Security on the Internet

Statement of
F. Lynn McNulty
Associate Director for Computer Security
National Institute of Standards and Technology
U.S. Department of Commerce

Before the
Subcommittee on Science
Committee on Science, Space, and Technology
U.S. House of Representatives

March 22, 1994

I. INTRODUCTION

Mr. Chairman and Members of the Committee:

Thank you for inviting the National Institute of Standards and Technology (NIST) to speak about security of the Internet and the role NIST plays in its security. We share your belief in the importance of security on the Internet. We also believe that recent events affecting the security of Internet users reinforce the need for attention and action. I want to address the specific concerns and issues you have identified and discuss the role that NIST plays in the security of both the Internet and the evolving national information infrastructure.

A. NIST's Computer Security Mission

First, let me briefly review NIST's role in the computer security area. Under the Brooks Act (P.L. 89-306), NIST is tasked with developing Federal Information Processing Standards (FIPS) for unclassified federal computer systems. Our security activities in this area were re-enforced by Congress in 1987 when it passed the Computer Security Act of 1987 (P.L. 100-235). The Act stipulates that NIST shall "have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems" (excepting classified systems and those used to process "Warner Amendment" information covered by 10 U.S.C. 2315). This role was essentially reiterated in P.L. 102-194, the High-performance Computing Act of 1991.

In essence, then, NIST has the responsibility -- through standards, guidance, and technology transfer -- for helping agencies protect their information technology and applications. It is important to recognize that it remains the responsibility of agencies, service providers, and users of information technology to develop, implement, and manage security programs based on their specific risks and needs.

II. THE RECENT INTERNET SECURITY INCIDENT

Let me now turn briefly to the recent incident that was perhaps the primary impetus for these hearings. The testimony of the representative from the Computer Emergency Response Team (CERT) describes the technical details of the incident. I will try to put the incident in a context and perspective. Later, I will address more general Internet and NII security concerns.

A. The Incident

The recent incident involved the discovery of "password sniffer" programs on hundreds of systems throughout the Internet. This "incident" was really a series of incidents on host systems around the Internet involving the exploitation of a combination of vulnerabilities present in the Internet. First, I should note that over the last few years there have been many security alerts and incidents involving systems on the Internet. This incident was different from "routine" or ongoing incidents primarily in that it developed rapidly into a widespread pattern of similar attacks and that it resulted in threats to many other systems.

B. Major Vulnerabilities Exploited

There were two major types of vulnerability that were exploited in this incident -- neither, by the way, being actual vulnerabilities of the Internet itself, but rather problems in systems connected to the Internet.

Obtaining Privileged Access - The first step in the password sniffer attack requires the attacker to obtain privileged status on a target host system. This can be done by exploiting any of a wide range of known attacks. This normally can happen only when that host system has not been properly configured and administered to prevent unauthorized access. As such, this is not an Internet vulnerability. Rather, it is a general problem that all computer system administrators face and must address.

Access to Passwords - The next steps in the attack involve the installation of the "sniffer" program to monitor the system's network interface port and the collection of log-in information, including passwords. The problem was not the ability of a properly authorized user to monitor the network port; this is needed for effective system administration. The vulnerability here was due to the fact that most computer systems on the Internet (and other networks) employ re-usable passwords to authenticate users. There was no exposure for host systems or user accounts which employed non-reusable passwords or other advanced methods (such as tokens or "smart cards") for user authentication. This, again, is not an Internet vulnerability; Internet protocols do not require host systems to use passwords for user authentication. It should also be noted that encryption of network layer information would not have solved this specific problem, because the monitoring occurs at a point in the compromised systems where messages are unencrypted anyway.

In summary, while there were known vulnerabilities exploited in this incident, they were vulnerabilities in the security mechanisms of host systems, not the Internet itself. Nevertheless, there was a serious and widespread impact of the incident affecting many other systems on the Internet.

C. Impact

The serious impact of the recent incident should be recognized; log-in information (i.e., account numbers and passwords) for potentially thousands of host system user accounts appear to have been compromised. It is clear that this incident had a negative impact on the operational missions of some Government agencies. Moreover, this should be viewed as ongoing incident, not an incident that has happend and been dealt with. Indeed, administrators of systems throughout the Internet were advised, in turn, to direct their users to change their passwords. This is, indeed, very significant, and we may be seeing its effects for some time to come. Not only is it difficult, if not impossible, to identify and notify every user whose log-in information might have been compromised, it is unlikely that everyone, even if notified, will change his or her passwords. Therefore, we will probably continue to see unauthorized access to user accounts resulting from the password "sniffing" activity of this incident. Clearly, we need ways to minimize this kind of problem in the future.

D. Alerting and Response to the Incident

A Success Story - Despite the serious impact of this incident, it should be viewed as a clear and major success for organized incident response activities. The existence and cooperation of several operational security incident response teams was instrumental in identifying this as more than a "routine" incident and ensuring rapid response to it. A formal coalition of response teams, known as FIRST (the Forum of Incident Response and Security Teams) played an important role in the process. All of the teams central to the incident are members of FIRST. The Department of Energy's Computer Incident Advisory Capability (CIAC) at Lawrence Livermore Laboratory first identified the incident. CERT led efforts to analyize and assess the emerging threat and issued initial alert messages to the other security incident response teams that are members of FIRST (including NIST). Individual teams then spread the word among their constituencies. Also of particular note was the DoD Automated System Security Incident Support Team (ASSIST), which has coordinated world-wide response efforts for all of DoD. When it was clear that the incident was particularly wide-spread, notices were posted on several Internet "bulletin boards" and other forums. A press release was also issued. (It is important to note, however, that, because of the specific and inherently technical nature of most such incidents, press releases are not normally part of the alert process.)

E. Lessons Learned

This incident was the result of known vulnerabilities and already-hypothesized attack scenarios. Rather than teach us new lessons, it really re-emphasizes some lessons we've already learned and simply increases a sense of urgency for advanced authentication methods and other actions. Additional lessons learned were:

Effective incident response teams and alerting mechanisms can (and, in this case, did) play an important role in minimizing the impact of such incidents.

Traditional user authentication by means of re-usable passwords does not provide strong security in today's networked environment -- with or without encryption.

Exploitation techniques (and software which automates such techniques) are rapidly shared across the network and can be easily used by otherwise unskilled miscreants. In other words, you don't have to be smart (or ambitious) enough to build these "weapons" to be able to obtain them and use them against others.

Any host system, if improperly configured or managed, can become an "unwitting" platform for an attack against other systems in a network. Therefore, we need to mimimize the need for reliance on the integrity of individual hosts for the security of other hosts and users on the Internet.

System administrators (which, because of the growing number of workstations on the net, include an increasing number of relatively unskilled users) need better awareness, skills, and competence in protecting their systems;

The importance of security to users of the Internet (and by extension the evolving national information infrastructure) can no longer be seen as secondary. If this valuable national resource is to achieve its full potential, its users must have confidence in the security of their data and activities on the network.

III. IMPROVING SECURITY ON THE INTERNET

Clearly, much can be done to improve security in the Internet. The initial, research-oriented Internet and its protocols were designed for a more "benign" environment than now exists. It could, perhaps, be described as a collegial environment in which the users and host computer systems are mutually trusting and interested in unrestrained sharing of information. The new environment in which the Internet (and the NII) must operate is much less collegial and trustworthy. It contains all the situations, people, and risks that we find in the society as a whole. Thus, we have begun to reexamine and adjust our "design requirments" to reflect those new realities. Security is now a primary concern. The collegial Internet of the past cannot be the basis for the NII of the future.

A. A Short History of Internet Security Incidents

Despite the previous comment, security in the Internet is not something that has never occurred to its users and operators. It is important to understand what has taken place and what is currently underway.

In recent years, a number of security problems with networks in general and the Internet in particular have received public attention. The media have carried stories of high-profile malicious hacker attacks via the Internet against government, business, and academic sites. It often seems that hackers roam the Internet with virtual impunity, masking their tracks while moving from system to system.

The Recent Incident Wasn't the First - Perhaps the first and still most significant major incident involving the Internet was the so-called Internet Worm, caused by Robert Morris, Jr. in November of 1988. This incident, in effect, woke up the Internet community to at least three facts:

Everyone out there isn't a "good guy";

Internet protocols and applications had many inherent or implementation vulnerabilities that create exposures to misuse or intrusion; and

The network community needed better methods of cooperation to identify and react to network incidents and emergencies.

The first two of the above factors won't change; the last remains true, but has been and continues to be addressed.

And It Won't Be The Last - In the years subsequent to the Internet Worm, there have been some significant trends:

Use of the Internet has grown exponentially -- and continues unabated. With this has come a corresponding increase in the number of people with a detailed technical understanding of Internet systems -- and the potential vulnerabilities of those systems.

"Security" incidents, such as attempted system access, actual system intrusions, and other exploitations of various weaknesses of systems on the Internet, also have grown dramatically. It is likely that almost every host system on the Internet already has had at least some sort of security-related incident.

The number of unskilled users who must (or should) be assuming network system administrator functions will continue to increase -- simply because the number of systems connected to the Internet is increasing.

There are now growing organized efforts of Internet user organizations to identify and deal with intrusions and unauthorized system use.

B. Internet Vulnerabilities vs. Host System Vulnerabilities

It is important to recognize that the vast majority of security problems seen "on the Internet" are not really Internet problems at all. We need to understand a subtle but important distinction between the Internet and its host systems.

The Internet is, in essence, a collection of computers, usually called host systems, which are connected to underlying data communications networks. These host systems (which may support one or more human users) communicate with each other by means of internet protocols. The internet protocols may be thought of as the standard message formats by which the host systems establish connections to each other and exchange information -- much like the use of standard forms and procedures in an office environment.

Security vulnerabilities can exist in the underlying communications network and its nodes, in the internet protocols, in network administration, or in host systems. To use the highway analogy, a communications problem might be like a pothole, a bridge failure, or a closed road. A protocol problem might be like a mis-marked exit sign or a failure of slower traffic to stay in the slow lane. A network administration problem might be the lack of emergency vehicle access or notification and response procedures for accidents. Last, a host system problem might be likened to a store proprietor along the highway leaving the doors open and the store unoccupied. The problem is not the proximity of the highway, but the carelessness of the store proprietor (and the fact that not everyone on the highway is honest). Most "Internet" security problems to date have been careless -- or unknowlegeable -- proprietors.

C. The Role of the Internet in the NII

The national information infrastructure is not some system that will be "switched on" at some specified date in the future. The NII, at least in its initial form, is here now, and like many other national infrastructures, is made up of many -- often disjoint -- elements. The issues that we in government and industry must address are the directions in which we want the NII to evolve and how to make that happen. In the administration's guiding document on the development of the NII, The National Information Infrastructure: Agenda for Action, one of the nine guiding objectives is to "Ensure Information Security and Network Reliability".

One of the important elements in the current NII is the Internet. The Internet may not, however, be the ultimate model or technology for the NII. Nevertheless, it serves important roles in the evolution of the NII. First, it is a working example of effective global computer networking. Second, it is a possible model for future network technology. Last -- and perhaps most importantly -- the Internet serves as a sort of living laboratory in which we can develop and experiment with technologies, applications, and concepts of information sharing that will be useful or necessary in the next century. Again, security mechanisms are central to the process.

D. The National Performance Review

The importance of information technology security in general and Internet security in particular was recognized in the Vice President's National Performance Review. In the area of information technology security, the following primary objectives were identified:

- Development of cryptographic standards
- Development of a set of generally-accepted system security practices
- Establishment of a national crisis response clearinghouse
- Improved security awareness
- Security of the public switched telecommunications network
- Internet security
- Coordinated security research and development

In addition, the NPR report cited specific objectives in the related area of Privacy:

- Establishment of a Privacy Protection Board
- Development of a set of Fair Information Handling Practices

NIST has the lead responsibility in some of these items and a role in all of them. Although each has some relevance to Internet security, two items are of particular relevance.

Internet Security - This specifically focuses on the Internet. It involves the development of an overall Internet security plan. The Federal Networking Council has the lead in this activity, with the participation of several other organizations, including NIST.

National Crisis Response Clearinghouse - This will be, in essence, the expansion and application of the FIRST concept to the entire Federal Government. NIST has the lead responsibility for this item.

E. A Self-Fulfilling Prophecy

One of the clear directions of the administration is for agencies to "get connected". Initially, that means electronic mail, and to most agencies, that means "on the Internet". This presents us with an interesting situation. For years, the reason that many agencies used as a reason not to connect to the Internet was concern over security -- "We don't want to open ourselves up to hackers." Now, agencies are likely to rush headlong "onto the Internet" without careful planning, personnel skills, and knowledge of the security considerations. The likely result, if we are not careful, is that we will see significant occurrences of those security problems that the agencies were always worried about -- a self-fulfilling prophecy.

This is not to suggest that we should not be moving forward agressively on connecting to the Internet; the benefits of this initiative are clear and compelling. However, it does require that we undertake this effort with care and intelligence.

NIST's Computer Systems Security and Privacy Advisory Board (CSSPAB) will be examining this very issue at their quarterly meeting on March 23rd and 24th. They will be examining the several agencies' plans for putting agency mission critical systems on the Internet.

F. Security Incident Response Efforts

The Need - Regardless of the security technology and other measures we put in place on the Internet -- or any other network -- we will always have security incidents. We will discover exploitable vulnerabilities. We will suffer intrusions, attacks, thefts, fraud, network failures, errors and omissions, and uncountable other possible risks. Since we will never be able to anticipate, much less prevent all of these problems, we must have in place effective mechanisms for dealing with them when they do occur. This is the role of security incident response efforts. The recent Internet incident reinforces the need for such activities and demonstrates their value and effectiveness.

FIRST - Beginning with the aftermath of the 1988 Internet worm incident, it was recognized that better methods for incident response and information sharing were needed. It was also clear that the establishment of a single team or "hot line" would not work; it would simply be overwhelmed. Out of this was born the concept of a coalition of response teams -- each serving its own constituency, but working with the others to share information, provide alerts, and provide mutual support in the response to incidents and potential incidents. That concept was embodied in FIRST, the Forum of Incident Response and Security Teams. FIRST has grown from an initial group of eleven, mostly Government, teams to over thirty teams now. These teams include Government, industry, computer manufacturers, and academia -- both U.S. and international.

Sharing Sensitive Security Incident Information - In discussing these well-publicized problems, I think it is important to stress that we at NIST believe that it is not a good idea to just publicly announce system security weaknesses, in the hope that such publicity will result in immediate solutions. Some, indeed most, security weaknesses cannot be fixed overnight -- for example, it takes time to correct errors in operating systems, test the new code, distribute the updated code, and install the code. Inappropriate publicity about some kinds of weaknesses will merely serve as a call for their exploitation by malicious hackers.

The FIRST concept addresses this problem by establishing a means for developing a level of trust and cooperation among teams that permits sharing of information. The FIRST "membership" process involves endorsement from an existing member, thus providing an initial level of confidence. Further interactions among teams have build a level of trust and cooperation that probably could never have existed otherwise.

We believe we have demonstrated the success of this concept over the last few years of FIRST's existence. Groups who would have never discussed security problems outside their own confines have been able to work together with the confidence that they can gain from the knowledge and experience of other groups without exposing their organizations to attack in the process.

NIST's Role in FIRST - NIST has played a leadership role in FIRST from the beginning. NIST led efforts to bring together existing teams, develop an operational framework, and get the activity underway. NIST continues to serve as the secretariat of FIRST. In that role, we provide coordination and technical support. For example, we established and administer the electronic mail alerting network used by FIRST members. We are currently developing plans for a much more aggressive expansion of FIRST membership throughout the Government. To date, the most active FIRST members in the Government have been teams from the "traditional" Internet communities -- the DoD and research agencies. We are anxious to see more active participation on the part of the rest of the civilian agencies of Government as they increasingly become "network players".

Individual Response Teams - The role of the individual response team cannot be ignored. These teams are the essence of FIRST. They must establish procedures for managing incidents within their defined constituencies, and they must be able to communicate with the other FIRST teams. The major hurdle we have seen for agencies to become active in incident reponse activities (aside from the lack of Internet connectivity in many cases) is the need to develop an incident response "mindset" to complement the traditional policy and procedures approach of many computer security programs. To help address this problem, we published in 1991 a guidance document, NIST Special Publication 800-3, Establishing a Computer Security Incident Response Capability.

In summary, we believe that organized, coordinated, and effective security incident response efforts throughout government (and beyond) are critical to the security of the Internet (and the NII) now and in the future.

G. Security Technology

Security technology is important for the effective enforcement of security policies in any computer system. Such technology is especially important in a highly distributed, networked environment -- such as the Internet -- in which physical and administrative controls are limited.

Security Services - Five major security services are identified in International Standard 7498-2. This standard was developed to specify the security aspects of the Open System Interconnect (OSI) model of computer networks. The security services (and a short explanation of each) include:

Authentication - Verification of the claimed identity of a computer or computer network user;

Access Control - Verification and enforcement of the authorized uses of a computer network by a user subsequent to authentication;

Data Integrity - Verification that the contents of a data item (e.g., message, file, program) have not been accidentally or intentionally changed in an unauthorized manner;

Data Confidentiality - Protection of the information content of data from unauthorized disclosure;

Non-repudiation - Protection against denial of sending (or receiving) a data item by the sender (or receiver).

These major security services should be augmented by a number of auxiliary services (audit, availability assurance) and support services (key management, security maintenance, network management). An integrated security system must offer all these services with a number of security mechanisms implemented in a number of security products. Technology will advance and provide for newer, cheaper, better products but the overall security system need not be changed drastically if it is designed properly. NIST is working with several organizations seeking an overall security architecture for unclassified information. An integrated security system can then be designed with interchangeable and interoperable parts as needed.

Advanced Authentication - Since reusable passwords are the weakest security link in the present Internet, better, more advanced, authentication techniques are needed. A spectrum of solutions exist ranging from "one-time" passwords to high tech, biometric identification systems. Token based authentication and access control systems appear to be a reasonable compromise among the goals of low cost, high security and system simplicity. NIST has developed several token based security systems and continues to evaluate several new alternatives. Most are based on something a user carries with them, like a "smart card" or "smart token" or "smart disk." Software modules unique to an individual will also suffice if good software protection is provided to the information in the module.

Public Key Infrastructure - A public key infrastructure (PKI) is a part of an integrated security system that is needed to support certain user authentication, data integrity and data confidentiality services. A PKI is a distributed system consisting of people and computers that will verify the correct identity of a person seeking authorization to use a computer system or network and then associate a public key with that user in a highly secure manner. The certificate issuer in the PKI produces an electronic certificate which contains the identity of a user, the user's public key, some auxiliary information for the security system and the digital signature of the CERTIFICATE ISSUER. The PKI should be established so that a secure "chain of certificates" is established between any pair of users anywhere, perhaps, in the world. This allows someone to sign a secure message, funds transfer or electronic contract and then allows anyone else to verify the source and authenticity of the message, etc. NIST, along with several other organizations, are seeking to design, implement and coordinate the requisite security services of the PKI.

Obstacles to Deployment and Use of Security Technology in the Internet - There are several current impediments to widespread adoption and use of advanced computer security technologies within the Internet. However, these should be viewed as obstacles, not barriers.

Historic Community Culture - The Internet community has historically emphasized openess in communications. Computer security has been viewed as interfering with this goal.

Internet Management Organization - The Internet is a loosely coupled coalition of organizations and activities without a central management structure. Minimal rules must be followed in order to connect to the Internet backbone communication system, and certain protocols must be followed in order to communicate with others on the network. There are few policies or practices which specify acceptable use or adequate security (even though policies for both of these have been developed). The National Performance Review (NPR) has identified a need for such policies.

Availability of Security Systems - While there are many individual security products (seeking a small number of narrow niche markets), there is still a lack of integrated security systems. An example of such an integrated security system would be a commercially supported electronic mail security mechanism (integrating a comprehensive key management support system, user authentication and authorization support services, and user message security services).

Interoperability - The commercial security products that solve similar security problems usually are not interoperable. A given product may have a large number of features and interfaces, but will not interoperate with those of other products. Thus, communities of interest may adopt and use one product, but those users must obtain a second product in order to communicate with someone in another community of interest. Lack of interoperable products often delay a user from selecting and using any security until either a de facto or de jure standard emerges.

Costs - Since there is yet no universal market for security products fitting into a seamless security system, the costs of individual security products built to fill niche markets are currently high. However, costs will go down as volume and competition increase.

IV. ORGANIZATIONS, ROLES, AND RESPONSIBILITIES

There are several organizations in the Government and in the private sector that have roles in the security of the Internet. It would be difficult to identify them all here. Therefore, I will describe briefly NIST's activities and our involvement in other Internet-related organizations or activities.

NIST computer security activities have both direct and indirect relevance to security on the Internet. In general, our programs address information technology security in all environments. Howerver, since the Internet is such an important element in our work and of an increasing number of Government agencies, we have a number of activities directed specifically at the Internet.

A. NIST's Computer Security Activities

Overall Program - In carrying out its mission, NIST seeks to develop cost-effective security standards and guidelines for federal systems. These are often voluntarily adopted by those outside the federal community. We are working in many areas to develop both the technology and standards and technology that will be needed in the long term, and addressing short term requirements for better training and awareness. We have issued guidelines or standards on many facets of computer security, including: computer security awareness training, cryptographic standards, password generation, smart card technology, security of electronic commerce, viruses and other malicious code, risk management, and PBX security. We have also issued bulletins on many computer security issues, which may be of interest to federal agencies and private sector organizations, including a July 1993 bulletin on security considerations in connecting to the Internet. NIST works directly with federal computer security program managers through our Federal Computer Security Program Managers' Forum. We also participate on many voluntary standards activities, and participate in various interagency forums.

While NIST has published guidance in a wide variety of areas, including Internet-specific topics, NIST's computer security program is not focused primarily on the Internet -- or any other specific network or technology. Operational responsibility for the Internet, and thus specific, operational responsibility for security, rests outside NIST. Nevertheless, the Internet is central to much of the information technology activities and plans of Government agencies, and NIST has a responsibility to address those needs.

General Activities Affecting the Internet - Some of the general research, standards, and guidance activities of NIST that affect the Internet include the following:

Smartcard technology development and application
Advanced authentication technology development and application
Trusted systems criteria and evaluation
Cryptographic methods, interfaces, and applications

Specific Activities Affecting the Internet - In addition, NIST has undertaken a number of activities that focuse directly on Internet security issues. These include the following:

CSL Bulletins - guidance on connecting to the Internet
Special Publications - guidance on Incident Response Capability

FIRST leadership and support

Firewalls Research - One of the most actively examined methods of protecting systems or subnetworks connected to the Internet is the use of "firewalls" -- specially-programmed machines to control the interface between a subnetwork and the Internet. NIST has established, with the assistance of the National Communications System and others, a new Firewalls Research Laboratory effort to extend and share knowledge in this important area.

In addition to these programmatic activities, NIST is involved in a number of groups and activities that are directly involved in Internet security.

B. Information Infrastructure Task Force

Security is being addressed on several fronts in the Information Infrastructure Task Force (IITF). There are specific security efforts in each of the three main committees of the IITF, plus the Privacy Working Group of the Information Policy Committee. NIST is involved all of these efforts.

C. OMB Circular A-130

NIST is working with the Office of Management and Budget (OMB) in the revision of Appendix III of OMB Circular A-130. This appendix specifically addresses agency information technology security programs. Although this does not address the Internet specifically, we expect the new appendix to include the requirement for agency incident response capabilities.

D. Federal Networking Council

The Federal Networking Council (FNC) is an interagency group which coordinates the computer networking activities of federal agencies that serve general and specific research communities. The FNC established a security working group to address various security needs and seek common security services and mechanisms meeting these needs. The security working group, under the leadership of NIST, has initiated the following activities:

Security Policy for Use of the National Research and Education Network - a high level security policy which specifies the principles and goals of security in the NREN and then assigns responsibilities to six categories of participants in the NREN (completed and approved by the FNC).

Security Architecture for the NREN - a comprehensive but generic categorization of the components of security needed to satisfy the security requirements of the NREN. This activity has been initiated but not completed.

Security Action Plan for the NREN - a first draft of an action plan for developing and fielding security prototype components (e.g., smartcards, access control tokens) has been developed; participants in the user acceptance testing are being solicited.

E. Internet Society Security Activities

The sponsors and supporters of the Internet have conducted several security activities over the past several years. The CERT and FIRST activities, previously described, were major activities to alert users of potential and on-going security problems and to provide information on what to do about them. The following are other activities and the roles that NIST has played in each of them.

Internet Security Policy - The Internet Engineering Task Force (IETF) sponsored the development of a policy for secure operation of the Internet. This policy specified six basic guidelines for security:

assure individual accountability;
employ available security mechanisms;
maintain security of host computers;
provide computers that embody security controls;
cooperate in providing security; and
seek technical improvements.

These guidelines were expanded and clarified in the Security Policy for Use of the National Research and Education Network. NIST participated in the development of the Internet security policy and was a major player in development of the NREN security policy.

Privacy Enhanced Mail - The IETF sponsored the development of the Privacy Enhanced Mail (PEM) system. PEM provides the ability to protect the integrity and confidentiality (i.e., privacy) of electronic messages on a user-selected basis. PEM utilizes the popular Simple Mail Transfer Protocol as the foundation for private (sometimes also called, trusted or secure) mail. PEM uses the Federal Data Encryption Standard for confidentiality protection. Digital signatures are used to assure the integrity of a message and to verify the source (originator) of the message. NIST was a participant in the group that developed the specifications for PEM. It is available both as a free, unsupported software package and a licensed supported software system.

V. SUMMARY AND RECOMMENDATIONS

In summary, then, I think that recent Internet security experiences have taught us -- or have reinforced -- some important lessons, and there are some obvious actions that should follow.

A. Lessons and Conclusions

The Internet Is a Lightning Rod - The public already knows about the Internet and understands that the Internet will be a part of the national information infrastructure. Thus, any security problems affecting the Internet reflect on the entire NII effort and could undermine the public's confidence in and willingness to use that developing infrastructure.

Internet Security is Not a "Second Tier" Issue - The attention that security incidents receive in the media and the impact that recent incidents have had on the operations of some agencies and other Internet users make it clear that security is now a first level concern that must be addressed.

Organized Incident Response Efforts Work - Despite the widespread impact of recent incident, it is clear that organized, cooperative incident response efforts -- which we in the Federal Government had in-place -- were instrumental in identifying and mitigating its effect. This incident reinforces the importance and need for such efforts.

Traditional, Re-Usable Passwords are Inadequate in a Network Environment - The nature of data communications networks makes unacceptable the continued reliance on traditional, re-usable passwords for user authentication.

Secure Systems Operations Require Skilled Personnel - The highly powerful and sophisticated workstations that are increasingly being connected to the Internet are often operated by technically unskilled users. Further, most systems come "out of the box" configured for the easiest-to-install-and-use options -- usually also the most insecure configuration. To be installed, connected, and operated securely, these systems currently require the users to be full-fledged system adminstrators, not just "ordinary users". This is an unreasonable and unrealistic expectation.

B. Recommendations for Action

Implement the NII/NPR Action Items - The recommendations of the National Performance Review in the area of information technology security address specifically some of the needs for the Internet. NIST and the other action agencies will be working to implement those recommendations.

Deploy Advanced Authentication Technology - We must move forward agressively to deploy already-available technology to replace the traditional re-usable password as the method of choice for user authentication. Technologies developed at NIST and those becoming available in the marketplace can make marked improvements in the near term. In the longer term, we must begin establishment of sectoral and national certificate infrastructures to enable more generally available and interoperable methods of authentication.

Promote and Expand Incident Response Activities - The concept works. We must now move actively to ensure that agencies throughout Government and constituencies nation-wide establish active and cooperating incident response capabilities. NIST plans to continue to lead such efforts within the Government and promote them world-wide through FIRST and similar activities.

Educate and Train System Administrators - In the long run, we cannot demand that users of increasingly sophisticated technology be technical experts, i.e., system administrators. We must find ways to deliver secure systems "out of the box". In the short term, however, we must better train system users. If agencies are going to connect their networks (and thereby their agencies) to the Internet and other external networks, their technical personnel must understand the risks involved and be trained and equipped to manage such connections securely. NIST and others have published technical guidance to assist in this process and will be developing additional guidance in the future. Agencies must take it upon themselves, however, to ensure adequate technical training of their personnel.

Use Available Security Technology - Computer users, system administrators, and service providers should evaluate and, where cost-effective, employ current security products and technologies to reduce risks to acceptable levels.

C. Conclusion

There are always trade-offs involved in the use of new or complex technology -- especially in something as potentially universal as the Internet and the evolving national information infrastructure. The challenge, of course, is to find the right balance of risks and costs against the benefits. However, I must emphasize that even with a complete restructuring and replacement of the current Internet we would continue to have security incidents and other problems. Historically, with the introduction of any new technology, the miscreants and charlatans are not far behind. Our task is to work as hard as we can to anticipate and avoid such problems and, we hope, get and stay a step or two ahead of the game. I would also like to assure you that NIST -- in concert with the several other key players in the Internet -- is both aware of the importance of Internet security in the context of the evolving national information infrastructure and actively undertaking efforts to meet that need.

Mr. Chairman, I want to thank you again for the opportunity to speak to your committee. We at NIST -- and the other communities of interest involved in the Internet and the NII -- look forward to working with your committee and others in the Congress on this.