Security Risks in the Computer-Communication Infrastructure

Peter G. Neumann
Computer Science Laboratory, SRI International
Menlo Park, California 94025-3493
Telephone: 1-415-859-2375
Neumann@CSL.SRI.com (Peter G. Neumann)
25 June 1996

Written testimony for the U.S. Senate Permanent Subcommittee on
Investigations of the Senate Committee on Governmental Affairs

Thank you for the invitation to appear before you today. It is a very special privilege for me. (For the record, I have included some of my personal background at the end of this testimony.)

My written statement addresses some of the fundamental risks facing us in our present uses of computer-communications technology, and assess how those risks might change as we depend increasingly on that technology.

These written comments address issues that I understand to be at the heart of the intended scope of these hearings: an assessment of security vulnerabilities and risks in computer-communication systems within the Department of Defense, non-DoD U.S. Government, and private sector (including the NII and its future evolution). I include a few recommendations that might contribute to improved security. In the present context, security implies techniques for the prevention of intentional and – to some extent – accidental misuse in computer-communication systems.

Brief Summary

To give an idea of the scope of this testimony, here are a few talking points.

- We are becoming massively interconnected. Whether we like it or not, we must coexist with 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.
- There are fundamental vulnerabilities in the existing computer-communication infrastructure, and serious risks that those vulnerabilities will be exploited – with possibly very severe effects. Our national infrastructure depends not only on our interconnected information systems and networks, but also the public switched network, the air-traffic control systems, the power grids, and many associated control systems – which themselves depend heavily on computers and communications.
- There are many past cases of security misuse worthy of your attention, such as the 1988 Internet Worm, the Citibank penetration, and the Rome Lab case (Reference 8). (See the attached Reference 3 for a summary of other cases as well.) However, there are many serious security vulnerabilities that have been discovered by friendly parties and fixed before they could exploited. In addition, there have been various cases of misuse of government databases,

including IRS data and law-enforcement data (Reference 9). In general, we have been lucky, but should not count on that in the future as the stakes and risks increase.

- Global problems can result from seemingly isolated events, as exhibited by the early power-grid collapses, the 1980 ARPANET collapse, and the 1990 long-distance collapse – all of which began with single-point failures.
- Our defenses against isolated attacks and unanticipated events are inadequate. Risks include not just penetrations and insider misuse, but also insidious Trojan horse attacks that can lie dormant until triggered.
- Our defenses against large-scale coordinated attacks are even more inadequate. The unintended effects of the nonmalicious 1988 Internet Worm must be interpreted properly – hinting at the devastating effects that could have resulted if that case had been carried out maliciously.
- Reliability and system survivability are closely interrelated with security.
- Attaining dependable security and reliability is a very difficult problem that has not been adequately understood by most people. It is essentially impossible to have any guarantees whatsoever that a system will work properly when and where it is needed. Security and reliability are both weak-link phenomena, and there are far too many weak links.
- Cryptography is an absolutely essential ingredient in achieving confidentiality, user authentication, system authentication, information integrity, and nonrepudiability. U.S. cryptographic policy has generally not been sufficiently oriented toward improving the infrastructure, in that it has been more concerned with limiting the use of good cryptography. U.S. crypto policy has instead acted as a deterrent to better security. (See Reference 6 for an elaboration of that point.)
- 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. This is a widespread problem, and is not limited to either government or private-sector systems. (References 3 and 4 provide numerous examples of development fiascos.)

My testimony amplifies all of these points, addressing a few questions that have been suggested to me as being of particular interest to you.

RISKS

What Are the Intrinsic Risks in Our Information Infrastructure?

• **Vulnerabilities.** Our infrastructure depends on the adequate functioning of many computer-communication systems, including (for example) the public switched network, power distribution, air-traffic control, nuclear-power systems, and – increasingly – the Internet itself. We focus here on the security vulnerabilities, although we observe a relationship with reliability failures and system survivability issues in the presence of adverse conditions. Many of these systems have serious potential security vulnerabilities, exploitation of which could cause massive disruptions.

These problems must be properly addressed in the emerging global information infrastructure, particularly as more systems become interconnected. One of the biggest risks is that typically not enough effort is expended on prevention until after a disaster has occurred.

• **Security requirements** are typically not being met with sufficient assurance in the computer systems and networks that are commercially available today. Most systems are flawed in one way or another, and some of those flaws are potentially very serious. Furthermore, in general, adequate security cannot be attained unless there is adequate reliability – namely, that a system will do what it is expected to do, when it is expected, with some suitably high probability. The converse is also true: a system is not likely to be reliable unless it is adequately secure – for example, because of maliciously caused deviations from expected behavior. (Reference 4 exhibits examples of each type.) Security and reliability are both required for system survivability and may also be required for assuring system safety – although they are not enough by themselves. It is essential that a complete set of requirements be understood in advance, encompassing (for example) security, reliability, safety, and survivability (as needed) and the interactions among them. If these requirements are not clearly defined, the risks are much greater that systems will not do what they ought to do.

• **Software development** is a labor-intensive effort. Very few large development efforts are developed on time, on budget, and with acceptable functionality. Development of complex systems and complex software requires intelligent, well-trained, experienced individuals, especially when critical requirements are involved. Those individuals typically must have a range of abilities and specialties spanning expertise in technology, systems, hardware, software, management, human factors, and other system aspects. The absence of any particular expertise can and often does reflect adversely in the resulting systems. Each system development has its own characteristics: air-traffic control systems, law-enforcement database systems, medical systems, and nuclear-power plants share some common infrastructure such as operating systems, database management systems, networking, cryptographic techniques and other common security solutions, but each type of system presents special problems of its own. (These problems ar considered further in the section beginning on Page 9.) People who have both system development skills and security expertise are quite rare.

• **Crises can have widespread consequences,** nationally and even globally. However, responding to crises is difficult. The cause of a problem cannot always be quickly determined. Disseminating remedial actions can be complicated – especially if the infrastructure used for remediation has itself been impaired. The year-2000 problem (discussed below) and the ongoing personal-computer virus problem illustrate the point that there are no quick fixes.

Do Past Incidents Suggest Perils That We May Face in the Future?

• **Case histories.** Cases experienced in the past span an enormous range, including losses of human lives (particularly in aviation and medical care – see Reference 3), serious injuries, long-term effects on human well-being, and financial integrity and stability of individuals, organizations, and governments. The attached list of cases (Illustrative Risks to the Public in the Use of Computer Systems and Related Technology) (Reference 3) summarizes many cases that I have collected over the past many years. The security-related cases include many serious security flaws, insider misuse, system breakins and penetrations (including one reported case involving the computer system of Senator John McCain, who at the time was a Congressman), trapdoors that can be used to gain surreptitious access, and pest programs such as Trojan horses, viruses, programmed logic bombs and time bombs that can be used to create arbitrary havoc because they are able to operate with all of the permissions normally attributed to the users and systems they have invaded. There are also financial frauds, election irregularities and possible frauds, many cases of accidental and intentional denials of service, satellite television channel spoofs, electromagnetic and other interference (including effects on pacemakers, with renewed warnings concerning microwaves and digital cell-phones), electronic eavesdropping and jamming, and numerous problems related to violations of privacy and proprietary rights. In addition, there are many complicating factors: information-based fraud is becoming increasingly prevalent (San Francisco police report that well over half of the fraud cases are so attributable); the international software theft problem is intensifying, whereby something on the order of one-half of the market value of all software worldwide is attributable to unauthorized copies, according to the Software Publishers Association; electronic attackers may be located anywhere in the world, and are typically very hard to track; international laws are not sufficiently helpful.

• **Global implications**. Several widespread power blackouts in our now distant memories, the ARPANET collapse of 1980 in which the precursor of the Internet was incapacitated for four hours, and the 11-hour collapse of AT&T's long-distance service of 1990 attributed to a software flaw illustrate one high-risk type of problem in distributed systems – namely, that a fault in a single node can seriously effect every other node in the system. It is significant to note that each of these problems could alternatively have been triggered maliciously by relatively small individual actions. Similarly, in many supposedly secure systems, a single penetration can often be parlayed into widespread adverse consequences.

• **Controls**. We are inevitably embarked on a course toward a worldwide information infrastructure that can potentially permit access to computer systems from anywhere, but that will require controls over who has access to what sensitive information and who has the ability to modify or delete data and programs. Existing controls are not adequate. Recent incidents such as a Russian remotely breaking into Citibank computers and the continual discovery of serious security flaws in popular computer systems demonstrate just a few of the security risks in our infrastructure.

• **Risks of anecdotal evidence.** Anecdotal evidence is by itself generally not convincing enough. However, in computer-communication systems, there is a serious absence of systematic data that is really definitive. Thus, it is very important to examine the enormous existing body of evidence and understand its implications. In addition, it is important to understand that a considerable portion of the evidence is hidden from public scrutiny.

Are Things Happening That We Just Don't Know About?

One of the biggest problems relating to security incidents is that many incidents are never reported officially, including cases of financial fraud and computer security violations. Furthermore, many exploitations are very difficult to detect and trace – such as interception of unencrypted communications via cell-phone, remote phones, and microwave links, and in some cases even financial losses.

Above all, it is important to keep an overall view on security in the emerging information infrastructure. Security will always be a problem, and it is a problem that cannot be addressed effectively in the small and that cannot be retrofitted onto systems that were not originally designed to be secure. As a consequence, there are many risks. See Reference 3 for a broad examination of vulnerabilities and risks and what can be done to minimize them. Another recent view is provided by Teresa Lunt of DARPA (Reference 2).

THE FUTURE

Where Are We Going in the Next 10 Years? Is the concept of an "electronic Pearl Harbor" or a "Global Chernobyl" on the Internet something that the country must take seriously and prepare for? Or are these terms just euphemisms for an ill-defined uneasiness that we feel about the security of our information systems? What threats really exist? What form might a widespread security disaster take? What needs to be done? And over what time period? Are we thinking adequately about the security ramifications in our rush to become Internetted?

• Actually, I do not like to use such popular metaphors, because they tend to trivialize some very difficult problems. However, they do convey the message of the urgent need for a realistic assessment of the risks and what can be done to minimize those risks.

• **We will be massively interconnected.** Major functions of Government will be automated or semiautomated. Security will always be a major problem, because it is difficult to assure – for technological, operational, and managerial reasons. There is a threat of attacks by outside intruders and misuse by insiders, as well as risks that Trojan horses planted long ago may finally become activated and that backup mechanisms have themselves long since been contaminated. Security has typically been considered only as an afterthought. It *must* become a fundamental part of our thinking, beforehand, and not after the crises have occurred. In addition, we must address reliability and survivability issues as well, to prevent repetitions of the types of large-scale outages noted above. We would be very foolish not to be proactive with respect to these risks, with short-term measures to shore up the existing infrastructure and long-term measures to plan for the future.

• Desires for **privacy** and **anonymity** are generally incompatible with the desire for **accountability** – that is, the ability to know the identity of participants and what they are doing (for billing purposes in the case of commercial transactions, for scheduling and resource management, and many other purposes). Attempts to create completely anonymous services such as anonymous cash tend to run counter to practical notions of accountability, authenticity, integrity, revocability, nonforgeability and nonrepudiability, and would seriously impair law enforcement when confronted with massive fraud. There are also privacy risks relating to monitoring and surveillance activities – whether those activities are done clandestinely or with full knowledge of system users. Such risks include the misuse of the information that is thus obtained for other than the intended purposes, and harmful effects that can result from dependence on incorrect, misinterpreted, or maliciously falsified information. As discussed in the National Research Council crypto report (Reference 6), escrowing cryptographic keys presents some enormous potential risks that must be considered very carefully in advance. Ideally, a balance must be struck between privacy and accountability, and that balance must be carefully guarded. Therefore, it is desirable to minimize the information that is monitored and to control strictly who has access to it, and also to ensure the correct identity of all individuals engaged in potentially risky activities – whether arising because of monitoring activities or because of being monitored. Otherwise, slight deviations from the desired balance can result in extensive compromise of privacy or accountability (or possibly both!).

• **Digital commerce.** It would be prudent to tiptoe into the era of digital commerce, beginning with small transactions, until confidence is attained that the infrastructure is ready. Eventually, electronic commerce will be commonplace (irrespective of how secure it is), simply because of marketplace factors. However, there must be suitable controls and oversight on the electronic distribution of financial assets and intellectual property, including software and other content.

• **There are no easy answers,** although everyone always seems preoccupied looking for them. Great care is required to avoid global problems such as in 1980 ARPAnet outage and the 1990 AT&T outage. The oncoming year 2000 is likely to cause surprising reliability problems, resulting from programming languages and operating systems that do calendar arithmetic using two-digit years – for example, with software believing that the year 99 comes *after* the year 00 because 99 is obviously larger than 00! The efforts to fix this problem are decidedly nontrivial, particularly because many computer systems are expected to be affected, some of which were implemented many years ago and are already very difficult to maintain. It is not yet clear whether the year-2000 problem is overhyped, although the estimates of the cost to fix it within Government computers alone are astoundingly high.

• **Simple solutions and draconian solutions are both risky.** Simplistic solutions such as the V-chip, indecency filters, and other efforts to censor our communications media are at best likely to have little or no positive impact, and at the same time present many negative and counter-productive effects. Similarly, the concept of mandatory crypto-key escrow found in the Escrowed Encryption Initiative is full of potential risks; it would require an extensive infrastructure to make it work securely, and that infrastructure would itself be vulnerable to attack. Furthermore, even if the infrastructure could be made feasible (for example, through nonmandatory commercial key escrow), there are still serious problems that must be overcome – such as the almost total lack of business incentives for escrowing communication keys (whereas there is a business incentive for escrowing storage keys). No matter how many safeguards are in place, there are always risks. Similar comments apply to the socalled Clipper III, whereby certain private keys would have to be escrowed, exposing the concept of public-key cryptography to abuse. In general, systems that require complex operational and administrative procedures are often vulnerable to people who ignore those procedures. In another direction, outlawing computer misuse would not be likely to succeed if the infrastructure still permits fraud, privacy violations, and unethical behavior to occur – and worse yet, to remain undetected. Similarly, outlawing certain forms of cryptography is not likely to succeed, partly because cryptography is already available worldwide, and partly because of the ability to hide information undetectably (through steganographic techniques) without using cryptography. Above all, security is an overall system problem, and requires that there be no significant weak links. Thus, attaining adequate security usually requires much greater effort than people are used to investing. Furthermore, in the absence of colossal losses, people find few incentives to invest in defensive measures. The evolution of U.S. crypto policy is also highly relevant to your Subcommittee, and is reviewed extensively in the just-released National Research Council report (Reference 6).

Another simplistic solution would be to cut the United States off from the Global Information Infrastructure, relying instead on a totally isolated National Information Infrastructure. That seems draconian. The most intelligent solution would be to significantly improve the infrastructure! In that way, the potential benefits could be realized and the risks dramatically reduced.

THE ROLES OF GOVERNMENT

What Roles Should Government Play? What Roles Should It Not Play?

• The Government should strive to increase public awareness of the risks, and to work actively toward reducing those risks. The various branches of Government need to work more closely together, both proactively and reactively with respect to crises. Above all, the Government should actively promote steps that improve the security of the infrastructure. I hope that these hearings will help in those directions.

• Government-set standards are not likely to be effective unless they are closely aligned with commercial and consumer interests. The Government must encourage the development of commercially viable systems that can adequately satisfy stringent requirements for security, reliability, survivability, performance, etc. It can do so by encouraging the development of critical system and network components and the establishment of effective criteria for combining those components into complete systems that are strongly secure. It is not enough to merely have a bunch of components; those components must be capable of rapid integration, with high assurance that the overall systems will function securely.

• The Government must take a strong position relating to the protection of personal and corporate privacy. Privacy is something that you often never realized you had until after you have lost it. Defending it requires special care, and a keen awareness of the risks involved. H.R.3011, Security and Freedom Through Encryption (Representative Goodlatte), S.1726, Promotion of Commerce On-Line in the Digital Era (Senator Burns), and S.1587, Encrypted Communications Privacy Act of 1996 (Senator Leahy) all have significant merit.

• The Government must also take a strong position relating to nontrivial individual authentication and system-to-system authentication in computer-related activities. Good system security and good encryption properly implemented are essential for authentication as well as for ensuring privacy. Fixed passwords for user authentication are inherently dangerous, especially when they traverse unencrypted links or reside in system memory, and can be easily captured; some sort of cryptographically or biometrically based authentication is desirable for cases in which penetrations and masquerading represent serious threats.

• The Government must review in great depth the critical role of cryptography in the emerging infrastructure as it relates to need for national well-being in the context of the international evolution of the infrastructure. Good cryptography is absolutely essential for ensuring confidentiality of sensitive information in the private and public sectors, and is also absolutely essential for achieving much greater information integrity and user authentication. It also presents new problems for intelligence-gathering and law-enforcement communities. I sincerely hope that the just completed National Research Council study of U.S. cryptographic policy (Reference 6) will be helpful in your review. (See also Reference 11.)

• The Government must defend itself against anarchy, oligarchy, and other unhealthy forms, and diligently avoid the pitfalls such as those found in Orwell's "1984". There are dangers in underreacting to the security risks discussed here, as well as dangers in overreacting (such as might occur with censorship, outlawing or limiting free speech, outlawing or blocking access to domestic use of good encryption, undermining privacy rights, and microcontrolling media content). There are also corresponding dangers of negative impacts that can result from attempts to overcontrol domestic business in a global marketplace. In general, national security must be understood to include national economic survivability and political stability, as well as military and intelligence strength. The so-called equities should not be pitted against one another as adversaries. Once again, improving the infrastructure would be a major step forward.

• The Government has gotten some useful mileage out of past studies such as those conducted by the National Research Council. (For example, see References 5 and 7.) Even though the concept of "another study" may seem boring, here are a few topics that could benefit from some incisive thinking:

1. What should be the research and development priorities relating to the emerging infrastructure? How can we develop meaningfully secure components out of which much more secure systems can be readily configured? What fundamental gaps must be filled – for example, with respect to authentication and proper use of cryptography.

2. What can be done to foster the effective development of complex systems, especially those that have critical requirements for security?

3. It is time to revisit and broaden the "Computers at Risk" report from 1991 (Reference 5). There has been some significant progress since that report was written (for example, toward the establishment of a comprehensive set of generally accepted security principles, taking certain recommended short-term measures to improve the infrastructure, establishing incident repositories to help promote public awareness, and reevaluating cryptographic export control policies. However, one particular recommendation of that report has still not been adequately addressed – how best to represent end-user interests and needs, particularly in the private sector (which NSA and NIST cannot represent). Unless commercial systems are adequate for critical applications, U.S.Government systems will not be adequate for national needs.

4. Recognizing the overall system perspective required to achieve adequate security in the infrastructure, it might be desirable to establish a representative working group that cuts across a broad range of fields and interests, including computer and communication technologists, lawyers, and people deeply involved in private-sector applications such as medical information systems and critical control systems, to act as a standing advisory group relating to the evolution of the infrastructure and able to focus on issues such as security and system survivability.

5. What can be done to ensure that computer system and software professionals perform in ways that more closely approach engineering disciplines – in which there is substantial enforcement of licensing, accreditation, responsibility, ethical behavior, and legal liability, both individually and corporately, and well established incentives for risk management? I am not comfortable with professional societies policing themselves, and I am also not comfortable with state and Federal governments attempting to legislate or micromanage software quality or professional standards. What works for conventional engineering does not seem to work for software, where a single bit in error can have disastrous results. However, I do believe that a thorough study should be made of how best to achieve a level of professionalism in software development that should be absolutely essential when developing very-high-risk systems – and particularly, systems with stringent security requirements. Achieving a true professionalism among software personnel is a very difficult task, but certainly worthy of study.

All in all, the U.S. Government must be a leader in addressing the difficult problems noted here.

Security is an International Problem

National boundaries are disappearing in the on-line world. The so-called National Information Infrastructure must be viewed as part of a Global Information Infrastructure. The problems are increasingly international, and require international solutions. Transborder data flows run afoul of differing national laws. Cryptography presents its own problems worldwide. Access is now possible economically from anywhere in the world, which is both a wonderful opportunity and a serious risk – because of the much greater need for system security to prevent misuse.

Bob Morris, former Chief Scientist of the National Computer Security Center and NSA employee, addressed the Computer Science and Technology Board of the National Research Council on Sept 19, 1988, relating to computer security risks. He observed that

> To a first approximation, every computer in the world is connected with every other computer.

This is even truer now than it was then, because of the recent surge of Internet activity, with browsers over the worldwide web. The vulnerabilities and risks of our technocratic era are ubiquitous.

FURTHER OBSERVATIONS ON SYSTEM DEVELOPMENT

Although there has been significant progress in recent years, there are still some major problems and major risks relating to the development of large and complex systems – and particularly so in accommodating critical security requirements.

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 in air-traffic control systems, law-enforcement systems, the IRS Tax Systems Modernization effort (see Reference 10), and procurements for military and commercial aviation and defense systems. We desperately need the ability to develop complex systems – within budget, on schedule, and with high assurance compliant with 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 understood somewhat better than in other systems.

The U.S. Government is increasingly dependent on commercial systems. Except for a few special cases, it is no longer feasible to develop custom-designed systems – the costs are prohibitive, the time schedules are awful, and the risks of system failures are considerable. As a consequence, we must encourage system developers to produce systems that are at the same time truly useful for Government needs and for commercial markets as well – and especially when it comes to attaining adequate security. If we ignore security, it seems that the technology has advanced to the point where the required functionality can be configured out of off-the-shelf products. However, when we insist on meaningfully secure systems that are resistant to all sorts of attacks and insider misuse, we discover that it is still very difficult to configure such systems from off-the-shelf products.

The serious difficulties experienced in the past in attempting to develop large systems are amplified when those systems have critical security requirements. Being able to configure secure system environments readily from commercially available components is one of our biggest challenges.

Here are a few of the many factors that have slowed progress in the security of commercially available high-security products – above and beyond the many reasons why complex systems are inherently difficult to develop and operate in the first place.

1. The vulnerabilities in the existing infrastructure are poorly understood. The risks that can result from those vulnerabilities tend to be seriously underestimated. This lack of awareness pervades Government, developers, vendors, users, and even bystanders who would like to believe that their lives are independent of the technology.

2. Another factor that has slowed progress in security is that, despite the very considerable vulnerabilities and risks in today's telecommunications infrastructures, digital commerce, and national security systems, serious disasters have not yet struck critical systems. Major security-related events have not yet occurred that in their effects on public awareness might be considered to correspond in scope to a Chernobyl, Bhopal, or Exxon Valdez. The security-related cases that have occurred have generally not caused massive damage or affected many people adversely. The 1988 Internet Worm, the Citibank penetrations, and a few other similar cases are more like the tip of an iceberg. Fortunately, many serious security flaws have been detected by friendly people who have reported them before those flaws could be exploited.

   People tend not to worry until they have been seriously affected (either individually or as part of a nationwide or worldwide effect), and by then it may be too late. It is generally unwise to wait until after the disaster to plan on what to do. The situation is perhaps akin to earthquake preparedness – you know it is going to happen eventually. In this case, the cost of preparedness should be chosen commensurate with the consequences of the risks that could be avoided.

3. A third factor has been a generally dampening effect on U.S. commercial development. This effect has resulted in part from the U.S. export control laws relating to cryptographic products. That is a very complex subject, and I refer you to the National Research Council report on U.S. crypto policy (Reference 6).

The situation is in some ways improving, and in some ways worsening. Infrastructural components that can improve security are emerging, such as firewalls and cryptographically based authentication. At the same time, the would-be attackers are getting smarter and more sophisticated, many fundamental flaws remain even with firewalls and better authentication, and the advent of new systems continually create new flaws that introduce new risks or new manifestations of old risks.

CONCLUSIONS

In these few pages, I have merely surveyed some of the important issues. Here is a brief summary.

Security is very difficult to attain with any certainty. Computer systems, networks, and human beings are all generally imperfect. As a consequence, today's infrastructure is seriously flawed and seriously at risk. The infrastructure may be good enough for low-risk applications, but it is not good enough for high-risk applications such as protection of sensitive corporate and national data, preservation of privacy, large-scale financial transactions over the Internet, and life-critical systems.

In the long run, **better computer-communication security** is absolutely fundamental to the preservation of a well-ordered society, and for national security and economic competitiveness reasons as well. Digital commerce could be very dangerous unless the infrastructure is greatly improved, with huge potential financial losses possible. **Good cryptography** that is properly embedded within the infrastructure is absolutely essential.

Privacy is also very difficult to attain. Undesired database access is often surprisingly easy to attain, in Government, corporate, commercial, and private databases. Detailed life profiles of arbitrary individuals can be obtained by aggregating information from different databases, with serious risks of impersonation, fraud, and harassment – which are becoming increasing prevalent. (See Reference 3 and 4 for examples, including misuses of Social Security Numbers.) Privacy is often considered to be a less important aspect of security, but it is something on which our lives all rest. It must be respected and cherished.

Research and prototype development are fundamental. The availability of adequately secure systems and networking cannot occur without appropriate high-quality research and prototype development, particularly that related to the configuration of trustworthy systems with both trustworthy and untrustworthy components. Above all, the necessary progress in computer-communication security requires that the U.S. Government must play a truly enlightened role in encouraging relevant research and prototype development in the public sector. Much greater effort must be devoted to having the system development community produce products that are so badly needed, such as better secure operating systems, secure networking, secure wireless communications, and well-constructed applications of cryptography. Beyond that, development of life-critical systems and Government systems with extreme requirements for dependable behavior demands extraordinary efforts.

Much greater awareness is essential – of security flaws and risks in the use of computer-communication systems, on the part of governments, businesses, and private citizens. (This seems to be a rather simple statement, but it is not easy to attain.) As systems become more complex, the more difficulties seem to arise, particularly relating to security.

Education is absolutely essential. Computer literacy is increasingly necessary, even to deal with daily life. Attempts to make computer systems "user-friendly" typically ignore the problems that arise when something goes wrong or assume that there are enough competent people around to keep the infrastructure sound.

The U.S. Government is vitally dependent on commercial technological developments for its computer-communication systems. Custom developments have often been counterproductive in the past. The Government must encourage developers to provide better security as a part of their normal product line. The Government must also encourage greater interconnectivity between government systems and the private sector – albeit with adequate protections for security and privacy.

We have been fortunate thus far, in that attacks on computer security have been relatively limited in their effects. However, the potential for enormous damage is present. We must not be complacent. Proactive prevention of serious consequences requires foresight and a commitment to the challenge ahead. The technology is ready for much better security than we have at present, although there will always be some risks. The Government has a strong role to play in ensuring that the information infrastructure is ready for prime time.

Perhaps the most fundamental question today is this: How much security is enough? The answer in any particular application must rely on a realistic consideration of all of the significant risks. For simple home-grown computing that has only local sensitivity, some security is needed merely to prevent the system from being trashed by intruders. For situations with very high risks, significantly greater computer-communication security is prudent. There are many stages in between those two cases, and no easy answers. There is also a serious risk of ignoring risks that are difficult to deal with – unknown, unanticipated, or seemingly unlikely but with very serious consequences.

As noted in Reference 4, there are three fundamental gaps – all of which must be narrowed if we are trying to significantly improve the security of the infrastructure: (1) a technological gap between what computer systems and networks are actually *capable* of enforcing and what they are *expected* to enforce; (2) a sociotechnical gap between the expected computer system policies and the *social policies* such as laws and codes of ethical practice; and (3) a social gap between the social policies and actual human behavior. Closing all three of these gaps must be an ongoing challenge in our emerging infrastructure.

REFERENCES

1. Susan Landau, S. Kent, C. Brooks, S. Charney, D. Denning, W. Diffie, A. Lauck, D. Miller, P.G. Neumann and D. Sobel, Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy, ACM, June 1994.

2. Teresa Lunt, Securing the Information Infrastructure (Inside Risks, monthly column, edited by Peter Neumann), *Communications of the ACM,* vol 39, no 6, June 1996.

3. Peter G. Neumann, *Illustrative Risks to the Public in the Use of Computer Systems and Related Technology.* [Attached]

4. Peter G. Neumann, *Computer-Related Risks,* Addison-Wesley, 1995.

5. *Computers at Risk: Safe Computing in the Information Age,* National Academy Press, 5 December 1990. [Final report of the National Research Council System Security Study Committee.]

6. *Cryptography's Role In Securing the Information Society,* National Academy Press, prepublication copy, 30 May 1996; bound version in early August 1996. (The executive summary is on the world-wide web at http://www2.nas.edu/cstbweb) [Final report of the National Research Council System Cryptographic Policy Committee.]

7. *The Unpredictable Uncertainty: Information Infrastructure Through 2000,* National Academy Press, 1969. [Final report of the NII 2000 Steering Committee.]

8. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks,* U.S. General Accounting Office, May 1996, GAO/AIMD-96-84. [Briefed to this Subcommittee on 22 May 1996.]

9. *"National Crime Information Center: Legislation Needed to Deter Misuse of Criminal Justice Information,"* statement of Laurie E. Ekstrand, U.S. General Accounting Office, as testimony before the U.S. House of Representatives Subcommittee on Information, Justice, Agriculture, and Transportation, of the Committee on Government Operations, and the Subcommittee on Civil and Constitutional Rights, of the Committee on the Judiciary, 28 July 1993. The appendix to that testimony documents 62 cases of misuses of law-enforcement computer data.

10. For example, see the collection of IRS-related GAO reports, including *Status of Tax Systems Modernization, ...,* GAO/T-GGD/AIMD-96-88, 14 March 1996; *Tax Systems Modernization: Management and Technical Weaknesses Must Be Overcome to Achieve Success,* GAO/T-AIMD-96-75, 26 March 1996; *Progress in Achieving IRS' Business Vision,* GAO/T-GGD-96-123, 9 May 1996.

11. The New Encryption Universe, *The New York Times,* editorial, 10 June 1996.

Personal Background

By way of introduction, I note that I have been involved with the U.S. Government in different technological contexts for many years, including (for example) national security, law enforcement, air-traffic control, and NASA (for example, in the early stages of fly-by-wire research and space-station planning). My first computer-related job was for the Navy in the summer of 1953, 43 years ago.

I have long been concerned with security, reliability, human safety, system survivability, and privacy in computer-communication systems and networks, and with how to develop systems that can dependably do what is expected of them. For example, I have been involved in designing operating systems and networks, secure database-management systems, and monitoring systems that seek to identify abnormal patterns of behavior. I have also been seriously involved in identifying and preventing risks. Some of this experience is distilled into my recent book, *Computer-Related Risks* (Reference 4).

Last week I completed a 2.5-year term on the Internal Revenue Service Commissioner's Advisory Group, where I addressed privacy and security issues as well as the Tax Systems Modernization effort; I also appeared with Senators John Glenn and David Pryor on an IRS training video stressing the importance of taxpayer information privacy and data integrity throughout the IRS operations. From 1987 to 1989, I served on an expert panel for the House Judiciary Committee Subcommittee on Civil and Constitutional Rights, addressing law-enforcement database systems, at the request of Congressman Don Edwards.

In other activities, I was a member of the National Research Council committee (1994-96) study of U.S. cryptographic policy, which released the prepublication version of its final report on 30 May 1996 (Reference 6). I participated in an earlier study of the same subject sponsored by the ACM U.S. Policy Committee (USACM) (Reference 1). I was a coauthor of the 1988-90 National Research Council study report, *Computers at Risk* (Reference 5) that many of you saw when it came out in 1990. I am chairman of the Association for Computing (ACM) Committee on Computers and Public Policy, and Moderator of its widely read Internet *Risks Forum* (`comp.risks`).

I am a Fellow of the American Association for the Advancement of Science, the Institute for Electrical and Electronics Engineers, and the Association for Computing (ACM). My present title is Principal Scientist in the Computer Science Laboratory at SRI International (not-for-profit, formerly Stanford Research Institute), where I have been since 1971 – after ten years at Bell Telephone Laboratories in Murray Hill, New Jersey. I have doctorates from Harvard and the Technische Hochschule, Darmstadt, Germany (the latter obtained while I was on a Fulbright from 1958 to 1960).