QinetiQ

EMERGING TECHNOLOGIES

APRIL 2015

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, CESG, QinetiQ or those acting on their behalf. 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contained within this document is believed to be accurate at the date of publishing but is expected to become outdated quickly (particularly in areas where research and development is occurring more rapidly).

This material is provided for general information purposes only. You should make your own judgement as regards use of this material and seek independent professional advice on your particular circumstances. To the fullest extent permitted by law, QinetiQ, CPNI, CESG and each and every author or contributor to this document excludes all liability for loss or damage caused by an error or omission in this guidance or caused by any person relying on or otherwise using the information contained in the guidance or its references. This exclusion applies however the loss or damage is caused including where it is the result of negligence.

Supported by

CPNI
Centre for the Protection
of National Infrastructure

CESG

Contents

Introduction

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

About This Document

This document is composed of short summaries of technologies, also referred to as forecasts.

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

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 relevance to protective security. All of the technology pieces have been written and compiled 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.

Technologies and Techniques

This work covers technologies primarily within the Cyber 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 at three, five and ten years from time of writing (April 2015).

Enhanced Protection / Security Compromise

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

a) Offer an opportunity to enhance existing protective security measures.

b) Present an opportunity to compromise protective security measures.

c) Both of the above.

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

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

Security Resources

A number of resources are available to assist organisations with improving cyber defences. Resources include the Critical Security Controls[1], the 10 Steps to Cyber Security[2] and the Cyber Essentials[3].

Each technology within this document is linked to one or more Cyber Security Controls – for this work we have directly referenced against the Critical Security Controls. The Controls given are only those assessed as being of most relevance.

QinetiQ's Technology Map

QinetiQ's 'technology maps' are designed to be short but 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.

[1] *Critical Controls for Effective Cyber Security, Centre for Internet Security, http://www.cisecurity.org/*

[2] *10 Steps to Cyber Security, Cyber Security Guidance for Business, https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility*

[3] *Cyber Essentials, https://www.cyberstreetwise.com/cyberessentials/*

Advanced Threat Detection

Description

Advanced Threat Detection is a set of technologies that are used to aid the detection of computer network intrusions that are part of targeted attacks, typically conducted by well-resourced adversaries such as nation-states, state-sponsored groups or organised criminals. Such adversaries will initially attempt to use simple methods to access systems, for example by exploiting poor patching or misconfiguration of target infrastructure. If the target has implemented good cyber defences – then these approaches will prove difficult and the adversary will employ advanced tools, techniques and procedures.

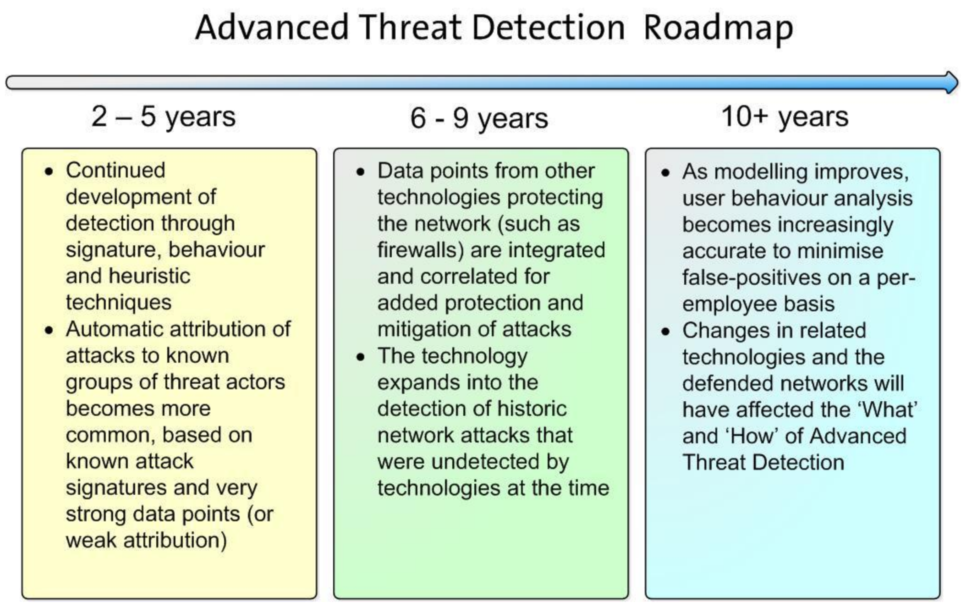
During a targeted attack, in-depth knowledge of a target will be collected and will be used to evade traditional security measures. Advanced Threat Detection is used to detect activity by adversaries that have knowledge of undisclosed vulnerabilities and resources to develop and deliver exploits. Vulnerabilities that are unknown to the vendor or the security community will be exploited. These are known as "zero-day vulnerabilities" and conventional signature-based detection (including anti-virus and network monitoring devices) will not detect attempts to exploit them.

Current Advanced Threat Detection focuses on detecting attacks in the Delivery, Exploitation, Installation and Command and Control stage of a Cyber-attack (See Source 1 below for more details of these stages).

Most Advanced Threat Detection solutions use a mixture of software and hardware-based sandbox capabilities in order to detect exploitation. A sandbox is a virtual environment, in which an un-trusted application can be executed, or file from an untrusted source can be opened. Once the file or application is under test, the behaviour of the system (programs, operating system and network connections) can be monitored to detect any unusual, abnormal or malicious behaviour. Other solutions can use correlation across large data sets to identify slow but persistent attacks and behaviour that do not trigger specific rules in conventional defences, but still indicate an attack or compromise.

Most Relevant Cyber Security Controls

- Malware Defences



Advanced Threat Detection Roadmap

2 – 5 years

- Continued development of detection through signature, behaviour and heuristic techniques
- Automatic attribution of attacks to known groups of threat actors becomes more common, based on known attack signatures and very strong data points (or weak attribution)

6 - 9 years

- Data points from other technologies protecting the network (such as firewalls) are integrated and correlated for added protection and mitigation of attacks
- The technology expands into the detection of historic network attacks that were undetected by technologies at the time

10+ years

- As modelling improves, user behaviour analysis becomes increasingly accurate to minimise false-positives on a per-employee basis
- Changes in related technologies and the defended networks will have affected the 'What' and 'How' of Advanced Threat Detection

Relevant Applications

Advanced Threat Detection technologies should be adopted on networks and systems containing sensitive information, as an added layer of defense against attacks from advanced adversaries.

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: Continued development of detection through signature, behaviour and heuristic techniques. Automatic attribution of attacks to known groups of threat actors becomes more common, based on known attack signatures and very strong data points (or weak attribution).

Within 6 – 9 years: Data points from other technologies protecting the network (such as firewalls) are integrated and correlated for added protection and mitigation of attacks. Technology expands into the detection of historic network attacks that were undetected by technologies at the time.

10+ years: As modelling improves, user behaviour analysis becomes increasingly accurate to minimise false-positives on a per-employee basis. Changes in related technologies and the defended networks will have affected the 'What' and 'How' of Advanced Threat Detection.

General Issues and Challenges

With the increase in functionality and complexity of modern firmware, operating systems and application software, vulnerabilities will always be present. Efforts to improve the way in which software is developed are ongoing with efforts such as the Trustworthy Software Initiative (TSI). However, vulnerabilities will continue to be an issue and creates a constant race to identify vulnerabilities and patch to prevent potential breaches. Advanced adversaries will identify vulnerabilities and develop exploits, which will eventually become part of the toolkit of less advanced adversaries. Today's advanced threat eventually becomes tomorrow's common (but no less dangerous) threat.

Adversaries will often utilise malware in order to achieve their goal. Malware is moving to "Malware-as-a-Service" and adversaries are monitoring the development of Advanced Threat Detection products. Malware is being developed to be sandbox aware with anti-sandbox techniques that supress malicious behaviour to evade Advanced Threat Detection systems. Adversaries are increasingly using cryptography in order to evade signature-based detection and make analysis harder.

Most Advanced Threat Detection solutions heavily focus on detecting attacks in the delivery stage via vectors such as phishing emails and do not currently monitor less common delivery routes, such as USB or hardware implants. Some products are primarily focussed on addressing risks to the most common business systems, meaning that their coverage of protocols and behaviour patterns seen on more specialist systems (particularly SCADA) may be lower than for those used more widely within commercial organisations.

The attack surface of a modern network (and its users) is such that some attacks will inevitably be successful. This means that post-attack solutions can still be useful, but need to be able to alert as soon as possible to minimise the impact and damage.

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

Lockheed Martin’s Computer Incident Response Team has created an intelligence-driven defence process, Cyber Kill Chain®, which allows information security professionals to proactively remediate and mitigate advanced threats in the future.

Source 1: Lockheed Martin “Cyber Kill Chain®”: http://www.lockheedmartin.co.uk/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html, accessed 20 March 2015.

Given the threat of advanced targeted attacks, also known as advanced persistent threats (APTs), Gartner has produced a document that provides security managers with a framework to select and deploy the most-effective threat defence technologies. The key findings of this paper include the following:

- *“The traditional defence-in-depth components are still necessary, but are no longer sufficient in protecting against advanced targeted attacks and advanced malware.”*
- *“Today's threats require an updated layered defence model that utilizes "lean forward" technologies at three levels: network, payload (executables, files and Web objects) and endpoint.”*
- *“Combining two or all three layers offers highly effective protection against today's threat environment.”*

Source 2: Gartner, **‘**Five Styles of Advanced Threat Defense’, Orans L., D’Hoinne J., G00253559, 20 August 2013, reviewed 13 October 2014.

Standards and policy (Government and non-Government)

There are no formal documented standards or policies produced by either Government or Industry on Advanced Threat Detection. However, documents such as the Council on Cyber Security’s Top 20 Critical Controls for effective Cyber Defence (formerly SANS controls) look at key technologies that will aid detection and investigation when dealing with advanced threats.

Gartner has produced a best practice document for mitigating against Advanced Persistent Threats and a report on the “styles” of defence and the areas that these technologies cover (see Information Sources). While these documents are neither formal standard nor policy, they can inform best practice thinking.

QinetiQ comment

QinetiQ recommends the use of Advanced Threat Detection solutions as part of a wider Cyber Defence strategy. An Advanced Threat Detection solution on its own is not a sufficient defence, as a highly motivated persistent adversary will find a way to evade such a solution and defenders must be able to react accordingly.

Affective Computing and Emotion Recognition

Description

Affective Computing is a field of computing that is concerned with the study and development of systems and devices that can recognise, interpret, process, and simulate human affect. It researches the recognition of human emotion by machines and also the means through which machines can understand emotion and express it.

The emotional state of the user can be assessed from a number of indicators, such as the tone of speech, facial features, body postures and physiological measures such as Skin Conductance Level (SCL), respiration and heart rate analysis (see Source 1).

There is increasing interest in techniques that combine multiple indicators or modalities. For example, recent research has looked at automated techniques to detect users' affective states from a fusion model of facial videos and physiological measures (see Source 2).

One of the primary goals of Affective Computing research is to improve Human Computer Interaction (HCI). If Affective Computing systems can support functions such as attention, memory and decision-making then the ‘emotion modality’ will be a valuable addition to HCI in future command and control environments.

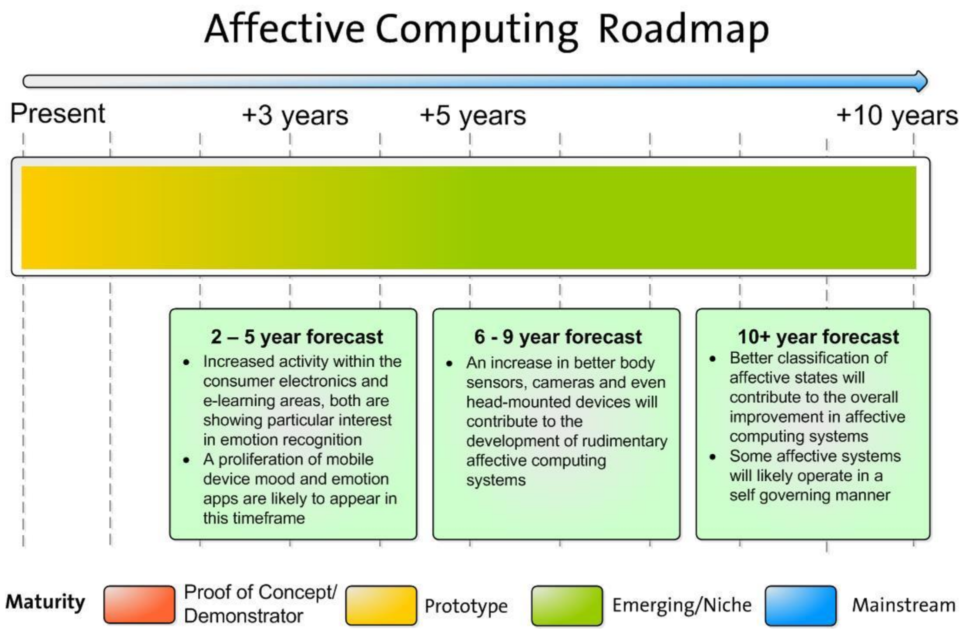
Besides HCI there are a growing number of other applications that could potentially benefit from the technology, these are listed below.

Relevant Applications:

- Biometric surveillance systems – there have been a number of studies concerning the role of affective computing in surveillance (see Source 3).
- Robotics - Affective Computing could endow robots with the ability to communicate so they can perceive human emotion, adapt their behaviour to humans, and sense situations even without explicit instructions.
- Training and simulation – emotion Recognition could enable social interaction between human and machines - enabling machines to behave more realistically.
- User behaviour monitoring – (see Source 4).
- Learning and education - advanced learning systems are being developed that are exploiting aspects of affective computing to adjust teaching styles according to the detected psychological state of the student.

Most Relevant Cyber Security Controls

- Wireless Access Control
- Security Skills Assessment and Appropriate Training to Fill Gaps
- Controlled Use of Administrative Privileges
- Controlled Access Based on the Need to Know
- Secure Network Engineering



2 – 5 year forecast

- Increased activity within the consumer electronics and e-learning areas, both are showing particular interest in emotion recognition
- A proliferation of mobile device mood and emotion apps are likely to appear in this timeframe

6 - 9 year forecast

- An increase in better body sensors, cameras and even head-mounted devices will contribute to the development of rudimentary affective computing systems

10+ year forecast

- Better classification of affective states will contribute to the overall improvement in affective computing systems
- Some affective systems will likely operate in a self governing manner

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: There is likely to be increasing activity within the consumer electronics and e-learning areas, both are showing particular interest in Emotion Recognition. This activity is driven, to a large extent, by changes to the user interface, which is the current competitive factor in mobile devices such as smart phones and smart watches. A proliferation of mobile device mood and emotion apps are likely to appear in this timeframe.

Within 6 – 9 years: An increase in better body sensors, cameras and even head-mounted devices such as Google Glass will contribute to the development of rudimentary affective computing systems.

10+ years: During the same period, computational intelligence techniques and machine learning should have advanced sufficiently to make significant improvements to pattern matching and the processing and analysis of the large sample sets e.g. of facial expressions. Better classification of affective states will result. This will contribute to the overall improvement in Affective Computing systems. The more advanced affective-based systems will be able to deal with more challenging problems/decisions (such as affective evaluations, ethical quandaries, and other innovations) in a self-governing manner.

General Issues and Challenges

Affective Computing is an emerging technology and is still very much a topic of research. There are a number of issues and challenges that are proving difficult to overcome. The success of emotion recognition will always be measured on the accuracy of correctly classifying emotion and as a result these issues are having a significant negative impact on success.

Information Sources, Supporting Extracts and Quotations (Websites, Forums, Publications etc.)

A good overview of Affective Computing maybe found on Wikipedia. This introduces the main areas supporting and enabling affective computing, namely: emotional speech, facial expression, body gesture and physiological monitoring.

Source 1: Affective Computing, http://en.wikipedia.org/wiki/Affective_computing, accessed 11 Dec 2014.

This research study introduces automated techniques to detect users' affective states from a fusion model of facial videos and physiological measures.

Source 2: Monkaresi H. et al.: ‘Classification of Affects Using Head Movement, Skin Colour Features and Physiological Signals’, IEEE International Conference on Systems, Man, and Cybernetics, October 14-17, 2012, COEX, Seoul, Korea. 2012.

This paper describes how visual surveillance systems based on affect recognition could play an important role in the development of future HCI biometric systems. Facial expression representing individual’s emotional state could be perceived by analysing real-time images captured from security cameras.

Source 3: Wang R., Fang B.: ‘Affective Computing and Biometrics Based HCI Surveillance System, IEEE International Symposium on Information Science and Engineering, 2008.

This paper proposes a browser extension utilising affective feedback to provide warnings on detection of risky behaviour. The paper concludes that a solution utilising a browser extension is a suitable method of monitoring potentially risky security behaviour. Ultimately, future work seeks to implement an affective feedback mechanism within the browser extension with the aim of improving security awareness.

Source 4: Shepherd L.A. et al.: ‘Reducing Risky Security Behaviours: Utilising Affective Feedback to Educate Users’, Proceedings of Cyber-forensics 2014, https://personal.cis.strath.ac.uk/george.weir/.../1_shepherd.pdfCached, accessed 12 Dec 2014.

The origins of much of the recent work on affective computing stem from the seminal work conducted by Prof Rosalind Picard who leads the MIT Media Lab's Affective Computing Group. This group is researching new techniques that enable computers to assess human states such as frustration, stress and mood and appropriately modify their response to improve HCI.

Source 5: Affective Computing, MIT Media Labs, http://affect.media.mit.edu/, accessed 11 Dec 2014.

Standards and policy (Government and non-Government)

Affective computing is in an early stage of development, but some efforts at standardisation are evident. The Emotion Markup Language (EmotionML) 1.0, is undergoing standardisation at the World Wide Web Consortium (W3C). The language will represent emotion and related affective states.

QinetiQ comment

Although rudimentary forms of Affective Computing are appearing, multimodal (multi-sensor) forms of the technology are still in a proof of concept phase. The centre of excellence for research in this field is the MIT Media Lab's Affective Computing Group. (Source 5) and their research output shows the many areas where this technology could be applied. The technology (and emotion detection in particular) certainly offers promise in areas such as surveillance and user behaviour monitoring, but there will be many obstacles to overcome, not just in terms of development of the technology, but also in terms of ethics and privacy.

Automotive Electronic Systems Vulnerabilities

Description

Recent years have witnessed a sharp increase in the number of automotive electronics systems installed within vehicles. This trend is continuing and the media now talks about the “Digital Car” which is as much a software product as hardware product and where connectivity is a key factor (see Source 1). The “Digital Car” is essentially a mobile network with complex computer systems and with interfaces to other electronic computing devices and systems external to the vehicle. As such, it is vulnerable to Cyber-attack.

Automotive electronics systems are distributed systems with a number of components that include the Engine Control Unit (ECU), Driver Display Units, Driver Assistance Systems and the In-Vehicle “Infotainment” (IVI) System. The latter delivers both entertainment and information (such as navigation), and can enable the driver to control and monitor elements through devices (such as a smartphone), voice commands and/or touchscreens. The IVI can often access external information sources (such as weather reports, traffic information etc.) making them vulnerable to attack.

Increased connectivity (through the addition of Wireless LANs (Local Area Networks) and Ethernet) and eventually more widely through the emergence of the “Internet of Things” (IoT), could lead to other vulnerable devices being used as a conduit to attack motor vehicles, or vice versa. The increased adoption of “smart machine” technologies within automotive systems will enable vehicles to have greater autonomy. Both trends are likely to lead to a significant change in the risk profile of automotive systems.

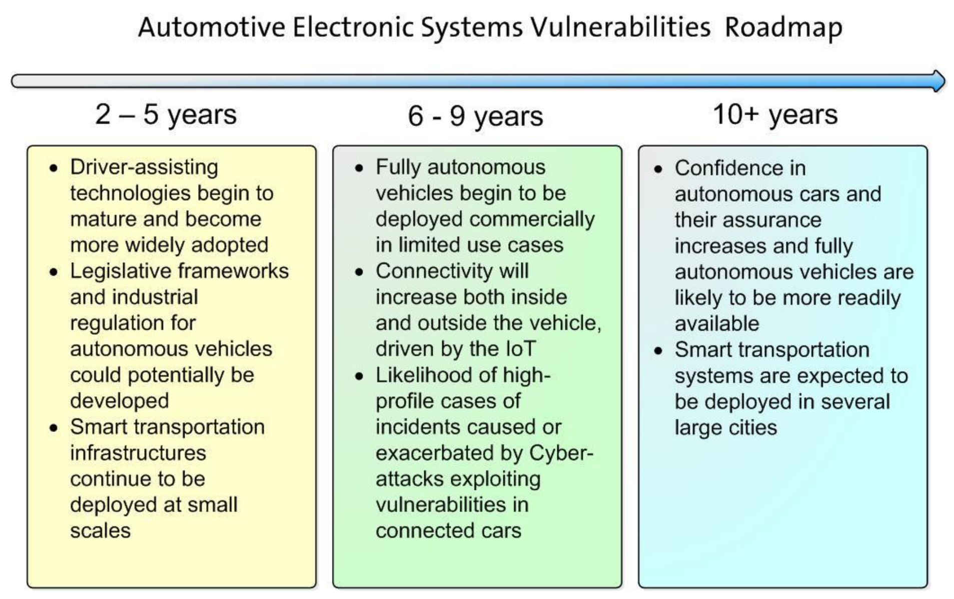
Most Relevant Cyber Security Controls

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Malware Defences
- Wireless Access Control
- Data Recovery Capability
- Limitation and Control of Network Ports, Protocols, and Services
- Controlled Use of Administrative Privileges
- Maintenance, Monitoring, and Analysis of Audit Logs
- Controlled Access Based on the Need to Know
- Secure Network Engineering

Relevant Applications

The following are current and emerging examples where automotive electronics can support the vehicle's occupants:

- **Driver Assistance**. Technologies such as Lane Departure Warnings, Adaptive Cruise Control and Mood Awareness can issue warnings or offer partial automation.
- **Keyless entry and ignition**. Near-field communication (NFC) can be used to unlock doors and start cars based on the proximity of a token (such as a key fob) or a smartphone.
- **Integration with Smart Homes**. Cars communicating with "Smart Homes" could allow garage doors, alarm systems, heating or lighting to be controlled by the car on the user's behalf, based on their location.
- **Smart Transportation**. Speed and location data can be shared with other vehicles to provide information about traffic conditions. Active traffic management, road pricing and parking information could also be based on real-time traffic conditions, perhaps shared via mesh networks.



Automotive Electronic Systems Vulnerabilities Roadmap

2 – 5 years

- Driver-assisting technologies begin to mature and become more widely adopted
- Legislative frameworks and industrial regulation for autonomous vehicles could potentially be developed
- Smart transportation infrastructures continue to be deployed at small scales

6 - 9 years

- Fully autonomous vehicles begin to be deployed commercially in limited use cases
- Connectivity will increase both inside and outside the vehicle, driven by the IoT
- Likelihood of high-profile cases of incidents caused or exacerbated by Cyber-attacks exploiting vulnerabilities in connected cars

10+ years

- Confidence in autonomous cars and their assurance increases and fully autonomous vehicles are likely to be more readily available
- Smart transportation systems are expected to be deployed in several large cities

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: Driver-assisting technologies begin to mature and become more widely adopted, with smartphones and wearable computing devices (such as the smartwatch) becoming much more integrated with automotive electronic systems (for example see Source 4). Legislative frameworks and industrial regulation for autonomous vehicles may be developed. Smart transportation infrastructures continue to be deployed at small scales.

Within 6 – 9 years: Autonomous vehicles begin to be deployed commercially in limited use cases; the automation and deployment of driver-assisting technologies continues. Connectivity within cars will increase dramatically through Ethernet and wireless LAN technology. At the same time, there is likely to be more connectivity outside the vehicle, with vehicles communicating with each other and the wider infrastructure through the IoT. Smart transportation techniques are likely to become more integrated, both across systems and with vehicles. By this time high-profile cases of incidents caused or exacerbated by cyber-attacks exploiting vulnerabilities in connected cars will likely receive major media attention.

10+ years: As confidence in autonomous vehicles and their assurance increases, fully autonomous vehicles are likely to be more readily available. Smart transportation systems are expected to be deployed in several large cities.

General Issues and Challenges

Connectivity and communication with external computer devices and systems increases the capability of automotive technology but also the attack surface of the car and the potential for exploitation. Interfering with the control of a car obviously has large potential to cause physical damage and harm. Increased connectivity also provides opportunities for cars to be targeted or used as part of cyber-attacks.

Previously, direct physical access to the vehicle was required to exploit vulnerabilities in cars, usually as a means to steal the vehicle and therefore automotive security was mostly focused on preventing theft. However, the current trend of digitisation, increased connectivity and rising complexity of automotive electronic systems has raised the need for security controls that focus on cyber security. Motor vehicles fitted with such systems are now more susceptible to remote attacks through the adoption of technologies including Wi-Fi, Bluetooth and keyless entry systems. It is also possible that vulnerabilities in electronic devices interacting with the vehicle, such as smartphones, could affect the vehicle's security.

As cars become more connected and complex, separation of privilege will be critical; Source 3 describes an attack where basic car functions were tampered with following an initial attack via the in-car CD player. Hypervisor technologies typically associated with virtualisation techniques may help to reduce this risk.

As the IoT and the idea of "Smart Cities" develop, it is likely that active traffic management techniques and vehicle-to-vehicle communications will be available, but they may lead to privacy concerns if information concerning the drivers' location is required. Another concern is the possibility that vulnerabilities in individual cars could be leveraged to affect an entire city's transport systems.

The integration of cars into the Smart Home and IoT (see Source 5) offers great increases in functionality, but the level of assurance typically present in these devices is currently much below what could be required for applications to automotive security. Machine-to-machine services and maturing security technologies for the IoT may provide some solutions.

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

Prime Research, a communications research and consulting company, has produced an overview of automotive trends and has recognised the concept of the "Digital Car". Their "World Car Trends 2014" study identifies in-car electronics and connectivity as becoming increasingly important. To quote:

"For 71% of automotive journalists, connectivity already is or is quickly becoming a key factor in evaluating a car."

Furthermore, they note that:

"Cars are no longer only hardware, they are also software products. Cars already have more lines of code than aircrafts and operating systems like Windows 8 or Apple Tiger."

Source 1: Prime Research, 'World Car Trends 2014', New York, April 2014, www.world-car-trends.com/download.php, accessed 17 March 2015.

This article highlights the need to move from physical to Cyber protection for cars. To quote:

"Half the cars broken into in London last year were hacked, not forced open, according to the Met Police."

Source 2: 'Half Of All Stolen Cars Are Hacked' Says Met Police', The Huffington Post UK, 8 May 2014, http://www.huffingtonpost.co.uk/2014/05/08/hacked-cars_n_5286590.html, accessed 19 March 2015.

At Defcon 2013, Charlie Miller gave a presentation about exploitable automotive vulnerabilities.

Source 3: Miller C., Valasek C.*:* 'Charlie Miller to tell Vegas punters how to hack your car', 25 June 2013, http://www.theregister.co.uk/2013/06/25/miller_car_hacking/, accessed 19 March 2015.

Smartphones can be used to control many aspects of high-end vehicles, for example Jaguar describe their InControl Remote system as follows:

"Jaguar InControl Remote allows users of iOS and Android smartphones to connect to the car from wherever they are and control a range of vehicle functions. These include seven-day timed pre-setting of the XE's climate control system, locking or unlocking the doors, or starting the engine."

Source 4: Jaguar Media Centre, 'The New Jaguar XE: Better-Connected by Far', 19 August 2014, http://newsroom.jaguarlandrover.com/en-in/jaguar/news/2014/08/jag_xe_incartech_release_190814/, accessed 19 March 2015.

This article describes the integration of cars into "Smart Homes"

Source 5: Nayak M.: 'AT&T to hook up its automated home and connected car services', Reuters, 2 March 2015, http://www.reuters.com/article/2015/03/02/us-at-t-connectedcar-idUSKBN0LY0MX20150302, accessed 19 March 2015.

The European Commission requested the standardisation of some aspects of connected car technologies, recognising the value that they may offer:

"Direct communication between vehicles and infrastructures will ensure safer and more efficient traffic flows, with great benefits for drivers & pedestrians, our environment and our economy."

Source 6: Kroes N.: 'New connected car standards put Europe into top gear', European Commission Press Release, 12 February 2014, http://europa.eu/rapid/press-release_IP-14-141_en.htm, accessed 19 March 2015.

Source 7: UK Government Policy Paper 'Driverless cars in the UK: a regulatory review', 11 February 2015. https://www.gov.uk/government/publications/driverless-cars-in-the-uk-a-regulatory-review, accessed 11 February 2015.

Standards and policy (Government and non-Government)

There are a number of standards of relevance, of which the following are illustrative.

ISO 26262 (a derivative of IEC 61508) is a standard that defines functional safety requirements for automotive electrical and electronic systems.

In 2014, ETSI and CEN specified a basic set of standards for Cooperative Intelligence Transport Systems, which includes connected cars and intelligent infrastructure. The ISO 15638 series "Telematics Applications for Regulated commercial Vehicles" includes standards compatible with these systems. IEEE 802.11p specifies wireless access in vehicular environments to support vehicle-to-vehicle and vehicle-to-infrastructure (V2X) communications.

The UN Working Party on Road Traffic Safety has agreed an amendment to the 1968 Convention on Road Traffic to allow autonomous cars, provided that the system can be overridden or switched off by the driver.

The GENIVI Alliance is a non-profit industry alliance targeting the adoption of an In-Vehicle Infotainment (IVI) open-source development platform.

Finally, it is worth noting that in February 2015 the UK Government released a policy paper for driverless cars in the UK (see Source 7).

QinetiQ comment

The changing risk profile of automotive electronic systems is not well understood. Security, reliability and privacy concerns have the potential to hold back the development of these technologies. Although there is some awareness of automotive vulnerabilities, a more coherent approach to tackling this problem is required from industry. Eventually, high-end automotive electronics technology will appear in more affordable vehicles and become much more widespread; as this occurs, the possible impact of attacks will drastically increase.

The main interaction with most cars' ECUs is currently by mechanics to provide diagnostic information. As the system becomes more sensitive (e.g. containing the software that provides automated driver-assistance technologies), it may be necessary to partition the system (possibly using virtualisation techniques) so that the automated and autonomous systems can operate at higher assurance levels.

Big Data and Advanced Analytics (for Network Monitoring)

Description

'Big Data' is the term applied to datasets that due to their size are beyond the ability of conventional database software to capture, store, manage and analyse in an efficient manner. Products now exist to store and analyse these massive datasets. These products are often open source, making the software free to use, extend and modify. The current scalability trend is to distribute and process the data across large numbers of modest specification servers, making them more cost-effective than conventional high-end database solutions.

Network monitoring is an essential part of an organisation's security posture, with current generation solutions analysing traffic in near real-time, but this approach has limitations. Advanced Analytics using Big Data technology allows pattern inspection over much longer periods to detect "low and slow" attacks.

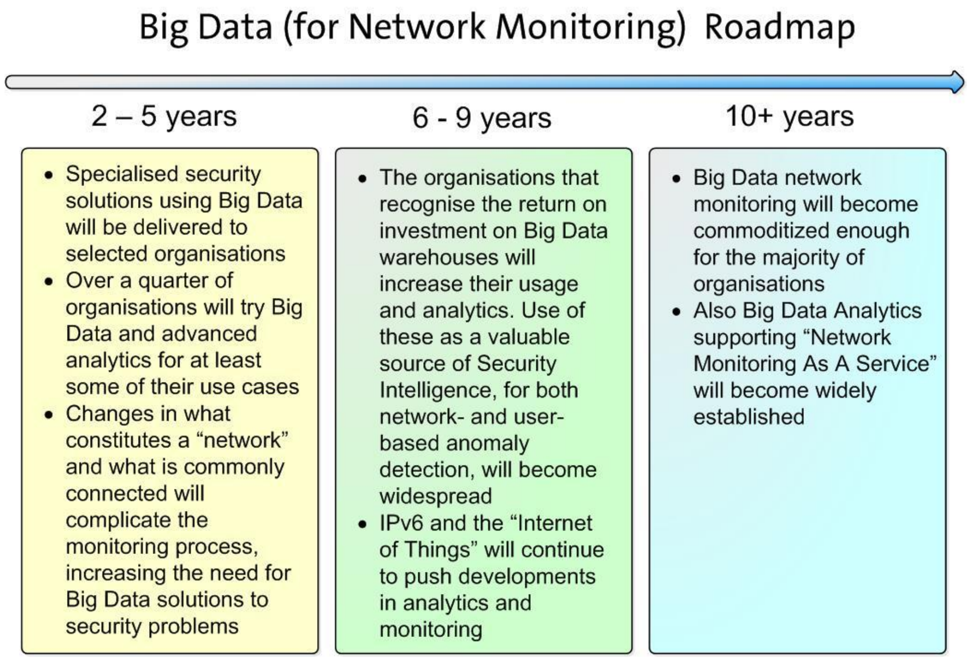
Two market trends currently exist: firstly, specialist security companies are providing their own Big Data solutions for advanced analytics and attack detection; secondly, many large enterprises are beginning to adopt Big Data warehouses for storage of diverse enterprise datasets, which could support security analysis.

Relevant Applications

A Big Data warehouse offers a flexible solution for many kinds of enterprise data. Modern network speeds, increasing file sizes and increased network usage lead to increased data generation that will require Big Data approaches. This plays well with the idea of using a Big Data warehouse for storing and analyzing the data. These techniques are complementary to an existing Protective Monitoring process.

Most Relevant Cyber Security Controls

- Limitation and Control of Network Ports, Protocols, and Services
- Controlled Use of Administrative Privileges
- Boundary Defence
- Maintenance, Monitoring, and Analysis of Audit Logs
- Data Protection
- Incident Response and Management
- Secure Network Engineering



Big Data (for Network Monitoring) Roadmap

2 – 5 years

- Specialised security solutions using Big Data will be delivered to selected organisations
- Over a quarter of organisations will try Big Data and advanced analytics for at least some of their use cases
- Changes in what constitutes a "network" and what is commonly connected will complicate the monitoring process, increasing the need for Big Data solutions to security problems

6 - 9 years

- The organisations that recognise the return on investment on Big Data warehouses will increase their usage and analytics. Use of these as a valuable source of Security Intelligence, for both network- and user-based anomaly detection, will become widespread
- IPv6 and the "Internet of Things" will continue to push developments in analytics and monitoring

10+ years

- Big Data network monitoring will become commoditized enough for the majority of organisations
- Also Big Data Analytics supporting "Network Monitoring As A Service" will become widely established

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: specialised security solutions using Big Data (such as Teradata, QinetiQ's AIW, and Detica CyberReveal) will be delivered to selected organisations. Other organisations will begin to announce similar services and offerings. Some businesses will develop their own solutions. Over a quarter of organisations will try Big Data and advanced analytics for at least some of their use cases. Changes in what constitutes a "network" and what is commonly connected will complicate the monitoring process, increasing the need for Big Data solutions to security problems.

Within 6 – 9 years: organisations that recognise the return on investment on Big Data warehouses will increase their usage and analytics. Use of these as a valuable source of Security Intelligence, for both network and user-based anomaly detection, will become widespread. IPv6 and Internet of Things continue pushing developments in analytics and monitoring - both in terms of the devices, connectivity and volume of data monitored and in the devices and metrics used for monitoring.

10+ years: Big Data network monitoring will become commoditized enough for the majority of organisations. Also Big Data Analytics supporting "Network Monitoring As A Service" will become widely established.

General Issues and Challenges

For many organisations, the "big" part of Big Data is the key issue. The speed and quantity of traffic running across a modern network usually necessitates fast capture and very large storage requirements. Merely having sufficiently fast *and* reliable capture capabilities is only the first step in gaining useful intelligence from the network. There is a potential issue regarding where the data is analysed (centrally or in a more distributed environment) and the associated communications overheads that could arise. The captured data may also be retained for future analysis, as analytics methods improve, necessitating many servers with lots of storage. As the data may be important, systems must also incorporate redundancy, further increasing the required size of the infrastructure. Data will need to be processed once it has been captured, and similarly large-scale analytical methods need to be applied. Many technologies exist in the Big Data space for such processing. Hadoop is the current market leader, and includes a variety of ways of handling the data, including MapReduce and Spark for distributed processing, Hive and Impala for SQL-style querying, Apache Mahout for distributed machine learning, and Hadoop Pig for data flow control and execution. Selecting the right one will depend on the skills available, the analytics required and the investment in learning to use the tools.

The Harvard Business Review webinar on the myths of Big Data highlights the staff-related issues of introducing Big Data. Not only must staff be appropriately trained to properly utilise and analyse Big Data, but the resistance of staff to new techniques and "black box" analytics must be overcome. An emerging job role of "data scientist" (a phrase which has been around for decades, but has risen to the fore in recent years with the rise of Big Data) highlights the differing skills required for working against such large data stores. The individual must be able to determine not only what they want to know, but also how they can discover it, how they can distribute the processing, what it means, whether it is statistically significant, and what analysis actually makes any meaningful sense. Merely allocating software developers and other staff to a Big Data role will not bring the complete benefit from Big Data, as they will not fully understand its implications and constraints.

Not all issues are technical – there are also legal issues to consider. While conventional protective monitoring is accepted as part of operating a network, it generally only records the malicious traffic. A full Big Data solution for network monitoring can record all traffic, whether overtly malicious or not. While this is necessary to allow subsequent analytics to detect previously unknown attacks, it also results in potentially personal communications and data being captured, and hence increased issues relating to the Data Protection Act. As the purpose of the Big Data system is to understand the norm then this sensitive data cannot be discarded as doing so would invalidate analytic results. Instead, a combination of legal precedent, process, policy and protective measures will need to develop to appropriately handle the additional risks. This is obviously in addition to the commercial risk of holding all network communications (which will include all manner of proprietary information from within the organisation) for an extended period.

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

"Many organizations use analytics, but Big Data is a different animal. It requires new technologies and new management approaches to facilitate fast, continuous decision making."

Source 1: Davenport T.: 'Big Data at Work: Dispelling the Myths, Uncovering the Opportunities', Harvard Business Review, 3rd March 2014.

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

"Gartner predicts that by 2016, 25 percent of large global companies will have adopted Big Data analytics for at least one security or fraud detection use case, up from 8 percent today, and will achieve a positive return on investment within the first six months of implementation."

Source 3: Gartner Newsroom Press Release, 6th Feb 2014, http://www.gartner.com/newsroom/id/2663015.

Standards and policy (Government and non-Government)

At the current time (January 2015) the author has no knowledge of any standards and policies related to Big Data. However, in September 2011, 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.

Some de facto standards are emerging in some parts of Big Data technologies, often formed around a single vendor with large investment backing, however no formal standards exist and the development of Big Data technologies is still such that new technologies are likely to supplant current technologies.

QinetiQ comment

Big Data is currently still close to the "peak of inflated expectations" part of the Gartner hype cycle in many areas, where it gains huge investment for nebulous offerings promising coverage of almost every use case. However, there is an inherent kernel of truth in the claims when it is applied to network monitoring: if the correct analytics are used and no data is disposed of then an attack against a network (particularly novel and advanced attacks) are increasingly likely to be detected because the attack must interact with the network. Assuming that the legal issues can be overcome, the main technical issues that need to be addressed to complete on these promises are around how well the data can be captured and whether the analysts can appropriately query that data and understand it, or whether the haystack is too large and complex to be able to reliably find the needle.

Cloud Security *(this forecast covers security of the technology – a forecast on cloud computing has been published previously)*

Description

Cloud computing relies on users sharing resources such as infrastructure platforms or software applications to achieve economies of scale. A cloud can either be public, private or a hybrid solution and the level of security risk will differ between them. This significantly changes the security risk profile when compared to stand-alone systems. Users place considerable trust in the cloud providers, who will manage and maintain their systems to ensure that unauthorised access of information does not occur.

Security and privacy concerns have been a common feature of discussions concerning cloud-based systems (source 5), as have concerns over data ownership and usage rights (source 6). Despite this, cloud computing is attractive because of its ability to take advantage of economies of scale, cope with rapid changes in user requirements, and provide access for users from a wide range of locations and devices.

The Cloud Security Alliance has launched its CSA Security Trust and Assurance Registry (STAR), a registry documenting the security controls provided by various cloud computing providers.

Most Relevant Cyber Security Controls

- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Malware Defences
- Application Software Security
- Data Recovery Capability
- Controlled Use of Administrative Privileges
- Boundary Defence
- Maintenance, Monitoring, and Analysis of Audit Logs
- Controlled Access Based on the Need to Know
- Data Protection
- Incident Response and Management
- Secure Network Engineering

Relevant Concepts

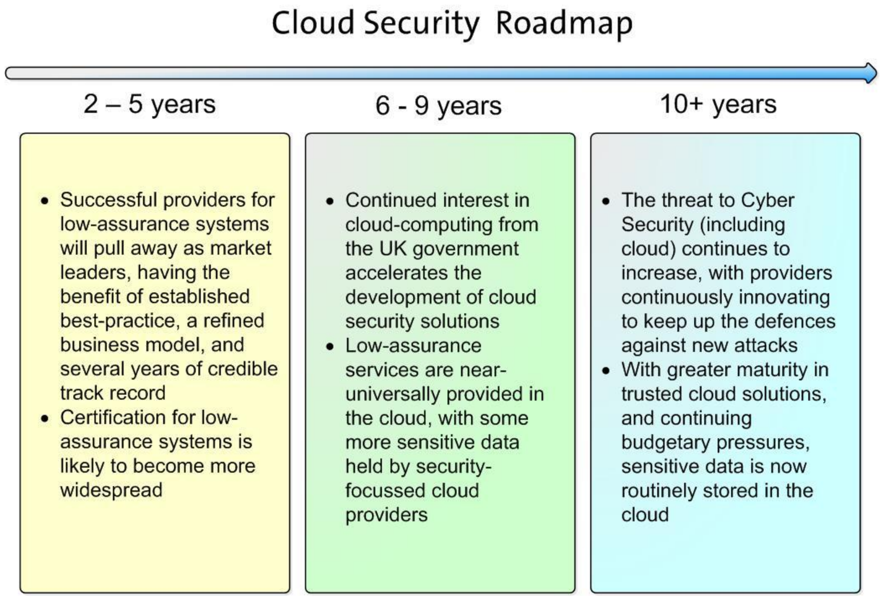
Assurance: Users and providers of cloud services need systems to assess the security and continuity offered by those systems in order to have confidence in their performance.

Identity Management: User authentication and the ability to bind identities to user attributes (across diverse locations and devices) avoiding unauthorised access to cloud-based systems.

User Separation: Ensuring that other users cannot affect the memory and processes of one user is typically achieved using a hypervisor.

Encryption: If data is encrypted, there will be greater confidence on the part of the user that the cloud provider (or other users) will be unable to access their data held in the cloud.

Resilience: In addition to the physical infrastructure and non-virtualised servers, the recoverability of virtual machines is critical in cloud-based systems.



Cloud Security Roadmap

2 – 5 years

- Successful providers for low-assurance systems will pull away as market leaders, having the benefit of established best-practice, a refined business model, and several years of credible track record
- Certification for low-assurance systems is likely to become more widespread

6 - 9 years

- Continued interest in cloud-computing from the UK government accelerates the development of cloud security solutions
- Low-assurance services are near-universally provided in the cloud, with some more sensitive data held by security-focussed cloud providers

10+ years

- 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 routinely stored in the cloud

General Issues and Challenges

Perhaps the largest issue relating to cloud security is that of assurance; it is necessary to trust the cloud provider to provide appropriate security mechanisms. This includes mechanisms relating to the confidentiality, integrity and availability of user information, but also the operational, personnel, and supply-chain security. Certification frameworks are being developed and as these frameworks mature, greater trust will be placed in cloud-based solutions. The inconvenience of current risk assessment processes is currently inhibiting the cloud computing market.

Identity management is an area in which rapid progress is being made; weak authentication and access control may allow unauthorised changes to a consumer's service, theft or modification of data, or denial of service. Two-factor authentication and federated identity management is becoming more common and we may eventually see public identity providers able to give very strong user authentication.

Ensuring that users cannot affect the data and processing of other users sharing the same cloud infrastructure is a critical concern; compromising the hypervisor potentially compromises all processes and data on that cloud-based system. The development of high-assurance hypervisors and the necessary protections to avoid successful attacks or the bypassing of the hypervisor is a difficult problem.

The implementation of cryptographic protection for data in the cloud is maturing. There has been great commercial interest in tokenisation (replacing sensitive data with a surrogate value, known as a token), driven by compliance with PCI Data Security Standards. Secure deduplication, private information retrieval, and fully homomorphic encryption are mainly of academic interest at the moment, but potentially offer great advantages to both users and providers, as they allow users to encrypt data so that the provider cannot access it, but so that the provider can de-duplicate, search, or process the data on behalf of the user.

As cloud-based services become more widely used, there is a risk that the data centres will become targets; the frequency and sophistication of cyber-attacks is rapidly increasing. Resilience against data loss and mechanisms for ensuring business continuity are also important considerations for cloud-based solutions.

One issue that is becoming very prominent is the question of which legislative framework applies to data held on servers in one country, operated by a cloud provider (perhaps based in another), on behalf of a user (maybe in a third country) (see Source 7 below). The locations at which consumer data is stored, processed and managed must be identified so that organisations can understand the legal circumstances should their data be accessed without their consent.

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

The IT analyst, Gartner has produced one of its "Hype Cycles" devoted to Cloud Security. To quote:

"Those who are looking for a "quick fix" to cloud security concerns need to recognize that this is an immature product and practice space, with many product types that are not expected to reach full maturity within the next five years."

Source 1: Gartner, 'Hype Cycle for Cloud Security, 2014', Heiser J., G00260756, 25 July 2014.

The UK Government published its Cloud Strategy as part of its ICT Strategy in 2011. To quote:

"These [cloud-based] solutions must balance the need to be open, accessible and usable with the growing cyber security threat and the need to handle sensitive information with due care."

Source 2: HM Government 'Government Cloud Strategy', March 2011,

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266214/government-cloud-strategy_0.pdf , accessed 27 January 2015.

The CSA Security, Trust & Assurance Registry (STAR) is a publicly accessible registry that documents the security controls provided by various cloud computing services. To quote:

"CSA believes that encouraging transparency and positive competition among cloud providers, with security as a market differentiator, is the right way to think about security in our computer systems."

Source 3: CSA Cloud Security Alliance Website, https://cloudsecurityalliance.org/star/#_faq , accessed 27 January 2015.

Further useful sources:

Source 4: The NIST definition of cloud computing - http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf , accessed 28 January 2015.

Source 5: Editorial on the privacy concerns relating to the cloud - http://cacm.acm.org/magazines/2011/1/103200-cloud-computing-privacy-concerns-on-our-doorstep/fulltext , accessed 28 January 2015.

Source 6: Editorial on data ownership and usage rights in the cloud - http://articles.latimes.com/2012/apr/26/business/la-fi-tech-savvy-cloud-services-20120426, accessed 28 January 2015.

Source 7: Article on applying legislative frameworks to data in the cloud - http://www.theguardian.com/technology/2014/apr/29/us-court-microsoft-personal-data-emails-irish-server, accessed 28 January 2015.

Standards and policy (Government and non-Government)

The UK Government continues to encourage the use of cloud-based systems; the “Cloud-First Policy” requires public sector organisations to consider and fully evaluate potential cloud solutions in addition to considering any other option. The Digital Marketplace (https://digitalmarketplace.blog.gov.uk/) is designed to facilitate the public sector buying cloud-based services. CESG offers a `Pan-governmental Accreditation Scheme’ to help manage the risks relating to shared infrastructure and services. CESG and the Home Office have released (a beta version of) a `Guide to Cloud Security Principles’.

A number of ISO/IEC standards are being applied to cloud service providers as part of formal third-party assessments: ISO/IEC 27001 is becoming the norm for cloud services targeting enterprises; ISO/IEC17017 is being developed to add specific controls relating to cloud security to ISO/IEC 27002; ISO/IEC 27018 will address privacy in the public cloud. The Cloud Standards Customer Council is an end user advocacy group aiming to accelerate the adoption of the cloud, by working to resolve issues relating to standards, security, and interoperability.

OAuth 2.0 was standardised by the IETF in 2012 and is beginning to be deployed, increasing the maturity of user authentication for cloud-based services.

QinetiQ comment

The ability for public cloud-based resources to be used to launch attacks (such as DDOS, malware, or attacks against cryptographic schemes) has also increased; this massively increases the computing power available for these purposes and it is not currently clear how providers can protect against this threat or what recourse would be available to organisations under attack in these circumstances.

Computer Network Defence (CND)

Description

Computer Network Defence (CND) is the name given to a range of measures and actions taken to monitor and protect a network against internal and external attacks that aim to disrupt operations, or corrupt or compromise information and computers on that network. It is the cyber security equivalent of real-world mechanisms such as guards, fences, CCTV cameras and operating procedures.

At its simplest and least effective level, CND uses logs and periodic checks to ascertain whether unauthorised activities have taken place. Intrusion Detection Systems (IDS) and other active monitoring sources aimed for nearer real-time detection. In the past, this was an adequate approach when anomalies could be identified by signature or simple heuristics, but the rise in Advanced Persistent Threats (APTs) and Advanced Evasion Techniques (AETs) that can go undetected by hiding below the noise threshold, reduces its effectiveness. New approaches involving large-scale correlation and Big Data Analytics are now emerging to address these threats.

Relevant Applications

CND is an essential component of any system where the services provided, or the data held and processed, are of value. Use of shared network services and rich interconnectivity means as well as operational systems, other apparently less critical applications must also be well protected and monitored. All networks that are critical to operations should have a high degree of CND design, planning and infrastructure.

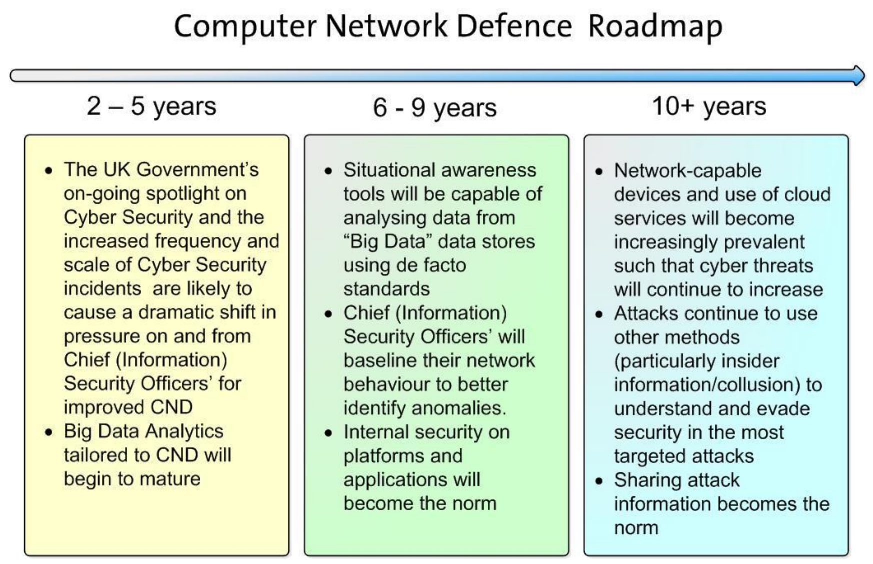
Most Relevant Cyber Security Controls

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Malware Defences
- Wireless Access Control
- Secure Configurations for Network Devices such as Firewalls, Routers…
- Limitation and Control of Network Ports, Protocols, and Services
- Controlled Use of Administrative Privileges
- Boundary Defence
- Maintenance, Monitoring, and Analysis of Audit Logs
- Controlled Access Based on the Need to Know
- Account Monitoring and Control
- Incident Response and Management
- Secure Network Engineering

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: The UK Government's on-going spotlight on cyber security and the increased frequency and scale of cyber security incidents that hit the mainstream media are likely to cause a dramatic shift in pressure on and from Chief (Information) Security Officers' (CSO/CISO) for improved CND. Solutions based on "Big Data Analytics" for CND for detecting advanced attack and post-incident forensic analysis will begin to mature. The need for internal security to monitor applications, desktops, smart tablets, and smart phones will become the focus of industry solutions and CND approaches. The majority of CISOs/CSOs will continue with currently available standards and existing products.

Within 6 – 9 years: Analytics-based approaches to identify APTs and AETs on a network are likely to be used by mature mainstream products. Situational awareness tools will be capable of analysing data from "big data" data stores using de facto standards. CSOs/CISOs will baseline their network behaviour to better identify anomalies. Internal security on platforms and applications will become the norm. Use of formal standards and policies within organisations becomes more common in more industries.



Computer Network Defence Roadmap

2 – 5 years

- The UK Government's on-going spotlight on Cyber Security and the increased frequency and scale of Cyber Security incidents are likely to cause a dramatic shift in pressure on and from Chief (Information) Security Officers' for improved CND
- Big Data Analytics tailored to CND will begin to mature

6 - 9 years

- Situational awareness tools will be capable of analysing data from "Big Data" data stores using de facto standards
- Chief (Information) Security Officers' will baseline their network behaviour to better identify anomalies.
- Internal security on platforms and applications will become the norm

10+ years

- Network-capable devices and use of cloud services will become increasingly prevalent such that cyber threats will continue to increase
- Attacks continue to use other methods (particularly insider information/collusion) to understand and evade security in the most targeted attacks
- Sharing attack information becomes the norm

10+ years: Network-capable devices and the use of cloud services will become increasingly prevalent such that cyber-threats will continue to increase. Tool and service providers continuously innovate to keep up the defences against new attacks. Attacks continue to use other methods (particularly insider information/collusion) to understand and evade security in the most targeted attacks. Shared data warehouses will becomes widespread offering new opportunity for data mining for CND purposes. Sharing attack information becomes the norm.

General Issues and Challenges

CND is an on-going, asymmetric conflict between the attacker and the attacked where the prize is often sufficiently large that the attacker will continue to innovate as each new defence thwarts previous attacks. Defenders are hampered in this arms race by the fact that increased security often comes at the expense of reduced functionality, which has an impact on operational capability as well as meeting resistance from the users of the computer system. Furthermore, anyone with legitimate access to a system, such as staff and administrative users, must be trusted not to compromise it. Arguably the greatest threat to the security of any system is from an insider and therefore checks and balances need to be considered.

News coverage of network compromises shows that not all organisations take security sufficiently seriously. Those organisations that do take security seriously can still be targeted by advanced techniques and bespoke attacks that bypass conventional tools, especially when conducted in conjunction with insider knowledge or help. However, all attacks against a network must utilise that network at some point and so there are always opportunities to increase the likelihood of detecting and limiting or stopping such attacks.

The challenges for those who wish to implement effective CND have much in common with other system decisions. Organisations often treat security as an add-on rather than as a core part of a design, thereby limiting its effectiveness. “Big data” techniques that collect all of the data about systems and networks can increase awareness and detect attacks that may otherwise hide in the noise, but such techniques need large infrastructure and investment to store such data. Until such “big data” tools are commoditised then they will also require specialist tools and skills to exploit them properly. Sharing attack information effectively within a community would help defend the community as a whole; however, security departments must fight a convention of keeping such data secret to avoid embarrassment. Finally, we live in an era when the probability is that a computer system or network has already been compromised, either by accident or deliberately. This means that any data from a network cannot be assumed to be “clean”, and so any baseline of “normal” may actually include malicious behaviour. This must be taken into account when defenders examine data and consider their comparison point.

Any CND capability is better than no capability, and increased capability generally brings improved results. The technical or human aspects of a system will always have some vulnerabilities, but these can be minimised through improved CND. The challenge is to find sufficiently effective measures for the current risk appetite and budget.

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

The following selected quotes are drawn from a variety of sources and are relevant to CND.

“CND involves actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD [Department of Defense] information systems and computer networks. CND actions not only protect DOD systems from an external adversary but also from exploitation from within, and are now a necessary function in all military operations.”

Source 1: ‘United States Joint Publication 3-13: Information Operations’, (p II-5), 13/02/2006, http://www.fas.org/irp/doddir/dod/jp3_13.pdf.

“I divide the entire set of Fortune Global 2,000 firms into two categories: those that know they’ve been compromised and those that don’t yet know.”

Source 2: “Revealed: Operation Shady RAT”, Dmitri Alperovitch, Vice President, Threat Research, McAfee, 15/01/2010, http:// www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

“Today, more and more of them [malware “bad guys”] are adopting a very different approach: the targeted tactic. Advanced Persistent Threats (APTs) [in April 2011] have, according to the latest Messagelabs Intelligence report, risen to their highest number since March 2009.”

Source 3: "The relentless rise of Advanced Persistent Threats", ITPro, 5/05/2011, http://www.itpro.co.uk/blogs/2011/05/05/the-relentless-rise-of-advanced-persistent-threats/.

"…the increasing opportunity is for intelligence exchange between products and services to assist in correlation, and to provide context rather than a single solution that protects all infrastructure components."

Source 4: Gartner, 'Hype Cycle for Infrastructure Protection, 2014", Young G., G00263740, 30 July 2014.

Standards and policy (Government and non-Government)

CESG, the National Technical Authority for Information Assurance (IA), used to publish a set of policy documents for IA under the common title of 'HMG IA Standard' (known as IS1 and IS2). These policies provided guidance on assessing risks, securing assets and assuring the confidentiality, integrity and availability of computer systems, but have now been withdrawn. Despite this, their content and that of related standards is likely to remain as the basis of common best practice amongst IA practitioners. The Good Practice Guides (GPGs) augment this guidance with recommend technologies and processes for specific topics, including GPG13 for Protective Monitoring. The GPGs can be requested from CESG as they are not publicly available. Non-government standards, such as BS7799 and the ISO27000 family of standards, provide similar guidance on securing information systems for those outside the government space. Much of the existing policy is from an era of static defences, but dynamic defences and monitoring are increasingly gaining coverage as part of policies and standards.

Context-aware Computing and Context-enriched Services

Description

Context-aware computing (also known as Contextual computing) and the services that it can provide concerns the delivery of personalised information to the user based on their identity, previous interactions and preferences. Instigation of these services can be by a user's location or their environment as well as the time of day or activity. Presently, these services focus on supporting mobile users and are therefore particularly applicable to mobile devices such as smartphones.

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 iBeacons, BLE (Bluetooth Low-Energy), GPS (Global Positioning System), 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 and third generation iPad is a good example of the current state-of-the art. This is a context-aware personal virtual assistant that uses a natural language user interface to answer questions and make recommendations.

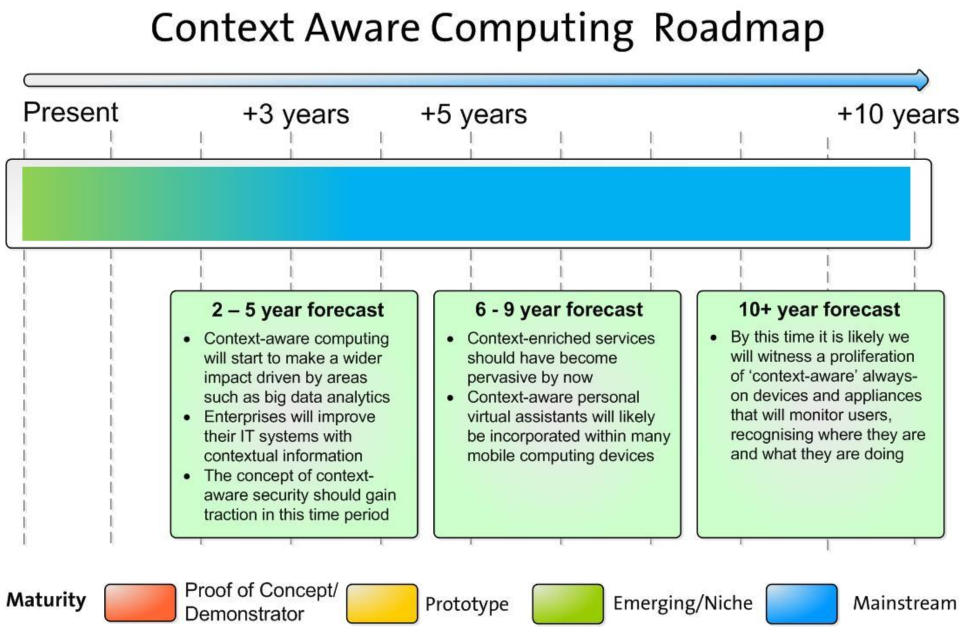
Some analysts believe context-enriched services will have a transformational impact [see Source 1]. Indeed, context-enriched services have already demonstrated business benefits and once the supporting and enabling technologies are mature, they could become a pervasive influence in our lives.

Relevant Applications

Applications in the near term will include virtual personal assistants, e-Business (particularly customer relationship management), television and media advertising. In the long-term, context-awareness could be applied to Cyber Security enabling more agile security infrastructures through supplying supplemental information to inform security decisions [see Source 2].

Most Relevant Critical Security Controls

- Continuous Vulnerability Assessment and Remediation
- Controlled Access Based on the Need to Know



Context Aware Computing Roadmap

2 – 5 year forecast

- Context-aware computing will start to make a wider impact driven by areas such as big data analytics
- Enterprises will improve their IT systems with contextual information
- The concept of context-aware security should gain traction in this time period

6 - 9 year forecast

- Context-enriched services should have become pervasive by now
- Context-aware personal virtual assistants will likely be incorporated within many mobile computing devices

10+ year forecast

- By this time it is likely we will witness a proliferation of 'context-aware' always-on devices and appliances that will monitor users, recognising where they are and what they are doing

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: Context-aware computing will start to make a wider impact driven by areas such as big data analytics. The benefits to business will be more widely appreciated and it is likely we will witness enterprises improving their IT systems with contextual information. Social networking sites will become more 'context oriented' such that individuals personal preferences and behaviour will directly affect their social networking experience. Also, the concept of context-aware security [see Source 2] should gain traction in this time period.

Within 6 – 9 years: Context-enriched services should have become pervasive in this timescale assuming there is no backlash caused by privacy and security concerns. Also it is likely that next generation "Siri-like" context-aware personal virtual assistants will be incorporated within mobile computers. These will act as digital companions.

10+ years: By this time it is likely we will witness a proliferation of 'context-aware' always-on devices and appliances that will monitor users, recognising where they are, what they are doing, who they are with and the time this all occurs.

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 3 below examines these issues, to quote:

"It is important to address security and privacy issues in context-aware mobile computing. There are two key security concerns with context-aware systems: firstly, ensuring privacy of location and identity information, and secondly, ensuring secure communications."

Context-aware computing makes it 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. So although contextual information could help businesses decide what products or services an individual is most likely to be interested in purchasing, it could also be used to conduct surveillance.

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 4 below].

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

The IT analyst company Gartner views context-aware computing as the means to refine the output of services and improve their relevance. In this respect they refer to so-called "Context-enriched services" which they predict will have a transformational impact on business and define it as follows:

"*Context-enriched services are those that combine demographic, psychographic and environmental information with other information to proactively offer enriched, situation-aware, targeted, personalised and relevant content, functions and experiences."*

Source 1*:* Gartner, 'Hype Cycle for Web Computing, 2014', Phifer G., G00263878, 23 July 2014.

Although several years old, this further Gartner source examining "context-aware security" is still relevant. To quote:

"Context-aware security is the use of supplemental information to improve security decisions at the time the decision is made, resulting in more-accurate security decisions capable of supporting more-dynamic business and IT environments. Context information that will be relevant to security decisions is not limited to environmental context and will include context information from multiple sources. Application awareness, identity awareness and content awareness are all examples of the broader shift to context-aware and adaptive security infrastructures."

Source 2: Gartner, 'The Future of Information Security Is Context Aware and Adaptive', MacDonald N., G00200385, 14 May 2010, refreshed 6 February 2014.

This source provides a review of Context-aware computing in mobile computing where the authors present the case that context awareness is increasingly gaining applicability in interactive ubiquitous mobile computing systems. This review recognizes two types of context, active context and passive context, thus:

"Different perspectives on how mobile applications can take advantage of context have been advanced. Thus applications can automatically adapt their behaviour according to discovered context (active context), or present the context to the user on the fly and/or store it for the user to retrieve later (passive context). This has led to context-aware computing, defined in two ways: firstly, active context awareness automatically adapts to discovered context by changing the application's behaviour; and secondly, passive context awareness presents the new or updated context to an interested user or makes the context persist for the user to retrieve later."

Source 3: Musumba G.W., Nyongesa H.O.: 'Context-awareness in mobile computing: A review', International Journal of Machine Learning Applications, 2013;2(1), http://dx.doi.org/10.4102/ijmla.v2i1.5.

The following research paper has examined issues in context-aware systems that are still relevant.

Source 4: 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.

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

Digital Cryptocurrency (Digital Currency)

Description

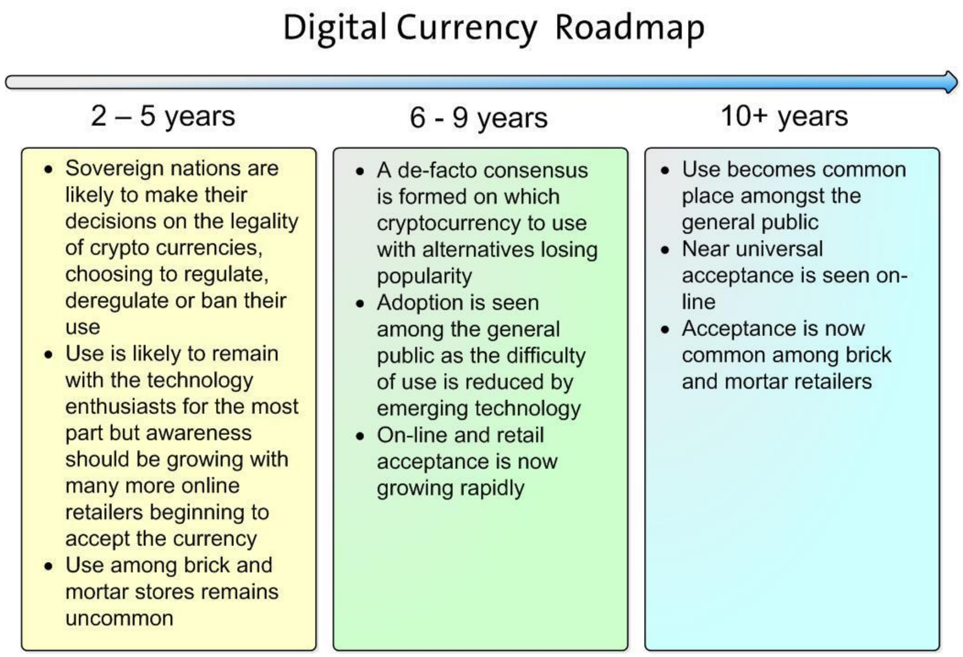
Digital currency is an electronic based medium of exchange that is created, transferred and stored electronically. Digital currency can be used in exchange for goods and services on-line or in traditional stores that accept the currency.

A key difference between a standard currency and a cryptocurrency is that with a cryptocurrency no physical asset exists and the users themselves are solely responsible for the security of the funds in a digital wallet. The digital wallet is a computer file that contains your digital credential of ownership of the funds.

A digital cryptocurrency is a form of stored wealth where the users themselves are solely responsible for their own funds security (think storing a wallet in a home safe, the file is a wallet holding the funds and the safe is the encryption placed around the wallet file to protect the contents, the user is responsible for encrypting the file). The loss of a wallet file will cause a permanent loss of funds unless a valid backup of the wallet is used; stolen funds have no recovery process. A cryptocurrency (such as Bitcoin) is a token that relies on cryptography to secure the records of transactions, in a public ledger called a block chain, which provides evidence for ownership of coins and prevents fraudulent transactions from taking place. The mathematical algorithms, which govern creation, movement and validation of transactions, are processed by computer systems on the network, these systems are called “Miners”. Miners are compensated for processing transactions by being entered into lotteries to win or “mine” a reward of cryptocurrency. Users of the network may also pay small sums of the currency to the “miners” to receive transaction priority. Digital cryptocurrencies are considered pseudo-anonymous; this is because transactions are conducted through cryptocurrency wallet addresses that are simply a long string of letters and numbers. Only the wallet address is shared publically as part of the transaction for destination and verification process no personal details are associated directly with the wallet address which makes attribution to an individual difficult.

Most Relevant Cyber Security Controls

- Continuous Vulnerability Assessment and Remediation
- Maintenance, Monitoring, and Analysis of Audit Logs
- Data Protection



Digital Currency Roadmap

2 – 5 years

- Sovereign nations are likely to make their decisions on the legality of crypto currencies, choosing to regulate, deregulate or ban their use
- Use is likely to remain with the technology enthusiasts for the most part but awareness should be growing with many more online retailers beginning to accept the currency
- Use among brick and mortar stores remains uncommon

6 - 9 years

- A de-facto consensus is formed on which cryptocurrency to use with alternatives losing popularity
- Adoption is seen among the general public as the difficulty of use is reduced by emerging technology
- On-line and retail acceptance is now growing rapidly

10+ years

- Use becomes common place amongst the general public
- Near universal acceptance is seen on-line
- Acceptance is now common among brick and mortar retailers

Relevant Applications

- Very fast movement of funds globally, transactions take minutes not days.
- Transferring money across borders with minimal cost paid to the miner for performing the validation and verification of the transaction. There are no additional fees such as those levied by banks which are often around 10% of the value of the transaction.
- Protecting funds from central authority control or remote seizure. As long as the user holds access to the wallet file the funds can be spent, for example transactions cannot be blocked by court order.
- Pseudo-anonymous transactions, this could be for illicit or legitimate reasons, money laundering and funding criminal/terrorist action is a major concern;
- Protects retailers from chargebacks.
- Global currency, there are no conversion fees if people remain within the cryptocurrency economy, moving between national currency and cryptocurrency will still incur fees if a broker is used.

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: Sovereign nations are likely to make their decisions on the legality of crypto currencies, choosing to regulate, deregulate or ban their use. Use is likely to remain with the technology enthusiasts for the most part but awareness should be growing with many more online retailers beginning to accept the currency, use among brick and mortar stores still uncommon.

Within 6 – 9 years: A de-facto consensus is formed on which cryptocurrency to use with alternatives losing popularity. Adoption of cryptocurrencies among the public become more likely assuming regulatory impact is non-hostile and technology to improve accessability is developed . On-line and retail acceptance is now growing rapidly.

10+ years: Use becomes common place among the general public, near universal acceptance is seen on-line and acceptance is now common among brick and mortar retailers.

General Issues and Challenges

- Criminal transactions could move into cryptocurrencies as the movement of funds is easier to hide. This is already seen with black market websites such as Silk-road where users could buy and sell illegal drugs.
- Volatility in the value reduces confidence in cryptocurrencies as a currency, the volatility makes cryptocurrency more akin to a stock or asset.
- Users lack of understanding of personal liability, volatility of currency and unregulated market puts those with poor understanding of the technology at risk of exploitation and loss.
- As the Blockchain grows in size so does the amount of space required to store the transaction history, in the space of a few years the size has grown from megabytes to tens of gigabytes and will accelerate rapidly as users join the network.
- Vulnerabilities and exploits in the network could exist allowing attackers to cause financial loss to users.

- Enthusiasts have previously been the driver behind establishing cryptocurrency exchanges and businesses. They may lack relevant experience in the field of Cyber Security. There have been several examples of exchanges and businesses losing funds to hackers and fraud recently; one recent example was the MtGOX exchange which used to handle the majority of Bitcoin exchange traffic.
- Most cryptocurrencies have a deflationary model, this could encourage users to hoard currency in expectation of an increase in value. This has historically been bad for economies as it can stifle economic growth when users refuse to spend. Some see this as an advantage preventing economic manipulation by the injection of currency to force inflation which devalues individuals savings.

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

"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers."

Source 1: Publication: Bitcoin: A Peer-to-Peer Electronic Cash System – Satoshi Nakamoto creator of Bitcoin, https://bitcoin.org/bitcoin.pdf, accessed 17 February 2015.

"The cryptographic Bitcoin protocol may sound like a mouthful, but essentially it's a security related function based upon a complex mathematical algorithm that needs to be solved, and the mining hardware completes the task autonomously"

Source 2: Lawn A.: Publication: yBitcoin, Volume 2 Issue 1, 2014, page 45.

"From about December 2011 to October 2013, SHREM's co-defendant, Robert M. Faiella, ran an underground Bitcoin exchange on the Silk Road website, a website that served as a sprawling and anonymous black market bazaar where illegal drugs of virtually every variety were bought and sold regularly by the site's users. Operating under the username "BTCKing," Faiella sold Bitcoins – the only form of payment accepted on Silk Road – to users seeking to buy illegal drugs on the site."

Source 3: Press Release, United States Attorney's Office, December 19th 2014,

http://www.justice.gov/usao/nys/pressreleases/December14/ShremCharlieSentencingPR.php, accessed 17 February 2015.

HM Revenue and Customs have produced a policy paper entitled "Revenue and Customs Brief 9 (2014): Bitcoin and other cryptocurrencies". It sets out HM Revenue and Customs (HMRC) position on the tax treatment of income received from, and charges made in connection with, activities involving Bitcoin and other similar cryptocurrencies, specifically for VAT, Corporation Tax (CT), Income Tax (IT) and Capital Gains Tax (CGT).

Source 4: HM Revenue and Customs 'Revenue and Customs Brief 9 (2014): Bitcoin and other cryptocurrencies', 3 March 2014,

https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies, accessed 17 February 2015.

Standards and policy (Government and non-Government)

Government policy within the UK is limited, and currently only addresses issues related to tax. Standards relating to the management of the Bitcoin network and derivatives are enforced through the collective decisions of the network. Changing the software would require a consensus between the network of users to support it. A change that was not agreed to the Bitcoin protocol would cause what is referred to as a "fork" in the Blockchain, unless this fork is supported it won't grow and will fail. The popular support of the standard in effect causes a de facto standard to exist.

The UK Government have produced a UK VAT policy on cryptocurrency (see source 4 above).

Outside of the UK decisions have been polarising with many countries embracing the technology with little to no regulation, others have imposed strict control and some have outright banned it as an economic or criminal threat:

Some examples include:

- the USA have opted to regulate cryptocurrency exchanges as a money service business similar to banks.
- Ecuador and Bangladesh have banned its use entirely.
- China has made it illegal for banks to cooperate with Cryptocurrency exchanges but stopped short of a full ban for individual users.

QinetiQ comment

Digital cryptocurrencies are a relatively new disruptive technological innovation, with little or no overarching regulation. Due to their open source nature, cryptocurrencies can evolve and change frequently. In 2013, many different cryptocurrencies were created and abandoned in the space of a few months, all in the name of short term profiteering. Although unlikely to replace a nation's existing economy, especially in the short term, in a relatively short time digital currencies have grown from an experiment, to their own global economy with thousands of users worth billions of dollars.

There is significant risk associated with cryptocurrencies to law enforcement because of its pseudo-anonymous properties that make attribution to a person difficult but not impossible. All transactions through the Blockchain are transparent and visible, if attribution can be made to a particular wallet the funds can be followed back to the origin. Particularly vulnerable points are exchanges where money laundering laws require most exchanges to confirm users' identities before funds can be deposited or withdrawn. It may be infeasible in some instances to attribute the transaction to a user, particularly if the transfer involved new coins, cash was used to pay, encrypted communications were used such as Tor and the identities of the transacting pair remain anonymous to each other.

Future Protocols for Network Security

Description

Protocols, in the context of computer networking, are the digital rules (standards) that two or more items of hardware or software follow to transfer data or instructions between them. The underlying encryption used is established and well understood and the biggest risk to the security of a network and the underlying data is the implementation of the protocols themselves.

Security protocols provide the means to achieve particular security objectives. A common objective is to prevent unauthorised users from accessing the information being held or transferred within a system and reading or modifying the content of messages (confidentiality and integrity). Increasingly, protocols provide other functionality such as authenticating a device or a user's identity, in order to support the security model being used for the network and the services being provided.

Standardising protocols aims to increase the likelihood that devices (possibly from different suppliers or manufacturers) will successfully interoperate in a secure manner, reducing the possibility that information and devices are misused or accessed by unauthorised individuals. See the work being done by the FIDO (Fast Identity Online) Alliance.

Relevant Applications

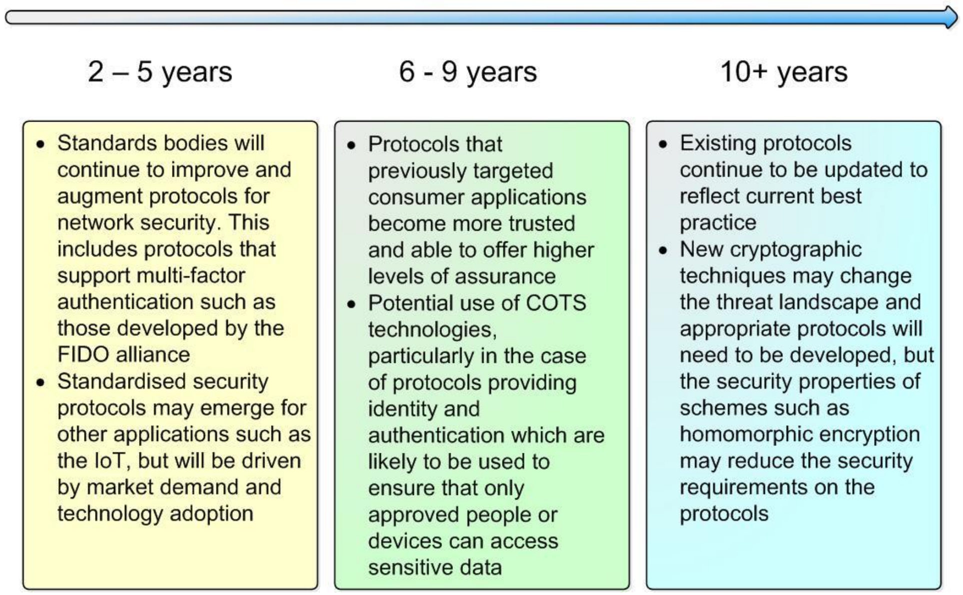
Network security protocols are relevant to all computer networks that contain information and functionality requiring protection, such as systems holding personal information, commercially sensitive or nationally sensitive information.

This is not just limited to business networks or national infrastructure networks, but is also relevant to the anticipated networks required for smart homes/smart cities and the "Internet of Things" (IoT) and the levels of trust / authentication that should be assigned to devices and applications running on them.

Most Relevant to Cyber Security Controls

- Wireless Access Control
- Boundary Defence
- Data Protection
- Secure Network Engineering

Future Protocols for Network Security Roadmap



2 – 5 years

- Standards bodies will continue to improve and augment protocols for network security. This includes protocols that support multi-factor authentication such as those developed by the FIDO alliance
- Standardised security protocols may emerge for other applications such as the IoT, but will be driven by market demand and technology adoption

6 - 9 years

- Protocols that previously targeted consumer applications become more trusted and able to offer higher levels of assurance
- Potential use of COTS technologies, particularly in the case of protocols providing identity and authentication which are likely to be used to ensure that only approved people or devices can access sensitive data

10+ years

- Existing protocols continue to be updated to reflect current best practice
- New cryptographic techniques may change the threat landscape and appropriate protocols will need to be developed, but the security properties of schemes such as homomorphic encryption may reduce the security requirements on the protocols

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: Standards bodies will continue to improve and augment protocols to enhance the capabilities that devices can provide. This includes the internet based solutions via Internet Engineering Task Force, protocols which support multi-factor authentication such as those developed by the Fast IDentity Online (FIDO) Alliance or low bandwidth home networking protocols such as Zigbee for smart homes. Standardised security protocols may emerge for other applications such as the IoT, but will be driven by market demand and technology adoption.

Within 6 – 9 years: Protocols that previously targeted consumer applications become more trusted and able to offer higher levels of assurance. This could lead to the use of COTS technologies within a commercial context, particularly in the case of protocols providing identity and authentication which are likely to be used to ensure that only approved people or devices can access sensitive data

10+ years: Existing protocols continue to be updated to reflect current best practice. New cryptographic techniques may change the threat landscape and appropriate protocols will need to be developed, but the security properties of schemes such as homomorphic encryption may reduce the security requirements on the protocols.

General Issues and Challenges

The commercial sector is already solving many security problems for the lowest impact levels. Groups such as the Internet Engineering Task Force (IETF) will continue to develop solutions for IP (Internet Protocol) type networks, including improving protocols or addressing issues as they emerge. This includes protocols such as browser based Hypertext Transfer Protocol Secure (HTTPS), Encapsulating Security Protocol (ESP) or Internet Keying Exchange (IKE) for IP cryptographic applications or Domain Name System Security Extensions (DNSSEC) to protect networking components. To bring these solutions to more critical systems, higher assurance solutions will be required, for some cases this will be just more robust implementations, but in others it may require modifications. Key protocols will be assessed by GCHQ - as the UK's National Technical Authority for Information Assurance to determine their suitability.

Other commercial initiatives that are developing protocols such as the FIDO Alliance and Zigbee Alliance will need to incorporate security into their protocols, for example to provide suitable authentication and protection of the key information in transit across a network. While these types of capabilities are emerging, their development is largely driven by commercial forces and so it may take time to fully address security issues. This will initially limit their usage to lower assurance applications, until their characteristics can be determined, in order to minimise the risks to organisations before adopting the technology.

Organisations increasingly want to reduce their IT costs and hope to outsource capability where possible, leading to interest in cloud-based options; confidence in data security is critical to realising this. New protocols will be required to enable emerging, immature techniques (such as homomorphic or attribute-based encryption) to be used securely to support this transition.

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

Active IETF Working Groups Webpage.

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

"…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 2: Bernardo D.V.; Hoang D.B.: 'Future Networks, 2010', IEEE Computer Society. 2010.

The EU Agency for Network and Information Security (ENISA) is the EU's response to Cyber Security issues. It is described as the 'pace-setter' for Information Security in Europe, and a centre of expertise. ENISA's web site is the European 'hub' for exchange of information, best practices and knowledge in the field of Information Security.

Source 3: https://www.enisa.europa.eu/activities/identity-and-trust.

Standards and policy (Government and non-Government)

The IETF is a key public body focused on network security for internet type networks, their Working Groups (WG) are categorised according to topic e.g. 'Security Area'. Source 1 above lists active WG. Security aspects 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. Specific security protocols and algorithms emerge from institutes such as National Institute of Standards and Technology (NIST) and American National Standards Institute (ANSI).

There are industry specific standards such as Zigbee from the Zigbee Alliance, a radio communications protocol of interest to smart homes initiatives. The FIDO Alliance have recently issued v1.0 of their multifactor authentication protocols, which they anticipate will remove the need for users to remember many complex passwords.

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, unless a disruptive technology emerges or vulnerability identified. A recent competition (October 2012) resulted in the Keccak algorithm being named to become the new Secure Hash Algorithm (SHA)-3 hash algorithm providing algorithm options following recommendations to deprecate use of SHA-1. The European Union Agency for Network and Information Security (ENISA) regularly publishes its findings and recommendations on cryptographic algorithms, key size and security protocols (see Source 3 above).

There is a possibility that newer protocols may use more secure cryptographic algorithms or larger keys, but these will generally be incremental improvements over the current state of the art. Novel cryptographic schemes such as homomorphic encryption and attribute-based encryption will provide new ways to secure information and network communications while binding identity and security into the business workflow; these schemes may require some protocols being updated and will need to be integrated closely with protocols for authentication and identity.

In addition to network protocol developments, advanced key management concepts are still being researched and improved. This includes protocols for the distribution of keys, techniques for managing cryptographic communities and methods to assure the delegation of key management authority within an organisation. Identity and authentication are central to these ideas to ensure that keys, privileges and access rights are delegated to appropriate users and devices. Security controls can also be implemented outside the protocol space, within hardware and applications; both of these approaches are also important in enhancing the overall security of the network and should not be overlooked.

High Security Wireless Communications for Civilian Use

Description

Wireless communications for civilian use have become ubiquitous over the past two decades. In the early days of analogue cellular systems, security was not provided, hence eavesdroppers were able to listen in to conversations. 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 is a plethora of modern wireless communications systems and technologies and 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:

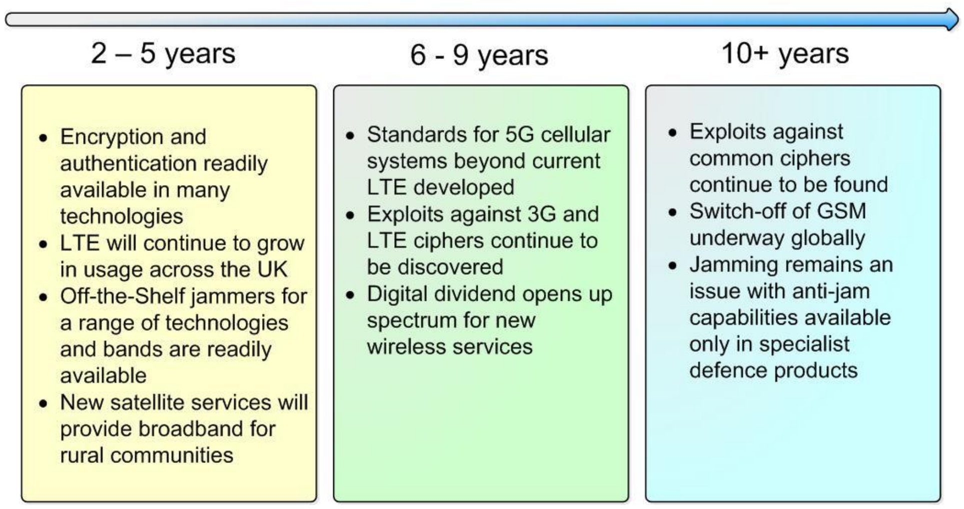
- Confidentiality - prevent eavesdropping
- Integrity - ensure that information has not be tampered with or changed in transit
- Authentication/access control - ensure only valid users and devices can use the services
- Availability - ensure that a service can be used when required

In some applications, the information being communicated may not be particularly sensitive, however validating who the sender is and that the information has not been modified en-route may be critical. Similarly, availability of the communications will be important, ensuring the communications channels are not blocked or jammed.

Most Relevant Cyber Security Controls

- Inventory of Authorized and Unauthorized Devices
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Wireless Access Control

High Security Wireless Communications Roadmap



2 – 5 years

- Encryption and authentication readily available in many technologies
- LTE will continue to grow in usage across the UK
- Off-the-Shelf jammers for a range of technologies and bands are readily available
- New satellite services will provide broadband for rural communities

6 - 9 years

- Standards for 5G cellular systems beyond current LTE developed
- Exploits against 3G and LTE ciphers continue to be discovered
- Digital dividend opens up spectrum for new wireless services

10+ years

- Exploits against common ciphers continue to be found
- Switch-off of GSM underway globally
- Jamming remains an issue with anti-jam capabilities available only in specialist defence products

* LTE (Long Term Evolution)

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 be noted that security requirements might 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 controls to an IT system will be provided by the system itself, such as username / password challenges and two-factor authentication mechanisms (e.g. RSA SecurID Tokens). These latter capabilities are out of scope of this forecast. Also, since this forecast covers civilian use, so-called “high grade” evaluated security solutions aimed at defence and government customers are also not to in scope. Nevertheless, modern cryptographic solutions available to civilian customers can be very robust.

Relevant Applications

There is a wide variety of relevant applications that could benefit from high security wireless communications. The following applications are particularly important with respect to national infrastructure. These include voice and video communications, distributed control systems, Supervisory, Control and Data Acquisition (SCADA), telemetry, imaging systems (e.g. wireless CCTV) and wireless physical security systems.

Distributed control systems and SCADA systems are used widely across many sectors, including utilities, manufacturing, environmental control systems and communications networks. There exists the potential for more of these systems to use wireless communications to enable personnel to interact with them from remote locations. This presents a significant new attack vector.

Wireless CCTV and physical security 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 considerable in the coming years. The demand from consumers for robust security will not diminish, but will be largely 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 LTE, has already been deployed and will see continued growth in usage. LTE brings with it a new encryption technology. However, jammers for a range of technologies and bands (e.g. GSM/3G, Wi-Fi) 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. Network operators will consider when to switch off GSM to free more spectrum for 3G and 4G services.

Within 6 – 9 years: Standards and products for cellular services beyond the current LTE technology will be developed (so-called 5G). 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. Exploits against the LTE cipher may emerge, but again will be difficult to put into practice.

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 cat and mouse game which helps evolve crypto capability. It is unlikely the vulnerability of GSM to spoof base stations will be addressed over this period as operators globally gradually move away from GSM. However the installed base of GSM devices will be hard to migrate, including non-phone related applications. The vulnerability of wireless systems to jamming is likely to remain, with legislation ensuring jamming remains illegal being the main bulwark against widespread use of jamming. 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 Wi-Fi products implement the more robust WPA2 standard which provide an AES-based encryption algorithm with a maximum key length of 256 bits.
- Attacks have been shown against the ciphers used in GSM systems (A5/1 and A5/2). Attacks against the A5/3 Cipher for 3G (Kasumi) have been published (see source 2). 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.
- 4G/LTE uses a different encryption algorithm to 3G. However, whereas 3G supported encryption across the radio medium and to the radio network controller (RNC – a device coordinating the behaviour of base-stations across an area), LTE only offers encryption to the base-station. Operators need to use alternative encryption technologies (e.g. IPSec) to protect communications from the base-station back towards the core network, but it is not clear that all operators will implement this (see source 3).
- 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 prohibiting the use of jammers is only partially effective, with jamming devices targeted at a number of technologies (Wi-Fi, GSM, 3G etc.) readily available. However, legislation may not always be effective, with even large corporations using jamming technologies (Source 4). In addition, attacks on the availability of the wireless communications may prompt a fall back to failsafe operation that may significantly impact the normal operation of the supported system.
- Network spoofing attacks have been demonstrated for GSM systems (Source 5 and 6). 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 not 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 (see source 7).
- 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 "guerrilla artists" recording CCTV images and using them to make statements about the level of surveillance in the UK.
- Security has not been a priority for many companies and developers, particularly in the control and SCADA fields. This has been illustrated recently by research targeting traffic light systems in the US which demonstrated it is possible to take control of traffic lights across almost 100 intersections in the US city of Michigan (with the permission of the local authorities) (see source 8).

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

The US Federal Bureau of Investigation (FBI) has recently acknowledged 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, 13 December 2011, http://nakedsecurity.sophos.com/2011/12/13/fbi-acknowledges-more-scada-attacks-increases-cyber-budget/, accessed 9 March 2015.

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

There are concerns that only half the globally deployed LTE base-stations will support encryption into the operators' core networks by 2017, with many of the operators not recognising the threat exposed nor the need to provide additional protection.

Source 3: Donegan P.: 'The Security Vulnerabilities of LTE: Opportunity & Risks for Operators', Heavy Reading/Juniper, October 2013,

http://forums.juniper.net/jnet/attachments/jnet/IndustrySolutionsEMEA/326/1/Download%20Here%20-%20The%20Security%20Vulnerabilities%20of%20LTE%20Opportunity%20and%20Risks%20for%20Operators.pdf, accessed 9 March 2015.

Hotels in the US have recently been fined $600,000 for using techniques to block personal Wi-Fi hotspots in public areas. They are currently in the process of lobbying the US Federal Communications Commission (FCC) to clarify the law and allow them to continue using the practice.

Source 4: Thomson I.: 'Hilton, Marriott and co want permission to JAM guests' personal Wi-Fi', The Register, 23 December 2014,

http://www.theregister.co.uk/2014/12/23/us_hotel_chains_and_tech_firms_square_off_with_fcc_over_wifi_hotspots/, accessed 9 March 2015.

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 5: Greenberg A.: 'Despite FCC "Scare Tactics" Researcher Demos AT&T Eavesdropping', 31 July 2011, http://www.forbes.com/sites/firewall/2010/07/31/despite-fcc-scare-tactics-researcher-demos-att-eavesdropping/, accessed 9 March 2015.

Source 6: Greenberg A.: 'Smartphone Data Vulnerable To Base Station Spoof Trick', 19 January 2011, http://www.forbes.com/sites/andygreenberg/2011/01/19/smartphone-data-vulnerable-to-base-station-spoof-trick/, accessed 9 March 2015.

Source 7: ReadWriteWeb, ‘Baseband Hacking: A New Frontier for Smartphone Break-ins’, 19 January 2011

http://www.readwriteweb.com/archives/baseband_hacking_a_new_frontier_for_smartphone_break_ins.php, accessed 9 March 2015.

Recent research by the University of Michigan illustrates the vulnerability of traffic light systems to hackers exploiting vulnerabilities in the wireless solution used and other aspects of the system. The work raises concerns about the general lack of regard for robust security measures when developing products and solutions.

“The real problem, however, is not any individual vulnerability, but a lack of security consciousness in the field. A clear example can be seen in the response of the traffic controller vendor to our vulnerability disclosure. It stated that the company, ‘has followed the accepted industry standard and it is that standard which does not include security.’”

Source 8: Ghena B. et al.: ‘Green Lights Forever: Analyzing the Security of Traffic Infrastructure’, University of Michigan Computer Science and Engineering Dept, 19 August 2014, https://www.cse.umich.edu/eecs/about/articles/2014/Green-Lights-Forever.html, accessed 9 March 2015.

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 therefore important to remember that wireless security is only one element of the security solutions necessary to protect systems, and that mitigating security risks involves technology, people and processes.

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

Homomorphic Encryption

Description

Processing data while it is still encrypted offers many advantages for cyber security and could drastically change how data is protected when using remote systems, such as cloud services. Homomorphic encryption is the best known technique, but many similar techniques are also being developed with related security objectives.

- **Homomorphic Encryption** has many applications for cloud services, as it allows encrypted data to be mathematically processed without needing to decrypt the data.
- **Multi-Party Computation** has applications to protecting cryptographic keys, and combining datasets while preserving user privacy, as it allows many entities to share and compute on information in a verifiable way, without exposing private data.
- **Functional Encryption** can be used to realise encrypted searches (where the platform does not learn the content of the query or the response) and enforce access control policies (without needing to reveal the identity of a user or the security policy).

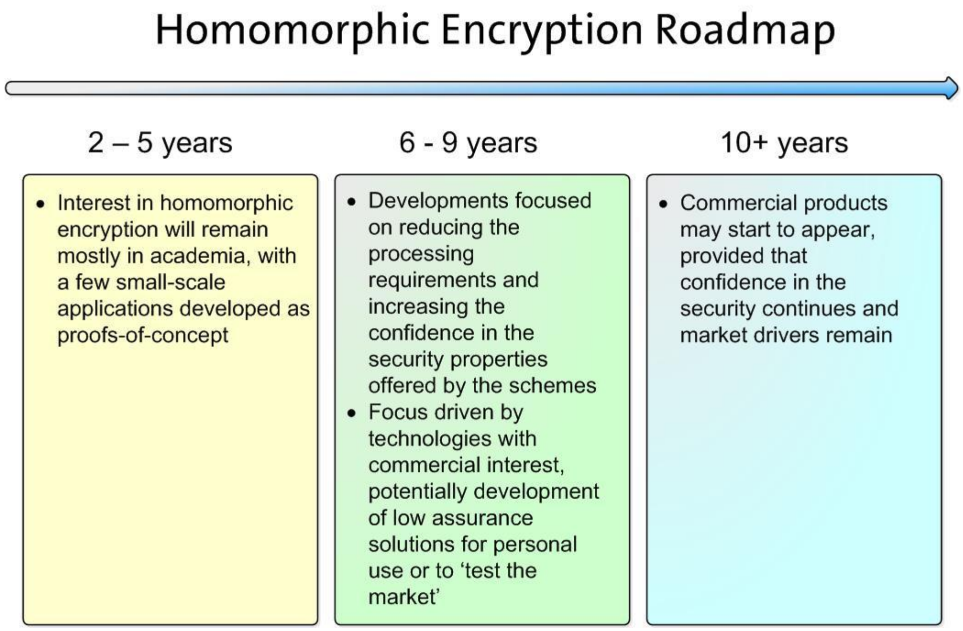
Relevant Applications

These techniques are enablers for cloud-based services, as they avoid exposing sensitive data to the provider while still allowing them to manipulate the data, although it is computationally expensive. Similarly, access control policies can be cryptographically enforced without revealing the policy.

Other potential applications include: cryptographically enforced auctions, where only the identity of the highest bidder and the value of their bid are revealed; and private information retrieval schemes, where users query a database without revealing the queries or responses to the platform hosting the database.

Most Relevant Cyber Security Controls

- Controlled Access Based on the Need to Know
- Data Protection
- Secure Network Engineering



Homomorphic Encryption Roadmap

2 – 5 years

- Interest in homomorphic encryption will remain mostly in academia, with a few small-scale applications developed as proofs-of-concept

6 - 9 years

- Developments focused on reducing the processing requirements and increasing the confidence in the security properties offered by the schemes
- Focus driven by technologies with commercial interest, potentially development of low assurance solutions for personal use or to 'test the market'

10+ years

- Commercial products may start to appear, provided that confidence in the security continues and market drivers remain

General Issues and Challenges

The main challenges that these approaches will need to address are the processing requirements, the technological maturity and the assurance levels provided.

Most of these techniques require very computationally intensive operations during processing and are currently too slow for general use. This is changing: for a homomorphic evaluation of AES approximately 40 minutes per input bit was required in 2012 whereas in late 2014 this was down to approximately 2 seconds. While impressive, this is still several order of magnitude higher than the milliseconds it takes standard devices to perform the same tasks.

Improving and enhancing these techniques is a significant area of interest within academia, suggesting that there is some maturation required before the techniques could be commercialised. For example, software toolboxes are available for homomorphic encryption, but these focus on supporting further academic study.

A major challenge in this area will be to demonstrate that these techniques can be applied in a suitably assured manner, with sufficient confidence. This will require suitable evaluation and accreditation processes to be developed, which will robustly and sufficiently test an implementation. There will be an additional need to ensure that accreditors understand the new paradigm and that appropriate policies have been put in place.

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

Known as "fully homomorphic encryption" this encryption method has long been an ultimate goal for computer scientists, and IBM in particular, has been seeking this particular prize for years. The company's receipt of a patent is a strong hint it may be inching close to a practical solution, rather than simply a concept on paper.

Source 1: Yegulap S., 'IBM's homomorphic encryption could revolutionize security', InfoWorld TechWatch, 2 Jan 2014,

http://www.infoworld.com/article/2609755/encryption/ibm-s-homomorphic-encryption-could-revolutionize-security.html, accessed 26 January 2015.

This Dyadic Security White Paper discusses the use of multi-party computation to protect cryptographic keys

Source 2: Dyadic Security White Paper, https://www.dyadicsec.com/media/1080/dyadicwhitepaper.pdf, accessed 17 February 2015.

This example, where there is a requirement for privacy to be preserved between two data sets, is a good case where homomorphic encryption could be applied.

Source 3: Brave New Privacy, http://sharemind.cyber.ee/stories_privacy-preserving-policy-decisions.html, accessed 17 February 2015.

Standards and policy (Government and non-Government)

As these techniques are currently still being investigated within academic research, they are too immature for general assured use within sensitive or critical applications. There do not yet appear to be any specific standards or policies relating to their use and it is expected that as they mature, they will be covered by standards and policy frameworks. Commercial appetite and market factors are likely to drive the specification of standardised protocols using these concepts, by either industry or Government.

QinetiQ comment

Many technologies are closely related to homomorphic encryption and achieve various security goals, aiming to avoid leaking information about encrypted data while it is being processed. Most are a long way from being sufficiently mature for commercial application, although some areas are developing particularly rapidly, with secure deduplication as one example (this allows cloud providers to recognize when two users are storing the same file, without learning the content of that file), perhaps due to this solution's commercial applicability.

Processing encrypted data is particularly relevant to cryptographic applications, where side-channel attacks (those that use timing, power consumption, EM-emissions, and sound as extra sources of information) are a concern. There are existing countermeasures, however new techniques will greatly increase the protection available, with distributed security modules (which split keys across several servers and use them without reconstructing them) as one such example. Attribute-based encryption is a similar technique that associates decryption keys to attributes held by users and can be used to enforce a security policy.

Indoor Navigation

Description

As satellite navigation (in particular GPS) has become a ubiquitous part of daily life so the use of accurate position, navigation and timing information is relied upon for a wide range of applications and services. The enduring problem with satellite navigation, the most prominent position and timing technology, is that it performs very poorly indoors, in built up areas (urban canyons) and in other environments that are hostile for radio frequency signals.

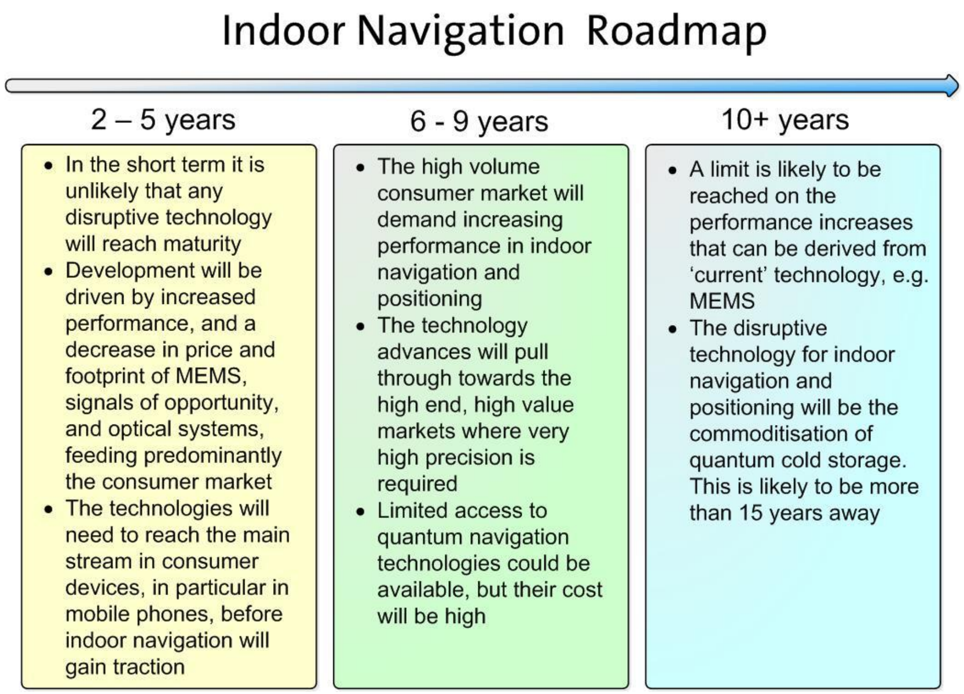
The ability to navigate indoors with a high level of precision, continuity and integrity will enable new services and applications to be developed. Integrity is a growing concern as the threat of meaconing[4] and spoofing attacks raises the possibility of hazardously misleading information being received.

There are a large number of technologies competing to deliver the capability, primarily through reduction of reliance on satellite navigation. It is likely that systems that combine these technologies will ultimately provide the best performance at the lowest cost. Although not an exhaustive list, these technologies include:

- High sensitivity satellite navigation, advanced signal processing can enabled a receiver to use the very weak satellite navigation signals which arrive inside buildings (source 1).
- 'Signal of opportunity' devices which can use fixed signals (usually radio) such as Wi-Fi and cell-phone towers (source 2).
- MicroElectroMechanical Systems (MEMS), microscopic accelerometers, gyroscopes and compasses which can be integrated onto microchips (source 3).
- Ground based systems and pseudolites (ground based "pseudo-satellites"), using similar (or, in the case of pseudolites, the same) signals as satellite navigation but broadcast from ground stations at high power to penetrate the walls of buildings (source 5).
- Quantum technologies, such as cold atom storage will enable the development of very high accuracy accelerometers, gyroscopes, and atomic clocks.

Most Relevant Cyber Security Control

- Wireless Access Control



Indoor Navigation Roadmap

2 – 5 years

- In the short term it is unlikely that any disruptive technology will reach maturity
- Development will be driven by increased performance, and a decrease in price and footprint of MEMS, signals of opportunity, and optical systems, feeding predominantly the consumer market
- The technologies will need to reach the main stream in consumer devices, in particular in mobile phones, before indoor navigation will gain traction

6 - 9 years

- The high volume consumer market will demand increasing performance in indoor navigation and positioning
- The technology advances will pull through towards the high end, high value markets where very high precision is required
- Limited access to quantum navigation technologies could be available, but their cost will be high

10+ years

- A limit is likely to be reached on the performance increases that can be derived from 'current' technology, e.g. MEMS
- The disruptive technology for indoor navigation and positioning will be the commoditisation of quantum cold storage. This is likely to be more than 15 years away

[4] Meaconing is the interception and rebroadcast of navigation signals.

Relevant applications

Tracking – e.g. goods in a warehouses, staff in hazardous environments, passengers in airports, or secure building access control and geo-fencing.

Contextual services and applications – e.g. location targeted advertising or internet searching, dissemination of travel information to passengers.

Training and simulation – e.g. enhanced augmented reality using large, complex training and simulation scenarios of hazardous or impractical locations, e.g. airports, power stations.

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: In the short term it is unlikely that any disruptive technology will reach maturity. Development will be driven by increased performance, and a decrease in price and footprint of MEMS, signals of opportunity, and optical systems, feeding predominantly the consumer market . Until these technologies reach the main stream in consumer devices, in particular mobile phones, the development of services and applications is likely to be slow. At the same time, without the demand of services and applications, the pull to put capability into consumer devices will be low. The turning point is likely to be around the 3 to 6 year mark.

Within 6 – 9 years: In the medium term, the high volume consumer market will demand increasing performance in indoor navigation and positioning. Once a large number of mobile phones are capable of indoor navigation the innovative applications and services that make use of positional information will boom. The technology advances will pull through towards the high end, high value markets where very high precision is required. Some limited access to quantum navigation technologies could be available, but their cost will be high.

10+ years: In the long term, there is likely to be a limit to the performance increases that can be derived from 'current' technology, e.g. MEMS. The disruptive technology will be the commoditisation of quantum cold storage. However, this is likely to be more than 15 years away.

General Issues and Challenges

A number of key security challenges surround the use of navigation in general. Interference and spoofing are becoming an increasing problem, leading respectively to reduced availability (no position available) and integrity (reported position is not correct/usable and is potentially hazardously misleading). Satellite navigation jamming has been seen, anecdotally, to negatively impact the delivery of critical services in airports, hospitals, banking, and power distribution.

Another area of security concern is around personnel security owing to the abuse of position information. This may raise concerns over security or safety threats where the person's location is sensitive (e.g. security personnel), or release of personal information in contravention of data protection laws.

The technical challenge for indoor positioning is to achieve the same or better level of accuracy that users have come to expect from outdoor positioning services provided by satellite navigation. No individual technology currently foreseen is likely to achieve the desired level of performance and ubiquity for at least 15 years. High performance and ubiquity is likely to come from the integration of multiple different technologies, which presents technical challenges in size, weight, power and cost.

Mapping can also be a challenge. Global maps are very mature, facilitated by national mapping agencies and satellite imagery, but mapping of indoor locations is far less mature, generally depending on need on a case-by-case basis.

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

Good introductions many of the technologies discussed may be found on Wikipedia. The following are also useful sources.

This article may be found in an industry on-line magazine. It provides a good overview of the challenges faced by a satellite navigation receiver indoors, and some of the techniques used to increase receiver sensitivity.

Source 1: Evaluation of High Sensitivity GPS Receivers, http://mycoordinates.org/evaluation-of-high-sensitivity-gps-receivers/all/1/, accessed 6 Feb 2015.

This presentation provides an excellent guide to the concepts behind Signals of Opportunity navigation, some of the issues, and some examples.

Source 2: Yang C.: 'http://socal.ion.org/wp-content/uploads/2013/06/ChunYang_sep_2011.pdf', ION Southern California Section Meeting, September 29, 2011, Torrance, CA. 2011.

Although a few years old and the state of the art has moved on, this technical report provides a wide ranging introduction to the concepts and technologies developed under the banner of inertial navigation, and in particular MEMS technologies.

Source 3: Woodman O.: 'An introduction to inertial navigation', University of Cambridge Technical Report number 696, August 2007.

This article presents some of the basic concepts behind optical navigation systems.

Source 4: 'Optical Navigation Systems: The foundation of modern pointing devices', http://www.edn.com/design/sensors/4419587/1/Optical-Navigation-Systems--The-foundation-of-modern-pointing-devices, accessed 6 Feb 2015.

This article in the technical press introduces Locata, a prominent example of a ground based positioning system.

Source 5: 'Locata wants to fill holes in GPS location, navigation', http://www.cnet.com/uk/news/locata-wants-to-fill-holes-in-gps-location-navigation/ accessed 6 Feb 2015.

Standards and policy (Government and non-Government)

There are no known standards and policies that are directly relevant to indoor navigation. Two areas of policies that are indirectly relevant are:

- Personal data security – there is already significant legislation and policy around the use of personal data, but as people offer up more and more data (including location) it is likely that controls will become more and more restrictive. At the same time, it is not clear yet what the public appetite for sharing position with on-line services is.
- eCall – the eCall legislation will embed a satellite navigation receiver into every new car sold in Europe (an eCall device will automatically alert emergency services, including location, when a vehicle is involved in an accident). Once there, it is likely that manufacturers will look for other value added services that can make use of the technology.

QinetiQ comment

Indoor navigation is a growing area. The sharp uptake of consumer navigation through GPS has been driven predominantly through the integration of devices into smartphones. The very high volume of sales has led to rapid progress and competition in the price, size footprint and power consumption of devices.

It is harder to foresee the consumer demand for indoor navigation where, typically, distances are smaller and locations are better known. Instead, it is likely that the high volume demand for indoor navigation may come from online information service providers such as Google, and retailers who will use accurate positioning to increase the relevance of personal data through tailored content, e.g. advertising. The challenge for service providers will be that they do not purchase or specify the user devices. They must demonstrate to users the value of the tailored content, in the face of questions around personal data security.

From the point of view of non-consumer users, it is easier to see the capability and efficiency gains from indoor navigation, in particular asset tracking. However, history has taught us that, without a very high value application, technological progress will be significantly slower without consumer demand.

The potential disruptive technology is quantum devices. Early demonstrations have shown that significant increases in position and timing accuracy may be possible over conventional MEMS and atomic clock technologies, but the maturity of these devices is very low, and not likely to be available for mainstream applications in the short or medium terms.

The area of secured navigation (in particular ensuring the availability, integrity of navigation data) is a related and growing field, in particular in light of a rise in instances of jamming threats and the increased viability of spoofing devices. While instances are limited at present, their use is growing at an alarming rate, in particular as many higher value assets (e.g. cars) are now fitted with trackers as a deterrent against theft. The impact of jammers and spoofers are often not fully recognised as navigation and, in particular, timing services may be deeply embedded into complex systems. There is a broad correlation between the technologies that provide secured navigation and those that can be used to deliver indoor navigation. Increased investment in developing technology for secured navigation may therefore also benefit the indoor navigation market.

Internet of Things (IoT)

Description

The Internet of Things (IoT) is a relatively new computing concept that is difficult to define. In simple terms, it consists of a collection of physical devices and objects connected to the Internet and each other allowing them to communicate with people or machines to monitor, simplify life, improve automation or provide an enhanced experience. These physical objects range from everyday items (such as household appliances, cars or mobile computing devices) to more specialist items (such as biomedical implants, pollutant sensors or wildlife trackers). The IoT is under-pinned by embedded sensors and control systems, communications protocols, identity management and is highly dependent on Machine-to-Machine (M2M) communications technology.

The vision of the IoT is a world where almost anything can be connected and communicate in an intelligent fashion. Although many benefits will be realised, the scale of the IoT phenomenon will significantly increase cyber security risks and will provide many opportunities for abuse. There is concern that there is no real incentive to address vulnerabilities that become present due to the IoT (see Source 1). As such, the issues and challenges arising from the IoT are numerous.

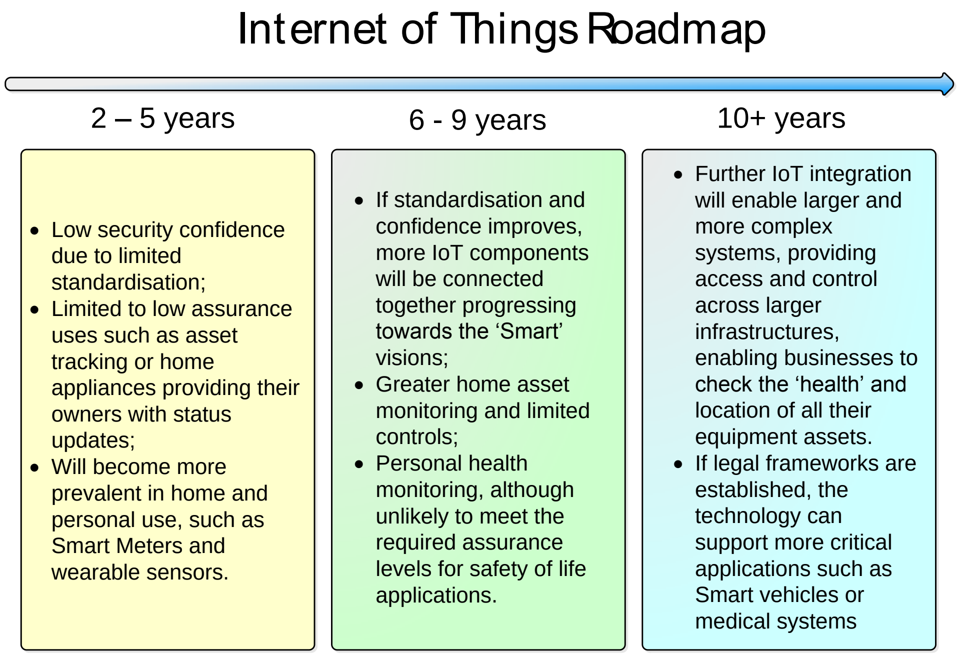
Relevant Applications

The IoT has the potential to be used in a wide variety of different applications. Examples devices that will become part of the IoT include: cars, lighting systems, refrigerators, telephones, SCADA systems, traffic control systems, home security systems, TVs, Digital Video Recorders and so on (see Source 2).

A list of 50 IoT related applications are presented in Source 3 below. These are categorised under Smart Cities, Smart Environment, Smart Watering, Smart Metering, Security & Emergencies, Retail, Logistics, Industrial Control, Smart Agriculture, Smart Animal Farming, Home Automation and eHealth.

Most Relevant Cyber Security Controls

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Malware Defences
- Application Software Security
- Boundary Defence
- Secure Network Engineering



Internet of Things Roadmap

2 – 5 years

- Low security confidence due to limited standardisation;
- Limited to low assurance uses such as asset tracking or home appliances providing their owners with status updates;
- Will become more prevalent in home and personal use, such as Smart Meters and wearable sensors.

6 - 9 years

- If standardisation and confidence improves, more IoT components will be connected together progressing towards the 'Smart' visions;
- Greater home asset monitoring and limited controls;
- Personal health monitoring, although unlikely to meet the required assurance levels for safety of life applications.

10+ years

- Further IoT integration will enable larger and more complex systems, providing access and control across larger infrastructures, enabling businesses to check the 'health' and location of all their equipment assets.
- If legal frameworks are established, the technology can support more critical applications such as Smart vehicles or medical systems

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: Low assurance uses, such as asset tracking or home appliances providing their owners with status updates, will become more prevalent. The proliferation of Smart Meters will enable users to become comfortable with the technology, leading to greater adoption within areas where it saves users time and effort, for example with wearable sensors.

Within 6 – 9 years: Greater adoption of the technology and improved security may enable IoT to be applied in a larger system context rather than point technologies, progressing towards the 'connected home' vision with greater integration of different solutions, provided standards can be agreed and implemented. Uses could extend to personal health monitoring, although unless the system can meet required assurance levels for applications with potential safety implications this may be limited to informing users rather than providing data to and response from the wider IoT infrastructure.

10+ years: Further IoT integration can be achieved enabling larger and more complex systems, expanding access and control across larger infrastructures, enabling businesses to check the 'health' and location of all their equipment assets. The technology may start to support more safety-critical applications if the legal framworks required for applications such as automated vehicles or medical based systems can be established.

General Issues and Challenges

Issues and challenges arising from the IoT are numerous. The enabling technologies of the IoT are rapidly maturing and innovators are constantly devloping new applications that are further driving the hype of the entire concept (see Source 2 below). Unfortunately, this rate of development is being matched by an equally large growth in security concerns. Recent presentations at both the Black Hat and Defcon security conferences highlighted weaknesses in various IoT devices (see Source 1). The Open Web Application Security Project (OWASP) (see Source 2) has constructed a list of what it considers are the top ten security problems for IoT devices. The breadth of these illustrates the challenges ahead. To quote the list:

"Insecure Web Interface; Insufficient Authentication/Authorization; Insecure Network Services; Lack of Transport Encryption; Privacy Concerns; Insecure Cloud Interface; Insecure Mobile Interface; Insufficient Security Configurability; Insecure Software/Firmware; Poor Physical Security."

There are clearly major challenges related to protecting the IoT and the people or devices that are connected to it. As an example, it is worth noting that while individuals may not be concerned if someone manages to determine the content of their fridge, they may well be concerned if that device is turned into a netbot and is used as part of a Distributed Denial of Service (DDOS) attack.

The nature of the application will, to a large extent, determine the required protection and the necessary assurance levels. For example, automating the control of a vehicle will require significantly greater assurance in the security than the ability to inspect the content of someone's fridge due to the potential consequences of control system failure or a security compromise. A lack of standardisation would limit how secure systems could be. A standard approach, with a framework of agreed / mandated standards, interfaces and protocols needs to be applied within the entire system to achieve the level of assurance required.

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

Source 1 highlights the concern that the IoT will remain vulnerable for years and that security updates will not keep pace with its development.

"An ineffective or non-existent plan for deploying security updates will be the single largest impediment to security for the Internet of Things. The reality is that vulnerabilities appear in all code from time to time. A solid security lifecycle that considers security throughout design and development will have notably fewer security issues. However, all software manufacturers must be ready to quickly respond to a vulnerability and release a patch to protect their users."

Source 1: Coates M.: **'**The Internet of Things will be vulnerable for years, and no one is incentivized to fix it', VentureBeat, http://venturebeat.com/2014/08/23/the-internet-of-things-will-be-vulnerable-for-years-and-no-one-is-incentivized-to-fix-it/, 23 August 2014, accessed on 18 Dec 2014.

The OWASP is described in Source 2 as a worldwide not-for-profit charitable organisation that is focused on improving the security of software. Their mission is to make software security visible, so that individuals and organisations can make informed decisions about true software security risks. The project walks through the top ten security problems that are seen with IoT devices, and provides tips on how to prevent them.

Source 2: 'OWASP Internet of Things Top Ten Project',

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_10_for_2014, accessed 18 Dec 2014.

Source 3 provides a list of 50 sensor IoT application areas which illustrates the wide variety of potential applications.

Source 3: '50 Sensor Applications for a Smarter World', http://www.libelium.com/top_50_iot_sensor_applications_ranking/ accessed 18 Dec 2014.

The IEEE Computer Society recently released a report surveying 23 innovative technologies that could change industry by the year 2022. Unsurprisingly the IoT is included:

"The IoT is here to stay, driven, among others, by device technology advances, the opportunities created by the billions of smartphones with their rich built-in sensors, Internet connectivity to fixed facilities, increased mobile connectivity, the new functionalities it enables, and business reasons, such as the desire to reduce cost through automation, reduced loss/wastage, and shorter durations for supply chains."

Source 4: IEEE Computer Society 2022 Report.

This source reports on the development of standards for the IoT:
"There's "…a land-grab in standards development, with multiple groups each hoping to set de facto standards..."
"With so much interest, it's clear that multiple standards will be developed to govern myriad aspects of the burgeoning IoT."

Source 5: McKendrick J.: Slowly but surely, standards on the way for Internet of Things', ZDNet, http://www.zdnet.com/slowly-but-surely-standards-on-the-way-for-internet-of-things-7000034388/ , 7 Oct 2014, accessed 18 Dec 2014.

Standards and policy (Government and non-Government)

The IoT is still in its infancy, particularly with regard to efforts at standardisation (see Source 5 above). Nevertheless, there are currently some frameworks and work being done to create standards to support developments. The Global Standards Initiative on IoT is promoting a unified approach within the ITU-T for developing technical standards and has created ITU-T Y.2060 (06/2012) which provides an overview of the IoT, clarifies its concept and scope, identifies its fundamental characteristics and high-level requirements and describes the IoT reference model.

QinetiQ comment

The IoT concept is being driven forward rapidly, but this is also opening up many security risks. Some bodies like the OWASP are publicising the potential threats and providing some awareness of the vulnerabilities of the IoT, but a more coherent approach to tackling this problem is required from industry.

Machine to Machine (M2M) Communications for the Automated Sharing of Cyber-threat Information

Description

Machine-to-Machine (M2M) communications refers to technology that allows the automatic exchange of data or information from one device to another through wired and wireless communications links.

M2M communications are an integral part of the “Internet of Things” (IoT) and in this context, are concerned with enabling the transfer of data from sensors and electronic devices in a network. The technology also has a raft of other applications and coupled with technologies such as autonomic computing (that aims to develop computer systems capable of self-management) and machine learning (that allows a computer program to predict an outcome or make a decision) can be used to share information automatically, machine-to-machine.

The ability to automatically transfer and share information is particularly useful in the cyber domain where there is a need to share information on cyber-threats and mitigation strategies in a timely manner.

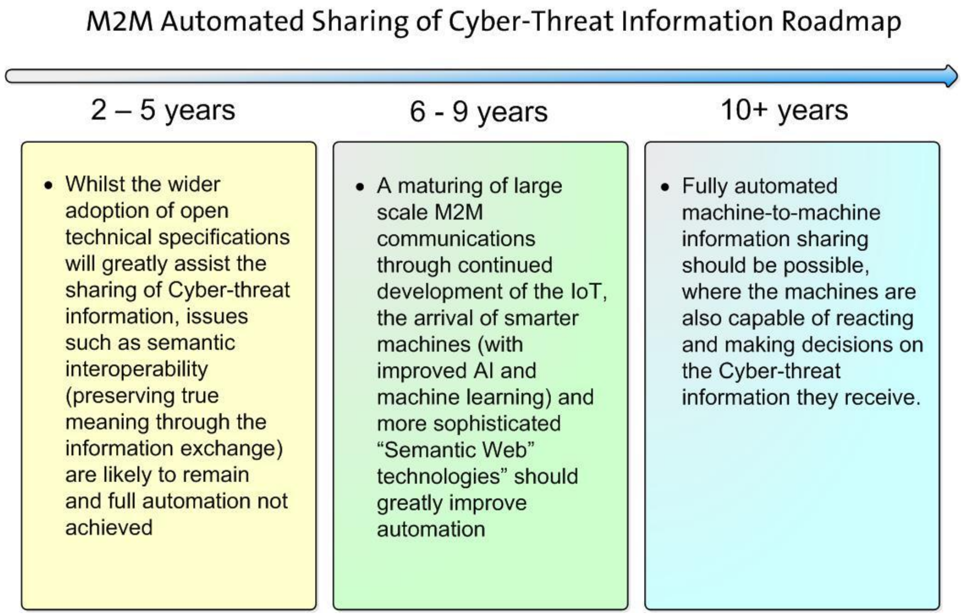
Automatic information sharing presents many challenges, many of which are non-technology in nature (see issues and challenges below). Furthermore, it is worth emphasising that potential solutions will require the implementation of information management and collaboration technology in addition to the M2M communications and supporting technologies.

Relevant Applications

The range of M2M applications is increasing in areas such as: telemetry, data collection, remote control, remote monitoring, security systems, logistic services, fleet management and the sharing of cyber-threat information, which is the focus of this paper (see source 1 below).

Most Relevant Critical Security Controls

- Malware Defences
- Incident Response and Management



M2M Automated Sharing of Cyber-Threat Information Roadmap

2 – 5 years

- Whilst the wider adoption of open technical specifications will greatly assist the sharing of Cyber-threat information, issues such as semantic interoperability (preserving true meaning through the information exchange) are likely to remain and full automation not achieved

6 - 9 years

- A maturing of large scale M2M communications through continued development of the IoT, the arrival of smarter machines (with improved AI and machine learning) and more sophisticated “Semantic Web” technologies” should greatly improve automation

10+ years

- Fully automated machine-to-machine information sharing should be possible, where the machines are also capable of reacting and making decisions on the Cyber-threat information they receive.

General Issues and Challenges

There are a number of issues and challenges that will need to be addressed if M2M technology is to be effective at sharing cyber-threat information, machine-to-machine and at machine speed as envisaged in Source 1. These include the following:

- Impact on Communications Infrastructure and Services. An OECD report (see source 2) examines M2M and notes the impact that numerous connected devices could have on infrastructure and services. It highlights the impact of such devices on the use of the electromagnetic spectrum and the demands that this could put on regulators and suppliers, which will present significant challenges.
- Standards. Whilst standards are being developed for M2M, particularly in the context of the IoT (see source 3) a greater challenge will be to establish standards for the representation of the data and its meaning (semantics) to allow information to be shared (see standards below).
- Data Syntax and Semantics. Effective information sharing between organisations is only possible if agreed meanings and representations of information exist. A key technological challenge in information exchange is ensuring that all the parties have a common understanding of the meaning of the data items transferred. This has proven to be difficult when passing data to human beings, but for M2M exchanges if the receiving machine is intended to automatically process and react to the received information then the scale of the challenge increases dramatically. Semantic web technologies such as Resource Description Framework (RDF), Web Ontology Language (OWL) and eXtended Markup Language (XML) provide the building blocks to develop and formalise these syntactic and semantic agreements and potentially to allow the development of sophisticated translation engines. The difficulty is that developing these representations has proven to be extremely time consuming, requiring domain knowledge as well as information modelling skills. There are initiatives underway that concern the sharing of information about Cyber-threats. A summary of these can be found in Source 4 below. The Department of Homeland Security (DHS) Office of Cyber Security and Communications, the National Cyber Security and Communications Integration Centre, and the US Computer Emergency Readiness Team (CERT) (see source 5) are leading efforts to automate and structure operational Cyber Security information sharing techniques across the globe. As part of this endeavour, the following services and tools are offered free for public use: TAXII™ (Trusted Automated eXchange of Indicator Information), STIX™ (Structured Threat Information eXpression) and CybOX (Cyber Observable eXpression). Both STIX and TAXII are summarised in the standards section below.
- Security. The security challenges of more automated information sharing are significant and have many different aspects. It is important to ensure that the information is only shared with appropriate receivers and that the information received has come from a known and trusted source and has not been compromised in any way. Automated exchange potentially provides a vector through which an attack could be made, inserting false information to confuse the receiver or encourage incorrect decisions and actions to be taken. Use of existing mechanisms to digitally sign information exchanges and use of certificates and encryption are all possible.
- Legal considerations. Before sharing any information, any organisation must consider whether it has the legal right to do so, considering such aspects as privacy and data protection, commercial and intellectual property rights, security constraints, etc. Establishing the legal framework for such sharing will be necessary, and the rules associated with this will need to be automatically enforced and auditable. Technologies that can examine M2M message content against the rules for release will be required. Content checking technologies will need to become more sophisticated and be able to adapt to changing needs in appropriate short timeframes. Commercial interests may also lead to reluctance to share certain information.
- Complexity. Complex M2M systems could exhibit undesirable and unpredictable behaviour. Such emergent behaviour will need to be closely monitored and managed.

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

In a recent news article released by the US Department of Defence, the commander of U.S. Cyber Command, director of the National Security Agency and chief of the Central Security Service Admiral Michael S. Rogers was reported to have discussed the use of M2M in the context of a legal framework for sharing Cyber information. To quote:

"Rogers said the command needs a legal framework "that enables us to rapidly share information, machine-to-machine and at machine speed, between the private sector and the government."

"The framework, he added, must be fashioned in a way that provides liability protection for the corporate sector and addresses valid concerns about privacy and civil liberties."

Source 1: Pellerin C.: 'Cybercom Chief Details U.S. Cyber Threats, Trends', DoD News, Defense Media Activity, http://www.defense.gov/news/newsarticle.aspx?id=123696, 21 Nov 2014, accessed on 17 Dec 2014.

The OECD report 'Machine-to-Machine Communications: Connecting Billions of Devices', Organisation for Economic Co-operation and Development, has as a focus the impact of M2M and the explosion in the number of connected devices.

Source 2: Machine-to-Machine Communications: Connecting Billions of Devices', Organisation for Economic Co-operation and Development, DSTI/ICCP/CISP(2011)4/FINAL, 30-Jan-2012.

The Open Mobile Alliance (OMA) is promoting a common set of standards for M2M.

Source 3: M2M enablers, Open Mobile Alliance, http://openmobilealliance.org/about-oma/work-program/m2m-enablers/, accessed 3 March 2015.

This source states the requirements for a Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) and presents the case that improved information sharing and automation should be forthcoming in the Cyber Security domain.

Source 4: Dandurand L., Serrano Serrano O.: 'Towards Improved Cyber Security Information Sharing, 2013 5th International Conference on Cyber Conflict, 2013 © NATO CCD COE Publications, Tallinn.

In the US, the Department of Homeland Security (DHS) Office of Cyber Security and Communications, the National Cyber Security and Communications Integration Center, and the US Computer Emergency Readiness Team (CERT) are leading efforts to automate and structure operational Cyber Security information sharing techniques.

Source 5: 'Information Sharing Specifications for Cybersecurity', US-CERT, https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity, accessed 24 Feb 2015.

Source 6: STIX™ Website, https://stix.mitre.org/ , accessed 3 March 2015.

Source 7: TAXII™ Website, http://taxii.mitre.org, accessed 3 March 2015.

Source 8: SOLTRA Website, http:// www.soltra.com, accessed 3 March 2015.

Standards for Information Sharing

To be able to share information between machines requires standards to be agreed and implemented. How general and widely used these standards need to be is highly dependent on the scope of the desired sharing. The close relationship between M2M and the IoT means that many of the fundamental standards to support communication are those of the Internet such as TCP/IP and associated standards for naming and addressing, messaging protocols, etc. However, as previously stated, the greatest challenge will be to establish standards for the representation of the data and its meaning (semantics) to allow information to be shared.

STIX™ and TAXII™ are community-driven technical specifications designed to enable automated information sharing for cyber security situational awareness, real-time network defence and sophisticated threat analysis.

- STIX is an effort to define and develop a standardized language to represent structured Cyber-threat information. The STIX Language intends to convey the full range of potential Cyber-threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible. Interested parties are invited to participate in the collaborative community that is evolving STIX (see source 6);
- TAXII defines a set of services and message exchanges that enable sharing of actionable Cyber-threat information across organization and product/service boundaries. TAXII is not an information sharing initiative or application and does not attempt to define trust agreements, governance, or other non-technical aspects of Cyber-threat information sharing (see source 7). TAXII defines how STIX messages can be transported over HTTP protocols'.

These open standards have been adopted by commercial companies who provide services and products such as SOLTRA (see source 8) whose Edge product takes large amounts of complex threat information across communities, people and devices and analyses, prioritizes, and routes it to users in real-time.

QinetiQ comment

Experience has shown that there is often difficulty in reaching agreement on standardisation when large groups of stakeholders are involved and that compromises, complexity and delays can result.

Nano-computing

Description

Nano-computing is the class of extremely small and low cost computer devices. It extends from the class of microcomputers that have been in the mainstream for approximately thirty years and are also sometimes referred to as ‘single board’ or ‘credit card’ computers.

Traditionally these small form factor type devices have not had enough computing power to be used for computationally intensive tasks and/or were typically application specific (e.g. process controllers, network switches etc.).

The advent of the Raspberry Pi, popularised the usage of low cost, small form factor, networked multi-media capable devices with accessible external control interfaces for educational, hobbyist and professional usage resulting in significant on-line community resources and projects. This has led to a proliferation of nano-computing platforms, including the Raspberry Pi, the BeagleBoard, the Arduino and the Intel Edison.

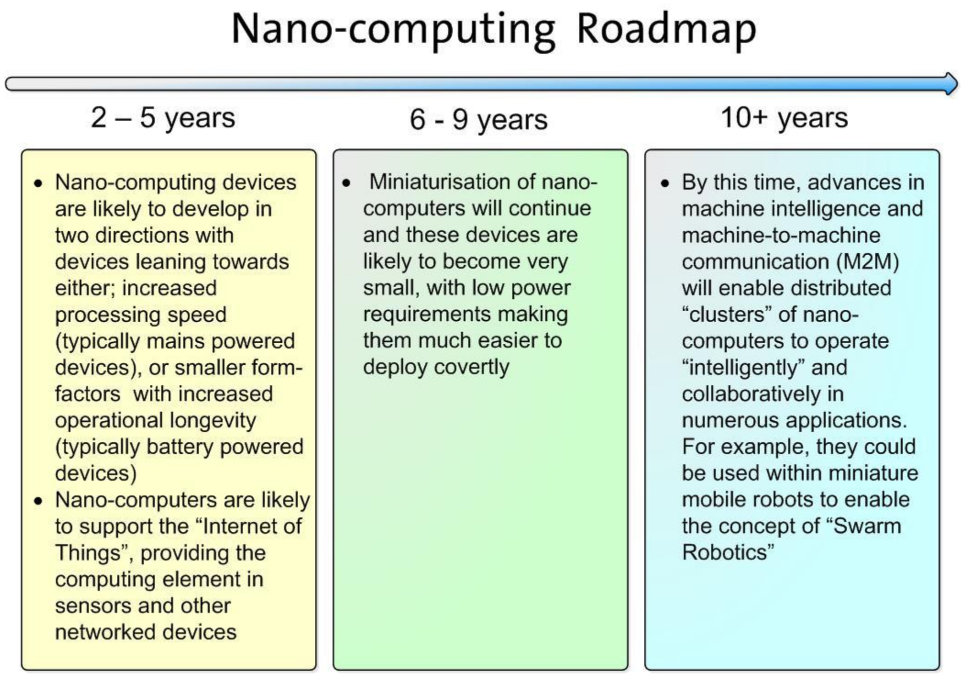
Relevant Applications

Nano-computing has developed rapidly over the last few years and is widely used in the following areas:

- Building automation: These devices can be easily concealed in ceiling, wall or floor voids and are silent in operation making them ideally suited to automation applications in the built environment.
- Education: Due to the low cost and portability of these devices coupled with funding from organizations’ such as Google (see source 3).
- Training and prototyping: Because these devices are extremely low cost they are well suited to training programmers and prototyping software and hardware applications.

Most Relevant to Critical Security Controls

- Inventory of Authorized and Unauthorized Devices
- Wireless Access Control
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Boundary Defence
- Controlled Access Based on the Need to Know
- Secure Network Engineering



Nano-computing Roadmap

2 – 5 years

- Nano-computing devices are likely to develop in two directions with devices leaning towards either; increased processing speed (typically mains powered devices), or smaller form-factors with increased operational longevity (typically battery powered devices)
- Nano-computers are likely to support the “Internet of Things”, providing the computing element in sensors and other networked devices

6 - 9 years

- Miniaturisation of nano-computers will continue and these devices are likely to become very small, with low power requirements making them much easier to deploy covertly

10+ years

- By this time, advances in machine intelligence and machine-to-machine communication (M2M) will enable distributed “clusters” of nano-computers to operate “intelligently” and collaboratively in numerous applications. For example, they could be used within miniature mobile robots to enable the concept of “Swarm Robotics”

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: Nano-computing devices are likely to develop in two directions with devices leaning towards either; increased processing speed (typically mains powered devices), or smaller form-factors with increased operational longevity (typically battery powered devices). This latter form are likely to support the "Internet of Things", providing the computing element in sensors and other networked devices.

Within 6 – 9 years: Minaturisation will continue and these devices are likely to become very small, with low power requirements making them easier to deploy.

10+ years: By this time, advances in machine intelligence and machine-to-machine communication (M2M) will enable distributed "clusters" of nano-computers to operate "intelligently" and collaboratively in numerous applications. For example, they could be used within miniature mobile robots to enable the concept of "Swarm Robotics".

General Issues and Challenges

Nano-computing is still relatively immature, but is gaining ground in other areas of computing and benefitting from the support of more operating systems.

Such technology has the potential to have a major impact on cyber security by disrupting existing security measures. For example when deployed covertly over long periods of time (see source 2) these devices could be used to monitor and/or modify network traffic (particularly wireless traffic) either through a 'dummy' access point or by sniffing out vulnerabilities in nearby networks.

Power sources and battery technology remain one of the limiting factors for this type of device when used covertly.

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

The Computing magazine recently reported on developments of the Raspberry Pi, highlighting its increased processing speed and that it will be able to run the Windows operating system.

"The Raspberry Pi Foundation revealed the official second edition of its Raspberry Pi SOC (system-on-a-chip) computer today, promising speed increases of up to six times, and compatibility with upcoming ARM builds of Windows 10."

Source 1: Gothard P.: 'Raspberry Pi 2 launches with 6x faster processor and Windows 10 promise', Computing 2393184, 2 February 2015.

A niche security research company has managed to shoehorn a Raspberry Pi into a VOIP phone for covert monitoring:

"Earlier this year, the security company Portcullis published a detailed a project called the ph0wn wherein a Raspberry Pi was implanted into a standard VoIP telephone with the intention to create a device for covert network access and exfiltration. Holding true to the over used maxim of Picasso, we decided to gleefully steal the idea, and expand upon it."

Source 2: Xiphos Research.: 'Hiding in Plain Sight – A Raspberry Pi VOIP Phone Covert Device, Xiphos Research Labs, 21 August 2014.

The use of the Raspberry Pi to inspire children into becoming the next generation of computer scientists was reported by the BBC

"Schools around the UK are to be given 15,000 free microcomputers, with a view to creating a new generation of computer scientists. Funded by Google, the Raspberry Pi Foundation hopes the free devices will inspire children to take up coding. The pared-down Raspberry Pi, launched a year ago, is already a huge success. There are concerns that current information and communications technology (ICT) teaching is inadequate preparation for the future jobs in technology."

Source 3: Wakefield J., Rich L. J.: 'Google to give schools Raspberry Pi microcomputers', BBC News, 29 January 2013, http://www.bbc.co.uk/news/technology-21243825, accessed 25 February 2015.

Standards and policy (Government and non-Government)

Nano-computing technology is still maturing and standardisation has yet to happen, and it is questionable whether it is needed. There does not appear to be an independent national or global body that is driving standards, manufacturers are promoting their own devices and maintaining control over their development, for example the Raspberry Pi Foundation promotes all things to do with the Raspberry Pi. There are no known Government policies relating to this technology at the current time.

QinetiQ comment

Advances in battery technology, driven particularly by the communications (smartphones) and transportation (electric vehicle) sectors are likely to have a significant influence on the direction that nano-computing takes. As battery life improves and size and price per watt-hour reduces, the deployment of these devices in key locations for long periods of time will become much easier and will open up yet further opportunities for cyber-criminals. As a final point, QinetiQ believes that the hype behind clusters of nano-computers performing as a supercomputer do not really add up. It would take a countless number of nano-computers to match the performance of current supercomputers and this is unlikely to change.

Near Field Communication (NFC)

Description

Near Field Communication (NFC) is a short-range high frequency wireless communication technology that evolved from 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) at 13.56MHz. Typically, NFC occurs between a reader (often 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 does not, 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.

The technology has seen slower adoption than initially anticipated, Gartner predicts that NFC will account for about 5% of global mobile payment transaction value by 2017 (see Source 1 below).

Relevant Applications

NFC has numerous applications although its most common application is to enable contactless payment with mobile smartphones. Other applications include:

Access control – supporting authentication and providing access to secure areas;

Information collection and exchange – information can be passed from reader to reader (e.g. by touching devices) and picked up from targets (tags) on objects (which might be marking particular locations);

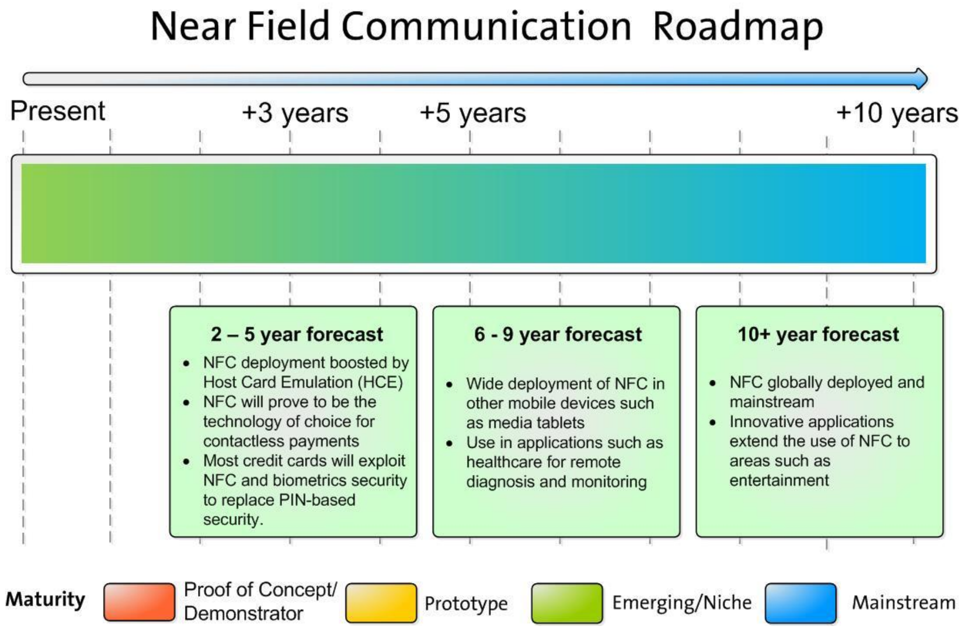
Marketing – Use in interactive posters.

NFC has also been deployed in areas such as public transport, social networking, point-of-sale loyalty and for improving user interaction with mobile devices.

Source 2 lists many of the areas where NFC has been deployed.

Most Relevant Cyber Security Controls

- Wireless Access Control
- Controlled Access Based on the Need to Know



2 – 5 year forecast

- NFC deployment boosted by Host Card Emulation (HCE)
- NFC will prove to be the technology of choice for contactless payments
- Most credit cards will exploit NFC and biometrics security to replace PIN-based security.

6 - 9 year forecast

- Wide deployment of NFC in other mobile devices such as media tablets
- Use in applications such as healthcare for remote diagnosis and monitoring

10+ year forecast

- NFC globally deployed and mainstream
- Innovative applications extend the use of NFC to areas such as entertainment

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: NFC will continue its deployment boosted by Host Card Emulation (HCE). The debate over Blue Tooth Low Energy and NFC should be resolved in this timeframe with NFC proving to be the technology of choice for contactless payments. Most credit cards will exploit NFC and biometrics security to replace PIN-based security.

Within 6 – 9 years: Wide deployment of NFC in other mobile devices such as tablets and use in applications such as healthcare for remote diagnosis and monitoring.

10+ years: NFC will be mainstream and deployed globally. One can expect a broader range of innovative applications extending to areas such as entertainment.

General Issues and Challenges

There has been a lot of hype and expectation set on NFC although examining Source 2 below will show it is currently being deployed world-wide, albeit slower than initially anticipated.

Privacy and security are still 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 one device thereby infecting other devices that the original communicates with later).
- Theft of a device when it is not protected by an appropriate form of authentication.

Good sources covering security and NFC are Source 3 below and the paper entitled 'Security in Near Field Communication (NFC)' which may be found here: http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf

There has also been some comparison of NFC with alternative wireless technologies and with Bluetooth in particular. It has been claimed that Bluetooth Low-Energy (BLE) technology could offer an attractive alternative to NFC. The NFC forum (see Source 4 below) explains that both technologies have their benefits, but believes both technologies will work together to serve users' data transmission needs.

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

Gartner's hype cycle for consumer services and mobile applications mentions a number of reasons for the slow deployment of NFC, two of these reasons are as follows: that NFC is not necessarily more convenient than cash or credit card and that merchants do not see how NFC payments will increase sales. Gartner do however believe that Host Card Emulation (HCE) may speed up NFC deployments by simplifying the infrastructure and reducing costs. The following are key findings from this source:

"NFC payment has seen slow adoption across all markets."

"We expect NFC to account for about 5% of global mobile payment transaction value by 2017."

"Host Card Emulation (HCE) may speed up NFC deployments by simplifying the infrastructure and reducing costs. HCE enables service providers such as banks and merchants to offer NFC services directly to their customers, without going through third-parties such as communication service providers (CSPs) or trusted service managers (TSMs)."

Source 1: Gartner, 'Hype Cycle for Consumer Services and Mobile Applications, 2014', Blau B., G00263598, 29 July 2014.

Wikipedia has listed deployments of NFC by country.

Source: 2: 'List of applications of near field communication', http://en.wikipedia.org/wiki/List_of_applications_of_near_field_communication, accessed 8 Dec 2014.

This source provides an easy-to-read overview of NFC security. The key points it raises are as follows: NFC is very short range and the signals are extremely sensitive in terms of direction, so eavesdropping is difficult. More likely a hacker will compromise the target microchip (the example given is a tag in a promotional movie poster) in order to get malicious code on to the reader (in this case, a smart-phone). Privacy is a concern and this source closes with tips on how to use NFC with minimum risk.

Source 3: Chandler N.: 'How secure is NFC tech?' http://electronics.howstuffworks.com/how-secure-is-nfc-tech1.htm, accessed 5 Dec 2014.

The NFC Forum (see standards and policy below) aims to provide accurate, factual information about the growth of NFC and how it relates to the user.

Source 4: http://www.nfc-forum.org/aboutnfc.

Standards and policy (Government and non-Government)

The NFC Forum (see Source 4 above) which was formed by Nokia, Sony, and Royal Philips Electronics in 2004, promotes the sharing, pairing, and transactions between NFC devices and develops and certifies device compliance with NFC standards. The NFC Forum states: "*Standards exist to ensure all forms of near field communication technology can interact with other NFC compatible devices and will work with newer devices in the future. Two major specifications exist for NFC technology: ISO/IEC 14443 and ISO/IEC 18000-3. The first defines the ID cards used to store information, such as that found in NFC tags. The latter specifies the RFID communication used by NFC devices."*

QinetiQ comment

The adoption of NFC has been slower than initially predicted, but support from big name players such as Google, PayPal and MasterCard are helping to drive it forward. Recently Apple has joined the fold with Apple Pay, which uses NFC to enable contactless payment on the iPhone 6. Such a move is yet another sign that the world is moving towards NFC payment rather than alternatives such as "CurrentC" that uses a payment method based on a QR code.

It is worth emphasising that although the terms NFC and contactless payment may seem virtually synonymous, there are many other innovative uses for the technology as highlighted in the applications section above. One area to watch will be the up-take of the technology in public services and transportation.

Finally, it is worth keeping a watch on Bluetooth Low Energy (BLE) technology (Apple is using this in its iBeacon initiative) although it is doubtful that it will have a major impact on the development and deployment of NFC as it mostly serves different use cases.

Networked Medical Devices and Equipment

Description

Advances in medicine have lead to a wide range of medical devices, which are used for both diagnosis and treatment. This includes those used acutely within a healthcare environment (e.g. for medical imaging) and long-term implanted devices, such as pacemakers and medication pumps (including those for insulin).

Telemedicine (using communications technologies to deliver healthcare at a distance) reduces the need for patients to physically visit their doctor. Home health monitors and wearable electronic devices (which are able to provide real time information such as heart rate wirelessly to other devices) are becoming more widespread.

Increased connectivity of these devices offers many advantages, including earlier warning of health events, reduced need for invasive investigations and increasing healthcare providers' efficiency. However, this connectivity also increases the risks faced by these systems.

Most Relevant Cyber Security Controls

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Malware Defences
- Wireless Access Control
- Data Recovery Capability
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Controlled Use of Administrative Privileges
- Maintenance, Monitoring, and Analysis of Audit Logs
- Controlled Access Based on the Need to Know
- Data Protection

Relevant Applications

The following are a few examples of potential applications for connected medical devices:

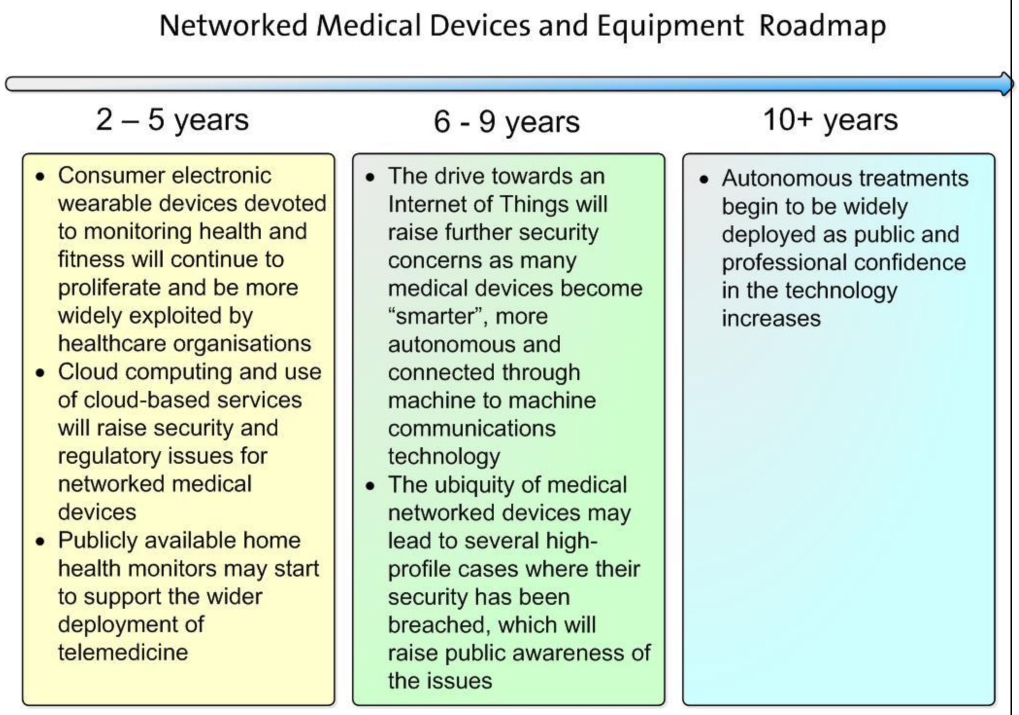
- **Remote care and monitoring:** vulnerable patients could be monitored remotely, with an alarm raised or medicine administered if necessary.
- **Implanted monitoring and treatment:** continously monitoring conditions such as diabetes via implants that communicate wirelessly may lead to greater safety and convenience. If an implanted sensor detects that a drug is required, it could trigger its release.
- **Connected hospitals:** as connectivity in hospitals increases, diagnostic measurements, imaging results and perhaps recordings of surgical procedures will be more accessible to healthcare workers. This also offers advantages for staff training and integration with patient records.

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: In this period, consumer electronic wearable devices devoted to monitoring health and fitness will continue to proliferate. Such technology is likely to become more widely exploited by healthcare organisations. The continued adoption of cloud computing and use of cloud-based services will raise security and regulatory issues for networked medical devices. The development of publicly available home health monitors at the required assurance levels may start to support the wider deployment of telemedicine. Networked medical devices that improve diagnosis and treatment continue to be deployed at relatively small scales; similar technologies realise large gains in the efficiency of medical logistics.

Within 6 – 9 years: The drive towards an Internet of Things (IoT) will raise further security concerns as many medical devices become "smarter", more autonomous and connected through machine to machine (M2M) communications technology. Telemedicine matures and medical services at this time could include the remote monitoring of vulnerable patients. In this time, the ubiquity of networked devices in the medical domain may lead to several high-profile cases where their security has been breached, which will raise public awareness of these issues.

10+ years: Autonomous treatments begin to be widely deployed as public and professional confidence in the technology increases.



Networked Medical Devices and Equipment Roadmap

2 – 5 years

- Consumer electronic wearable devices devoted to monitoring health and fitness will continue to proliferate and be more widely exploited by healthcare organisations
- Cloud computing and use of cloud-based services will raise security and regulatory issues for networked medical devices
- Publicly available home health monitors may start to support the wider deployment of telemedicine

6 - 9 years

- The drive towards an Internet of Things will raise further security concerns as many medical devices become "smarter", more autonomous and connected through machine to machine communications technology
- The ubiquity of medical networked devices may lead to several high-profile cases where their security has been breached, which will raise public awareness of the issues

10+ years

- Autonomous treatments begin to be widely deployed as public and professional confidence in the technology increases

General Issues and Challenges

There are many security issues and challenges relating to networked medical devices and equipment and the current trend for more connectivity between electronic devices driven by a move towards an IoT will only exacerbate the situation. Source 1 (see below), identifies a number of specific issues and challenges relating to networked medical devices which includes concerns over the software they use and the need for upgrades set by regulation. The following are a number of other issues and challenges that will need to be addressed.

<u>Threats to individuals</u>

The impact of an attack against networked medical devices could be catastrophic for the individual involved. For example, the wireless capabilities of Dick Cheney's pacemaker were disabled due to fears of assassination attempts (see Source 6 below). Control of these devices (perhaps via a vulnerability) could provide one individual very powerful influence over another. Source 4 highlights that these devices can be compared to `Human Industrial Control Systems' and that their priorities are safety and reliability, rather than security (particularly for highly time-critical and emergency responses).

Security constraints

The physical characteristics (e.g. size, weight, power consumption, heat output) of implanted devices are often restricted. Similarly replacing, updating or patching these devices may be inconvenient and risky. This leads to the difficult situation where security is required for the lifetime of the device (perhaps several decades) but only lightweight security mechanisms are available. For existing devices, this is likely to become a significant issue.

Increased connectivity

The IoT and its associated technologies are likely to have a huge impact on connected medical devices. Unfortunately, the current levels of assurance in IoT devices are not yet sufficient to meet the needs of medical devices and equipment. For many devices incorporating sensors, providing accurate information is crucial; as medical devices become more automated, the impact of spoofed sensor data may also increase.

Privacy

The connectedness of these devices also raises several privacy concerns. The availability of medical records to other healthcare professionals (e.g. emergency doctors and ambulance staff) could be increased using cloud-based techniques, however this relies on the security and privacy of data in the cloud. Remotely monitoring patients' conditions could improve the preventative care for vulnerable patients, but that data may be very personally sensitive.

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

Wikipedia provides an article covering "Medical Device Connectivity", which includes reference to a paper in a Biomedical Instrumentation journal that discusses the growing Cyber-threat to medical devices. This paper highlights the following issues and challenges (quoted from Wikipedia):

- *medical devices often operate with commercial central processing units, operating systems, or off-the-shelf software, which place them at risk of Cyber-threat.*
- *due to tight regulations surrounding medical devices, upgrades to software and security installations must be approved by the manufacturer, resulting in delays.*
- *device operating systems are often early generation and may no longer be supported.*
- *homogenous device environments facilitate rapid spread of computer virus.*

Source 1: Wirth A.: 'Cybercrimes pose growing threat to medical devices', Biomedical instrumentation & technology/Association for the Advancement of Medical Instrumentation, Vol. 45, No. 1, pp. 26-34., January/February 2011.

The Cyber Security and privacy blog hosted by the company PWC provides a brief overview of the Cyber Security of networked medical devices, noting that:

"If the benefits of networked medical devices are momentous, so too are the potential security risks."

It continues, demonstrating the dire state of medical device security:

"The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an alert last year warning that 300 medical devices from 40 vendors have hard-coded

password vulnerabilities. Other potential weaknesses include the use of unpatched systems and devices, legacy equipment and software, and a general lack of security and privacy technologies."

Source 2: Coady M., Fisher G.: 'It's time to improve cybersecurity for networked medical devices', PWC, 11 December 2014, http://usblogs.pwc.com/cybersecurity/its-time-to-improve-cybersecurity-for-networked-medical-devices/, accessed 23 March 2015.

This source highlights the vulnerabilities and security issues concerning connected medical devices and equipment following a study in the US.

"In a study spanning two years, Erven and his team found drug infusion pumps–for delivering morphine drips, chemotherapy and antibiotics–that can be remotely manipulated to change the dosage doled out to patients; Bluetooth-enabled defibrillators that can be manipulated to deliver random shocks to a patient's heart or prevent a medically needed shock from occurring; X-rays that can be accessed by outsiders lurking on a hospital's network".

Source 3: Zetter K.: 'It's insanely easy to hack hospital equipment', Wired, 25 April 2014, http://www.wired.com/2014/04/hospital-equipment-vulnerable/, accessed 24 March 2015.

At Blackhat 2011, the author of this paper described some potential vulnerabilities in insulin pumps and blood sugar monitors.

Source 4: Radcliffe J.: 'Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System', 2011, https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf, accessed 24 March 2015.

The UK Government website has a page devoted to "Medical devices regulation and safety".

Source 5: UK Government, Medical devices regulation and safety, https://www.gov.uk/medicines-medical-devices-blood/medical-devices-regulation-safety, accessed 24 March 2015.

In an article entitled "Yes, terrorists could have hacked Dick Cheney's heart", the Washington Post highlights the lack of security on medical devices and presents the case of the US politician, Dick Cheney, where there were concerns that his heart implant could have been a potential target for hackers.

Source 6: Peterson A.: 'Yes, terrorists could have hacked Dick Cheney's heart', The Washington Post, 21 October 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/, accessed 13 April 2015.

Standards and policy (Government and non-Government)

There are many regulatory requirements for medical devices, covering safety, effectiveness, interoperability and security. The following are illustrative:

- ISO/IEEE 11073 (Medical/health device communication standards) enables the communication between medical, health care and wellness devices and with external information/computer systems.
- ISO 13485 describes quality management systems for medical devices.
- ISO/TR 21548:2010 is a set of guidelines for the security requirements when archiving electronic health records.
- British Standard BS8521 and the Telecare & Telehealth Integrated Code of Practice provide guidance when creating tele-health solutions.

- British Standard BS EN 80001 defines the roles, responsibilities and activities that are necessary for risk management of IT-networks incorporating medical devices to address safety, effectiveness and data and system security.
- the European Commission has issued directives 90/385/EEC and 2007/47/EC that concern “Active Implantable Medical Devices”.

In the US, the Food and Drug Administration (FDA) has issued draft guidance on the management of Cyber Security in medical devices.

The Medicines and Healthcare Products Regulatory Agency regulates medicines and medical devices in the UK (see Source 5).

QinetiQ comment

Many of the issues faced by connected medical devices are similar to those faced by industrial control systems and automated vehicles. Public awareness and concern over these issues is likely to be particularly high in medical devices, due to the impact on the affected individuals. The chance of interference affecting the wireless signals from these devices is likely to increase; to avoid this issue, widespread collaboration will be required between device manufacturers, users and regulators.

Next Generation Firewalls (NGFWs)

Description

Traditional firewall technologies have relied on policing network communications using well-known ports, basic protocol inspection and Internet Protocol (IP) addresses, to deliver host and network protection. These have worked effectively in the past but are no longer adequate to address the security issues of modern applications, especially the vast number that use web protocols or are encrypted. They are also not able to protect against the sophisticated threats, which have evolved to bypass static defences.

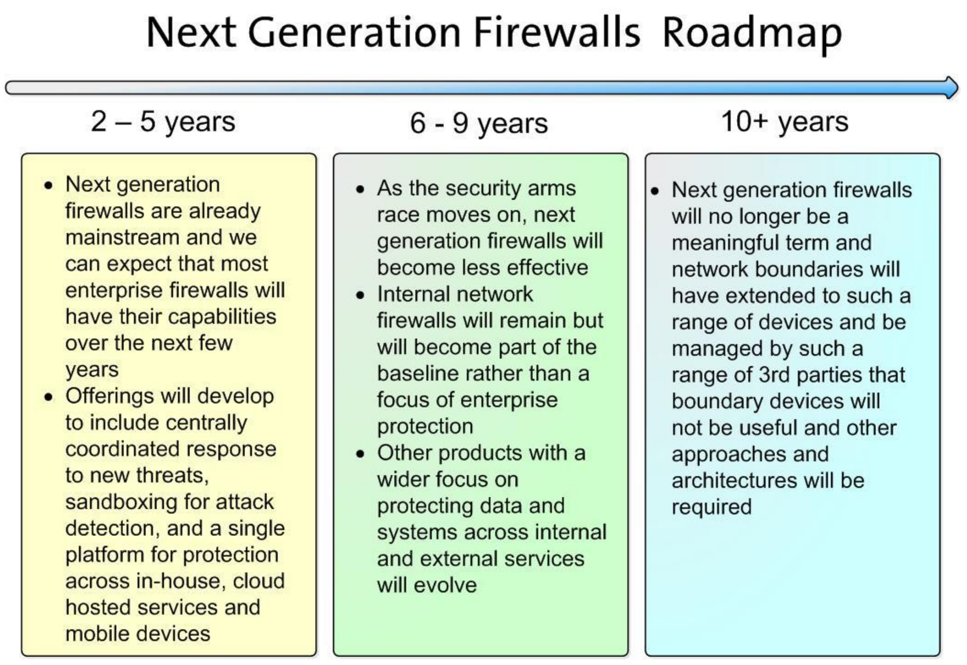
NGFWs augment the capabilities of traditional firewalls through a granular understanding of individual applications, the ability to identify the user as well as the IP address. Furthermore, some have the ability to inspect encrypted traffic, conduct intrusion prevention (also known as deep packet inspection) and can use "extra firewall" intelligence to improve blocking decisions, such as the use of identity services such as Active Director.

These capabilities allow the firewall to understand the application and the actions the user is taking (e.g. updating Facebook vs viewing Facebook), and to identify a wide range of security vulnerabilities and attacks at the firewall instead of relying on separate layers of protection.

Some NGFWs also integrate well with advanced intrusion detection systems (IDS) using, for example, Snort rules for advanced attack detection. These devices are effectively a combined firewall and IPS device. This information can be integrated with other sources to provide a holistic view of the security picture across the enterprise.

Most Relevant Cyber Security Control

- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches



Next Generation Firewalls Roadmap

2 – 5 years

- Next generation firewalls are already mainstream and we can expect that most enterprise firewalls will have their capabilities over the next few years
- Offerings will develop to include centrally coordinated response to new threats, sandboxing for attack detection, and a single platform for protection across in-house, cloud hosted services and mobile devices

6 - 9 years

- As the security arms race moves on, next generation firewalls will become less effective
- Internal network firewalls will remain but will become part of the baseline rather than a focus of enterprise protection
- Other products with a wider focus on protecting data and systems across internal and external services will evolve

10+ years

- Next generation firewalls will no longer be a meaningful term and network boundaries will have extended to such a range of devices and be managed by such a range of 3rd parties that boundary devices will not be useful and other approaches and architectures will be required

Relevant Applications

NGFWs (those that provide deep packet inspection) have now reached the mainstream and should be used in place of traditional firewalls wherever complex application traffic is being controlled. They are able to provide greater protection for networks and can provide more contextual information to support protective monitoring initiatives and intelligence about attacks on the network.

In many cases, NGFWs provide a more efficient platform for intrusion prevention than separate IPS, as they are able to monitor only traffic that is already passed by the configured firewall rules. This is now increasingly true as many traditional IPS and IDS rule sets can be integrated into traditional firewall technology.

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: NGFWs are already mainstream and over the next few years most enterprise firewalls will have these capabilities, albeit perhaps with a separate license cost. Offerings will develop to include centrally coordinated response to new threats, sandboxing for attack detection, and a single platform for protection across in-house, cloud hosted services and mobile devices. NGFWs are already often available as physical or virtual appliances, or integrated into software defined networks.

Within 6 – 9 years: As the security arms race moves on, NGFWs will become less effective. Many of these capabilities will be used as part of the core service by cloud providers where the focus for new capabilities will be total visibility of security across network hosts and applications. Internal network firewalls will remain but will become part of the baseline rather than a focus of enterprise protection. Other products with a wider focus on protecting data and systems across internal and external services will evolve from current firewalls and the burgeoning range of other security products.

10+ years: NGFWs will no longer be a meaningful term and network boundaries will have extended to such a range of devices and be managed by such a range of 3rd parties that boundary devices will not be useful and other approaches and architectures will be required.

General Issues and Challenges

Assessing the effectiveness and quality of NGFWs is challenging and there are no generally accepted standards against which the full range of capabilities can be measured. In addition, the nature of the threats is that they move rapidly and for a NGFW to offer good protection it must evolve constantly.

To make best use of threat sharing and global rapid response, firewalls automatically send suspicious content and session data for central analysis by vendor managed automated systems. This delivers rapid response to common global threats, but may prove challenging for government organisations and classified networks.

More services are moving onto cloud platforms, and there are real difficulties assessing the effectiveness of firewalls provided as part of these services. In addition, much can be learnt from effective protective monitoring with the output of these firewalls being a key component. The protective monitoring capabilities of most organisations are immature, and the cloud services are rarely able to provide sufficient data per-customer to enable protective monitoring services to get a complete picture of the security of all the systems they depend upon.

Finally, it is worth noting that whilst NGFWs offer greater protection, they are more complex and require both more time and a greater range of skills to manage effectively.

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

The IT analyst company Gartner identify NGFWs as mature and mainstream in their hype cycle for infrastructure protection. They consider that the technology will bring a high benefit and report that the current uptake of NGFWs as between 20% and 50%. The report includes the following recommendations:

"Consider NGFWs for your shortlist if you're replacing or upgrading a network firewall at the network edge, and you don't have a significant investment in a stand-alone IPS.

However, if you have such an IPS investment, ensure that any selected firewall has an NGFW as a current option (or on the near-term road map), so that, when the IPS needs to be replaced, you'll have the option to move to an NGFW with the least amount of disruption."

Source 1: Gartner, 'Hype Cycle for Infrastructure Protection, 2014', Young G., G00263740, 30 July 2014.

This source provides a good overview of NGFWs. It examines the evolution of network security, the rise of Enterprise 2.0 applications and their associated threats, the shortcomings of traditional firewalls, and the advanced capabilities found in NGFWs.

Source 2: Miller L.C.: 'Next-Generation Firewalls For Dummies®', Wiley Publishing Inc. 2011, http://www.bradreese.com/blog/firewalls-for-dummies.pdf, accessed 16 Feb 2015.

Network World identify that changes currently affecting enterprise IT will challenge the purpose and design of current firewalls, but offer no clear vision of the end result.

Source 3: 'The Firewall: Questions abound about its future role in cloud, mobile and SDN environments', Network World, 14 July 2014, http://www.networkworld.com/article/2452691/security0/the-firewall-questions-abound-about-its-future-role-in-cloud-mobile-and-sdn-environments.html, accessed 16 Feb 2015.

Firemon have produced some interesting analysis that includes the statement:

"And perhaps most significantly, threats continue to evolve, challenging the notion that a network firewall can effectively defend organizations against them."

Source 4: Brazil J.: 'Stated Inspection: The Future of the Firewall', Firemon, 28 October 2014, http://www.firemon.com/blog/firewall-management/stated-inspection-future-firewall/, accessed 16 Feb 2015.

Standards and policy (Government and non-Government)

There are still few standards for NGFWs and none that are universally supported by the main vendors. Although the same standards that apply to traditional firewalls (e.g. Common Criteria National Information Assurance Partnership (NIAP) standards and UK Commercial Product Assurance (CPA)) are increasingly being obtained for NGFWs, these standards test only a small part of the wide-ranging capabilities of these firewalls and are of limited value.

QinetiQ comment

The term 'Next Generation Firewall' is still loosely defined, and the relevance of this technology in the longer term is hard to assess. Network boundaries continue to evaporate, and there is a massive increase in connected devices every year, from the current widespread use of mobile technologies to the anticipated exponential growth of network connection sensors and SCADA systems (known as the term 'Internet of Things'). Certainly modern firewalls offer a range of capabilities that are better designed for managing porous network boundaries, but the long-term trend could lead to such devices becoming obsolete, or else they may evolve to manage the distributed enterprise boundary (and in the process will probably acquire a new name for an even wider range of capabilities).

On-line Social networking

Description

Social networking sites are Internet-based services that allow people to communicate and share information with a group. They enable the creation and maintenance of online personal and business relationships.

Over the last decade, the on-line social networking phenomenon has become truly global and has revolutionised the way people interact. It is now spreading information faster than any other media. Individuals, groups and organisations across society, including politicians, religious leaders and businesses are exploiting the technology.

The most popular examples of social networking sites include Facebook, Twitter, LinkedIn and Flickr.

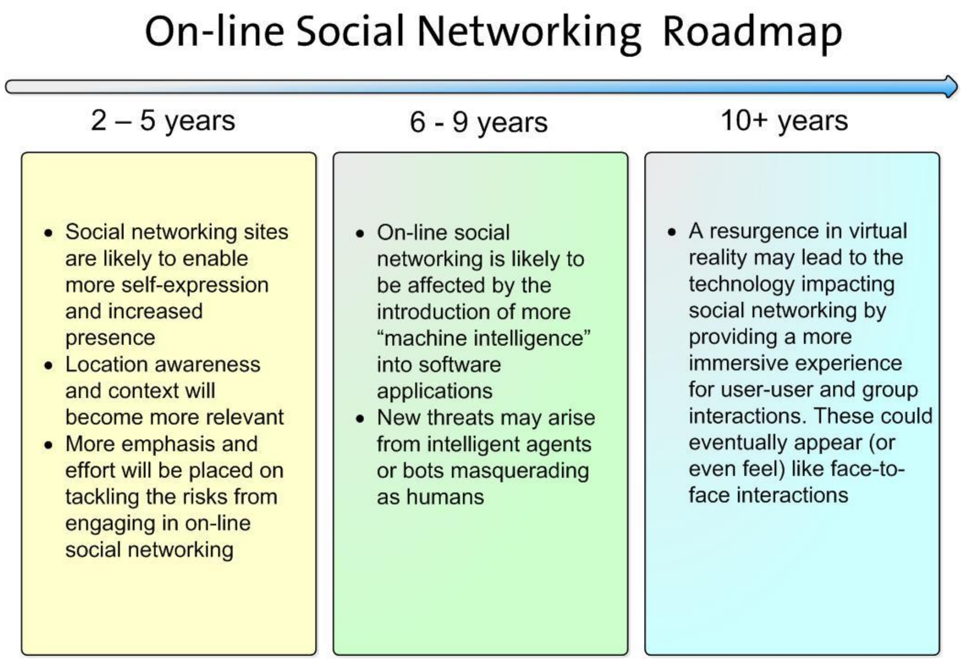
Whilst there are, many benefits there are also many negative aspects relating to the use of social networking sites (see Source 1 below). The risks from engaging in on-line social networking have gained more prominence and this has been reflected in the trust that people have in the content of social networking sites, lowering in recent years (see Source 4).

Relevant Applications

Social software has crossed over into business applications. Enterprise collaboration suites (such as Microsoft's SharePoint) enable social networking for business activities. Social networking is also a significant target area for marketers seeking to engage users. There are now numerous social networking applications available on the Internet, particularly for smartphone and tablet users.

Most Relevant Cyber Security Controls

- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Malware Defences
- Security Skills Assessment and Appropriate Training to Fill Gaps



On-line Social Networking Roadmap

2 – 5 years

- Social networking sites are likely to enable more self-expression and increased presence
- Location awareness and context will become more relevant
- More emphasis and effort will be placed on tackling the risks from engaging in on-line social networking

6 - 9 years

- On-line social networking is likely to be affected by the introduction of more "machine intelligence" into software applications
- New threats may arise from intelligent agents or bots masquerading as humans

10+ years

- A resurgence in virtual reality may lead to the technology impacting social networking by providing a more immersive experience for user-user and group interactions. These could eventually appear (or even feel) like face-to-face interactions

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: Social networking sites are likely to enable more self-expression and increased presence. Location awareness and context will become more relevant. More emphasis and effort will be placed on tackling the risks from engaging in on-line social networking. For example, attempts could be made to organise (or even regulate) the flow of information between organisations and social environments.

Within 6 – 9 years: Within this time frame social networking is likely to be affected by the introduction of more "machine intelligence" into software applications. Technologies such as virtual personal assistants (digital secretaries) may have a huge impact, particularly if these entities are capable of posting content on behalf of their human users. In a similar vein, new threats may arise from intelligent agents or bots masquerading as humans.

10+ years: The recent resurgence in virtual reality may lead to the technology impacting social networking by enabling a more immersive experience to user-user and group interactions. These could eventually appear (or even feel) like face-to-face interactions (Facebook's acquisition of the Virtual Reality company Oculus VR is a clear sign that social networking companies are interested in the technology).

General Issues and Challenges

Social networking can present many risks and can pose threats to the unwary. Unfortunately, these threats are on the rise and can include data theft or attack through viruses or other forms of malware. Besides the threat of on-line predators, one of the most prevalent dangers involves individuals who are intent on stealing data for the purposes of identity theft and gaining access to other users' assets (e.g. bank details). In the future intelligent bots or agents may also take on these types of activities, claiming to be someone that they are not.

A good introduction to the risks posed by social networking is available on the Federal Bureau of Investigation's (FBI's) website (see Source 2). They see two primary areas where hackers can exploit on-line social networks:

- Through writing and manipulating computer code to gain access or install unwanted software on a user's computer or smartphone.
- Through exploiting personal connections within the social networks. Social hackers, sometimes referred to as "social engineers," manipulate people through social interactions (in person, over the phone, or in writing).

The FBI states that:

"Predators, hackers, business competitors, and foreign state actors troll social networking sites looking for information or people to target for exploitation.

Information gleaned from social networking sites may be used to design a specific attack that does not come by way of the social networking site." (see Source 2).

Ofcom (see Source 4 below) has conducted surveys concerning trust and data privacy on social networking sites. This highlights the increased risk to those users allowing "friend of friends" to have access to their data which is effectively sharing information with people who are potentially not known to them.

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

ProCon.org is a non-profit website that presents research, studies, and pro and con statements on questions related to social networking and its impact on society.

Source 1: 'Social Networking – Pros and Cons', ProCon.org, http://socialnetworking.procon.org/, accessed 5 Feb 2015.

The FBI counterintelligence website page on "Internet Social Networking Risks" provides guidance on mitigating the risk of using social networking sites.

Source 2: 'Internet Social Networking Risks', FBI Website, http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks, accessed 19 Jan 2015.

In 2008, Ofcom (the independent regulator and competition authority for the UK communications industries) released a study examining social networking. This report covers: attitudes and behaviours, how people use social networking sites, privacy and safety. Although dated now, much of their research is still valid.

Source 3: 'Social Networking - A quantitative and qualitative research report into attitudes, behaviours and use', 2 April 2008, Ofcom, http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/report1.pdf, accessed 1`9 Jan 2015.

In 2013, Ofcom released updated statistics on the usage of social networking sites showing that older users are driving the usage of social networking and that trust in social networking sites has declined. To quote:

"In 2012 just under two in three (64%) adult internet users said they had a social networking profile, a significant increase on 59% in 2011. This growth has been driven by users aged 55-64, 35% of whom now have profiles, compared to 24% in 2011."

"…despite this increase in use, trust in social networking sites is lower than in 2011, with 43% of UK adult internet users disagreeing that they trust what they read or see when they visit social networking sites, an increase from 35% in 2011."

This source also looks at data privacy and has established that:

"One in six social networking site users are potentially sharing their contact details with people not known to them."

Source 4: 'Adults' media use and attitudes report', Ofcom, April 2013, http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/adult-media-lit-13/2013_Adult_ML_Tracker.pdf, accessed 19 Jan 2015.

The following source presents the likely growth of social networking for the next four years. It also includes comments from a number of industry experts regarding the future of social media:

"..we should see global social media usage continue on its upward trajectory. In just four years, eMarketer projects it will nearly double by 32.7 percent. By then 2.44 billion of the world's population will be on social networks."

Source 5: Wellons M.C.: '11 Predictions on the future of social media', CNBC, 2 Oct 2014, http://www.cnbc.com/id/102029041#. accessed 19 Jan 2015.

The UK Government's has produced policy with regard to the use of social media by its civil servants.

Source 6: Social media guidance for civil servants, Cabinet Office, 20 Oct 2014, https://www.gov.uk/government/publications/social-media-guidance-for-civil-servants/social-media-guidance-for-civil-servants, accessed 5 Feb 2015.

Standards and policy (Government and non-Government)

There have been limited attempts at standardisation. ‘Friend of a Friend’ (FOAF) is a prospective ‘Social Web’ standard which is a machine-readable ontology describing persons and their activities, but it has had limited adoption.

The UK Government’s Cabinet Office has published social media guidance for civil servants. The purpose of this guidance is to encourage and enable civil servants to use social and other digital media appropriately to enhance their work. It also makes clear their responsibilities with respect to the Civil Service Code (see Source 6 above).

The Government Communication Service (GCS) has produced a supplementary document to the above that is relevant to those who are involved in more proactive communications roles.

QinetiQ comment

On-line social networking has becoming pervasive within our society and socially driven processes are disrupting traditional approaches to the way businesses operate. It is difficult to predict which direction the technology will go next in support of our need to interact with people in a social context.

Penetration Testing Tools and Techniques

Description

Penetration testing techniques involve the use of multi-step attack scenarios to find vulnerabilities in computer systems. The use of penetration tools and techniques also provide the means to uncover misconfigurations or vulnerabilities that could allow compromise in such systems (Source 1).

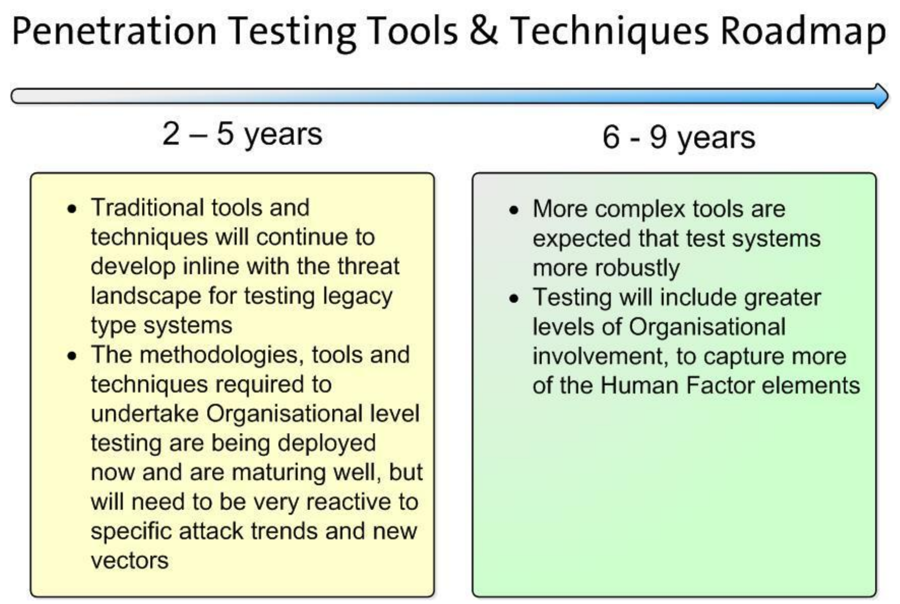
Traditionally Penetration Testing focuses on component level testing with only certain organisation elements being subject to testing. In response to high profile attacks against a number of well-known organisations, the industry has recently created much more covert and realistic services that look at overall organisational risk.

These services blend physical and Cyber-attack vectors along with both human factors and social engineering to provide a much more accurate simulation of how attackers actually attack networks. These simulations are the antithesis of traditional penetration testing being specifically designed to achieve defined goals (such as accessing key systems), by any reasonable means, without being detected by security monitoring regimes.

In certain market sectors, such as Finance, this has culminated in the creation of new governance frameworks that define the type of testing that players in the sector should do. The Bank of England, along with the Council of Registered Ethical Security Testers (CREST) has developed a scheme known as CBEST. Whilst solely finance sector focused and not, as yet, mandated this should be viewed as a potential model for other areas of Critical National Infrastructure (CNI) with respect to potential governance regimes.

Most Relevant Cyber Security Controls

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Security Skills Assessment and Appropriate Training to Fill Gaps
- Controlled Use of Administrative Privileges
- Secure Network Engineering
- Penetration Tests and Red Team Exercises



Penetration Testing Tools & Techniques Roadmap

2 – 5 years

- Traditional tools and techniques will continue to develop inline with the threat landscape for testing legacy type systems
- The methodologies, tools and techniques required to undertake Organisational level testing are being deployed now and are maturing well, but will need to be very reactive to specific attack trends and new vectors

6 - 9 years

- More complex tools are expected that test systems more robustly
- Testing will include greater levels of Organisational involvement, to capture more of the Human Factor elements

Relevant Applications

Any organisation can benefit from penetration testing. CBEST specifically targets finance sector customers but suppliers of such services report them being commissioned in multiple market sectors including finance, retail, transport, law, insurance and utilities.

Technology Readiness and Maturity (forecasted arrival and accessibility)

Penetration testing typically develops and evolves in response to identifying component or system vulnerabilities, through either analysis or direct exploitation via an attack. As such, it is difficult to forecast with any confidence as time progresses, therefore only two time-frames have been forecasted below.

Within 2 – 5 years: The methodologies, tools and techniques required to undertake Organisational level testing are being deployed now and are maturing well. That said the are likely to need to be very reactive to specific attack trends and new vectors both in the short and medium term.

Within 6 – 9 years: Whilst attackers are still innovating with new ways to attack organisations any service that looks to accurately simulate threat will also need to continue to innovate to keep pace with the evolving threat. For this reason the author does not foresee any time when the services will be mature in the traditional sense.

General Issues and Challenges

The main issue that exists is making sure that the testing accurately reflects the actual attack vectors being used by attackers. The industry is aware of this need and is very careful to ensure that the testing is intelligence led as far as it is possible. In essence, this means two things, the first is a need to have cognisance of the on-line threat landscape with respect to the specific sector in question. This information can be gathered from both open and closed sources. Common information sources include Twitter, Facebook, IRC Channels and Forums (be these open or closed communities). The second is maintaining an awareness of the current technical attacks actually being used in the wild. Entities providing testing services in this space often expend large amounts of time reverse engineering captured malware samples and undertaking incident response activities as the results of both of these pieces of analysis are useful in making sure that the service is effectively mimicking the actual threat.

Having better and more advanced tools is only part of the solution, the effectiveness of testing is largely dependent on the skills of the tester, which means that testers need to be continually training to acquire skills and maintain them at the required high level.

Over time, testing will become more complex as legacy systems and components will remain in use within organisations, sometimes without those organisations being fully aware of the associated risks. As a result, the quantity of systems and components requiring testing will continue to increase. Even well documented vulnerabilities are likely to continue to be found long after organisations thought they had fully addressed them. The skill set and knowledge of the testers has to encompass this ever-growing landscape.

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

The IT analyst company, Gartner have briefly reported on penetration testing in their hype cycle for infrastructure protection and give the following advice for organisations considering penetration testing:

"The effectiveness of network penetration tools largely depends on the skill of the practitioner. Enterprises that need to regularly perform penetration testing, but do not have the necessary technical skills, should focus on using services rather than buying products."

Source 1: Gartner, 'Hype Cycle for Infrastructure Protection, 2014', Young G., G00263740, 30 July 2014.

Source 2: PCI Security Standards Council, Data Security Standard, Information Supplement: Penetration Testing https://www.pcisecuritystandards.org/documents/information_supplement_11.3.pdf (accessed 18/12/2014).

Source 3: CESG CHECK http://www.cesg.gov.uk/servicecatalogue/service_assurance/CHECK/Pages/What-is-CHECK.aspx (accessed 18/12/2014).

Source 4: CREST CBEST www.crest-approved.org/industry-government/cbest/index.html (accessed 18/12/2014).

Entities such as CPNI, with the iData, and related, programmes, publish information around Cyber Security and targeted attacks. (www.cpni.gov.uk/advice/cyber)

The security industry itself publishes a number of briefing papers on attack trends and techniques, e.g. Mandiant (www.mandiant.com), Symantec (www.symantec.com/security_response/publications/monthlythreatreport.jsp) and McAfee (http://blogs.mcafee.com/category/mcafee-labs).

Standards and policy (Government and non-Government)

There is currently no globally recognised standard for Penetration Testing in general or Organisational Testing in particular. The UK has always been at the very forefront of this space with the CESG CHECK Scheme, along with partner organisations such as CREST and Cyber Essentials Scheme, providing certification of competence for both Organisations and individuals in the Penetration Testing space.

The Payment Card Industry Data Security Standard recommends "Penetration testing should be performed at least annually and anytime there is a significant infrastructure or application upgrade or modification" and provides guidance on the scope and methodologies that should be involved (Source 2).

Whilst currently industry specific many in the security testing arena see the joint Bank of England/CREST scheme, CBEST, as something that could, in time, be applied to other areas of national infrastructure. They also see it as something that, in regulated industries in particular, may ultimately become a mandatory exercise.

QinetiQ comment

Whilst QinetiQ still believes that “traditional” penetration, testing can offer value in any organisation the only way to get an accurate picture of the organisations risk profile to targeted attack is to simulate such attacks in a practical fashion.

Such simulations allow the end-to-end security of the targeted organisation to be assessed from their security culture, and resilience to Social Engineering, to the physical security of their sites and the Cyber Security posture of their networks and systems. The outputs of such an exercise generally fall into one of two categories. Firstly, these outputs identify areas where greater or improved technical controls are required. Secondly, in the human factors space, they identify a failure to apply policy or governance regimes. This may be because these governance regimes are non-existent or poorly defined or that the communications and training provided to end users is deficient.

An understanding of the actual real world susceptibility of an organisation to targeted attacks allows pragmatic decisions to be taken to allocate finite funds and finite effort to reduce risks.

Predictive Analytics

Description

The field of Predictive analytics encompasses a range of analytical and statistical techniques that can be applied to data to determine potential future events or behaviours. Such techniques include data mining, statistical modelling and machine learning to help analysts forecast what might happen in the future with an acceptable level of reliability. Predictive analytics allows organisations to become proactive, enabling them to look ahead at potential outcomes and in the case of security, potential threats that may affect their business (see Source 1 for a more detailed introduction to Predictive analytics and the techniques that support it).

Besides a raft of other applications, Predictive analytics has proven to be useful in detecting unknown or unusual behaviour on communication networks. The technology can analyse multiple parameters from live network traffic data and compare this with "normal" network activity acquired from modelling past behaviour and predict how entities within the network (host servers and users) should behave in the future. Such activities can help identify anomalies and behaviour indicative of potential threats.

There is a link between Predictive analytics is and Big Data with vendors offering the capability as the predictive element of their Big Data offerings.

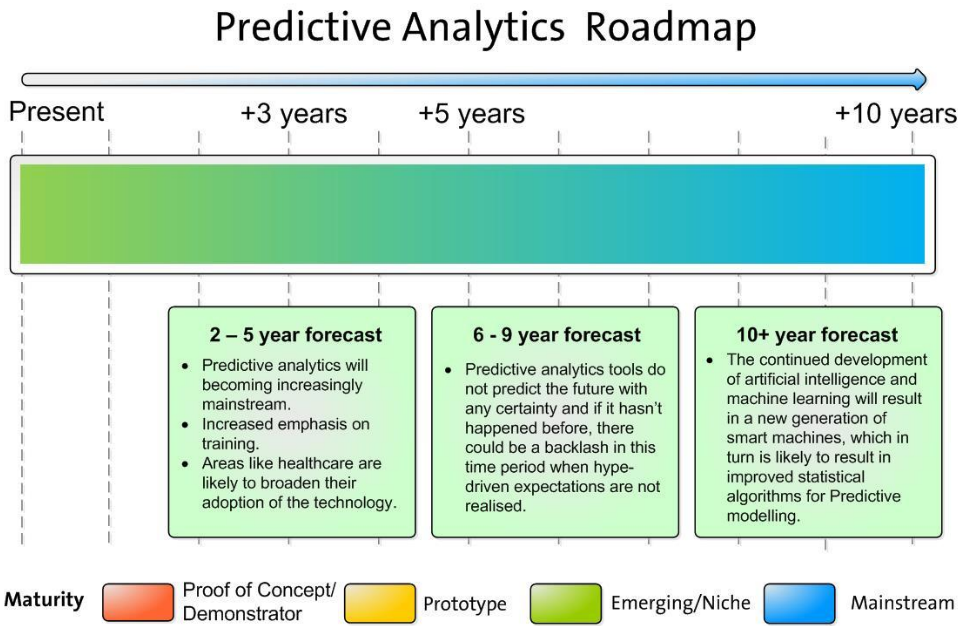
Relevant Applications

Predictive analytics, and its promise of determining likely future outcomes, is of interest to many organisations. The following are typical areas that are benefitting from the technology:

- Retail: predicting customers' probable future buying behaviour.
- Financial services: to check whether customers pose a potential credit or insurance risk and/or are attempting to undertake fraudulent activity.
- Cyber Security: identification of Cyber-threats (see Sources 2 to 4 below).

Most Relevant Cyber Security Controls

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Continuous Vulnerability Assessment and Remediation
- Limitation and Control of Network Ports, Protocols, and Services
- Boundary Defence



Predictive Analytics Roadmap

2 – 5 year forecast

- Predictive analytics will becoming increasingly mainstream.
- Increased emphasis on training.
- Areas like healthcare are likely to broaden their adoption of the technology.

6 - 9 year forecast

- Predictive analytics tools do not predict the future with any certainty and if it hasn't happened before, there could be a backlash in this time period when hype-driven expectations are not realised.

10+ year forecast

- The continued development of artificial intelligence and machine learning will result in a new generation of smart machines, which in turn is likely to result in improved statistical algorithms for Predictive modelling.

Maturity 🟥 Proof of Concept/ Demonstrator 🟨 Prototype 🟩 Emerging/Niche 🟦 Mainstream

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: Predictive analytics will become increasingly mainstream. More emphasis will be put on training such that more users can gain access to the technology. Areas like healthcare are likely to broaden their adoption of the technology.

Within 6 – 9 years: Predictive analytics tools do not predict the future with any certainty and if it hasn't happened before, there could be a backlash in this time period when hype-driven expectations are not realised.

10+ years: The continued development of artificial intelligence and machine learning will result in a new generation of smart machines, which in turn is likely to result in improved statistical algorithms for Predictive modelling.

General Issues and Challenges

Probably the most fundamental issue for Predictive analytics is a lack of good data and this represents the most common barrier to organisations intending to employ the technology. A lack of good data is of particular concern where the intention is to find meaningful anomalies that represent actual attacks or fraud, for this requires the collection and fusion of large volumes of data, including context.

Depending on the application, the assumption used by predictive models that the future will continue to be like the past can prove to be problematic, particularly with regard to human behaviour. People are known to establish strong patterns of behaviour that they usually adhere to over time. Sometimes, however, they change those behaviours, and the models that were used to predict them are likely to be no longer valid (see Source 5).

Finally, it is worth mentioning that the algorithms used by Predictive analytics are complex and provide raw data that requires specialist attention. Predictive analytics solutions typically require data science skills in-house and this can be a problem for many organisations. Fortunately, some analytics solutions come with Predictive analytics integrated within them, which tend to be easier to use than the more advanced analytics platforms.

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

This source provides a general overview of Predictive analytics including its applications and underlying technologies and techniques.

Source 1: 'Predictive analytics', Wikipedia, http://en.wikipedia.org/wiki/Predictive_analytics, accessed 9 Dec 2014.

Predictive analytics is increasingly being seen as a "detection capability", helping analysts identify hidden Cyber-threats within networks:

"The lack of visibility organisations have into today's "noisy" networks means persistent threats have plenty of places to hide. Fortunately, however, predictive analytics is an emerging detection capability that can help security professionals to seek out any trespassers."

"Predictive analytics doesn't necessarily mean seeing an attack before it happens but, rather, helping security professionals identify and track unknown malware, wherever it may be hiding."

Source 2: Newman S.: 'Securing the Future: Using Predictive Analytics to seek out hidden threats', Business Weekly, 21 Nov 2014, http://www.businessweekly.co.uk/blog/business-weekly-guest-blog/17822-securing-the-future-using-predictive-analytics-to-seek-out-hidden-threats, accessed 9 Dec 2014.

A US Website called GovInfo Security has reported on the use of Big Data and Predictive analytics to identify potential Cyber-threats:

"Predictive analysis is an emerging tool being used to identify potential Cyber-threats against organisations."

"[where there exists] *an individual that has intention to do something and they're starting to exercise a particular capability that leaves evidentiary marks inside the network itself…through* [the predictive analytics] *process, you have the ability to have forewarning of potential attacks."*

Source 3: Roman J.: 'Predicting the Next Cyber-Attack', GovInfoSecurity, http://www.govinfosecurity.com/predicting-next-cyber-attack-a-5716, dated 29 April 2013 and accessed 9 Dec 2014.

The US company 21CT (www.21ct.com) offers a number of products relevant to security intelligence and network security. The company offers a number of analytics-based solutions and predictive analytics features as part of these.

"21CT predictive analytics solutions are made to be used by any investigator, from healthcare fraud to network security, during every phase of their workflow, from generating new leads and examining facts, to discovering hidden relationships and building their case throughout the investigative lifecycle."

21CT's LYNXeon product is described thus:

"Using the data already coarsing through a network, LYNXeon connects the dots between system activity, threat event triggers, and perimeter alerts to fully visualize network behaviour. The on-demand analytics in LYNXeon track down threats, discover previously undetected attacks, and record network activities pre- and post-breach."

Source 4: 21CT LYNXeon | Network Security Analytics, http://www.21ct.com/products/lynxeon/, accessed 9 Dec 2014.

This source outlines some of the assumptions that underlie the predictive models of Predictive analytics tools.

Source 5: Davenport D.: 'A Predictive Analytics Primer', Harvard Business Review, https://hbr.org/2014/09/a-predictive-analytics-primer/, dated 2 Sept 2012, accessed 9 Dec 2014.

Standards and policy (Government and non-Government)

Predictive Model Markup Language (PMML) is a standard developed by the Data Mining Group (DMG) to represent predictive analytic models. Both Hadoop (enabling the handling of Big Data) and the open source software programming language for statistical computing known as 'R' also represent important standards for the field of Predictive analytics.

There currently exists no known UK Government policy regarding Predictive analytics.

QinetiQ comment

Predictive analytics is currently riding the Big Data bandwagon and the hype associated with it. Nevertheless, the field is relatively mature and a broad number of use cases exist that have benefitted from the technology. The use of Predictive analytics tools to identify potential Cyber-threats is still in its infancy however.

Security Information and Event Management (SIEM)

Description

Security Information and Event Management (SIEM) tools collate logs from a range of IT devices, including both security and audit based logs. The tools correlate the logged events, highlighting any concerning security events, enabling trends and anomalies to be analysed.

With IT systems continually increasing in complexity a SIEM capability is essential for all medium and large enterprises to assist in securing their IT systems.

When selecting a SIEM solution the following aspects of a product need to be considered:

- Functional capabilities and limitations.
- Scalability.
- A roadmap of development and ability to evolve as change occurs (2-3 years).
- Deployment and support requirements (including the IT and operational skills and training needs of users).

Most Relevant Cyber Security Controls

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Secure Configurations for Network Devices such as Firewalls, Routers, etc
- Limitation and Control of Network Ports, Protocols, and Services
- Controlled Use of Administrative Privileges
- Boundary Defence
- Maintenance, Monitoring, and Analysis of Audit Logs
- Secure Network Engineering

Relevant Applications

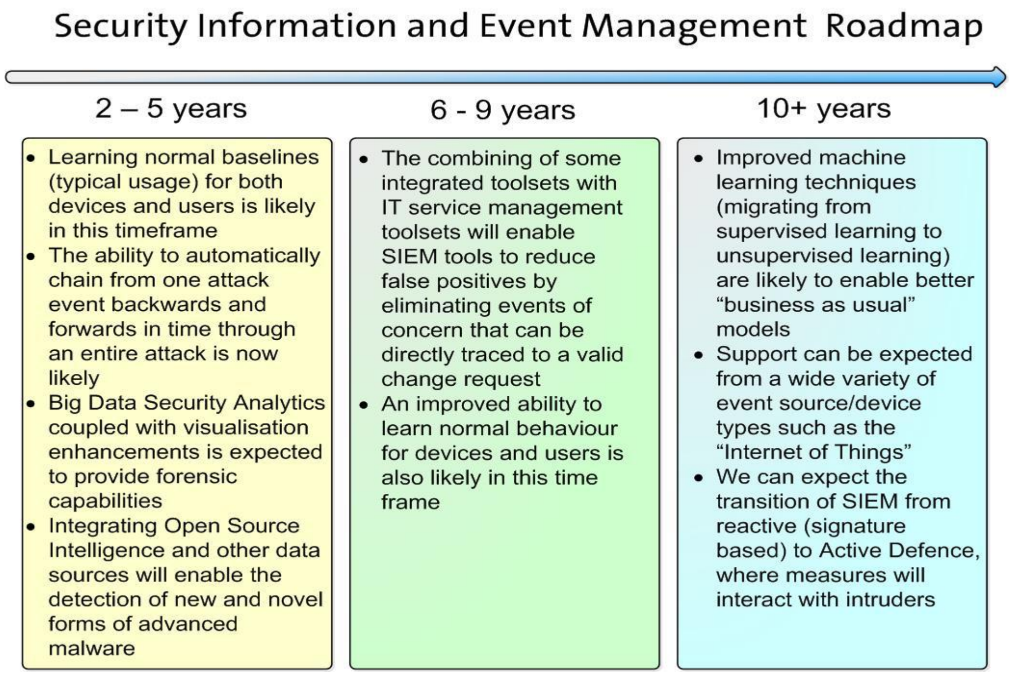
SIEMs are normally installed and operated by the IT security departments, but IT operations staff can gain extremely valuable information from the SIEM. By analysing useful trends and outputs during their tasks, operations staff may identify system optimisation opportunities, which may not readily be identifiable by standard tools.

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: Learning normal baselines (typical usage i.e. business as usual activities) for both devices and users is likely in this timeframe (which is currently only available on a very limited number of systems). The ability to automatically chain from one attack event backwards and forwards in time through an entire attack is also likely in this time frame e.g. from a suspicious use of a System Account the SIEM can identify how access was gained to that System Account, back to the initial spearphish email that provided the original infection, and forwards through all activity created by that System Account and subsequent activities. Big Data Security Analytics coupled with visualisation enhancements will likely provide forensic capabilities. The integration of Open Source Intelligence with other data sources is expected to enable the detection of new and novel forms of advanced malware.

Within 6 – 9 years: For some more integrated toolsets (e.g. HP ArcSight) integration is likely with an IT service management toolset, allowing the SIEM to eliminate events of concern that can be directly traced to a valid change request. An improved ability to learn normal behaviour for devices and users is also likely in this time frame.

10+ years: By this time improved machine learning techniques, including migration from supervised learning (classification) to unsupervised learning, will lead to better "business as usual" models. Support can be expected from a wide variety of event source/device types such as Internet of Things (IoT), and complex data types (binary) (see Sources 2 and 4 below). We can expect the transition of SIEM from reactive (signature based) to Active Defence, where measures will interact with intruders (see Source 3 below).



Security Information and Event Management Roadmap

2 – 5 years

- Learning normal baselines (typical usage) for both devices and users is likely in this timeframe
- The ability to automatically chain from one attack event backwards and forwards in time through an entire attack is now likely
- Big Data Security Analytics coupled with visualisation enhancements is expected to provide forensic capabilities
- Integrating Open Source Intelligence and other data sources will enable the detection of new and novel forms of advanced malware

6 - 9 years

- The combining of some integrated toolsets with IT service management toolsets will enable SIEM tools to reduce false positives by eliminating events of concern that can be directly traced to a valid change request
- An improved ability to learn normal behaviour for devices and users is also likely in this time frame

10+ years

- Improved machine learning techniques (migrating from supervised learning to unsupervised learning) are likely to enable better "business as usual" models
- Support can be expected from a wide variety of event source/device types such as the "Internet of Things"
- We can expect the transition of SIEM from reactive (signature based) to Active Defence, where measures will interact with intruders

General Issues and Challenges

The most common issues affecting deployment of a SIEM are similar to other security systems - in that once installed, the information produced is not used, tuned, or updated. A SIEM can easily produce logs of new privileged accounts, such as those that an attacker might produce, but if no one checks the list against expected changes then the information is of no use. Using experts to both tune the SIEM and review the output of it is essential, though care is needed to ensure that individuals are not reviewing reports relating to their own work if an "Insider Threat" is credible.

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

Securing CNI:

"[CNI network isolation] *is simply not practical. Laying private communications networks is expensive and innovations like smart metering are only practical because existing communications technology standards and networks can be used. Of course, better security can be built into CNIs in the first place, but this will take time. Many have essential components that were installed decades ago. A starting point would be better visibility of the overall network in the first place, and the ability to collect inputs from devices and record events occurring across* [Critical National Infrastructure] *CNI networks. If this sounds like a kind of SIEM (security information and event management) system … then that is because it is; a mega-SIEM for the huge scale of CNI networks."*

Source 1: 'Critical National Infrastructure: How to Protect Vital Systems', http://www.infosecurity-magazine.com/blogs/critical-national-infrastructure/ accessed 17 Dec 2014.

SIEM systems create a lot of controversy with security folks; they are one of the cornerstones on which the security program are built upon within every enterprise. Yet, simultaneously SIEM generates the most complaints and general angst.

Source 2: 'Security Management 2.5: Replacing Your SIEM Yet?' https://securosis.com/blog/security-management-2.5-replacing-your-siem-yet-new-series, accessed 17 Dec 2014.

"Current tools are too limited. Some observe the environment (such as SIEM, [Data Loss Protection] *DLP, and full packet capture), but they only show us narrow slices, leaving large gaps between them. This hampers our ability to acquire and relate the information we need to understand incidents. Once we receive an alert, we need to jump into different shells and command lines on multiple servers and appliances in order to see what's really going on. When current tools talk to each other, it is rarely in a meaningful or useful way."*

Source 3: 'The Future of Security', v1.0, https://securosis.com/assets/library/reports/Future-of-Security.v.1.pdf, 20 Feb 2014, accessed 17 Dec 2014.

Source 4: Pinto A.: 'Applying Machine Learning to Network Security Monitoring - Blackhat 2014', https://www.blackhat.com/docs/webcast/05152014-applying-machine-learning-to-network-security-monitoring.pdf, accessed 17 Dec 2014.

Further useful sources where documentation is available on product websites include:

- http://www.logrhythm.com/

- http://www8.hp.com/us/en/software-solutions/siem-security-information-event-management/
- http://www.splunk.com/product

Standards and policy (Government and non-Government)

There are no applicable standards for SIEM tools. Many SIEMs however do have built in rule-sets for specific government and industry compliance regimes such as GPG-13, the Federal Information Security Management Act (FISMA), the Sarbanes-Oxley Act (SOX), the Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA).

QinetiQ comment

A key challenge that SIEM capabilities have not yet successfully addressed is exploiting the knowledge gathered through user understanding. This knowledge is captured as information in different forms; an analyst's perspective via incident management, system engineer's via design documentation, system administrator's via Configuration Management DB (CMDB) and CERT (Threat intelligence databases). Big Data and advanced analytics will be required to process the wider range of data sources available and will enable users to acquire a better understanding of the target infrastructure being monitored.

Smart Machines

Description

The term “Smart Machines” is a broad term that covers a raft of emerging technologies that use Artificial Intelligence (AI) and “machine learning” techniques to perform traditional human tasks and/or deliver additional non-human insight or solutions.

The IT analyst company, Gartner (see Source 1 below) regards these as a “super class” of technologies that will constitute one of the most disruptive eras of technology innovation.

Most Relevant Cyber Security Controls

- Inventory of Authorized and Unauthorized Software
- Continuous Vulnerability Assessment and Remediation
- Malware Defences
- Limitation and Control of Network Ports, Protocols, and Services
- Controlled Use of Administrative Privileges
- Controlled Access Based on the Need to Know

Whilst AI and machine learning are terms that have been with us for some time, they have more recently been refined, improved and combined with natural-language processing, analytics, search and graphing techniques to create technologies with apparent human-like intelligence.

From a positive viewpoint, these technologies will have a major beneficial impact on the way people work with data and information. Indeed, they will have a huge impact on intelligence gathering and decision support.

More concerning however, is that some of these technologies have the potential to become serious threats. This is not the “rampant AI threat to humanity” that has received considerable media coverage of late (see Source 2), but technologies that are currently being developed, such as intelligent agents and cognitive computing, that promise adaptable, reasoning systems that can react and respond to humans in natural language (see issues and challenges below).

Relevant Applications

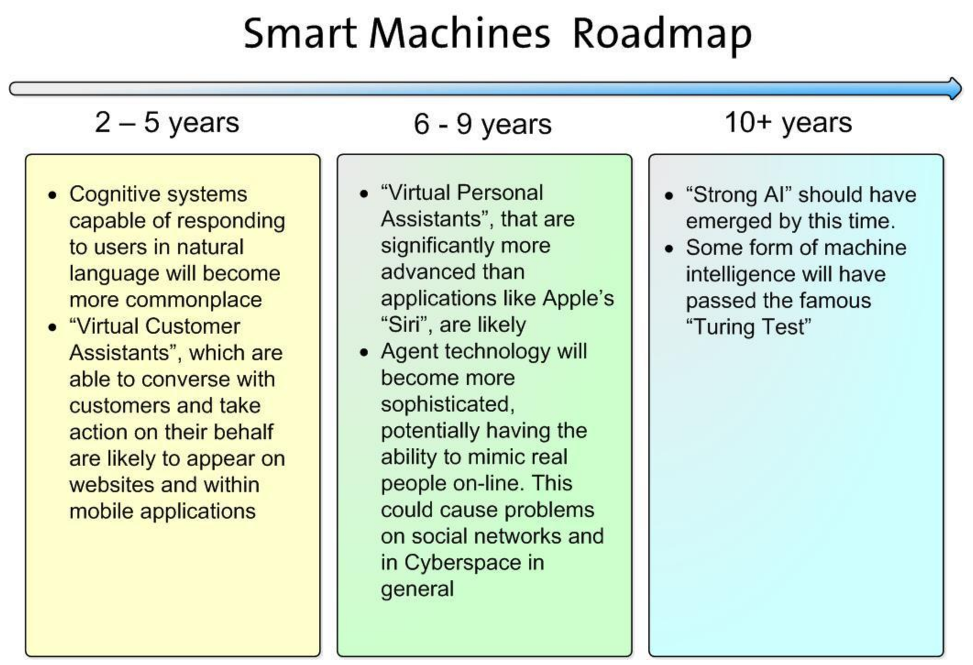
Smart machines are still emerging and have the potential to have an impact in almost every facet of our lives, ranging from smart software on mobile devices to enabling automation across areas such as the automotive industry, industrial control systems and the military. Smart machines are expected to greatly improve current business processes and will enable the creation of new business models and opportunities, yet at the same time, they will also cause disruption to the workforce and alternative technologies.

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: Cognitive systems capable of responding to users in natural language will become more commonplace (a first generation example of this capability is IBM's Watson technology,which is famous for defeating human contestants on the Jeopardy game show). "Virtual Customer Assistants", which are able to converse with customers and take action on their behalf, are also likely to appear in this time period. Such technology is likely to begin to appear on websites and within mobile applications to reduce the need for typed interactions.

Within 6 – 9 years: "Virtual Personal Assistants" (VPAs) are likely to appear in this timeframe. These are similar to Apple's "Siri" application, but will be considerably more advanced, being able to observe their user's behaviour and needs in order to act autonomously as a "digital secretary" on their behalf. VPAs are essentially, a form of software agent. Besides supporting people in their everyday tasks, agent technology will have reached a state where it could be used to realistically mimic real people on-line. This could cause problems on social networks and in cyberspace in general.

10+ years: "Strong AI" should have emerged by this time. It is highly likely that some form of machine intelligence will have passed the famous "Turing Test", which is a test of a machine's ability to exhibit intelligent behavior equivalent to, or indistinguishable from, that of a human.



Smart Machines Roadmap

2 – 5 years

- Cognitive systems capable of responding to users in natural language will become more commonplace
- "Virtual Customer Assistants", which are able to converse with customers and take action on their behalf are likely to appear on websites and within mobile applications

6 - 9 years

- "Virtual Personal Assistants", that are significantly more advanced than applications like Apple's "Siri", are likely
- Agent technology will become more sophisticated, potentially having the ability to mimic real people on-line. This could cause problems on social networks and in Cyberspace in general

10+ years

- "Strong AI" should have emerged by this time.
- Some form of machine intelligence will have passed the famous "Turing Test"

"Turing Test", is a test of a machine's ability to exhibit intelligent behavior equivalent to, or indistinguishable from, that of a human.

General Issues and Challenges

Whilst smart machines will increase productivity, they will also disrupt workplaces. They will profoundly affect employment patterns and current roles as well as forcing debate about new realms of ethics and liability. Last, but not least, they will raise legal implications, particularly in some areas where decisions are taken by the machine rather than the human, such as after a road traffic accident when the car was driving – where is the legal responsibility held (by the car or by the human?).

In the context of cyber security, we can expect more frequent use of smart machine technologies to identify new cyber-threats and deliver global threat intelligence (e.g. through big data and predictive analytics). Yet at the same time, there will be considerable scope for exploitation of the technology for nefarious purposes. One typical example concerns software entities such as autonomous agents. Autonomous agents and smart bots have already had an impact on social networks (e.g. by creating convincing, but fake profiles of real people), but the rise of more intelligent forms of agent, such as VPAs could spawn a new generation of threats. More advanced forms of agent have had emotions and personality modelled so as to accurately mimic human behaviour (see Source 3). Coupled with cognitive computing capabilities (the field of AI that is concerned with developing systems that are endowed with human-like intelligence) such entities have the potential to be harder to identify in cyberspace. Such attributes will create new opportunities and vulnerabilities.

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

Gartner produced their first hype cycle for smart machines in 2014. The following extracts from this report present their views on the capability and nature of smart machines:

"The many kinds of smart machines that are emerging now will (to varying degrees) be able to:

- *Understand problems and their context*
- *Mimic human reactions to questions in natural language*
- *Make decisions using probabilistic models*
- *Predict future states*
- *Learn from experience*
- *Act autonomously"*

"Like human intelligence, there are many forms of machine intelligence — some of which may be more appropriate and valuable in certain situations. We do not believe that all these characteristics are necessary for a machine to be considered "smart"; rather, we expect that certain combinations and strengths of these characteristics will coalesce and constitute the different classes of smart machines that will address a wide variety of use cases in our personal lives and workplaces".

Source 1: Gartner, 'Hype Cycle for Smart Machines, 2014', Brant K.F., Austin T., G00263827, 18 July 2014.

There has been considerable media coverage of late covering the threat of AI to humanity. Prominent scientists and engineers have voiced their concern about what follows when humans build a device or write some software that can properly be called intelligent. This recent BBC article captures the concerns of some of these individuals. To quote:

"Tesla boss Elon Musk in October….declared rampant AI to be the "biggest existential threat" facing mankind."

"Google's director of engineering, Ray Kurzweil, is also worried about AI, albeit for more subtle reasons. He is concerned that it may be hard to write an algorithmic moral code strong enough to constrain and contain super-smart software."

Source 2: Ward M.: 'Does rampant AI threaten humanity?' BBC News Website, 2 Dec 2014, http://www.bbc.co.uk/news/technology-30293863, accessed 10 February 2015.

This source presents research on "emotional agents" and their use in various applications.

Source 3: Nemani S.S., Allan V.H.: 'Agents and the Algebra of Emotion', Department of Computer Science, Utah State University.

The UK Government's policy paper on driverless cars analyses the existing legal and regulatory situation for testing, producing and marketing highly and fully automated vehicles in the UK.

Source 4: UK Government Policy Paper 'Driverless cars in the UK: a regulatory review', 11 February 2015. https://www.gov.uk/government/publications/driverless-cars-in-the-uk-a-regulatory-review, accessed 11 February 2015.

Standards and policy (Government and non-Government)

The field of smart machines covers many technologies that are still in development. Some standards exist for AI (e.g. ISO/IEC 2382-29:1999), but standardisation is still a matter of debate for many of the technologies involved.

Over the coming years there will be the need for Government policy on numerous aspects of smart machine technology. In February 2015 a policy paper for driverless cars in the UK (see Source 4), was released.

QinetiQ comment

Smart machines is a broad topic and includes many supporting and enabling technologies and potential applications. Coverage of all of these was clearly impossible for a small paper such as this, so our focus was biased towards smart software entities such as VPAs and autonomous agents. Firstly, because of the transformational impact they could have within the next decade and second, because of the potential cyber-threat that the technology could pose.

Smart Meters

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 upon not only the means to measure consumption of energy, but also a communications network to deliver 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), connecting energy-consuming devices to the meter and onwards to the supplier via a backhaul network likely using different technology to the HAN.

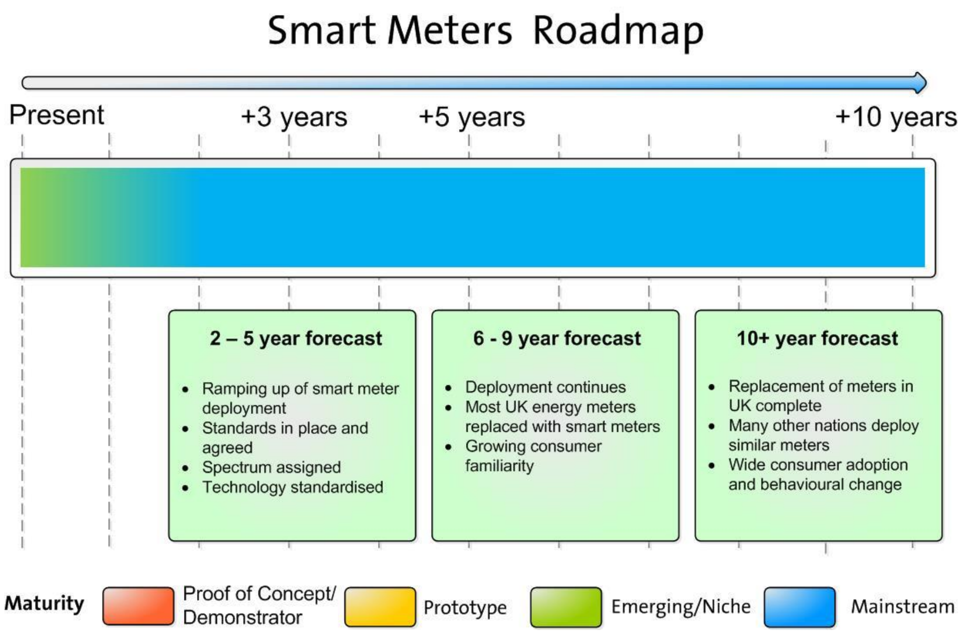
The technology is available now and is being widely promoted globally by both the energy industry and governments alike. Some smart meters only provide the consumption information to the suppliers, whilst others have a display that can provide instantaneous feedback to consumers on energy usage, or use a broadcast protocol in the property that an ‘In Home Device’ (IHD) can receive and report.

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).

Most Relevant Cyber Security Controls

- Inventory of Authorized and Unauthorized Devices
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers



2 – 5 year forecast

- Ramping up of smart meter deployment
- Standards in place and agreed
- Spectrum assigned
- Technology standardised

6 - 9 year forecast

- Deployment continues
- Most UK energy meters replaced with smart meters
- Growing consumer familiarity

10+ year forecast

- Replacement of meters in UK complete
- Many other nations deploy similar meters
- Wide consumer adoption and behavioural change

Maturity 🟥 Proof of Concept/ Demonstrator 🟨 Prototype 🟩 Emerging/Niche 🟦 Mainstream

Relevant Applications

Smart meters are part of the energy supply and billing system. They are installed in customer properties to record detailed information regarding energy consumption and to simplify pre-payment for supply. 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 consumption, 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 consumers property) 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: The rollout of smart meters has started within the UK with suppliers offering the devices to residential and business customers. By June 2014, around 900,000 smart meters had been deployed within the UK*. However, the Department of Energy and Climate Change announced that the deployment plan for smart meters is likely to be delayed for up to a year because the organisation responsible for building the national communications infrastructure to support smart metering (the Data and Communications Company, or DCC), will take longer to offer live services than had been envisaged. This is likely to slow deployment of smart meters over the near term. Other concerns around cost of deployment and benefits of the system may also contribute to delays. Political support for the project remains high and it is likely that deployment across this period will continue for business and domestic consumers.

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 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.

*Department of Energy and Climate Change: ‘Smart Metering Implementation Programme - Third annual report on the roll-out of Smart Meters’.

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, with key considerations including harmonisation (use of common frequencies across different countries (on which the UK is taking a lead) 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). Spectrum around 900 MHz has been suggested, but the current approach by OFCOM is to use this band on a “licence exempt basis” meaning that smart meters will have to share the radio spectrum with other devices. ZigBee* compatible devices appear to be the favoured solution for the HAN. For the backhaul to the service provider, a range of technologies may be used including wireless mesh networks, cellular radio, power-line and wired broadband.

*ZigBee is an open global standard for wireless technology.

Security: Concerns over the security of an AMI have been raised in recent years. In particular, the meter itself has been identified as a possible weak link in the chain. Given the global demand for smart meters, it is likely that the devices themselves will be manufactured abroad. For the UK rollout, all devices must be Commercial Product Assurance (CPA) approved and additional security measures are being applied. Since these devices are connected to a private, closed network, the risk of attacking the network leading to disruption of supply is reduced but still a possibility and therefore multiple layers of security have been added to the solution.

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. Recently, there have been negative reports suggesting the overall cost benefits to consumers and the UK as a whole have been overstated. There have also been 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 in “smart appliances”, for example, washing machines and similar products that can communicate with Smart Meters to automatically respond to pricing signals or energy supply disruptions, or that can be controlled remotely by the owner via a smartphone application. Gartner predicts that:

“In five years [by 2019], 10% to 20% of home appliances will be able to communicate with smart meters.”

Source 1: Gartner, 'Hype Cycle for Smart Machines, 2014', Brant K.F., Austin T., G00263827, 18 July 2014.

The Daily Telegraph recently reported on the delay on the installation of electricity and gas "smart meters" to UK households. To quote:
"The Government's £11bn plan to install "smart" energy meters in every home is being delayed by up to a year." [delayed until 2016].
"The meters, which will cost about £200 per household to install, monitor electricity and gas usage in real-time and send data back to suppliers daily, eliminating estimated billing. Energy suppliers are supposed to start the full national installation programme in late 2015, when a central communications system to handle data transfer between meters and suppliers was due to go live, and complete the roll-out by 2020."
Source 2: Gosden E.: '£11bn energy smart meter roll-out suffers fresh delay', The Daily Telegraph, http://www.telegraph.co.uk/news/earth/energy/11242115/11bn-energy-smart-meter-roll-out-suffers-fresh-delay.html, 19 November 2014, accessed on 17 December 2014.

This source examines privacy, security and health concerns with regard to the UK Government's proposed installation of smart meters into UK households:
"The Mail has quoted Cambridge IT professor Ross Anderson saying that smart meters pose a strategic risk to the UK, because the government plans to build the ability to connect and disconnect gas and electricity supplies remotely into the system.
…according to Anderson the function could create a "strategic vulnerability" to blackouts from "a nation state attacker, a terrorist or even a criminal group".
"The government will require companies to fulfil a set of data security requirements to combat identified risks before they can gain licenses to provide smart metering services. Companies will have to carry out security risk assessments, and there will be annual checks from independent data security auditors."
Source 3: Donald R.: The verdict on smart meter privacy, security and health concerns as UK smart meter rollout begins', The Carbon Brief, http://www.carbonbrief.org/blog/2012/06/does-my-smart-meter-know-when-i-am-on-the-loo/, 8 July 2014, accessed on 17 December 2014.

QinetiQ comment: Whilst these concerns have been widely reported in the popular media, the reports do not recognise that the safety functionality for disconnecting/connecting devices has been built into the system with strong controls to prevent abuse or misuse of the capability. For example, the numbers of this type of request will be monitored and excessive requests will be quarantined.

The BBC have recently reported on flaws discovered in smart meters deployed widely in Spain that would allow attackers to under report energy usage, and similar flaws may allow third parties with malicious intent to disrupt power supplies. "S*ecurity investigator Greg Jones who carried out similar work on smart meters being rolled out in the UK, said he was "not surprised" about the Spanish researchers' findings. Mr Jones's work uncovered shared IDs, poor protection against tampering and data formats that would be easy to fake. "I'm pretty sure that anyone who picked up one of these units would find similar problems," he said. Although many different researchers had found the security on smart meters wanting, so far, he said, this work had not prompted a big improvement in the way the gadgets worked."*

Source 4: Ward, M.: 'Smart meters can be hacked to cut power bills', http://www.bbc.co.uk/news/technology-29643276, 16 October 2014, accessed on 18 December 2014.

Source 5: 'Smart meter awareness campaign revealed', Utility Week, http://utilityweek.co.uk/news/smart-meter-awareness-campaign-revealed/1028212, 4 July 2014, accessed 19 Dec 2014.

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 coalition 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. The Department of Energy and Climate Change have published specifications for smart meters and the DCC have published a wide range of documents on the communications infrastructure for smart meters. OFCOM have published draft recommendations for the spectrum to be used for HANs.

QinetiQ comment

The deployment of smart meters continues 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 some reduction in the growth of energy demand over the coming years. For this to occur, a government sponsored awareness campaign (see Source 5 above) has already started. Whilst attacks are expected, risk assessments have been carried out and multi-layered security measures, including extensive use of cryptography, have been applied.

Software Defined Networks (SDN)

Description

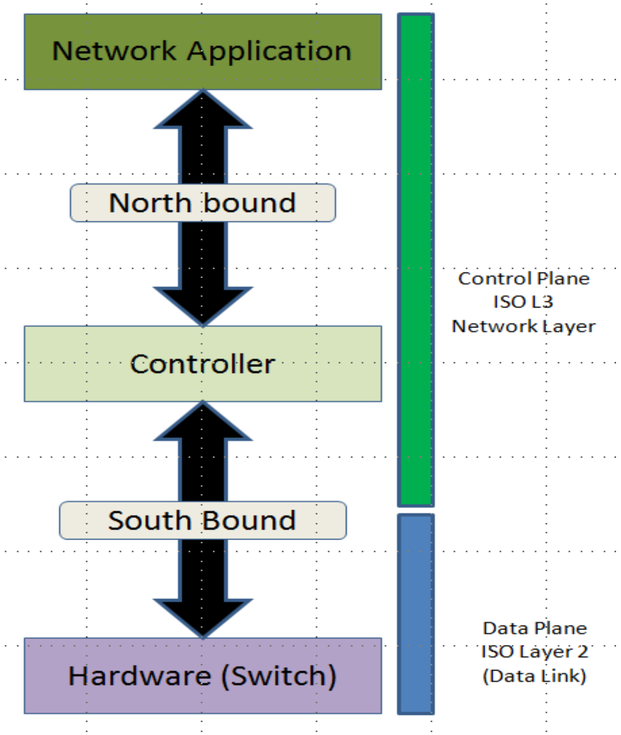
Software Defined Networks (SDN) is an emerging architecture that separates the network control from the actual forwarding functions, thus allowing the network control to be centralised in software and not contained within vendor-specific devices and protocols.

At the core of the SDN concept is a controller, which abstracts network elements and topology and provides a logical representation of a network, independent from the underlying infrastructure. This is significantly different from the current approach where each network element is configured individually and packet forwarding is controlled in a hop-by-hop manner. Consolidating the network control to an overarching controller allows traffic to be directed all the way through a network from an originating point to a terminating point based on information on the status of all network elements and any overarching policy decisions. Main benefits of SDN are:

- Centralised management in software based controllers, allows those controllers to maintain a global view of the network, thus controlling forwarding using a wider network view than that available at a single point in the network.
- An opportunity to enhance the security posture of the network infrastructure;
- Multiple Controllers (Master, Equal and Slave).
- Multiple Match Tables - allows the ability within an SDN network to create a complicated packet parsing capability.
- Meter Tables – for the implementation of a simple Quality of Service solution.
- Improved agility, due to the ability to provide network control from software that is not proprietary to the vendor providing the hardware, and can be tailored to the specific needs of the enterprise. Networks will be programmatically configured, rather than having to hand code lines of configuration into multiple different devices.

Most Relevant Cyber Security Controls

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Limitation and Control of Network Ports, Protocols, and Services
- Controlled Use of Administrative Privileges
- Boundary Defence
- Secure Network Engineering



Relevant Applications

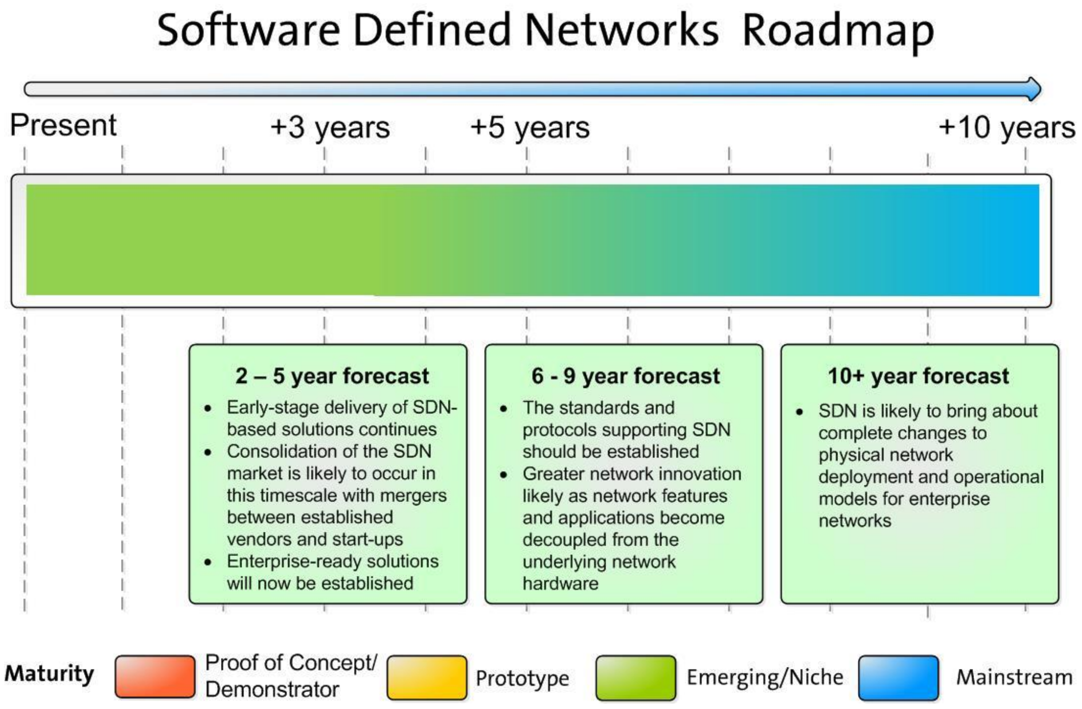
The majority of commercial interest in SDN is focussed at supporting network flexibility in large data centres at relatively fixed locations, which is not representative of all potential use cases. Successful and beneficial application in less localised instances such as in wide area networks (WAN) is yet to be proven. The focus of this forecast is therefore towards the use of SDN in the data centre.

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: Early-stage delivery of SDN-based solutions continues where focus is still on the data centre. Consolidation of the SDN market is likely to occur in this timescale with mergers between established vendors and start-ups. Enterprise-ready solutions will now be established.

Within 6 – 9 years: The standards and protocols supporting SDN should be established. As SDN continues to mature we can expect greater network innovation as network features and applications become decoupled from the underlying network hardware.

10+ years: SDN is likely to bring about complete changes to physical network deployment and operational models for enterprise networks (see Source 1).



Software Defined Networks Roadmap

2 – 5 year forecast

- Early-stage delivery of SDN-based solutions continues
- Consolidation of the SDN market is likely to occur in this timescale with mergers between established vendors and start-ups
- Enterprise-ready solutions will now be established

6 - 9 year forecast

- The standards and protocols supporting SDN should be established
- Greater network innovation likely as network features and applications become decoupled from the underlying network hardware

10+ year forecast

- SDN is likely to bring about complete changes to physical network deployment and operational models for enterprise networks

Maturity 🟥 Proof of Concept/ Demonstrator 🟨 Prototype 🟩 Emerging/Niche 🟦 Mainstream

General Issues and Challenges

Like many new technologies, SDN has received considerable hype and is currently one of the most talked-about areas in the networking marketplace (see Source 1). It is still in its infancy and is continuously evolving such that even the definitions of the meaning of SDN are contentious. There is still much work to do on standardisation, which is clear evidence of its immaturity.

SDN also appears to have significant potential security impacts of both a positive and negative nature. On the positive side, SDN offers better visibility of the networks and the way they are being used. Moreover, SDN's programmability feature provides opportunities to enhance the security posture of networks. For example, the Open

Network Foundation (ONF) (see Source 2) suggests that SDN techniques could be used to construct a data plane security solution that is able to coordinate both network and security devices to detect and react to attacks in a more flexible way. On the negative side the SDN architecture could present attackers with new opportunities (see Source 3). Such attack vectors could target each of the primary components of the SDN architecture and in particular, the controller layer where the centralised control is managed (see Source 2).

A number of Hybrid network switches are becoming available that can run in SDN or 'not SDN' mode as required and could be used by an organisation to replace network equipment in preparation for a switchover to an SDN solution.

Finally, it is worth highlighting that the adoption of SDN will require a new way of thinking that may challenge existing network engineers. The move to SDN will therefore have an impact on human resources.

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

Gartner's 2014 hype cycle on virtualisation covers SDN and comments on its relative immaturity:

"SDN is the most talked-about technology in the networking market today and represents a potential transformation in how the market will design, build, operate and procure network hardware and software. However, the technology is still nascent, with many complex vendor and organizational dynamics, and there is much standards work still to be done."

Source 1: Gartner, 'Hype Cycle for Virtualization, 2014', Dawson P., Hill N., G00263857, 23 July 2014.

The Open Networking Foundation (ONF) has recently produced a detailed report entitled "SDN architecture". This document specifies the architecture of software defined networking and expands the principles behind SDN, applying them to architectural components and interfaces. This report covers a number of implementation issues that includes security concerns. To quote:

"SDN security requirements may differ from those of a classical network due to their inherent characteristics and implementation choices. Depending on its physical implementation, centralized control may expose a single high-value asset to attackers, as distinct from a larger number of autonomous assets in a distributed control domain."

Source 2: 'SDN architecture Issue 1', Open Network Foundation, June 2014, https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf, accessed 16 Jan 2015.

This article presents a review of the potential attack vectors of SDN systems, coving attacks on: the data plane layer, the controller layer and the SDN layer. It closes by providing advice for hardening an SDN system and securing the various layers within the SDN architecture. To quote:

"We can only try to anticipate what the attackers may try to target with SDNs. The deployments are new, the protocols are new, the controller software is new, and the history of past SDN attacks is unknown. Based on the SDN architecture, we can predict where an attacker may be likely to strike. If we put ourselves in the attacker's shoes, we might be able to spot a weakness to exploit. Then we can harden that weakness ahead of time."

Source 3: Hogg S.: 'SDN Security Attack Vectors and SDN Hardening', NetworkWorld, http://www.networkworld.com/article/2840273/sdn/sdn-security-attack-vectors-and-sdn-hardening.html, accessed 16 Jan 2015.

Standards and policy (Government and non-Government)

As previously mentioned, there is still work to do on the introduction of standards for SDN. The Internet Engineering Task Force (IETF) has set up the SDN standards group, I2RS (Interface to the Routing System), to develop an SDN strategy and speed up the process of standardisation.

There is no known government policy concerning SDN.

QinetiQ comment

Organisations planning to adopt SDN should be aware that their current security architectures within their networks might affect the deployment of the technology. The security implications will need to be considered in the context of their business and work processes. Indeed, it is recommended that organisations preparing to exploit SDN technology should update their security strategy to incorporate the new needs and opportunities this technology offers.

It is also worth noting that the networks of many organisations consist of many legacy-networking devices. The transition to an SDN approach is likely to be complex and will require an overlay on top of existing physical equipment to be created at least in the short term.

Wearable Computing Devices

Description

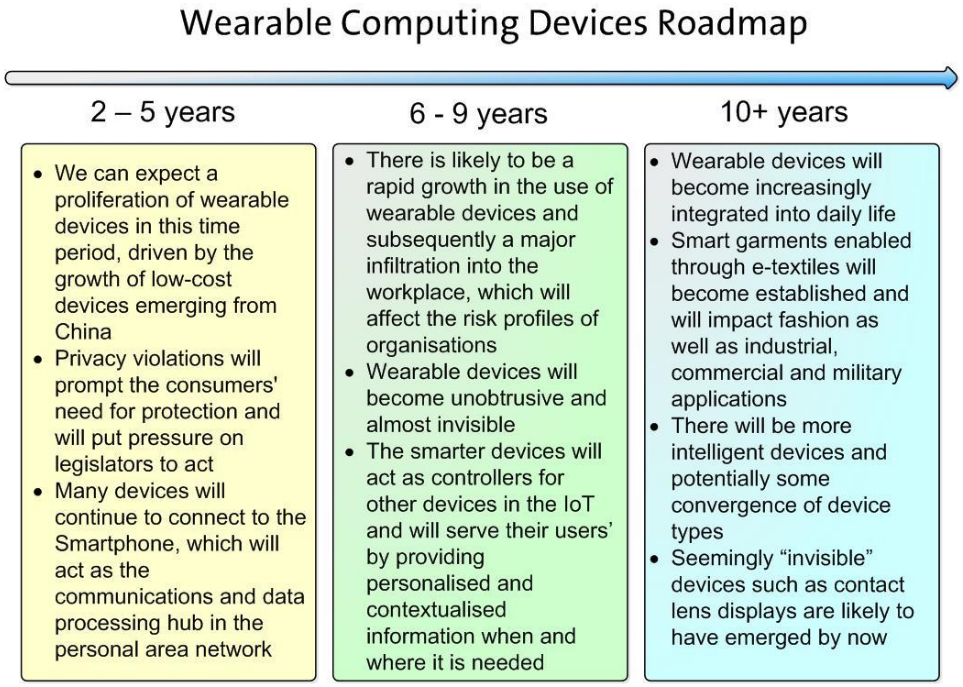
Wearable computing devices, also known as ‘body-borne’ or ‘wearables’, describe electronic systems worn by the user – under, within or on-top of their clothing. These devices range from wrist-worn devices such as smartwatches and fitness trackers, head-mounted devices such as smart glasses and body-worn devices that includes sensors built into jewellery and electronic clothing.

Over the next few years, we can expect a proliferation of these devices. Many new form factors and device types will emerge, becoming “things” in the so-called “Internet of Things” (IoT). As a result, wearable devices will appear more frequently in the workplace and will pervade our lives becoming smaller and less obtrusive, eventually becoming integrated within our clothing and potentially even our bodies.

The security implications will be enormous. New wearable technologies will appear and will evolve quickly and organisations will have difficulty keeping up with the threats that will inevitably emerge. Besides an array of traditional and more novel cyber-threats, we can expect privacy issues and frequent instances of personal identity theft. The rate of development of consumer wearable devices, driven by countries such as China, will make it difficult for companies to add sufficient security controls to protect their data and information. Much of the development of consumer wearable devices will be centred on health and fitness. Within the next five years a variety of smarter devices are likely to emerge. Many of these will continue to use the smartphone as the hub of communications and data processing; others however will be stand-alone and fully capable of supporting their user by delivering context-specific information at the point of need. New devices and form factors will appear on the market, including chest straps, smartwatches (with curved displays), wristbands and smart glasses (exploiting Augmented Reality (AR)). Many of these devices will connect to the smartphone, which will act as the communications and data processing hub in the Personal Area Network (PAN).

Most Relevant Cyber Critical Security Controls

- Inventory of Authorized and Unauthorized Devices
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Wireless Access Control



Wearable Computing Devices Roadmap

2 – 5 years

- We can expect a proliferation of wearable devices in this time period, driven by the growth of low-cost devices emerging from China
- Privacy violations will prompt the consumers' need for protection and will put pressure on legislators to act
- Many devices will continue to connect to the Smartphone, which will act as the communications and data processing hub in the personal area network

6 - 9 years

- There is likely to be a rapid growth in the use of wearable devices and subsequently a major infiltration into the workplace, which will affect the risk profiles of organisations
- Wearable devices will become unobtrusive and almost invisible
- The smarter devices will act as controllers for other devices in the IoT and will serve their users’ by providing personalised and contextualised information when and where it is needed

10+ years

- Wearable devices will become increasingly integrated into daily life
- Smart garments enabled through e-textiles will become established and will impact fashion as well as industrial, commercial and military applications
- There will be more intelligent devices and potentially some convergence of device types
- Seemingly “invisible” devices such as contact lens displays are likely to have emerged by now

Relevant Applications

Wearable computing devices will eventually become ubiquitous and it is easy to envisage numerous areas that could benefit from the technology. Their main advantage is their portability, where in many cases they can enable their users to work hands-free, alerting them of pertinent information relevant to their needs. The following areas are a few examples that will or are already benefitting from the technology: Health monitoring and fitness, manufacturing industries, retail and marketing (who will benefit from personalised data collection), the entertainment industry and the military and emergency services.

General Issues and Challenges

The technology will become pervasive and there is some uncertainty regarding its potential evolution. Some issues and challenges are recognised, but many more are yet to be identified. Amongst the more important issues, include concerns over security and privacy.

Privacy

Wearable devices, such as those found in health and fitness markets, collect, generate and transmit information to different services and the user to facilitate better quality of life. Securing this personal data and information will pose a challenge, particularly given that the technologies that process this data are emerging and evolving faster than privacy legislation, increasing pressure on regulators to catch up. The speed of growth of the consumer wearables market will put additional pressure on companies, forcing them to go to market faster. The smaller, lightweight devices that emerge will make it more difficult to add security controls to protect personal information. In addition, increased personalisation (contextualised information relevant to the user and refined through monitoring their behaviour) combined with location awareness will also be an important concern for privacy regulators (see Source 2). Finally, it is worth mentioning that cameras and life-blogging devices will exacerbate the situation (the case of Google Glass and the privacy concerns it triggered, particularly because of its camera, is a good example).

Security

In general, wearable devices pose unique security risks related to data, network, personal information and government regulation. Accenture (see Source 3), recognises the issues and recommends that organisations think about the scalability of their current network infrastructure and the manageability of the applications to be deployed on wearable devices such as smart glasses and smartwatches. It recommends that organisations should seek to understand the specific threats that these devices could pose and that appropriate controls should be implemented to decrease the risks. Accenture highlight four potential areas of concern (to quote):

Data leaks: Determine what data the wearable display may access within enterprise systems, as well as what data the device may capture during usage.

Network security: Consider how to protect against security threats such as phishing or man-in-the-middle attacks on wearable displays.

Personally identifiable information (PII): Data leaks via wearables may lead to identity theft of PII

Government-imposed violations of privacy: A related issue to address is privacy violation since companies could hypothetically collect employees' habits, behaviours and even health information via a wearable device.

Power

Small form factor wearable devices, which are required to be “always-on”, demand innovative power solutions. This issue is the subject of much research, where power solutions such as energy harvesting are being considered (see Source 5).

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

The market research company IDTechEx, has recently published a report that forecasts the likely development of the wearable technology market over the next decade:

“Wearable technology mainly concerns devices and apparel/textiles. Glasses, jewellery, headgear, belts, arm-wear, wrist-wear, legwear, footwear, skin patches, exoskeletons and e-textiles are involved and the device business is already large. As the wearable electronics business powers from $20 billion in 2015 to almost $70 billion in 2025.”

Source 1: Harrop P. et al.: ‘Wearable Technology 2015-2025: Technologies, Markets, Forecasts’, IDTechEx, January 2015.

This paper by the IT analyst company, Gartner, highlights privacy risks with respect to wearable computing devices, personalisation and location-based services.

“End users will ask specific security questions before selecting and buying wearable technologies and healthcare devices, particularly in the areas of access management and data protection. Device manufacturers and service providers should establish aggressive secure development and management strategies for their product and service offerings to provide proof to buyers that personally identifiable information and private data can be adequately protected.”

Source 2: Gartner, ‘Predicts 2015: Privacy Erodes, Prompts Action From Companies and Regulators’, Casper C. et al., G00271115, 4 December 2014.

Accenture have recognised that wearable devices may pose unique security risks related to data, network, personal information and government regulation and provides insight of potential Cyber-threats that could affect individuals and organisations that are using the technology.

Wearables can be thought of as mobile devices at the edge…with the added dimension of ultimate portability (i.e., wear anywhere) and visibility (i.e., the ability to actually “see” real-time enterprise data). Unlike mobile devices, which have distinct periods of use, some wearables are also potentially always-on and always gathering data. In these ways, wearables are unique.

Security executives need to pay extra attention to maintaining confidentiality, integrity and availability (aka CIA) for wearable displays. What’s more, it is important to prepare early and create security policies, procedures and encryption protocols before wearables are deployed.

Source 3: Blum B.: ‘Are Your Wearables Safe from Cyber-Security Threats?’ Accenture, 18 January 2015, http://www.accenture.com/us-en/blogs/technology-blog/archive/2015/01/18/are-your-wearables-safe-from-cyber-security-threats.aspx, accessed on 5 March 2015.

“No modern technology has needed to focus on aesthetics more than wearables, but even if the user experience can be perfectly designed, wearables pose an assortment of other concerns that could crush mainstream adoption even in the workplace. Two of the most significant barriers to adoption are questions about the true convenience of wearables and privacy concerns.”

Source 4: Draegar D.(ed): ‘Optimising You – Get the Gist on Wearable Information Technologies’, Shaping Tomorrow, http://www.shapingtomorrow.com/webtext/700, accessed 5 March 2015.

Source 5: EET Asia, **‘**Wearables uptake hindered by power issues’, EE-Times Asia, 14 January 2015,

http://www.eetasia.com/ART_8800708865_480100_NT_3c6eb267.HTM, accessed 10 March 2015**.**

Standards and policy (Government and non-Government)

Wearable technologies are still in their infancy although there has been some standardisation effort with regard to the networks and communications supporting such devices. For example, the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF) and a number of industry groups (e.g. Bluetooth) have done work concerning interfacing on WPANs (wireless personal area networks) and WBANs (Wireless body area networks), thereby offering a new classification of designs for interfacing and networking.

There is currently no known UK Government policy on the use of wearable computing devices.

QinetiQ comment

With a few exceptions, consumer wearable devices are likely to remain as extensions of the Smartphone for the immediate future. In the longer term, we will likely see wearable devices becoming more autonomous. When this happens, the technology is likely to become a more disruptive force and could even become a threat to the Smartphone as the mobile platform of choice. AR may feature prominently in the battle between the handheld and the wearable head-mounted form factor. Interest in AR is growing and the fact that head-mounted AR is preferable and more natural to handheld AR may be a deciding factor in this battle.

Wireless Mesh Networks

Description

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 connection between end-points or where one device acts as a central hub and relays information for all other devices.

In a wireless mesh network, 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.

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.

Most Relevant Cyber Security Controls

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Wireless Access Control
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Limitation and Control of Network Ports, Protocols, and Services
- Controlled Use of Administrative Privileges
- Boundary Defence
- Maintenance, Monitoring, and Analysis of Audit Logs
- Secure Network Engineering

There are two main types of wireless mesh network:

- 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.

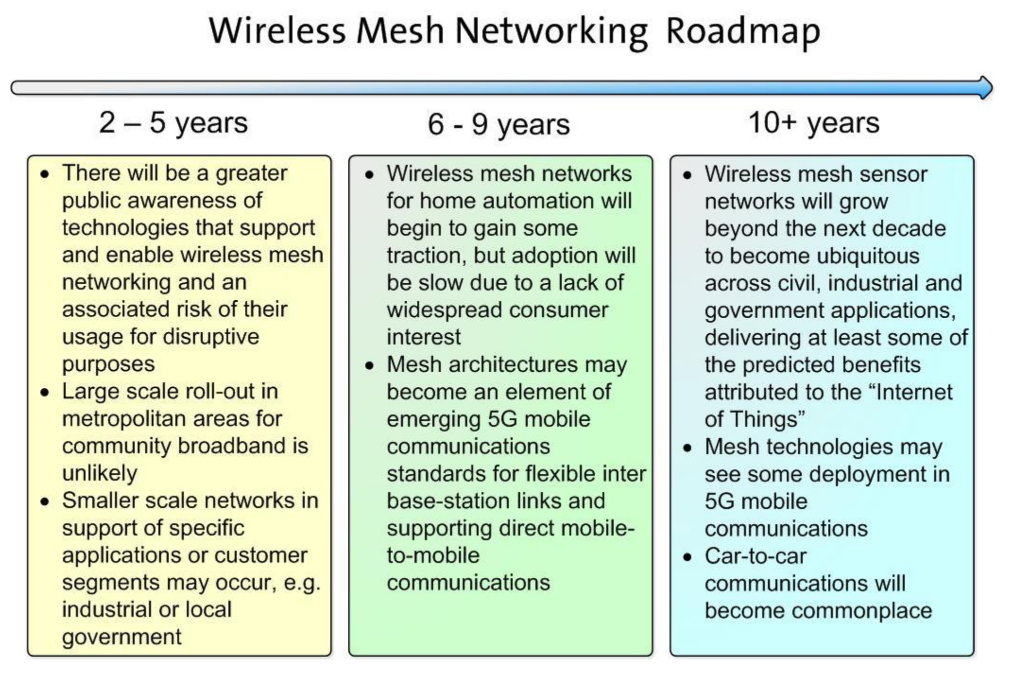
Relevant Applications

The following are a number of examples where wireless mesh networking could be applied:

- Urban and rural broadband, e.g. community broadband services, and future “5th Generation (5G) mobile communications.
- Sensor networks, e.g. remote sensing, industrial monitoring and control, home automation. A key element of the so-called “Internet of Things”.
- Communications for the “smart energy grid” and smart meters.
- Surveillance (e.g. video).
- Paramilitary and Defence, particularly tactical communications.
- Car to car communications (a form of MANET).
- Ad hoc networks for consumer use (e.g. gaming, messaging).

Technology Readiness and Maturity (forecasted arrival and accessibility)

Within 2 – 5 years: During this time period there will be a greater public awareness of technologies that support and enable wireless mesh networks for both broadband and sensor networks, which will increase the risk of their usage for disruptive purposes. Mobile apps such as those available from the iOS and Android App stores that provide ad hoc networking between devices using their Wi-Fi capabilities (e.g. Firechat, Serval) will become more prevalent (see Source 2). 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. For smart meters, ZigBEE compatible devices appear to be the favoured solution for the Home Area Network (HAN). Hence, ZigBEE solutions will deployed as the roll out of smart meters accelerates in the UK and other countries. This may gradually start to faciliate other uses of the HAN over time. There will be continued deployment of small scale sensor networks (e.g. 10s-100s of nodes). Some cars will come equipped with car-to-car communications.



Wireless Mesh Networking Roadmap

2 – 5 years

- There will be a greater public awareness of technologies that support and enable wireless mesh networking and an associated risk of their usage for disruptive purposes
- Large scale roll-out in metropolitan areas for community broadband is unlikely
- Smaller scale networks in support of specific applications or customer segments may occur, e.g. industrial or local government

6 - 9 years

- Wireless mesh networks for home automation will begin to gain some traction, but adoption will be slow due to a lack of widespread consumer interest
- Mesh architectures may become an element of emerging 5G mobile communications standards for flexible inter base-station links and supporting direct mobile-to-mobile communications

10+ years

- Wireless mesh sensor networks will grow beyond the next decade to become ubiquitous across civil, industrial and government applications, delivering at least some of the predicted benefits attributed to the “Internet of Things”
- Mesh technologies may see some deployment in 5G mobile communications
- Car-to-car communications will become commonplace

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 using ZigBEE progresses. 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. Mesh architectures may become an element of emerging 5G mobile communications standards for flexible inter base-station links and supporting direct mobile-to-mobile communications.

10+ years: Wireless mesh sensor networks will grow beyond the next decade to become ubiquitous across civil, industrial and government applications, delivering at least some of the predicted benefits attributed to the “Internet of Things”. Other forms of wireless mesh network for more general purpose networks will be relegated to niche applications such as defence and paramilitary, disaster recovery and occasional ad hoc use by consumers when the wider mobile infrastructure is not available. 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. Mesh technologies may see some deployment in 5G mobile communications. Car-to-car communications will become commonplace.

General Issues and Challenges

- Spectrum: many wireless mesh networks operate in the Industrial, Scientific and Medical (ISM) frequency bands based on Wi-Fi 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 therefore become increasingly congested. Other frequency bands are possible, but require a spectrum licence. Some "multi-band" mesh radios are available, for instance supporting both Wi-Fi and the 4.9GHz 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 ongoing 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 Wi-Fi 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 are 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.
- Technology Maturity: this is particularly true for wireless mesh sensor networks. There are a number of areas where academic research is ongoing.

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

Gartner has recently highlighted the potential for ZigBEE, noting its adoption by the smart meter industry but also citing concerns about technology fragmentation and competition from other technologies.

"ZigBee's first significant win was in the smart meter market. This foray into the home may parlay into ZigBee's inclusion in more home appliances. However, this is still mostly unrealized potential: While Nest's original thermostat included both ZigBee and Wi-Fi (with only the latter being enabled), its follow-on smoke detector included only Wi-Fi."

"Users should monitor ZigBee's market traction versus other key competing technologies, such as Wi-Fi and Bluetooth".

Source 1: Gartner, 'Hype Cycle for Wireless Networking Infrastructure, 2014', Fabre S., G00260634, 24 July 2014.

There are a number of mobile apps available on the Android and iOS app stores. These are aimed at supporting small ad-hoc networks when the traditional mobile communications infrastructure is either not available or undesirable to use. Such apps have been recently used by citizens during the protests in Hong Kong and Tawain, and also in Iran to provide an alternative and resilient medium for communicating and coordinating.

"So far, mesh networks have proven themselves quite effective and quickly adopted during times of disaster or political unrest, as they don't rely on existing cable and wireless networks…".

Source 2: Hu E.: 'How Hong Kong Protesters Are Connecting, Without Cell Or Wi-Fi Networks', 29 September 2014,

http://www.npr.org/blogs/alltechconsidered/2014/09/29/352476454/how-hong-kong-protesters-are-connecting-without-cell-or-wi-fi-networks, accessed 9 Mar 2015.

Wireless mesh technologies may play a role in emerging 5G mobile communications standards. ZTE, a major Chinese mobile telecommunications company, recently proposed a 5G architecture based on dynamic mesh networking.

"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 HAN-enabled devices are installed the network would actually strengthen."

Source 3: ZTE, 'ZTE releases first 5G architecture based on dynamic mesh networking', 23 June 2014,

http://wwwen.zte.com.cn/en/press_center/news/201406/t20140623_425167.html, accessed 9 March 2015.

Standards and policy (Government and non-Government)

There are a number of standards that have emerged, or are emerging, for wireless mesh networks. However these are used mainly in the lower layers of the communications protocol stack. For example Wi-Fi (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 through 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 notable attempts to standardise on wireless mesh networks include:

- 802.11p: for vehicle-to-vehicle communications.
- 802.11s: an enhancement of 802.11 (Wi-Fi) to allow access points to form a wireless mesh network. The 802.11s standard has been available for some time, but adoption by manufacturers has been very slow and the standard may never gain significant traction in the market.
- 6LoWPAN: standardised the use of IPv6 low-power wireless mesh sensor networks.

Mesh concepts and architectures may become an element of the emerging 5G standards for interconnects between base-stations and to support direct device-to-device communications. It is still early days in the development of the standards and it is notable that attempts to incorporate similar capabilities in the 3G standards in the past have failed, particularly for direct mobile-to-mobile communications.

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. It is also notable that the mesh standard 802.11s has failed to gain traction in the industry. However, wireless mesh networks will always have a role in some 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.
- Direct mobile-to-mobile communications avoiding the use of traditional operators. The recent use of ad hoc network apps in the Hong Kong and Taiwan protests is a good example of this.
- Vehicle-to-vehicle networks.
- Military and paramilitary networks where there is no fixed infrastructure available.
- Sensor networks.

QinetiQ agrees with other industry commentators that wireless mesh sensor networks are likely to become ubiquitous over time, but that it will take many years for that to happen.

END OF DOCUMENT