Computer-Related Infrastructure Risks for Federal Agencies

Peter G. Neumann
Principal Scientist, Computer Science Laboratory
SRI International, Menlo Park CA 94025-3493
Telephone: 1-650-859-2375
Internet: Neumann@CSL.SRI.com; Website: http://www.csl.sri.com/neumann.html

[Written testimony for the U.S. Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs included in *Weak Computer Security in Government: Is the Public at Risk?,* Hearing, S. Hrg. 105-609, 1998, pp. 52--70. ISBN 0-16-057456-0, 1998. Oral testimony is on pages 5-22. Testimony from seven members of the L0pht group is also included in that volume.]

I greatly appreciate being invited to appear before you. Some of you recall my June 1996 testimony for your Permanent Subcommittee on Investigations (Reference 4). I have tried not to simply duplicate that testimony (which is still surprisingly relevant). I begin by summarizing my main points and then examine what has changed in the past two years.

This written statement surveys the primary risks related to computer-communication technology, and what we might do to reduce them. The scope of my remarks broadly includes Federal Government systems, but is also applicable to State, local, and private sector systems as well. (The problems are essentially the same, although the perspectives are quite different.) I address security, reliability, availability, and overall survivability of those systems.

I appear here as a private citizen, although I have several affiliations that are worth noting. I am employed by a not-for-profit R&D institute (SRI International), where I am involved in several particularly relevant projects -- including an advanced system for detecting network misuse and related threats (for DARPA), and a study of the requirements and suitable system architectures for highly survivable systems and networks (for the Army Research Lab). I am a member of the General Accounting Office Executive Council on Information Management and Technology. I am the author of a book (*Computer-Related Risks*) on what has gone wrong and what we should expect to go wrong, and what we can do to reduce the risks involved in the use of computers. (For the record, I include at the end of this testimony some relevant further background.)

The Past and the Present

The final report of the President's Commission on Critical Infrastructure Protection (PCCIP) (Reference 1) addressed eight major critical *national infrastructures:* telecommunications; generation, transmission and distribution of electric power; storage and distribution of gas and oil; water supplies; transportation; banking and finance; emergency services; and continuity of government services. Perhaps most important is the Commission's recognition that very serious vulnerabilities and threats exist in all of these critical infrastructures. Perhaps equally important if not more so is that all of these critical infrastructures are closely interdependent; a failure on one sector can easily affect other sectors. Furthermore, all of the national infrastructures depend critically on the underlying *computer-communication information infrastructures,* such as computing resources, databases, private networks, and the Internet. The extent to which this is the case is not generally appreciated, and seems sublimated in the PCCIP report. (See Reference 7.)

The existing national infrastructures and the underlying information infrastructures are riddled with vulnerabilities, representing security, reliability and system survivability flaws as well as potential attacks that can affect hardware, software, communications media, and people's lives. Security concerns are important, but it must also be remembered that systems and networks tend to fall apart on their own, without requiring malicious attacks. (The impending Year 2000 certainly gives us such an opportunity on an unprecedented scale.) Because the Government has become totally dependent on commercial system offerings that are typically not capable of satisfying critical requirements, the situation is becoming unstable.

- **Vulnerabilities.** Serious security flaws and reliability glitches are abundant in most computer systems, networks, Web software, and programming languages. These have been widely reported. The extent of the risks is still not widely recognized, although the Eligible Receiver exercise is clearly suggestive of what is possible. Furthermore, there has not been enough work to develop adequate preventive measures. As-yet-undiscovered vulnerabilities may be even greater than those that are known today. Future disasters may involve vulnerabilities that have not yet been conceived as well as those that are already lurking.

- **Threats.** There are many realistic threats to the information infrastructures, including malicious insiders and intruders, terrorists, saboteurs, and incompetent administrative and operational staff, in addition to effects of the environment, natural phenomena, accidental interference, and so on. These threats may come from corporate, national, or terrorist interests as well as individuals. The list of threats is long and multidimensional (and discussed in the PCCIP report). Consequently, it is not possible to predict which threats will be exploited, and under what circumstances.

- **Attacks.** Malicious attacks can come from anywhere in the world, via dial-up lines and network connections, and often anonymously. Thus far, there have been relatively few truly serious malicious attacks on computer systems and networking (for example, see Reference 12, which includes analysis of the Rome Lab case and was briefed to the Permanent Subcommitee on Investigations during its June 1996 hearings), although such activities from both insiders and outsiders appear to be increasing, particularly in financial systems (such as the $588 million Japanese Pachinko frauds and the Citibank case). There have been numerous cases of more than mere nuisance value (for example, the hacking of Web sites of the Justice Department, CIA, US Air Force, and NASA), including many denials of service (for example, flooding attacks that have disabled entire networks). The recent attacks on Pentagon systems by the unsophisticated Cloverdale kids were claimed by Deputy SecDef John Hamre to be ``the most organized and systematic the Pentagon has seen to date'' -- but they really indicate only how flimsy Pentagon Internet computer security actually is, as representative of commercial product (un)security. Considering how easy it was for those kids, imagine what could happen if a terrorist group decided to use its resources for seriously nefarious purposes. (I know of several attacks that have never been acknowledged publically, some of which are quite startling.) Although it would be appropriate for the FBI to ratchet up its technical competence, expenditures of funds on prosecuting young system crackers might much better be spent in developing and procuring computer-communication systems that are substantially more secure than what is available today. Also noteworthy are the recent Masters of Downloading attack on the Defense Information Systems Network, and the Tamil Tigers in Sri Lanka. The random interception of a cell-phone conversation involving Newt Gingrich, and the more systematic interception of Secret Service pager messages involving the President (despite demonstrations four years ago at the Hackers on Planet Earth conference of how easy that was to do) are again symptomatic of weak security. Various penetration studies without malicious intent, failed experiments (such as the 1988 Internet Worm), and analyses have demonstrated actual flaws in deployed Web browsers, servers, protocols, algorithms, and encryption schemes. Eligible Receiver demonstrated further vulnerabilities. It is nice that we have so many friendly participants in this struggle to identify the vulnerabilities, although these efforts seem to have little impact on increasing the dependability of the systems thus penetrated. It appears that official concern will remain inadequate to the magnitude of the potential risks -- until we are hit by devastating attacks that demand immediate attention. The rapid acceleration of electronic commerce can be expected to inspire some ingenious massive frauds that systematically exploit various major vulnerabilities in the information infrastructure -- which could be a goldmine for organized crime. The weak security that is endemic today in many commercial systems is truly a travesty that we cannot afford to perpetuate in the future.

- **Reliability problems.** Examples of past accidental outages include the 1980 ARPAnet collapse, the nationwide 1990 AT&T long-distance collapse, the AT&T frame-relay business-network shutdown, many recent outages and saturations of Internet service providers, and many consequences of the spate of Western power outages two summers ago. These incidents demonstrate how apparently isolated events can propagate widely. The Year-2000 problem (Y2K) is of great concern to government agencies and the private sector alike. (See Reference 18 for a recent overview of the dramatic extent of the problem. Also, see U.S. Representative Stephen Horn's Y2K report card, which suggests that many Federal departments and agencies are failing badly.) However, the Y2K problem is really just another example of the difficulty of developing software systems that will operate correctly over a broader range of requirements than were considered in the original requirements. (Foresight is not that difficult, but is often co-opted by short-term commercial interests or incredible myopia. For example, I was a co-designer from 1965 to 1969 of a highly innovative advanced secure system that clearly recognized and avoided the Y2K problem -- Multics, a significant research and development effort jointly among MIT, Bell Labs, and Honeywell.) However, if the Y2K problem is causing the Federal Government so much grief, how can the Government expect to do security properly? Date arithmetic is not difficult if you know what you are doing. Security is much more difficult.

Many of the cases noted above are documented in Reference 3 and in the on-line Risks Forum.

With respect to the national infrastructures and the computer-communication infrastructures, it is clear that the threats are pervasive, encompassing intentional as well as accidental causes. Aviation is a serious concern. Power generation, transmission, and distribution are particularly vulnerable, as is the entire telecommunication infrastructure. However, it is certainly unpopular to discuss specific threats openly, and thus the risks tend to be largely downplayed -- if not almost completely ignored.

To give a more detailed example of the breadth of threats in just one critical-infrastructure sector not examined in much detail by the PCCIP, consider the safety-related issues in the national airspace, and the subtended issues of security and reliability. (See for example, my article for the International Conference on Aviation Safety and Security in the 21st Century, Reference 5.) Alexander D. Blumenstiel at the Department of Transportation in Cambridge, Massachusetts, has conducted a remarkable set of studies over the past 14 years. In his series of reports, Blumenstiel has analyzed many issues related to system survivability in the national airspace, with special emphasis on computer-communication security and reliability. His early reports (1985-86) considered the susceptibility of the Advanced Automation System to electronic attack and the electronic security of NAS Plan and other FAA ADP systems. Subsequent reports have continued this study, addressing accreditation (1990, 1991, 1992), certification (1992), air-to-ground communications (1993), air-traffic-control security (1993), and communications, navigation, and surveillance (1994), for example. To my knowledge, this is the most comprehensive set of threat analyses ever done outside of the military establishment. The breadth and depth of the work deserves careful emulation in other sectors. (See Reference 16.) Further problems relating to the FAA procurement practice and safety considerations have been subjects of various GAO reports.

In general, it may seem very unpopular to expend resources on events that have not happened or that are perceived to be very unlikely to occur. The importance of realistic threat and risk analyses is that it becomes much easier to justify the effort and expenditures if a clear demonstration of the risks can be made. Therefore, it is absolutely vital that you openly understand and acknowledge the pervasiveness of the existing vulnerabilities, threats, and risks, and the likelihood that they are getting worse rather than better. The General Accounting Office (e.g., Reference 12) and the National Research Council (e.g., References 2, 9, and 17) are two major sources of objective analysis.

The risks noted above are critical to U.S. Government departments and agencies, particularly those that are concerned with the critical national infrastructures -- such as the Departments of Defense; Energy; Health and Human Services; Commerce; Transportation; as well as the FAA and the Social Security Administration. (Ironically, almost all of those organizations are already seriously threatened by the Y2K problem.)

Conclusions

- **Interconnectivity.** Computer systems have become massively interconnected, dramatically more so than a few years ago. We are now dependent on people and systems of unknown and unidentifiable trustworthiness (including unidentifiable hostile parties), within the U.S. and elsewhere. Our problems have become international as well as national.

- **Risks.** The fundamental vulnerabilities in the existing computer-communication infrastructure are pervasive, and the situation is not getting better. Although some old vulnerabilities are occasionally removed, others remain, and new vulnerabilities are continually being created. Electronic commerce is particularly at risk. The national infrastructures are also at risk. Because of the interdependence of the infrastructures, the risks tend to propagate: each component that is compromised increases the danger that other components will also be compromised. Multidisciplinary preventive measures are essential, but most measures to date have been narrowly conceived.

- **Diversity.** Diversity of systems, algorithms, techniques, and implementations is one of our biggest allies. It is extremely unwise to put all one's eggs in a single basket, especially when that basket is as full of holes as is increasingly the case today.
- **Privacy.** Privacy is becoming an orphan step-child, with flagrant commercial abuses. There have also been various cases of misuse of Government databases, including IRS data (not to mention rogue operatives) and law-enforcement data (Reference 13). In general, we have been lucky, but should not count on that in the future as the stakes and risks increase.
- **Cryptography.** Cryptography is an absolutely essential ingredient in achieving confidentiality, user authentication, system authentication, information integrity, and nonrepudiability. The Adminstration's cryptographic policy has failed to realistically recognize this need, despite the essential nature of strong nonsubvertible cryptography in protecting the national infrastructures and the information resources of the Government and Federal agencies. U.S. crypto policy has instead focused on limiting the use of strong cryptography, rather than on encouraging its use in vital systems -- including the critical national infrastructures. It has deterred efforts to improve security, and is beginning to drive the cutting-edge applications of cryptography abroad. (See References 8 and 9 for an elaboration of difficulties related to U.S. crypto policy, and Reference 6 for my Senate Judiciary Committee testimony.)
- **Authentication and passwords.** Reusable user passwords present serious risks, especially when they transit unencrypted communication paths that can be intercepted, or can otherwise be obtained. (Many of the familiar penetrations have involved compromise of reusable passwords.) The use of cryptographically based authentication (with one-time tokens rather than often-reusable passwords) is essential to the security and survivability of our infrastructures. Even though cryptography used for authentication is treated differently by export controls, those controls have had the effect to dumb down the needed authentication techniques.
- **System development practice.** In general, efforts to develop and operate complex computer-based systems and networks that must meet critical requirements have been monumentally unsuccessful -- particularly with respect to security, reliability, and survivability. The U.S. Government (and almost everyone else) has experienced repeated difficulties in developing large systems, which are increasingly dominated by software. Significant problems have arisen, leading to cancellations of the en-route air-traffic control system upgrade, the IRS Tax Systems Modernization effort, law-enforcement systems (e.g., the fingerprint system), procurements for military and commercial aviation and defense systems, and the $300 million California Deadbeat Dads' and Moms' database system -- with expenditures of billions of dollars down the drain. (In the case of the federally mandated state database of deadbeats, as of the October 1995 deadline there were still 16 states that were unable to comply with the requirements.) However dire it turns out to be, the Y2K problem is merely the tip of an enormous iceberg relating to our inability to use greater foresight in developing complex systems. As a nation, we desperately need a better ability to develop complex systems -- within

budget, on schedule, and likely to meet their stated requirements. The shuttle is one successful example of a large and very complex system development in which software goals were met adequately, although the costs of that effort were not insignificant and the risks were understood in advance better than in other systems. The development of robust hardware-software systems is an extremely widespread problem, and is not limited to either government or private-sector systems. (References 3 and 11 provide numerous additional examples of development fiascos.)

- **System use.** Even if a system is developed according to the stated needs (which is very rare), the practice of using such systems seems to be exceedingly sloppy. Employees are often poorly trained to cope with the idiosyncrasies of the systems they must use. Individual data items are often incorrect, particularly in IRS, social services, law enforcement, and motor-vehicle information systems. Privacy requirements are often flagrantly disregarded, or else nonexistent. Systems are sometimes unavailable.

Recommendations

- **Systems and networks.** We must improve our nation's ability to develop complex systems. Such system efforts are characteristically short-sighted, over-budget, late, and functionally inadequate with respect to system and enterprise survivability, security, reliability, and performance -- all of which must be more comprehensively built into the systems.

- **Personal-computer inadequacies.** We must accept the fact that existing personal-computer operating systems typically do not provide a sufficiently robust base on which to build critical applications that can perform dependably in the face of threats to reliability and security. The marketplace is a marvelous incentivizer of technological innovation, but not an adequate motivation for really secure, reliable, and survivable systems. Overreliance on single systems and single developers is a disaster in the making, especially when those systems are not capable of fulfilling the real requirements.

- **The role of the U.S. Government.** Given the difficulties in system development and the fundamental inadequacies in baseline commercial products, the Government must rise to the challenge in several dimensions.

  -- The U.S. Government must get its own house in order. It must strive to improve the security, reliability, and survivability of its systems and networks. To do this, it must streamline its procurement process, with depth of understanding in what is being procured rather than merely pro forma attention to bean counting. The specified requirements must demand better systems, and contracts to the lowest-bid proposal without a reasonable chance of succeeding should be avoided. The procurement process must include technically knowledgeable Government personnel (not just contractors acting as project managers).

  -- Developers must somehow be encouraged or perhaps required to satisfy meaningful requirements for security and reliability in their baseline products. Y2K is merely one example. If you are overly concerned with the Y2K fiasco, you may be blindsided the deeper problems. Unfortunately, security is in the long run an even more critical problem.

-- You must have an accurate assessment of the appalling state of current systems with respect to security, reliability, and survivability in the face of realistic threats. You also need a realistic assessment of what is required to achieve sufficiently robust infrastructures. One way to do that might be to consider the computer-communication infrastructure necessary to provide the ability for Senators to vote remotely (for example, from a hearing room or while traveling). You would need a meaningfully secure system with no unauthorized access paths, strong cryptography, and nontrivial authentication with smart cards or biometrics. Even then, you would have only an inkling of the more general problem faced by the critical national infrastructures and digital commerce using the Internet and dial-up lines.

-- Funding vital research and prototype development is essential to help close the gap between commercial products and what is possible but not commercially desirable. Research on the composition of systems out of subsystems is particularly important, because seemingly simple combinations often result in complex and unpredicted behavior. This is also true of computer networks. In addition, we must find better ways of getting good research prototypes into the marketplace. Surprisingly perhaps, free software is sometimes preferable to proprietary products.

-- Better teaching and practice of good system engineering and software engineering must be encouraged, not just the fostering of computer literacy. Much deeper knowledge and experience is essential pervasively.

-- Better training of users is essential, aided by the development of systems with interfaces that are more user friendly.