protected system has been attempted or achieved through the use of tamper evident (TE) methods, principally seals. TE seals are tamper-indicating devices used to detect and report unauthorized access after the fact and help to deter attacks by ‘psychology’. TE seals do not need to physically resist the attack, usually they are intentionally physically weak systems incapable of providing physical protection. Despite their importance in protecting a wide range of systems, there is a shortage of meaningful standards, metrics, general understanding of fundamental principles of operation, theories and technology options for TE seals. The market is largely reliant on friable materials that are disfigured or destroyed when disturbed during an attack. The effectiveness of a TE seal is dependent on the use protocols for procurement, storage, record keeping, installation, inspection, removal, disposal, reporting, interpreting findings, and training.

Tamper Evident and Proof Seals Roadmap



Relevant applications

Seals are widely used to detect and record unauthorized access to equipment be it malevolent or unintentional/accidental. Unlike intrusion or burglar alarms, seals report unauthorized entry after the attack. Seals must be inspected regularly to determine if unauthorized access has taken place. Unlike locks, they do not prevent access but can perhaps discourage it. Once unauthorised access has been detected, the custodian has to investigate the breach and assess if the protected system has been compromised and then take the appropriate reporting and remedial steps.

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 - 5 years: We anticipate continued use of existing passive and active seal systems based on friable materials and RFID devices. The lack of meaningful standards and novel or emerging technology options mean that the current technologies are well understood by potential adversaries and can be easily defeated. The Vulnerability Assessment Team (VAT) at Argonne National Laboratory is expected to expand its work on seal assessment and metrics and to continue to lead on developing theory innovation and proposing standards. In this timeframe it is unlikely that significantly more robust seal technologies will become widespread unless there are successful attacks on IT systems.

Within 6 - 9 years: We can expect to see the introduction of meaningful standards and consequential improvements in TE systems. Instigated by the VAT team at Argonne, the publication of the standards are expected to raise awareness of custodians and to lead to more robust TE seals based on innovative and emerging technologies (these will include commercially available SMART materials whose exploitation is supported by academic involvement). We anticipate that there will be an increase in physical attacks as cyber security and encryption techniques become more difficult to defeat.

10+ years: In the longer term we can expect to see intelligent seal systems that operate automatically when a potential threat intent is sensed in the vicinity. Combined with advances in cryptographic computing, optical processing and data transfer, it is likely that there will be an overall reduction in risk to IT hardware vulnerability.

General issues and challenges

Once physical access to an IT system is achieved, it will only take a skilled operator a few moments more to bypass any TE seals at which point the system is vulnerable to undetected attacks. The attack could give the assailant access to information contained in or monitored by the systems and, crucially, relinquishing control of equipment and processes governed by the IT system. The high level of vulnerability of IT systems protected by current TE seals is clear from the statistics of recent study of 244 different tamper indicating seals performed at Argonne Laboratories. The seal attacks were undertaken by one individual, well-practised in the attack, using only readily available low-tech tools such as a hairdryer and household materials such as methylated spirits; 55 % were bypassed in <1 minute, 95 % in <5 minutes and 99 % in <10 minutes.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

Source 1: Johnston R.G., Warner J.S.: 'Magical Seals, Secure Voting Machines, and Other Fantasies', Election Verification Network Meeting, Chicago, March 24-26, 2011.

The VAT at Argonne National laboratories conducts multi-disciplinary research and development on physical security devices, systems and programs. *1The VAT's expertise and capabilities align extremely well with Argonne's work in national and homeland security1*, said Alfred Sattelberger, Associate Director of Physical Sciences and Applied Science and Technology at Argonne.

Arrogance maxim: The ease of defeating a security device or system is proportional to how confident/arrogant the designer, manufacturer, or user is about it, and to how often they use words like 'impossible' or 'tamper-proof', Roger Johnston. Read more security maxims at: www.ne.anl.gov/capabilities/vat/seals/maxims.shtml

Standards and policy (Government and non-Government)

No formal standards or policy relating to TE seals for IT equipment has been identified. International Standard 17712, Mechanical seals (ISO 17712) addresses all types of security seals usable on maritime containers and was published in September 2010. Although not directly targeted at TE seals for IT equipment this is the most relevant agreed standard found and can be interpreted to a limited extent for IT equipment. There is greater regulation of TE packaging for foodstuffs, pharmaceuticals and criminal evidence.

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a voluntary supply chain security program led by U.S. Customs and Border Protection (CBP) and focused on improving the security of private companies' supply chains with respect to terrorism, this forum could become a focus for developing tamper detection IT systems.

There is a trade body, The International Seal Manufacturer's Association (www.ismasecurity.com), and there are number of anti-tamper suppliers listed on their website. Reviewing these, the widest range of sector knowledge and technologies appears to lie with Tynden Brooks: www.tyndenbrooks.com/.

QinetiQ comment

In common with document security measures, TE seals would benefit from an injection of new technologies from the anti-counterfeit sector where it is widely agreed that even sophisticated anti counterfeit technologies have an operational lifetime of around six months. To counter this fast moving and adaptive threat, a large number of novel technologies are under continuous review and development. Many of these technologies could translate into improved TE seals.

Technology / Technique: The Future of Smart Meters for Home and Industry

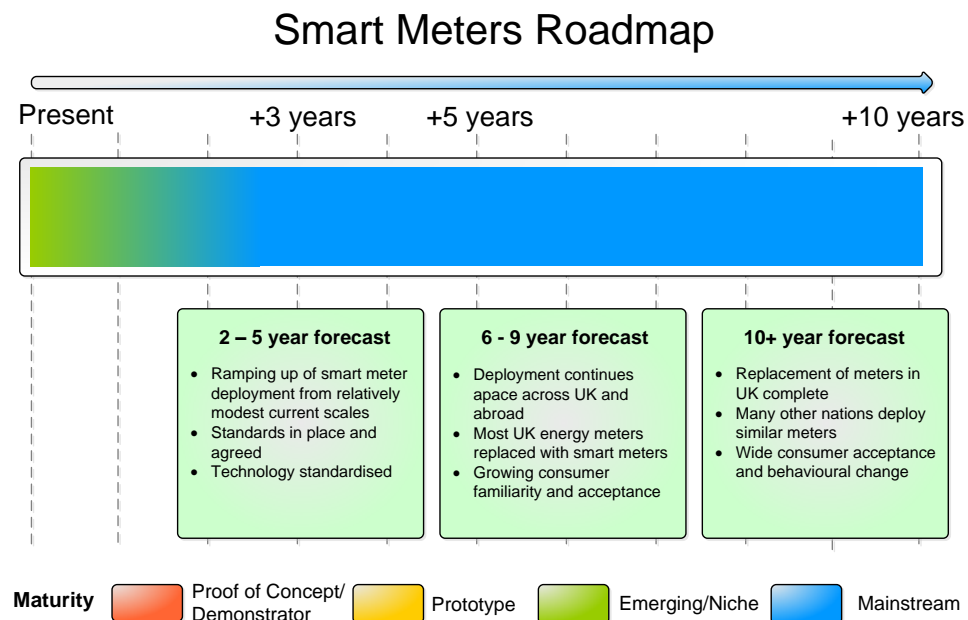
Description

The term smart meters is applied to devices that record the consumption of energy (e.g. electricity and gas), and provide those records regularly and frequently to suppliers and, in some cases, directly to consumers. They rely not only upon the means to measure consumption of energy, but also upon a communications network to deliver consumption information both to the supplier and to the consumer. To do this, it is likely that smart meters will provide elements of, or connect to, a Home Area Network (HAN). The HAN will connect energy-consuming devices to the meter and onwards to the supplier via a backhaul network likely using different technology to the HAN.

The technology is available now and is being widely promoted globally by both the energy industry and governments alike. Some smart meters only provide the consumption information to the suppliers, whilst others have a display that can provide instantaneous feedback to consumers on energy usage.

Governments see smart meters as key drivers in reducing energy demand (or the growth in energy demand) and hence delivering significant reductions in carbon output. Suppliers see opportunities for smoothing out peaks in energy demand, and more innovative ways of charging energy consumers. Customers will see opportunities to reduce their bills through greater awareness of how they consume energy. Recently, a number of governments throughout the world, including the UK, have accelerated deployment of smart meters.

The more advanced form of smart meters, including the communications network and energy usage data repository is called an Advanced Metering Infrastructure (AMI).



Relevant applications

Smart meters are part of the energy supply and billing system. They are installed in customer premises to record detailed information regarding energy consumption.

They enable a number of innovations in the consumption and billing of energy, including:

- Driving behavioural change of energy consumers through providing timely feedback on energy usage and charges. This can be enhanced through smart meters communicating with 'smart appliances' that are able to respond to pricing signals from suppliers;
- Reducing or eliminating the need to manually read meters;
- Supporting time of day billing of consumers, allowing suppliers' energy tariffs to reflect consumption patterns during the day, e.g. charging more for energy during peak consumption hours;
- Allowing more flexible energy consumption load balancing to occur through either direct means (suppliers switching off devices in the consumer's premises) or indirect means (behavioural changes in consumption from feedback).

Smart meters may also have application in the delivery and billing of other utilities, e.g. water.

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 - 5 years: Many businesses seek to use smart meters to reduce their energy bills. There will be a ramping up deployment of smart meters for domestic consumers over this time. This will be accompanied by a widespread awareness campaign by both energy companies and government to ensure consumers are aware of the benefits.

Within 6 - 9 years: Deployment of smart meters to UK businesses and domestic customers will continue with near complete roll-out by the end of the decade driven in part by Government policy. Familiarisation with real time control over energy usage will increase among domestic consumers with gradual acceptance of the technology.

10+ years: Deployment of smart meters by UK suppliers will be largely complete. A wide selection of appliances will be available that can communicate with smart meters allowing a detailed and real-time understanding of energy usage to be developed and automatic response to advantageous energy tariffs.

General issues and challenges

Spectrum: Wireless communications networks are expected to play a major role in the deployment of smart meters, both in connecting smart appliances to the meter, and in connecting the meter to the supplier. Availability of radio frequency spectrum to support this communication is a key issue that regulatory bodies and industry worldwide are currently addressing. A number of frequency bands are being considered. Key considerations include:

- Harmonisation (use of common frequencies across different countries - on which the UK is taking a lead by promoting economies of scale for vendors).
- Interference (in-channel if a shared band or adjacent channel for exclusive bands).
- Propagation (through building materials, generally favouring lower frequencies),

- Robustness and resilience (estimating the effect on HANs of future saturation of shared bands, and deployment of HANs in dense urban environments).

Early studies have shown favourable characteristics in the Digital Enhanced Cordless Telecommunications (DECT) wireless phone band though this is an exclusive band and HAN technology would need to be compatible with the DECT standard.

Security: Concerns over the security of an AMI have been raised in recent years. In particular, the meter itself has been identified as the weak link in the chain. In addition, given the global demand for smart meters, it is likely that the devices themselves will be manufactured abroad with little control exerted by the UK over the software residing within the device. If these devices attach to home automation networks and, by extension potentially the internet, disruption of supply by an outside agent is a risk that should be considered.

Cost of roll-out: The cost of deploying smart meters across the UK has been put at around £12bn and will involve the replacement of 53 million gas and electricity meters.

Energy consumer acceptance: Businesses and domestic energy customers alike will likely embrace smart meters so long as there is a tangible benefit in terms of reduced energy costs. However there have been recent cases of hidden service charges for smart meters and rental fees that have surprised customers. In addition, there is evidence, particularly in the US, that time-of-day sensitive tariffs actually increasing customers' bills substantially. There will also be issues with how the suppliers handle and use the personal data provided by smart meters, e.g. information on consumers' patterns of life implied through energy usage. Sustained reports of these issues could damage consumer confidence in the technology.

Information sources, Supporting extracts and quotations (websites, forums, publications etc.)

The analyst company Gartner charts the developments of 'smart appliances' in the following hype cycle.

Source 1: Escherich M: 'Hype Cycle of Consumer Devices, 2011', Gartner Research ID: G00214790. 2nd August 2011.

IBM predict that, by 2015, 200 million smart energy meters will be deployed worldwide.

Source 2: IBM: 'Smarter Computing The Next Era of IT1, April 2011.

The analyst company Pike Research has recently investigated the security of smart meters and AMI. In their report, Pike Research suggest that governments and industry have not considered all the security issues inherent in the deployment and use of smart meters. In the report, Pike researchers state: *'It would be naïve to think that smart meters will not be successfully attacked. They will be. In fact, smart meters represent a worst-case scenario in terms of security: the devices lack sufficient power to execute strong security software; they are placed in physically non-secure locations; and they are installed in volumes large enough that one or two may not be missed'*.

Source 3: Pike Research: 'Smart Meter Security', August 2010.

The UK Department for Climate and Energy Change (DECC) are leading the UK Government smart metering roll-out under the Smart Metering Implementation Programme (SMIP). Within this programme, the Smart Metering Design Group (SMDG) is providing the technical advice through a number of Working Groups. A large number of outputs are now available. For instance, the SMHAN working group has performed an initial assessment of wireless frequency challenges facing the HAN component of Smart Metering as reported in this forecast.

Source 4: Astutim: 'HAN Working Group, SMHAN Radio Spectrum Study, Phase 1 Draft Working Paper', May 2011.

Standards and policy (Government and non-Government)

The UK Government, like many governments around the world, has embraced smart meters as part of their drive to curb the growth in energy demand and reduce emissions of greenhouse gases. In late 2009, the then government announced the intent for all UK households and many businesses to have the technology by 2020. This has subsequently been endorsed by the UK Government, with some indications that the roll-out may be accelerated.

An array of standards will underpin smart meters allowing multiple manufacturers to provide meters across UK homes, compatible with the range of energy suppliers. However, recent news reports* citing problems found by energy customers with smart meters when switching suppliers have suggested that further standardisation activities are required. There have been a number of announcements over the past two years by standards bodies in the UK (e.g. the British Standards Institution (BSI)) and more broadly across Europe, with the intent of ensuring common standards for all smart meters. In addition, manufacturers have also joined forces with the aim of developing standards.

* The Telegraph: 'Smart meter users face hidden charges', 31st October 2011.

QinetiQ comment

The deployment of smart meters continues apace across the UK and in many other countries. QinetiQ agree that the adoption of smart meters is likely to change the behaviour of energy consumers and lead to at least a reduction in the growth of energy demand over the coming years. For this to occur, it is likely that a government sponsored awareness campaign will be required. However, QinetiQ are concerned that there has not been a full assessment of the security issues inherent in smart meters and AMI, and that suppliers may be deploying smart meters with vulnerabilities.

<p>Technology / Technique: Social Analytics</p>	<p>See also: Future Social Networking Tools</p>
<p>Description</p> <p>Social analytics is the analysis of social interactions and relationships between people, topics and ideas. With the massive boom in popularity of social media for both social interaction and business transactions there is a big move to exploit this data source for business and intelligence advantage.</p> <p>Social analytics is a term that encompasses a portfolio of specialized analysis techniques, such as social filtering, social network analysis, text analysis (including natural language processing and sentiment analysis), predictive analysis and complex event analysis that has the potential to reveal insight into this rich data source. Analysis can be performed at the group level to identify general trends and predictions or at a more fine-grained level to analyse and monitor individual behaviours.</p>	<div style="text-align: center;"> <h2>Social Analytics Roadmap</h2> <p>The diagram features a horizontal timeline arrow pointing right, divided into three segments: '2 - 5 years' (yellow), '6 - 9 years' (green), and '10+ years' (cyan). Below each segment is a corresponding colored box with a bulleted list of expected developments.</p> </div>
<p>Relevant applications</p> <p>The primary use of Social Analytics is by commercial entities to perform Customer Relationship Management (CRM), Marketing and Brand Protection. Anonymous users, vast amounts of very persistent content, the emergence of more powerful and real-time search engines and algorithms has motivated the use of social analytics to underpin tools and services to perform Enterprise internet Reputation Management. Commercial and Government Organisations have been quick to recognise the wealth of intelligence contained in this vast source that has the potential to provide customer feedback on new products and monitor and forecast trends such as flu outbreaks and political uprisings; all in real-time. Social analytics are used to analyse the content and interactions of groups and individuals so that behaviours can be identified and sentiment extracted to make predictions about future actions.</p>	

General issues and challenges

The primary challenge for social analytics is the '*Volume Velocity and Variety*' of the data to be analysed: Social media applications generate unprecedented amounts of data that require a Big Data infrastructure and the security implications of managing the huge data sets. In addition, traditional analytical techniques need to be adapted or completely redesigned to scale up to the required volume and/or be capable of analysing the vast data streams in real time. This is further compounded by the requirement for the analytic techniques to be able to deal with varying levels of structure from the highly structured networks of interactions to the completely unstructured messages written in informal languages (e.g. tweets). The main bottleneck in unlocking the potential will be having the skills to applying the social analytics techniques within this framework.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

The social data revolution is generating unprecedented amounts of data: *1In 2009, more data will be generated by individuals than in the entire history of mankind through 2008. Information overload is more serious than ever.1*

Source 1: Weigend A.: 'The Social Data Revolution', Harvard Business Review. blogs.hbr.org/now-new-next/2009/05/the-social-data-revolution.html. Retrieved July 15, 2009.

Gartner covers social analytics as an emerging technology in the following hype cycle.

Source 2: Fenn J., LeHong H.: 'Hype Cycle for Emerging Technologies, 2011', Gartner Research ID: G00215650, 28 July 2011.

There are conflicting views as to whether Social Media is starting to replace email as the primary tool for employee communication and collaboration:

Source 3: Social media www.microsoft.com/business/en-gb/Content/pages/news.aspx?cbcid=2012, retrieved December 16th 2011.

Source 4: www.v3.co.uk/v3-uk/news/1992180/social-networking-replacing-email-enterprises, retrieved December 16th 2011.

Source 5: www.bbc.co.uk/news/technology-16055310, retrieved December 16th 2011.

Source 6: www.cbronline.com/blogs/technology/atos-plan-to-abandon-email-could-be-a-disaster-13122011 retrieved December 16th 2011.

There are privacy worries as analytics providing face recognition are being developed and deployed by social media sites: *Facial recognition technology will ultimately culminate in the ability to search for people using just a picture. And that will be the end of privacy as we know it--imagine, a world in which someone can simply take a photo of you on the street, in a crowd, or with a telephoto lens, and discover everything about you on the internet.*

Source 7: J. Purewal, PC World magazine in Gayle D.: 'Facebook now knows what you look like as it rolls out face recognition by stealth'. June 2011.

Social Analytics practitioners recognise the need for global standards.

Source 8: 'Industry needs a wakeup call, says Big Ask Speaker', amecorg.com/2011/11/industry-needs-a-wakeup-call-says-big-ask-speaker/ retrieved December 18th 2011.

Standards and policy (Government and non-Government)

At the current time (December 2011) the author has no knowledge of any standards and policies related to Social Analytics; although practitioners recognise a need for standardisation and guidance. In February 2010 the Web Analytics Association (WAA) released a draft of its suggested standard definitions for social media measurement for public comment, however a final version has not appeared in the public domain.

At the AMEC (International Association for the measurement and evaluation of communication) conference known as 'The Big Ask' that was held in November 2011 '*Speakers were outspoken in their views that the AMEC and Coalition initiative to develop global social media measurement standards was overdue*'. AMEC has made the development of global social media measurement standards by 2020 a high priority (see source 8 above).

QinetiQ comment

There is a lot of interest and hype associated with social analytics and its related technologies (e.g. Big Data). Organisations need to cut through the hype and get a real understanding of what can be achieved, with the current portfolio of social analytic technologies and where the gaps are. The International AAAI Conference on Weblogs and Social Media (ICWSM) provides a forum for Social Analytics practitioners to increase their understanding of social media and its analysis. It also provides example datasets that can be used by organisations to develop their technology. There is currently a move towards social media replacing emails as the digital communication medium of choice (e.g. Atos email Ban, see sources 3 to 6). If the hype is to be believed, there is a big opportunity to harvest predictive actionable intelligence from social media data for commercial businesses, government agencies and rogue organisations.

Technology / Technique: Supply Chain Integrity

Description

A supply chain is a dynamic entity that includes all parties involved in ensuring the request from a customer for a product or service is fulfilled. This will almost always involve considerably more parties than a manufacturer and supplier, such as those responsible for storage, distribution and transportation.

Supply chain integrity, as the term suggests, is a means to ensure that the supply chain performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation (this definition was derived from that offered in source [2] below). It is intended to prevent activities such as tampering, 'grey market' distribution, counterfeiting and fraud.

Supply chain integrity should not only be applied to the physical elements of a supply chain (such as the containers, vehicles etc.) but also to the electronic and Information Communication Technology (ICT) elements such as the networks, tracking devices and even the software code.

Current supply chain systems exploit a range of state-of-the-art technology solutions which include GPS, A-GPS, cellular and RF technology-enabled tracking devices (RFID), along with Web-based user interfaces and visualisation tools to track, monitor and recover cargo.

Relevant applications

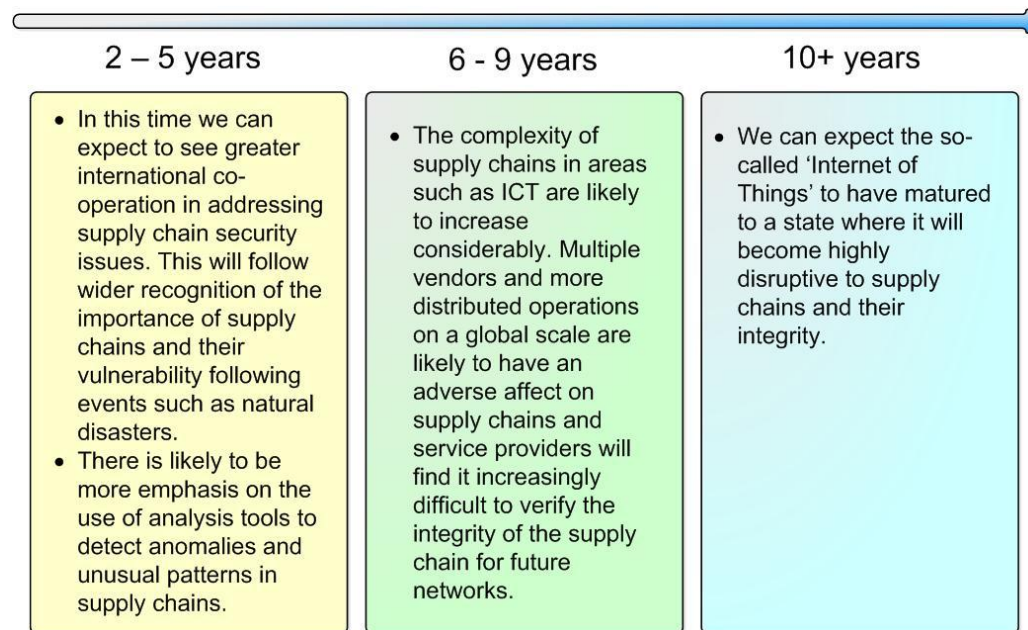
Supply chain integrity applies to all supply chains across business, governments and national infrastructure.

General issues and Challenges

The issues and challenges of ensuring supply chain integrity can broadly be split into two groups:

1. Those pertaining to the integrity of the supply chain systems themselves.

Supply Chain Integrity Roadmap



*Note: The following source contributed to the derivation of the forecast for the 6 to 9 year period: Resetko A.: 'IEEE CQR 2007 Software supply chain integrity and security', May 2007
committees.comsoc.org/cqr/CQR2007%20Presentations/Day%203/Session%2011/Aleksei%20Resetko.ppt#803,1,IEEE CQR 2007 Supply chain integrity and security.*

2. Those relating to the nature of the industry using the supply chain.

Amongst the most complex supply chains are those supporting the ICT industry. As this industry has become increasingly globalised and reliant on distributed sources for products, components and software development, it is one of the most vulnerable. Furthermore, it is one of the most critical as most businesses, governments and elements of essential services are heavily reliant on ICT systems.

The general issues and challenges are highlighted in a paper entitled '*Telecommunications Supply Chain Integrity - Mitigating the Supply Chain Security Risks in National Public Telecommunications Infrastructures*', to quote:

A new and growing security challenge is the mitigation of commercial and national security risks associated with the public telecommunications infrastructure. That infrastructure is increasingly composed of components and systems that are designed, developed, and manufactured by foreign firms, or home country companies relying on downstream suppliers integrating foreign components into their products. A prominent example is the substantial amount of network equipment and software for next generation networks (NGNs) being produced by non-traditional suppliers based in foreign countries that are not considered close allies. As service providers seek to reduce their operating costs, the testing, support, maintenance, and repair of NGN equipment may also be provided by these foreign-based suppliers.

Source: Kimmins J.: 'Telecommunications Supply Chain Integrity', IEEE Conference paper, Cyber Security Summit (WCS) 2011.

These challenges are particularly affecting the software development part of the ICT industry following the increased distribution of software development activities. To mitigate this problem SAFECODE (www.safecode.org/) has developed the first industry-driven framework for analysing and describing the efforts of software suppliers to mitigate the risk of software being compromised during its sourcing, development or distribution.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

Integrity is an EU-funded project that is intending to improve the reliability and predictability of door-to-door container chains. The quote below outlines their main goal:

[The] kernel of the project is the development of the so-called Shared Intermodal Container Information System (SICIS) allowing authorised companies and authorities to access planning and status information of selected transports. Proactive planning following the Supply Chain Event Management (SCEM) approach allows to forecast problems well before they might occur. Matching logistics data with security information, e.g. from electronic seals, container security devices, and scanning equipment together with the integration of the Authorised Economic Operator (AEO) approach allow to satisfy both the logistics industry and Customs Authorities fulfilling their duties thus creating win-win situations.

Source 1: Integrity Website www.integrity-supplychain.eu/

A good overview of Supply Chain Integrity was written as part of the EU-funded Building Radio frequency IDentification for the Global Environment (BRIDGE) project whose aim was to research, develop and implement tools to enable the deployment of EPCglobal applications in Europe (EPCglobal is an organisation set up to achieve worldwide adoption and standardisation of Electronic Product Code (EPC) technology).

Source 2: Soppera A. et al.: 'Supply Chain Integrity (D4.6.1)', [www.bridge-project.eu/.../BRIDGE_WP04_Supply_Chain_Integrity\[1\].pdf](http://www.bridge-project.eu/.../BRIDGE_WP04_Supply_Chain_Integrity[1].pdf) , December 2007.

The UK Government's Department for Business Innovation and Skills recently produced a report entitled 'Infrastructure supply chains: barriers and opportunities'. This study covering five infrastructure sectors: transport, energy, digital communications, water and waste. The remit was to identify issues affecting the delivery of UK infrastructure, including barriers to innovation and the efficient operation of supply chains, and identify opportunities to remove those barriers and learn from good practice.

Source 3: BIS Research Report - 'Infrastructure supply chains: barriers and opportunities', www.bis.gov.uk/assets/biscore/corporate/docs/i/11-1058-infrastructure-supply-chains-barriers-opportunities, August 2011.

A recent news article highlighted the problem of supply chain integrity for the pharmaceutical industry. To quote:

The US Pharmacopeial Convention (USP) is proposing a set of best practices to help ensure that drugs can be traced back to their manufacturer, are not adulterated or counterfeited and arrive at their intended destination with their quality intact.

The USP's guidance and best practice is primarily intended to be in support of the smaller pharmaceutical manufacturers who do not have the appropriate security approaches in place like their larger counterparts.

Source 4: Taylor L.: 'US proposals for pharma supply chain integrity', World News, www.pharmatimes.com/Article/12-0106/US_proposals_for_pharma_supply_chain_integrity.aspx, 6 January 2012.

On January 25 2012, the White House released Obama's National Strategy for Global Supply Chain Security. The document outlines the current issues in the supply chain, and prompts the international community and industry stakeholders to work together for the next six months to offer views and recommendations to Congress.

It shouldn't take international industry experts to come up with the solution we've known all along will sure up the supply chain's integrity – label compliance. If more manufacturers demand that their supplies have consistent, unadulterated label tracking and traceability, bootleggers and other industry threats get weeded out of the system.

Source 5: 'Obama calls for supply chain security', Enterprise labelling, enterpriselabeling.com/2012/01/26/obama-calls-for-supply-chain-security/, 26 January 2012.

According to LoJack, a firm that specialises in providing supply chain integrity:

Broken links in a supply chain are one of the top three threats to business operations. It's estimated that \$10 billion to \$30 billion in merchandise is stolen from cargo ships, ports, highways, railroads and freight yards each year.

LoJack's solutions are typical of the state-of-the-art.

Source 6: LoJack website www.lojacksci.com/total-solution/index.aspx

US National Institute of Standards and Technology (NIST) document referring to the mitigation of supply chain risks, see standards and policy below.

Source 7: Swanson N.: 'Draft NISTIR 7622 Piloting Supply Chain Risk Management for Federal Information Systems' csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7622, June 2010.

Standards and policy (Government and non-Government)

ISO 28000:2007 – The '*Specification for security management systems for the supply chain*' is the International Organisation for Standardisation's standard on requirements of a security management system and is of particular relevance when dealing with security assurance in the supply chain.

The US National Institute of Standards and Technology (NIST) provides best practice information with regard to mitigating supply chain risk. In particular the publication '*Draft NISTIR 7622 Piloting Supply Chain Risk Management for Federal Information Systems*' (see Source 7 above) covers this area in detail and builds on NIST Special Publications like NIST SP 800-53, '*Recommended Security Controls for Federal Information System*' and then expanded upon to include supply chain-specific implications. The UK Government's Department for Business Innovation and Skills website lists policies and has a 'supply chain group' present with the automotive business sector.

QinetiQ comment

QinetiQ notes that supply chain integrity has received considerable attention from both business and governments during the last year. President Obama's National Strategy for Global Supply Chain Security is the latest example (see Source 5 above), calling on the Departments of State and Homeland Security to devise a plan that will protect the U.S. economy from supply chain disruptions in the future.

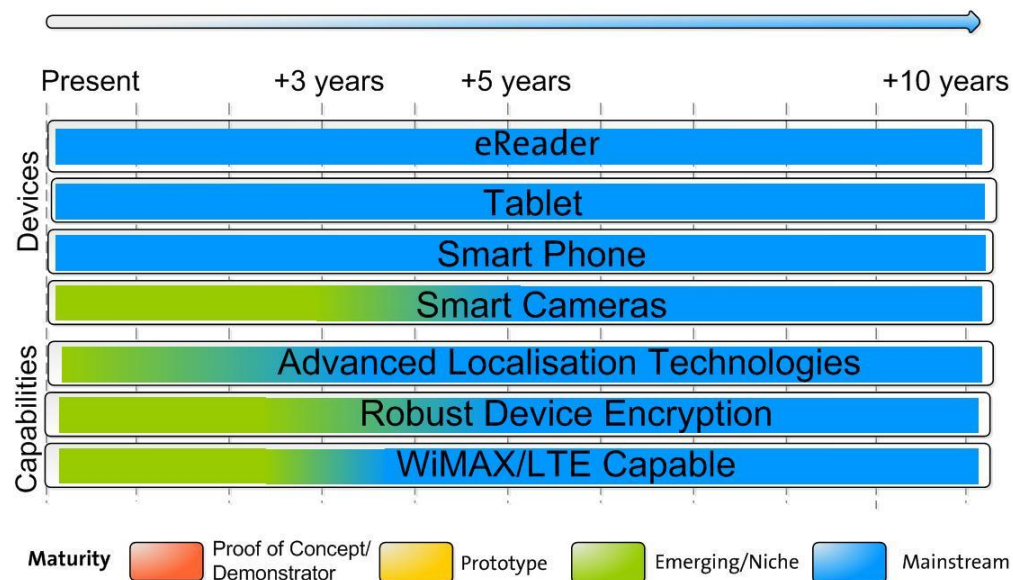
Technology / Technique: Ultra-Mobile Computing Devices (including Smart Cameras)

Relevant to SANS Critical Control: 1

Description

Ultra-Mobile Devices (hereafter UMDs) are computing devices that are designed to be low cost, low power, provide connectivity support for communication bearers (such as 3G, Wifi and Bluetooth) and deliver long battery life. UMDs include: ultrabooks, eReaders, tablet/slates, smartphones, personal digital assistants (PDAs) and mobile internet devices (MIDs). These devices are generally powered by either x86 Intel or ARM-based processors, and run either a Windows, Linux, Apple's iOS or a Symbian based operating system. ARM based mobile devices only support Linux-based operating systems such as Google's Android and the Symbian operating system, although recent demonstrations have shown variants of Microsoft Windows running on the processors. ARM processors are currently the most popular choice for devices which require 'always-on' capability such as smartphones (e.g. the Apple iPhone) and Tablets, and are geared to consuming content (e.g. browsing the internet and reading email). Intel x86 processors are on the other hand best suited to larger, ultra-portable laptop style devices such as the emerging ultrabooks which provide better performance than ARM processors, but at the cost of shorter battery life.

Ultra-mobile Computing Devices Roadmap



Smart Cameras are imaging devices that in addition to containing a standard digital camera's image capture circuitry; also have the capability to perform on-board image processing to enable specific information to be extracted from the images captured. For example in a factory, smart cameras could be used to perform defect detection and provide alerts directly over an Ethernet or Wifi interface to a control system. Today, consumer digital cameras are getting smarter and many now include face detection to aid in getting that perfect picture. There are also a growing number of surveillance systems, which can detect people in very crowded scenes, although generally this sort of intense processing is not currently carried out on the device itself.

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 - 5 years: Processor technology developed by manufacturers such as ARM and Intel will continue to advance and provide better battery life and performance. Intel will try to gain more market share in the smart phone and tablet market, but will struggle against ARM, the existing market leader. Linux based operating systems such as Android will capitalise on this due to their superior power-management support. Apple's iOS and Android will dominate, with Microsoft attempting to increase

its presence with Windows Phone OS. Symbian will die out. UMD feature set will continue to expand, to include capabilities such as greater integration with 'cloud' services, pico-projectors and true context aware digital assistants (e.g. Apple's Siri).

Within 6 - 9 years: Standalone 'Smart Cameras' which can perform person detection and tracking will become feasible allowing for the development of flexible surveillance systems which can be quickly built and dismantled. UMDs will continue to provide better performance, battery life and security features. Location-based services will become increasingly popular leading to the development of more accurate localisation technologies possibly using visual cues from the surrounding environment. Seamless integration of the UMD with devices in the immediate surroundings will allow content originating from the UMD to be played or displayed on other devices, e.g. HD televisions and other computers/screens.

10+ years: UMDs which deliver their displays directly to the eye may emerge in this timeframe. Novel technologies which detect gestures made using the hand and possibly basic brain-computer interface technology (BCI) may become integrated into mobile devices.

General issues and challenges

Battery Life: The average battery life in mobile devices continues to improve due to the development of more efficient processors, higher capacity batteries and better power management support within mobile operating systems. However, as devices begin to provide more communications options such as the Long-term Evolution (LTE), and use larger, brighter and higher resolution screens, it is going to be a constant battle to maintain this.

Security: Mobile device security is a big concern for corporate users in particular with employees more likely to lose a device such as a smartphone, which may contain sensitive information. To mitigate this risk many devices such as the Apple iPhone and Blackberry now encrypt data and provide a 'remote wipe' facility to enable lost or stolen devices to no longer function. However, even given these capabilities there is still concern over the security of such devices.

Communications/Infrastructure: A key driver in the growth of the UMD market has been the development of high-speed wireless communications technologies such as 3G and Wifi. Many mobile devices now rely upon 'cloud-based' services and 'always-on' connectivity to deliver their capabilities to users. This is somewhat of a risk, and needs to be carefully considered when looking to deploy UMDs.

User Interface Design: As devices have reduced in size it has become increasingly important that more novel user interfaces and supporting technologies such as multi-touch and gesture recognition have been developed to enable users to use devices easily. This will continue to be a challenge for the foreseeable future until visual displays can be delivered directly to the eye in a cost effective manner using glasses or retinal displays for example.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

The tablet market is becoming very competitive with a number of vendors attempting to challenge Apple's dominance with its iPad. This is reflected in a recent CNET article:

Source: CNET (2011), 'Kindle Fire cutting into consumer appetite for iPad—survey', news.cnet.com/8301-13924_3-57321423-64/kindle-fire-cutting-into-consumer-appetite-for-ipad-survey/

Ultrabooks are predicted to outpace tablet computers growing three times as fast as tablets in the next few years, according to Juniper Research. Still, the market

research firm expects tablets to win the battle of unit volume, predicting that 253 million tablets will be shipped in 2016, compared with 178 million.

Source: Walsh M.: 'Ultrabooks growth to outpace tablets', *Online Media Daily*, www.mediapost.com/publications/article/166429/ultrabooks-growth-to-outpace-tablets.html, 25 January 2012.

Sony has released three back-illuminated image sensors that the company said would improve the picture quality on smartphones and other equipment with cameras. The stacked sensors are purported to be more energy-efficient and faster. Sony reported that it would embed the technology in 8- to 13-megapixel cameras:

Sony announced today [23 January 2012] three new back-illuminated stacked CMOS image sensors optimised for bright and low-light conditions. The new compact sensors are faster, consume less power than previous versions, and will be available in 8- to 13- megapixel flavours. Most notably, the sensors feature new 'RGBW Coding' and 'High Dynamic Range (HDR) Movie' abilities baked directly onto the hardware. The iPhone 4S features a Sony 8-megapixel sensor, and it's possible that this may be a preview of the camera sensor inside the iPhone 5.

Source: MacManus C.: 'Sony reveals what could be the iPhone 5's camera sensor' news.cnet.com/8301-17938_105-57364173-1/sony-reveals-what-could-be-the-iphone-5s-camera-sensor/?tag=mncol, 23 January 2012.

Standards and policy (Government and non-Government):

CESG (2009), *Good Practice Guide: Remote Working*, March 2009

Wimax Forum (www.wimaxforum.org)

LTE Standard (www.3gpp.org/LTE)

QinetiQ comment

Although UMDs are becoming increasingly popular, there are still a number of challenges to overcome for these devices to become truly ubiquitous. As processor performance improves, the capabilities of these devices will increase to a point at which advanced augmented reality applications will become possible (i.e. applications which perform feature extraction and overlay in addition to the standard GPS localisation performed today). Security concerns will be a perennial problem for such portable devices. We can expect significant investment over the next several years by companies providing security-focussed products for smartphones and tablets. This is likely to mirror increased interest, and hence threat, from hackers and organised crime due to the prevalence of these devices and the range of activities for which they are used (e.g. increasingly banking and shopping transactions). It is also worth mentioning that wearable computers although sometimes small and lightweight are not strictly UMDs.

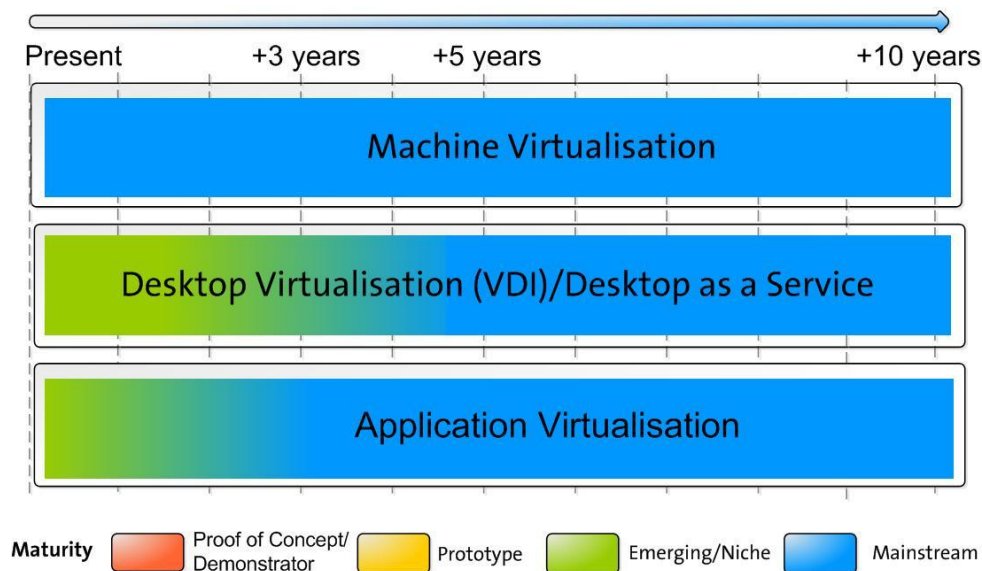
Technology / Technique: Virtualisation

Description

Virtualisation is a generic concept which can be applied and implemented in many different environments and at various levels of abstraction within an organisation’s IT infrastructure. This can range from the applications, through to user’s desktops and physical machines.

In the past virtualisation technologies have primarily been used to consolidate servers using machine virtualisation technologies, although it is now increasingly being used on standalone machines. In machine virtualisation, the layer of abstraction is called a ‘hypervisor’ or Virtual Machine Monitor (VMM) and is located between the hardware and the operating system. The hypervisor manages the safe sharing of hardware resources allowing for the concurrent running of multiple instances of an operating system on a single physical machine. More recently desktop virtualisation technologies such as Virtual Desktop Infrastructure (VDI) have come into vogue, allowing individual desktop instances running inside a Virtual Machine (VM) to be delivered over the network to clients. This has become popular as it allows an entire organisation’s IT infrastructure to be managed centrally, ensuring applications are up to date and operating systems fully patched to improve their security baseline.

Virtualisation Roadmap



Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 - 5 years: Market hype will continue as many of the technologies supporting virtualisation begin to mature. Desktop as a Service (DaaS) which is essentially a desktop environment provided on a subscription basis using VDI technology will become popular with organisations looking to reduce costs.

Within 6 - 9 years: Virtualisation is already a key component of the cloud computing eco-system, and will play an even more important role as standards and technology improves to enable the development of flexible IT infrastructures which can intelligently distribute workloads to provide high levels of service to clients. Mobile virtualisation will start to be widely used.

10+ years: We can expect to see virtualisation being more widely dispersed, spanning the space between the data centre and hand-held devices.

General issues and Challenges

Security and Separation: There are many concerns over the security of virtualisation technologies ranging from vulnerabilities in drivers allowing unauthorised communication between VMs to attacks on the hypervisor itself. While there are now a number of 'secure' virtualisation technologies that have been accredited by the National Security Agency (NSA) in the US (e.g. Green Hills Integrity and General Dynamics GHOST), organisations such as CESG (the UK National Technical Authority for Information Assurance) are still concerned and are working to understand the risks of deploying the technology in sensitive environments. Approval has recently been given to allow virtualisation to separate Restricted and Unclassified on shared hardware.

Input/Output (I/O) Issues: One difficult aspect of machine virtualisation is the mechanism by which the I/O (Input/Output) devices are virtualised, and while there are efforts to develop standards for this, currently it is not advisable to run highly I/O intensive applications (e.g. database servers) within a virtualised environment unless native hardware assistance is provided.

Virtualisation is as much as a business issue as a technology issue: When virtualisation takes place, boundaries of control and management responsibility change from the clearly defined tangible assets such as blade servers to 'virtual' resource pools, which may be supported by a whole host of physical assets. This move necessitates a cultural change which requires effective business processes to ensure that the virtual infrastructure is managed appropriately. To affect such a cultural change, any staff in an organisation involved in the delivery and use of virtualisation must be appropriately trained and strong governance put in place.

Software Licensing Issues: Virtualisation technology breaks most established software pricing and licensing models. Vendors are still trying to catch up with software licensing for applications being run in a virtualised environment. While virtualisation can reduce costs through the consolidation of physical hardware – some of this benefit is currently being impacted by software licensing costs.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

Gartner's 'Hype Cycle for Virtualization, 2011' presents the progress and development of a raft of technologies associated with virtualisation. As a collective IT initiative, Gartner rate virtualisation's effect as transformational although many of the individual technologies on its hype cycle are indicated as having only moderate benefit. To quote:

Although x86 server virtualization is mature, virtualization as an IT initiative is still in its adolescence, and is disruptive to IT users and providers. This has resulted in varying levels of hype, while delivering the foundation for cloud computing and greener data centre initiatives.

New technologies demonstrate the fledgling status of many areas of the virtualization market. They include server software appliances, cloud-bursting, memory overcommit and DMZ virtualization. Collectively, they demonstrate that virtualization is simultaneously maturing and broadening in its adoption across the portfolio, focusing on packaging, provisioning, efficiency and security collectively.

Source: Dawson P.: 'Hype Cycle for Virtualisation, 2011', Gartner Research ID: G00215434. 28 July 2011.

Current mobile phones have computing capabilities once found in mainframe computers and workstations. Such capability has enabled mobile phones to host mobile

virtualisation platforms with a range of accompanying benefits. As it does on servers and desktop computers, mobile virtualization offers device original equipment manufacturers (OEMs), mobile network operators (MNOs), and semiconductor suppliers enhanced security, portability, reliability, license IP isolation, and hardware consolidation.

TechNavio analysts forecast that the Global Mobile Virtualization market will reach \$1,198 million in 2014. One of the key factors contributing to this market's growth is the increasing need for cost reduction benefits. However, the increase in processor load and lack of mobile broadband infrastructure in developing countries could pose a challenge to the growth of this market. The Mobile Virtualization market has also been witnessing an emergence of enterprise dedicated devices. Key vendors dominating this market space include VMware Inc., Open Kernel Labs, Red Bend Software, and Citrix Systems Inc.

Source: 'Global Mobile Virtualization Market 2010 – 2014', TechNavio Report, Infiniti Research. May 2011.

Petri, D (2010). 'What You Need to Know About Securing Your Virtual Network', www.petri.co.il/what-you-need-to-know-about-vmware-virtualization-security.htm, 8th January 2010.

Brook et al. (2009), 1Technology Assessment: Virtualisation Technologies1, QINETIQ/IS/ICS/TR0901049, March 2009.

Price, M (2008). 'The Paradox of Security in Virtual Environments', Computer, IEEE Computer Society, November 2008, pp 22-28.

Karger, P.A and Safford, D.R. (2008) I/O for Virtual Machine Monitors: Security and Performance Issues1, IEEE Security & Privacy, vol. 6, no. 5, pp. 16-23, Sept/Oct 2008.

VMware security advisory, September 2007, www.cpni.gov.uk/Products/3401.aspx.

Standards and policy (Government and non-Government)

Centre for the Protection of National Infrastructure (CPNI) - Roles required for effective management of a virtualised environment

(See www.cpni.gov.uk/Docs/tn-01-09-security-server-virtualisation.pdf – see Appendix F.)

There is currently a lack of defined standards for virtual machine images, currently for example it is not possible to use VM images generated by VMWare on Microsoft's Hyper-V. However, there are efforts by VMWare, Microsoft and IBM to define an open standard for virtual machines called the Open Virtualisation Format (OVF).

(See www.vmware.com/appliances/getting-started/learn/ovf.html).

PCI-SIG is currently in the process of developing an industry standard for I/O virtualisation called PCI-IOV. These specifications, in conjunction with machine virtualisation technologies will allow virtual machines to natively share devices. (See www.pcisig.com/specifications/iov/).

QinetiQ comment

Virtualisation has become very widespread in data-centre environments, providing an easy way of matching workloads with computing resources. Although there are some large desktop virtualisation deployments, they are still few by number, and the move towards predominantly web delivered applications removes some of the motivation.

Virtualisation on hand-held platforms has been demonstrated very recently, but compelling end-user applications for this have not yet been presented.

<p>Technology / Technique: Visualisation for network security</p>	<p>Relevant to SANS Critical Control: 10, 11, 19</p>						
<p>Description</p> <p><i>Visual data analysis helps to perceive patterns, trends, structures, and exceptions [and] allows the audience to identify concepts and relationships that they had not previously realized.</i></p> <p><i>A single graph or picture can potentially summarize a month's worth of intrusion alerts... possibly showing trends and exceptions, as opposed to scrolling through multiple pages of raw audit data with little sense of the underlying events.</i></p> <p><i>Security Visualisation is a very young term. It expresses the idea that common visualisation techniques have been designed for use cases that are not supportive of security-related data, demanding novel techniques fine-tuned for the purpose of thorough analysis. [Quotes drawn from Shiravi et al.¹]</i></p> <p>Data sources for security visualisation typically include network packets (raw or aggregated), alerts from Intrusion Detection Systems (IDS), events from network servers, firewalls, switches and routers, and application-level events.</p> <p>¹ Source: Shiravi H., Shiravi A., Ghorbani A. A.: 'A Survey of Visualization Systems for Network Security', IEEE Transactions On Visualization And Computer Graphics, 2011.</p>	<h3 style="text-align: center;">Visualisation for Network Security Roadmap</h3> <table border="1" style="width: 100%; text-align: center;"> <thead> <tr> <th style="width: 33%;">2 – 5 years</th> <th style="width: 33%;">6 - 9 years</th> <th style="width: 33%;">10+ years</th> </tr> </thead> <tbody> <tr> <td style="background-color: #ffffcc;"> <ul style="list-style-type: none"> • Data visualisation tools and techniques will have minor improvements in this timescale. • These tools will be applied to areas such as Cloud Computing security and are likely to be implemented with the latest Web technologies. </td> <td style="background-color: #c8e6c9;"> <ul style="list-style-type: none"> • Further research and development of (largely stand-alone) visualisation tools, augmented by gradually improving data sources and prioritisation/analysis methods </td> <td style="background-color: #e0f2f1;"> <ul style="list-style-type: none"> • Likelihood of better-integrated systems with coherent sets of co-operating visualisations, and smarter prioritisation of events through better datasets and more CPU power. </td> </tr> </tbody> </table>	2 – 5 years	6 - 9 years	10+ years	<ul style="list-style-type: none"> • Data visualisation tools and techniques will have minor improvements in this timescale. • These tools will be applied to areas such as Cloud Computing security and are likely to be implemented with the latest Web technologies. 	<ul style="list-style-type: none"> • Further research and development of (largely stand-alone) visualisation tools, augmented by gradually improving data sources and prioritisation/analysis methods 	<ul style="list-style-type: none"> • Likelihood of better-integrated systems with coherent sets of co-operating visualisations, and smarter prioritisation of events through better datasets and more CPU power.
2 – 5 years	6 - 9 years	10+ years					
<ul style="list-style-type: none"> • Data visualisation tools and techniques will have minor improvements in this timescale. • These tools will be applied to areas such as Cloud Computing security and are likely to be implemented with the latest Web technologies. 	<ul style="list-style-type: none"> • Further research and development of (largely stand-alone) visualisation tools, augmented by gradually improving data sources and prioritisation/analysis methods 	<ul style="list-style-type: none"> • Likelihood of better-integrated systems with coherent sets of co-operating visualisations, and smarter prioritisation of events through better datasets and more CPU power. 					
<p>Relevant applications</p> <p>Security visualisation is relevant to both real-time and offline analysis of network data, to detect, identify, understand and mitigate network threats or vulnerabilities.</p>							

General issues and challenges

The volume of network data is a major challenge, and the level of noise and fine detail can hinder the maintenance of higher-level situational awareness. Systems therefore need to prioritize and highlight critical events (spot the needles in the haystack), reducing the load on the human. Underpinning data processing techniques are required to support the visualisations. Processing these large volumes of data in real-time is a computational challenge as well as a visualisation challenge; many systems are only capable of off-line forensic analysis. Different situations and users may require quite different visualisations (real-time dashboards versus off-line log analysis, for example). The complexity of the data, and the fact that users are struggling to piece together partial clues left by capable and evolving adversaries, calls for powerful tools and rich visualisations — but such tools are inherently difficult to learn and to use. Multiple tools and visualisations are often required for different tasks and situations, compounding the difficulty — integrated tool suites are rare at present. There are often very large numbers of entities (IP addresses, ports) to visualise — too many to plot on a screen without occlusion or some form of aggregation or filtering. These numbers will increase as IPv6 sees wider adoption. Correlating the raw packet data with specific applications and users is difficult but valuable. Usability studies of security visualisations are rare, and benchmark datasets are lacking, which makes the selection of tools and visualisations difficult. False positives are a particular problem for IDS. The recent emergence of Cloud Computing presents new challenges.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

Significant amount of work has been published in this area, but little work has been done to study this emerging visualisation discipline. [...]The complex, dynamic, and interdependent nature of network security demands extensive research during the development process. Without an in-depth understanding of security operations and extensive hands on experience, developing a security visualisation system will not be possible. A design process centred on the needs, behaviours, and expectations of security analysts can greatly influence and impact the usability and practicality of such systems. For best results, security experts and visual designers must thereby collaborate to complement each other's skills and expertise to innovate informative, interactive, and exploratory systems that are technically accurate and aesthetically pleasing.

Source: Shiravi H., Shiravi A., Ghorbani A. A.: *Survey of Visualization Systems for Network Security*, IEEE Transactions On Visualization And Computer Graphics, 2011 (Pre-print).

If you don't have the data, you cannot visualize it. A lot of companies are still struggling to collect the necessary data. In some cases, the data is not even available because applications do not generate it ... What does the cloud have to do with security visualisation? Well, it has to do with processing power and with application development. Applications generate logs and logs are used for security visualization. Cloud services are new pieces of software that are being developed. We have a chance here to build visibility into those applications, meaning we have an opportunity to educate these developers to apply logging in the right way. We are absolutely nowhere with [security visualisation tools]. There are a couple of simple tools out there, but there is no tool that really does what we need: brushing, linked views, supports large data sets, easy to use, contextualised, etc. Next year won't really change anything in this area. What we will see is that more and more tools are built on

the Web... What will we see in security visualisation? Well, as we saw earlier, we don't have the data. What that means is that we haven't really had a chance to learn how to visualise that data. And because we didn't have that chance, we don't really understand our data.

Security Visualisation - State of 2010 and 2011 Predictions, secviz.org/content/security-visualization-state-2010-and-2011-predictions.

Standards and policy (Government and non-Government)

Applicable 'standards' in this area (other than the underlying networking standards such as TCP/IP, UDP etc) are generally loose *de facto* standards for capturing IP packet data or server logs. Few standards exist for exchanging higher-level data such as attack signatures.

QinetiQ comment

Network Security Visualisation is a specialised and multidisciplinary area, requiring integration of applications, data, computing infrastructure, tools; expertise in visualisation and human factors; and domain knowledge in network security analysis. As a result, it evolves gradually and is not amenable to sudden technological breakthroughs, but requires sustained effort from multidisciplinary teams. This area is relatively immature so we expect significant, but gradual improvements over the next decade. Improvements will come from a whole-lifecycle approach to application design, data gathering, processing algorithms, visualisations, and their integration — rather than through the development of any particular novel visualisation technique in isolation. Despite this, it should be remembered that network security threats will be evolving too. Relevant hardware trends include the growth of storage capacity (disk and memory) and CPU, outstripping the growth in network bandwidth. This enables smarter and/or faster processing of data, and more real-time visualisation. However, the introduction of IPv6 and the proliferation of mobile IP devices will add new challenges. Other under-developed areas include training, benchmarks, and the exchange of attack data to enable a national and international 'immune system' for network security.

<p>Technology / Technique: Web-based mail and Instant Messaging in business</p>	<p>See also: Future tools for social networking and future collaboration tools.</p>	<p>Relevant to SANS Critical Control: 2, 6, 16, 17</p>						
<p>Description</p> <p>Web email (Webmail) refers to the accessing of email services via a Web browser and also to the case where the user’s email is being stored on a server that is ‘on the Web’, i.e. outside the Corporate Intranet. These features combined allow the user to access their email from any internet enabled terminal anywhere in the world. N.B. It is also possible to access Corporate servers using a Web browser though this is much less prevalent. As with traditional email, Webmail is a store-and-forward form of communication that does not rely on the recipient being ‘online’, but in turn is not ideally suited for interactive collaboration, especially across businesses.</p> <p>Instant Messaging (IM) refers to the interactive exchange of messages between users simultaneously connected to a computer network (not necessarily the internet). To work effectively, users must have a real time indication of the ‘presence’ of the people they wish to communicate with, i.e. whether they are available to receive the messages. Presence is typically provided by having users logging into a server supporting the IM system. Even if users are not currently connected, messages can be left for them (on the server), similar to email. The server also provides the ability to store transcripts of current and previous conversations. IM servers may be provided ‘on the Web’ or corporately.</p> <p>Both Webmail and IM are capable of transferring messages including text, documents, video, audio and other rich media. In addition, some IM systems now incorporate the ability to initiate real time teleconferencing rather than simple messages with attachments.</p>	<div style="text-align: center;"> <h2>Web-based mail - Instant Messaging Roadmap</h2> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 33%; text-align: center;">2 – 5 years</th> <th style="width: 33%; text-align: center;">6 - 9 years</th> <th style="width: 33%; text-align: center;">10+ years</th> </tr> </thead> <tbody> <tr> <td style="background-color: #ffffcc; vertical-align: top; padding: 5px;"> <ul style="list-style-type: none"> Standalone Webmail and IM will be subsumed (or migrated) into future collaborative environments such as Social Networking tools (and business equivalents). There will be a shift from access via desktop environments to mobile devices. IM interoperability will improve and allow the controlled use of inter-business IM. Improvements in rich presence integration with IM will provide compelling arguments for the transition to IM from Email. </td> <td style="background-color: #ccffcc; vertical-align: top; padding: 5px;"> <ul style="list-style-type: none"> Mobile devices will become the predominant source of Webmail and IM access for business. Webmail will be in decline compared to IM because IM will ubiquitously offer online (interactive) and offline (store and forward) facilities but with the additional features of presence, real time document sharing and interactive collaboration tools such as web-conferencing. Due to the natural way of human working, web-conferencing will only be used when appropriate. </td> <td style="background-color: #ccffff; vertical-align: top; padding: 5px;"> <ul style="list-style-type: none"> IM (within future collaborative environments) will still dominate electronic collaboration in the business environment, augmented with new real-time technologies such as future immersive tools (again, used when needed rather than as a replacement for IM). </td> </tr> </tbody> </table>		2 – 5 years	6 - 9 years	10+ years	<ul style="list-style-type: none"> Standalone Webmail and IM will be subsumed (or migrated) into future collaborative environments such as Social Networking tools (and business equivalents). There will be a shift from access via desktop environments to mobile devices. IM interoperability will improve and allow the controlled use of inter-business IM. Improvements in rich presence integration with IM will provide compelling arguments for the transition to IM from Email. 	<ul style="list-style-type: none"> Mobile devices will become the predominant source of Webmail and IM access for business. Webmail will be in decline compared to IM because IM will ubiquitously offer online (interactive) and offline (store and forward) facilities but with the additional features of presence, real time document sharing and interactive collaboration tools such as web-conferencing. Due to the natural way of human working, web-conferencing will only be used when appropriate. 	<ul style="list-style-type: none"> IM (within future collaborative environments) will still dominate electronic collaboration in the business environment, augmented with new real-time technologies such as future immersive tools (again, used when needed rather than as a replacement for IM).
2 – 5 years	6 - 9 years	10+ years						
<ul style="list-style-type: none"> Standalone Webmail and IM will be subsumed (or migrated) into future collaborative environments such as Social Networking tools (and business equivalents). There will be a shift from access via desktop environments to mobile devices. IM interoperability will improve and allow the controlled use of inter-business IM. Improvements in rich presence integration with IM will provide compelling arguments for the transition to IM from Email. 	<ul style="list-style-type: none"> Mobile devices will become the predominant source of Webmail and IM access for business. Webmail will be in decline compared to IM because IM will ubiquitously offer online (interactive) and offline (store and forward) facilities but with the additional features of presence, real time document sharing and interactive collaboration tools such as web-conferencing. Due to the natural way of human working, web-conferencing will only be used when appropriate. 	<ul style="list-style-type: none"> IM (within future collaborative environments) will still dominate electronic collaboration in the business environment, augmented with new real-time technologies such as future immersive tools (again, used when needed rather than as a replacement for IM). 						
<p>Relevant applications</p> <p>Webmail and IM are already used ubiquitously throughout the business environment to enable instantly accessible communications with rapid turnaround of information. In particular, the use of smartphones and other mobile internet devices are driving growth equally across personal and business users.</p>								

General issues and Challenges

Public Web based email services offer compelling advantages over traditional Corporate Email. For instance, Webmail can be globally accessed, will typically have much larger mail box size limits and allow the transfer of much larger files of any format (i.e. not restricted by Corporate content filtering). They are also likely to offer innovative new features given the pace of change that can be supported by the internet. For these reasons, employees become willing to use the same public services they use in their personal life as business tools to increase their efficiency. Unfortunately, this exposes businesses to many risks, including those related to:

- **Availability:** Access to the internet is required to access Emails stored on Web based Email servers. The business is at the risk of the external Email service (or their connection to the internet) failing thus data is inaccessible for the duration. Similarly, if emails are accidentally deleted (or maliciously deleted/mis-placed) then the recovery of that data may not be possible given the servers are being operated by a Third Party outside the Corporate back up domain;
- **Confidentiality:** Corporate documents are held on web based Email servers, which are outside the protective boundaries of the business and could easily be compromised causing loss of IPR and/or embarrassment;
- **Auditability:** Emails are legal transcripts that businesses must be able to produce if requested, e.g. in court cases, otherwise fines are incurred. If these documents are stored on externally owned and operated servers they become more difficult to find and could even be lost;
- **Viruses and phishing attacks:** Webmail circumvents content filtering at the Corporate Email server (because it is downloaded over Web protocols, not Email protocols) thus reducing a layer of network defence (though complex content filtering firewalls exist and/or blacklists of public Webmail services can be setup on standard firewalls). In addition, Webmail is particularly prone to phishing because there is less certainty of the validity of a sender/recipient than is the case with the Corporate Email address book.

Using third party (paid for) Web based email servers may give some recourse for overcoming (un)availability issues but this is unlikely to offset the financial impact to the business. Confidentiality issues also remain. Enabling web based access to Corporate email servers opens up the servers to external attack and this alone persuades businesses to mandate VPN based solutions to access corporate email, requiring corporate devices (laptops or Blackberries) to be used instead of innovative devices.

Similar issues exist for the use of Web based IM services with the added complication that the immediacy of the technology may cause rash statements leading to embarrassment or legal implications. Corporate IM solutions exist but there is a lack of interoperability between products for inter-business IM as well as a cultural mistrust of the technology, e.g. would a business want another business to know the whereabouts and working patterns of its staff, available via presence technologies?

The main challenge to business posed by Web based email and IM is that staff are able to use more advanced, more accessible tools for free on the internet than are currently available within the business. Simply blocking access to these services misses out on the potential gains in productivity they may offer. Businesses must therefore look to overcome the limitations of their own tools, while maintaining the necessary standards of confidentiality, availability and auditability. In addition to this, if new technologies (such as corporate IM) are introduced or the use of use of Web based IM is allowed for business purposes then it is imperative that staff are properly trained in their appropriate use and policy is defined and disseminated to back this up.

Information sources, Supporting extracts and quotations (websites, forums, publications etc.)

In relation to the uptake of mobile Email and IM services, typically offered by mobile phone network operators, handset vendors or third party internet providers, this Portio research report charts the explosive market uptake:

1By end-2010, there were 480.6 million users of mobile e-mail services worldwide, and this customer base will have nearly quadrupled come end-2015. The worldwide mobile IM user base stood at 311.2 million in 2010. With Mobile Network Operators making conscious efforts to enhance the instant messaging experience through additional features to make IM services more attractive and popular among their subscribers, user levels will rise to 1.6 billion over the next five years.1

Source 1: Portio Research: 'Mobile Messaging Futures 2011-2015', Portio Research ID: MMF11-15, January 2011.

In relation to IM being subsumed by social networking tools, another Gartner report predicts:

1Social networks and micro-blogging sites are recording increased usage on mobile devices, and are set to become hubs for mobile personal communications. In the long term, this trend will affect mobile IM and will allow it to become superseded by mobile social networks before it reaches 30% market penetration.

Source 3: Johnson, G.: 'Hype Cycle for Unified Communications and Collaboration, 2011' Gartner Research ID Number: G00215510, August 2011.

In response to the question 1In the next five years, do you think real-time workplace communication tools (including IM and Sharepoint) will be more or less popular than email among employees1, 54% of 1400 Chief Information Officers said it would be - with a further 38% saying it would be as least as popular.

1Email may soon become the new snail mail. More than half (54 percent) of chief information officers (CIOs) interviewed recently said real-time workplace communication tools will surpass traditional email in popularity within the next five years.1

Source 4: Robert Half Technology: 'Mobile Messaging Futures 2011-2015', Robert Half Technology Survey, rht.mediaroom.com/index.php?s=131&item=1201, Aug 2011.

Standards and policy (Government and non-Government)

Accessing Web based email via a Web browser uses the standard Web protocol, i.e. Hyper Text Transfer Protocol (HTTP) over Transmission Control Protocol (TCP). Web based email accounts (provided by the likes of Google, Microsoft and most internet Service Providers) can also typically be configured so that Email clients like Microsoft Outlook can access them via the standard Email protocols such as the Post Office Protocol (to receive Email) and Simple Mail Transfer Protocol (to send Email).

There are two emergent IM protocols vying for market share; namely eXtensible Messaging Presence Protocol (XMPP) and Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE) based on Session Initiation Protocol (SIP). XMPP is supported by Google Talk and Cisco (Jabber products). Microsoft Office Communications Server (now Lync) uses SIMPLE but has a gateway product to enable XMPP interoperability.

UK Government is developing its Government Cloud (G-Cloud) strategy (www.cabinetoffice.gov.uk/sites/default/files/resources/government-cloud-strategy_0.pdf), which it is hoped will lead to government robustly adopting a public cloud first policy. Cloud computing covers many web based services including Web based email and IM. Some local councils are beginning to embrace this strategy, e.g. Hillingdon Council (www.guardian.co.uk/government-computing-network/2011/dec/19/hillingdon-council-google-apps) which is outsourcing services including Email, IM, word processing, calendar etc. to Google Apps for Business cloud services.

QinetiQ comment

Corporations like Google offer impressive layers of network defence for their cloud services (www.google.com/apps/intl/en/business/infrastructure_security.html) with some degree of (US) government scrutiny. However, the security credentials of other providers are likely to be less stringent than Google and other reputable service providers have suffered high profile service outages and data loss. For example, the Amazon cloud service suffered a system crash in April 2011 (articles.businessinsider.com/2011-04-28/tech/29958976_1_amazon-customer-customers-data-data-loss) that caused hosted website to become unavailable for several days and included the loss of client data. Similarly, recent vulnerabilities on the Sony Playstation Network (PSN) (www.guardian.co.uk/technology/gamesblog/2011/apr/26/games-playstation) have highlighted that internet based services holding confidential information will always be susceptible to zero-day attack. Perhaps more importantly, while the vulnerabilities were being addressed, the PSN was unavailable for three weeks.

Nonetheless, Web based email and IM (and other web/cloud services) offer significant advantages for business in terms of accessibility, immediacy and usability. Therefore, a balance of offering these services through interoperable Corporate tools maintained within the business boundary but extendible across trusted business partners would seem to offer a better compromise in maintaining availability and security.

<p>Technology / Technique: Wireless Mesh Networks</p>	<p>Relevant to SANS Critical Control: 7</p>						
<p>Description</p> <p>Wireless mesh networks are a form of communications network that use a mesh topology. In a mesh network, devices relay information for other devices that are not directly attached to each other. This is in contrast to other forms of network topologies that require direct connections between end-points or, where one device acts as a central hub that relays information for all other devices.</p> <p>In wireless mesh networks, typically most or all of the links interconnecting mesh nodes are wireless, although one or more devices may also be attached to a fixed network to allow interoperability with corporate networks or the wider internet.</p> <p>In such a mesh, there are typically multiple paths through the network between any two end-points. This can provide a degree of fault tolerance in the network since if a path fails, other paths can still be used to route data to the intended destination.</p> <p>There are two main types of wireless mesh network:</p> <ul style="list-style-type: none"> • Fixed wireless mesh where the devices that form the main part of the network do not move; • Mobile mesh, or mobile ad hoc network (MANET), where the constituent nodes of the mesh are free to move. This creates a changing topology that the networking protocols that underpin the network need to respond to so that data can still be routed through the network. 	<div style="text-align: center;"> <h2>Wireless Mesh Networks Roadmap</h2> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 33%; text-align: center;">2 – 5 years</th> <th style="width: 33%; text-align: center;">6 - 9 years</th> <th style="width: 33%; text-align: center;">10+ years</th> </tr> </thead> <tbody> <tr> <td style="vertical-align: top; padding: 5px;"> <ul style="list-style-type: none"> • Technologies to support wireless mesh networks both for broadband and sensor networks are available from a number of manufacturers. Whilst there may be some limited deployment, large scale roll-out in metropolitan areas for community broadband is unlikely. • We can expect some wireless mesh networks to be used in support of smart meter installations and smart energy grids, these will occur in many regions and are likely to be based on ZigBEE. </td> <td style="vertical-align: top; padding: 5px;"> <ul style="list-style-type: none"> • Wireless mesh networks for home automation will begin to gain some traction in the market, but adoption will be slow. This may begin to change as the deployment of smart meters progresses, but only if the meters adopt a wireless mesh standard such as ZigBEE. • The use of wireless mesh networks for broadband delivery will remain niche in urban and rural areas. </td> <td style="vertical-align: top; padding: 5px;"> <ul style="list-style-type: none"> • The next generation of tactical radios for defence and paramilitary use will be mature and offer improvements over the current generation of radios. • 4G, conventional wired broadband and satellite are likely to have edged out wireless mesh networks from broadband provision to consumers and businesses almost entirely in the developed world. • Wireless mesh sensor networks will grow to become ubiquitous. </td> </tr> </tbody> </table>	2 – 5 years	6 - 9 years	10+ years	<ul style="list-style-type: none"> • Technologies to support wireless mesh networks both for broadband and sensor networks are available from a number of manufacturers. Whilst there may be some limited deployment, large scale roll-out in metropolitan areas for community broadband is unlikely. • We can expect some wireless mesh networks to be used in support of smart meter installations and smart energy grids, these will occur in many regions and are likely to be based on ZigBEE. 	<ul style="list-style-type: none"> • Wireless mesh networks for home automation will begin to gain some traction in the market, but adoption will be slow. This may begin to change as the deployment of smart meters progresses, but only if the meters adopt a wireless mesh standard such as ZigBEE. • The use of wireless mesh networks for broadband delivery will remain niche in urban and rural areas. 	<ul style="list-style-type: none"> • The next generation of tactical radios for defence and paramilitary use will be mature and offer improvements over the current generation of radios. • 4G, conventional wired broadband and satellite are likely to have edged out wireless mesh networks from broadband provision to consumers and businesses almost entirely in the developed world. • Wireless mesh sensor networks will grow to become ubiquitous.
2 – 5 years	6 - 9 years	10+ years					
<ul style="list-style-type: none"> • Technologies to support wireless mesh networks both for broadband and sensor networks are available from a number of manufacturers. Whilst there may be some limited deployment, large scale roll-out in metropolitan areas for community broadband is unlikely. • We can expect some wireless mesh networks to be used in support of smart meter installations and smart energy grids, these will occur in many regions and are likely to be based on ZigBEE. 	<ul style="list-style-type: none"> • Wireless mesh networks for home automation will begin to gain some traction in the market, but adoption will be slow. This may begin to change as the deployment of smart meters progresses, but only if the meters adopt a wireless mesh standard such as ZigBEE. • The use of wireless mesh networks for broadband delivery will remain niche in urban and rural areas. 	<ul style="list-style-type: none"> • The next generation of tactical radios for defence and paramilitary use will be mature and offer improvements over the current generation of radios. • 4G, conventional wired broadband and satellite are likely to have edged out wireless mesh networks from broadband provision to consumers and businesses almost entirely in the developed world. • Wireless mesh sensor networks will grow to become ubiquitous. 					

Relevant applications

- Urban and rural broadband, e.g. community broadband services;
- Sensor networks, e.g. remote sensing, industrial monitoring and control, home automation;
 - Underpinning communications for the 'smart energy grid';
 - Electronic imaging (e.g. video);
 - Paramilitary and Defence, particularly tactical communications;
 - The One Laptop Per Child (OLPC) devices used by school children in developing countries uses a mesh routing protocol to allow collaboration in areas without an established telecommunications network or internet service.

Technology readiness and maturity (forecasted arrival and accessibility)

Within 2 - 5 years: Technologies to support wireless mesh networks both for broadband and sensor networks are available now from a number of manufacturers. Whilst there may be some limited deployment, large scale roll-out in metropolitan areas for community broadband is unlikely. Rather specific, smaller scale networks in support of specific applications or customer segments may occur, e.g. industrial or local government. We can expect some wireless mesh networks to be used in support of smart meter installations and smart energy grids, these will occur in many regions and are likely to be based on ZigBEE. There will be continued deployment of small-scale sensor networks (e.g. 10s-100s of nodes).

Within 6 - 9 years: Wireless mesh networks for home automation will begin to gain some traction in the market, but adoption will be slow due to a lack of widespread consumer interest. This may begin to change as the deployment of smart meters progresses, but only if the meters adopt a wireless mesh standard such as ZigBEE. The use of wireless mesh networks for broadband delivery will remain niche in urban and rural areas and struggle to compete against other approaches, e.g. 4G mobile, xDSL, fibre and satellite.

10+ years: Wireless mesh sensor networks will grow beyond the next decade to become ubiquitous across civil, industrial and government applications. Other forms of wireless mesh network for more general purpose networks will be relegated to niche applications such as defence and paramilitary, and disaster recovery. The next generation of tactical radios for defence and paramilitary use will be mature and offer improvements over the current generation of radios in terms of capacity and scalability. 4G, conventional wired broadband (xDSL and fibre) and satellite are likely to have edged out wireless mesh networks from broadband provision to consumers and businesses almost entirely in the developed world, although there may still be some interest in the developing world.

General issues and Challenges

- **Spectrum:** Many wireless mesh networks operate in the Industrial, Scientific and Medical (ISM) frequency bands since they are based on WiFi or similar technologies. Since these frequency bands do not require an expensive spectrum licence, they are likely to see increased usage in the coming years and become increasingly congested. Other bands are possible, but would require a spectrum licence. Some multi-band mesh radios are available, for instance supporting both WiFi and the 4.9 GHz US public safety band;

- **Cost:** This has been a particular issue for community broadband networks in recent years. Whilst the initial deployment of the networks may have been relatively cheap, the on-going maintenance and operation of the network has been more costly than expected. This has contributed to the demise of many of the community broadband initiatives that were launched amid great fanfare in the mid-2000s;
- **Capacity and scalability:** The need to relay information through the network hop-by-hop limits the available capacity of the overall system, which can be a particular problem for networks providing broadband access. This will limit the maximum number of concurrent users, and the achievable data rates that can be supported by such a network. Whilst this can be ameliorated through the use of wired links at strategic points, the overall capacity of the system will always be limited unless more wired interconnects are used. In the limit, the wireless network ceases to be a mesh since all nodes may have a wired interconnect, and resemble a conventional cellular or WiFi network. The attendant costs that these interconnects bring hence remove the advertised benefits of a wireless mesh network, that of being faster and cheaper to deploy and sustain. For many sensor networks, capacity is not a major issue since each sensing node often requires only small data rates to support it;
- **Competition:** Whilst wireless mesh networks for broadband provision were touted as the next big thing in the mid-2000s, they have struggled against competing technologies for business and residential customers. The reach and data rates of xDSL technologies have improved greatly as costs to subscribers have fallen. Fibre deployments either to the kerb, cabinet or home are also greatly increasing data rates for customers to levels that wireless mesh networks will always struggle to achieve. Similarly, recent developments in satellite broadband services will deliver competitive broadband across entire regions. Hence the market for broadband provision will be increasingly challenging for wireless mesh networks;
- **Interoperability:** The technology underpinning wireless sensor networks is currently fragmented. For instance, whilst many products utilise 802.11 as the radio bearer, different networking protocols are used. Hence individual mesh networks can, in general, only be deployed with similar products. The same is largely true of wireless sensor networks, particularly those that require longer communications ranges. Short range sensor applications are generally converging on ZigBEE.

Information sources, Supporting extracts and quotations (Websites, Forums, Publications etc.)

On the subject of mesh sensor networks Gartner states:

Small-to-midsize implementations (that is, tens to hundreds of nodes) are being deployed using technology from several vendors for applications such as remote sensing, environmental monitoring and building management/automation. The market is commercially and technologically fragmented, and topics such as middleware and power-efficient routing are still areas of active academic research. The market potential is enormous (and long-term scenarios of tens of billions of installed units are likely); however, the slow adoption rate means it will take decades to ramp up.

Source 1: Fenn J., LeHong H.: 'Hype Cycle for Emerging Technologies', Gartner ID: G00215650, 28 July 2011.

Wireless mesh sensor networks are growing now, with the market reaching multi-billion \$US by 2021, as reflected in this forecast:

According to IDTechEx research in the new report 1Wireless Sensor Networks 2011-2021, WSN will grow rapidly from \$0.45 billion in 2011 to \$2 billion in 2021. These figures refer to WSN defined as wireless mesh networks, i.e. self-healing and self-organising. WSN will eventually enable the automatic monitoring of forest fires, avalanches, hurricanes, failure of country wide utility equipment, traffic, hospitals and much more over wide areas, something previously impossible. It has started

already with more humble killer applications such as automating meter readings in buildings, and manufacture and process control.

Source 2: IDTechEx: 'Wireless Sensor Networks 2011-2021', July 2011.

Wireless mesh networks are likely to play a significant role in the deployment of smart meters globally, as this next reference from a recent report from the Smart Metering Design Group of OFGEM indicates:

Note also that the use of a technology that allows mesh connectivity is very appealing from the propagation point of view, since 'far' devices can be connected via way-point devices (assuming they are powered). As more Home Area Network (HAN)-enabled devices are installed the network would actually strengthen.

Source 3: HAN Working Group (SMDG working group, OFGEM), 'SMHAN Radio Spectrum Study - Phase 1 Draft Working Paper', Stirling Essex, Rob Morland, Astutim Ltd, 16th May 2011.

Standards and policy (Government and non-Government)

There is a variety of standards that have, or are, emerging for wireless mesh networks. But these are used mainly in the lower layers of the communications protocol stack. For example WiFi (802.11) and ZigBEE are two notable standards. However, there is still a great deal of technology fragmentation in the market, particularly with respect to protocols that operate above these technologies, e.g. routing protocols. Whilst some standardisation has occurred in the internet Engineering Task Force (IETF) for mobile ad hoc networks, many products implement their own protocols as differentiators. There are no obvious drives for interoperability or standards conformance testing, and this is not likely to improve since the markets for these networks are niche, and customers tend to buy specific solutions to meet their need. Other standardisation attempts include:

- 802.11s: an enhancement of 802.11 (WiFi) to allow access points to form a wireless mesh network.
- 6LoWPAN: standardising the use of IPv6 for low-power wireless mesh sensor networks.

QinetiQ comment

It is clear that wireless mesh networks will struggle to compete with xDSL, fibre, 3G/4G mobile and satellite for residential and business broadband provision. In addition, services such as FON may further erode any potential market for mesh provided consumer and business broadband. The optimism of the mid-2000s for deploying large-scale metropolitan wireless mesh networks appears to have evaporated with the realisation of what these networks cost to sustain, and with the likely service levels achievable. However, wireless mesh networks will always have a role in niche applications, such as:

- Smart meters and smart energy grids.
- Rapidly deployed, temporary networks where wired networks are infeasible and where the use of mobile networks (3G/4G) is not possible, e.g. disaster recovery.
- Military and paramilitary networks where there is no fixed infrastructure available.
- Sensor networks.
- Home automation

QinetiQ currently believes that wireless mesh sensor networks will become ubiquitous over time, but that it will take many years for that to happen.

Technology / Technique: Wireless Power

Description

Wireless Power is a means of transferring energy through space to charge or directly power electrical and electronic equipment.

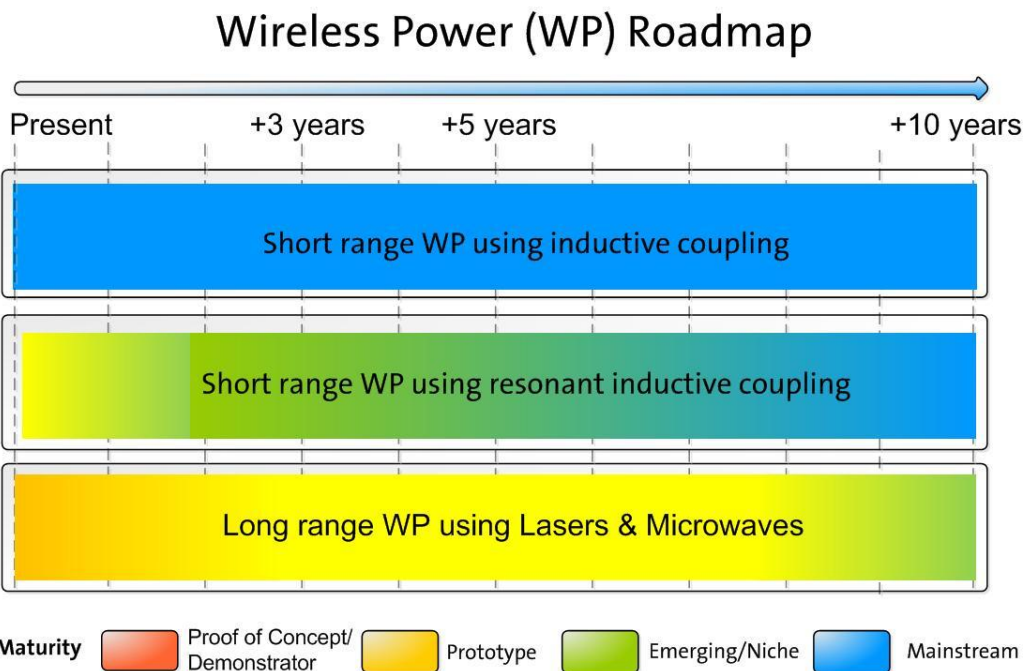
Short-range wireless power where energy is transferred by inductive coupling across no more than a few centimetres is widely used in mainstream appliances such as toothbrushes and mobile phone chargers or charging mats.

In 2007 MIT announced that they had successfully demonstrated efficient wireless power transfer over distances up to two metres. This was achieved using resonant inductive coupling which has the potential to power a wider range of electronic appliances (e.g. both Haier with Witricity and Sony have shown that televisions can be wirelessly powered up to a metre away from the power unit).

Long range wireless power transmission can be accomplished using microwaves and lasers providing there is a clear path from the transmitter to the receiver. Power beaming at kilowatt levels and kilometre range has been successfully demonstrated. Such technology could be used to power unmanned aircraft, potentially giving them unlimited endurance. In the longer term it is envisaged that long-range wireless power transmission using microwaves could beam Giga-watt streams of solar power down to Earth augmenting and replacing existing energy generation sources.

Relevant applications

Wireless power transfer can be applied in a wide variety of applications. The technology can be used to charge an existing power source e.g. through charging mats and surfaces for wirelessly charging battery powered mobile devices. It can also be exploited directly (where no other power sources are involved) in providing direct power to consumer electronics devices such as TVs, PCs and peripheral devices. There are also applications in areas such as defence, industry and transportation that would benefit from the technology.



Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 - 5 years: Short range wireless power using inductive coupling will become more sophisticated (e.g allow multiple devices to be charged at once).

Within 6 - 9 years: Short range wireless power using resonant inductive coupling is likely to become more widely available and the use of cables and wires will start to disappear.

10+ years: Long range power beaming will become suitable for powering devices in inconvenient locations (such devices could include security cameras and sensors).

General issues and Challenges

One of the main issues, although one not widely discussed, is that of health and safety. Charging a device on a surface is relatively safe, but walking into a room where there are strong magnetic fields raises important issues that the technology will have to address. A further issue is the limited range of current wireless power transmission. Research at Duke University in the US suggests that metamaterials could be used to boost power transmission without negative effects¹.

¹ Source: Page L.: *Much better wireless power transmission possible*. The Register, www.theregister.co.uk/2011/05/24/wireless_power_metamaterials/ 24 May 2011.

Finally it is also worth noting that currently the efficiency achieved with wireless power is somewhat lower than wired power and this will need to be considered by early adopters of the technology.

Information sources, supporting extracts and quotations (Websites, forums, publications etc.)

Wireless Power Planet provides regular news on commercial developments and standardisation for Wireless Power.

Source: Wireless Power Planet www.wirelesspowerplanet.com/

The following quotes are taken from the Gartner 'Hype Cycle on Emerging technologies, 2010'.

The idea of wireless charging is clearly attractive and several solutions have recently been demonstrated. For example, wireless charging schemes are being designed for use in table-top surfaces and similar environments that will charge a mobile device when it is placed onto the surface.

Adoption of the technology for mobile devices or PCs requires a degree of standardisation. A bigger obstacle is the question of why mobile equipment makers (such as handset vendors) should be interested in this technology.

Source: Fenn J., LeHong H.: 'Hype Cycle for Emerging Technologies, 2011' Gartner Research D: G00215650. 28 July 2011.

A LaserMotive white paper describes the use of lasers to transmit power directly to Unmanned Air Vehicles (UAVs), potentially giving them unlimited endurance. The authors acknowledge that power beaming at kilowatt levels and kilometre range has been successfully demonstrated in the field and suggest that silent, refuelling-free laser-electric UAVs are practical with current technology and could be developed and deployed quickly.

Source: Nugent T.J., Kare J.T.: *Laser Power for UAVs* LaserMotive White Paper 2010.

Standards and policy (Government and non-Government)

To date there has been some effort in the area of standardisation however more progress is required if the technology is to be widely adopted and exploited. The Wireless Power Consortium², a cooperation of independent companies who aim to set the standards for interoperable wireless charging, finalised a low-power standard in July 2010. However it is likely to be many years before an off-the-shelf charging platform will become available that can recharge any device placed on top of it, regardless of brand. Recently mobile phone makers have agreed a set of standards for chargers and this could set back the aspirations of wireless power vendors in this area.

To date there are no known specific policies available for the deployment of the technology.

²Source: www.wirelesspowerconsortium.com/

QinetiQ comment

Wireless power is a disruptive technology as it could eventually make radical changes to the way we power our electronic and electrical devices. Over the last few years, there has been considerable interest and hype over the potential of wireless power particularly as a 'green' carbon free and sustainable energy source. A potential threat to the technology (particularly for longer range forms) would be some form of interference between the power unit and the device being powered.

Technology / Technique: 'Big Data' - extreme information management

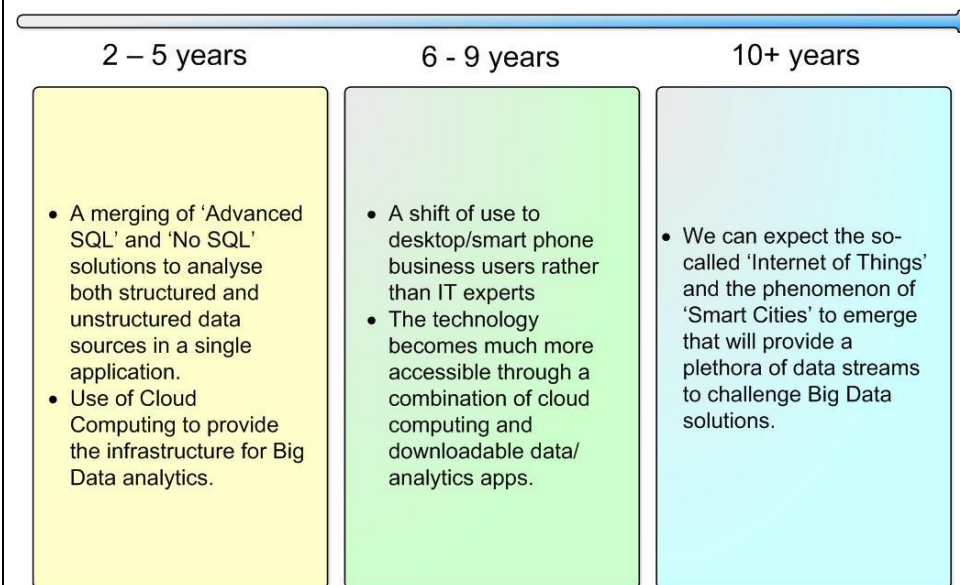
Description

'Big Data' is the term applied to large quantities of data (often hundreds of terabytes or petabytes in scale) that are beyond the ability of most existing software and technology to efficiently store, manage and analyse. With the massive boom in popularity of social media for both social interaction and business transactions there is a big move to exploit this data source for business and intelligence advantage.

However the vast infrastructure requirements and data/content analytics made possible by Big Data, pose big security implications for users (see General issues and challenges below).

New technologies, many of them open source, are emerging to handle and analyse these massive amounts of data. The current trend is to distribute and process the data across clusters of huge numbers of low spec servers to obtain cost effective scalable architecture. The data is distributed as a file system (e.g. Google File System, Hadoop Distributed File System (HDFS)) or as a distributed Structured Query Language (SQL) - or 'No SQL'- database (e.g. Cassandra, MongoDB). The analysis is then mapped across the data using 'Advanced SQL' or Hadoop/MapReduce.

Big Data Roadmap



Relevant applications

Scientists working in fields such as meteorology and genomics regularly encounter the challenge of working with Big Data. However it is the rise of the Social Data Revolution [1], the shift in human communication patterns towards increased personal information sharing, which has led to new levels of (unstructured) data being generated. Commercial and Government Organisations have been quick to recognise the wealth of intelligence contained in this vast source that has the potential to provide customer feedback on new products and monitor and forecast trends such as flu outbreaks and political uprisings; all in real-time. The major platform vendors such as IBM, Oracle, HP and Terradata have all recently launched a Big Data solution, but many of the components are Open Source.

General issues and challenges

Big Data provides a huge storage and management challenge. All the standard data management and security issues are further exacerbated by the inability to apply the standard solutions to the sheer volume of data. Big Data often consists of millions or even billions of small files, which are not suitable for traditional backup techniques. It is also a huge challenge to be able to verify integrity of the data and to perform standard virus checks. Maintaining an infrastructure of hundreds or thousands of servers is a non-trivial task. Organisations without the funds to invest in their own infrastructure can rent extensive shared server space through 'Cloud Computing' whereby resources are dynamically provisioned to the public over the internet, via web applications/web services, from an off-site third-party. However, this model requires organisations to hand over their data to a third party who can access their data and who may potentially have a less rigorous approach to cyber, personnel and physical security.

Furthermore, it is also the data content and data analytics that can lead to security issues and vulnerabilities. The personal information stored and published about individuals by social media apps can leave the individuals open to Social Engineering attacks. In addition, with the development of technology such as facial recognition available as apps on smart phones with cameras, there is the risk that individuals could be identified and targeted as the technology scans the internet for any available information linked to their image.

Information sources, supporting extracts and quotations (websites, forums, publications etc.)

The social data revolution is generating unprecedented amounts of Data:

'In 2009, more data will be generated by individuals than in the entire history of mankind through 2008. Information overload is more serious than ever.'

Source 1: Weigend A.: 'The Social Data Revolution'. Harvard Business Review. blogs.hbr.org/now-new-next/2009/05/the-social-data-revolution.html. Retrieved July 15 2009.

The analyst company Gartner include 'Big Data' in their hype cycle for emerging technologies.

Source 2: Fenn J., LeHong H.: 'Hype Cycle for Emerging Technologies, 2011', Gartner Research ID: G00215650, 28 July 2011.

The analyst company Ovum recognises the value of 'Big Data analytics' and how it is becoming more accessible and affordable:

'Technological advances such as in-memory, in-database analytics, the cloud, and MapReduce are improving the scale and performance of predictive analytics. Similarly, open source languages such as 'R' are helping to lower the cost and complexity of deployment.'

Source 3: Swenk H.: 'Getting More from your data with predictive analytics' Ovum, July 2010.

There are privacy worries as Big Data analytics allowing face recognition are being developed and deployed by social media sites:

Facial recognition technology will ultimately culminate in the ability to search for people using just a picture. And that will be the end of privacy as we know it - imagine, a world in which someone can simply take a photo of you on the street, in a crowd, or with a telephoto lens, and discover everything about you on the internet.

Source 4: Jacobsson Purewal S., of PC World magazine in Gayle D.: *Facebook now knows what you look like as it rolls out face recognition by stealth.* June 2011.

Standards and policy (Government and non-Government)

At the current time (December 2011) the author has no knowledge of any standards and policies related to Big Data. However, Martin Bellamy, director of change and ICT, National Offender Management Service, Ministry of Justice has stated that the government is using 'foundation delivery partners', which are public sector projects that will provide best practices for the rest of the public sector to adopt similar methods. For example, as part of the gCloud initiative, Warwickshire County Council is in the first phase of deploying Google email and apps to 4,000 users.

Source: www.computing.co.uk/ctg/news/2108855/government-set-adopt-style-cloud-policy.

QinetiQ comment

There is a lot of hype around Big Data and the associated technologies; organisations need to cut through the hype and get a real understanding of what can be achieved with the current Big Data technologies and where the gaps are. If the hype is to be believed, there is a big opportunity to harvest intelligence for both government agencies and rogue organisations. The future of Big Data will need little privately owned infrastructure and with the wide availability of open source/low cost applications the main bottleneck in unlocking this potential will be having the skills to apply the analytics techniques within this framework.

Big Data systems involve large numbers of nodes, and make products that use per node licensing models unaffordable. Most of the current Big Data users (like Google, Facebook, Amazon, e-bay) use mixtures of Open Source and home grown software. It seems unlikely that the vendor platforms can ever be cost effective competitors in this arena, and will give a commercial advantage to organisations that have in-house technical capabilities.

The rise of the *internet of Things* (where objects are connected to the internet) coupled with the rise to *Smart Cities* could lead to scenarios, for example, where a tracker installed in a car could use the internet to identify the nearest free parking space. This will give rise to a completely new level of Big Data streams to be analysed and exploited for business purposes.

Annex A – Critical security controls

This annex provides a list of the SANS Critical security controls – as detailed in Version 3.1 of the Twenty Critical Security Controls for Effective Cyber Defence: Consensus Audit Guidelines (CAG), published by SANS in October 2011.

- Control 1: Inventory of Authorised and Unauthorised Devices
- Control 2: Inventory of Authorised and Unauthorised Software
- Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- Control 4: Continuous Vulnerability Assessment and Remediation
- Control 5: Malware Defenses
- Control 6: Application Software Security
- Control 7: Wireless Device Control
- Control 8: Data Recovery Capability
- Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Control 12: Controlled Use of Administrative Privileges
- Control 13: Boundary Defense
- Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs
- Control 15: Controlled Access Based on the Need to Know
- Control 16: Account Monitoring and Control
- Control 17: Data Loss Prevention
- Control 18: Incident Response Capability
- Control 19: Secure Network Engineering
- Control 20: Penetration Tests and Red Team Exercises

For more information on the Critical Security Controls – www.sans.org/critical-security-controls/