Epilogue for RFC 1281, Guidelines for the Secure Operation of the Internet

Barbara Fraser
Cisco Systems, Inc.
byfraser@cisco.com

Steve Crocker
Shinkuro, Inc.
steve@shinkuro.com

We are responding to the selection of RFC 1281 as a paper of historic importance with a mixture of surprise and rue, with perhaps a small amount of pleasure thrown in. Surprise is surely dominant. Was it really seventeen years ago? Time surely passes more quickly than we realized. And definitely rue – perhaps even embarrassment. How hopeful and naive we were. How much simpler the world seemed then. And the pleasure, both at the recognition from colleagues and the opportunity of working together as our paths diverged since then.

1991 was a long time ago in Internet time. The CERT® Coordination Center was formed in 1988 in response to the Morris Worm. It was during this period of time that the Internet community began to recognize and respond to security issues and events. In 1988 there were approximately 66,000 computers on the Internet; in 1991 that number had was approaching a million, and we were seeing significant Internet growth across government institutions and agencies, academic and research institutions, commercial network and electronic mail carriers, non-profit research centers and an array of industrial organizations.

Personal computers were not yet widely used. The World Wide Web had not yet been launched; there was no WiFi, no DSL, or Cable Internet. The first Internet Café had yet to be opened, there was no e-commerce, and firewalls were in their infancy, based on simple packet filtering. Indeed it was deemed fairly easy and straightforward to track down who was sending packets on the Internet.

The IETF had emerged into roughly its current form around 1988. The Security Area was initiated in 1989. One of us (Crocker) was invited to be the Area Director and served until 1994. Most of the rest of the IETF is organized roughly along the layer structure of the protocols. We set up the Security Area to cut across all the other areas, not solely to own its own set of protocols. As part of this strategy, the Security Area Advisory Group (SAAG) was created to provide expertise to assist working groups in other areas. Fraser, then working at the CERT, was particularly active in the SAAG, contributing to the weighty RFC 1244, Site Security Handbook, in 1991 and then revising it as RFC 2196 with the same title in 1997. Rich Pethia, then manager of the CERT, provided constant guidance, data and support.

During this period of time, the Internet still retained much of its voluntary nature. The Internet ecosystem depended on the cooperation of Internet service providers, private network operators, users and vendors in order to keep the system functioning.

In this environment, we boldly attempted to offer guidelines to this growing, diverse, largely cooperating ecosystem. They were a common set of voluntary rules for the successful and increasingly secure operation of the Internet.

1063-9527/08 $25.00 © 2008 IEEE
DOI 10.1109/ACSAC.2008.57

Here's the advice we offered to users, service providers and vendors.

1. Users are individually responsible for understanding and respecting the security policies of the systems (computers and networks) they are using. Users are individually accountable for their own behavior.

2. Users have a responsibility to employ available security mechanisms and procedures for protecting their own data. They also have a responsibility for assisting in the protection of the systems they use.

3. Computer and network service providers are responsible for maintaining the security of the systems they operate. They are further responsible for notifying users of their security policies and any changes to these policies.

4. Vendors and system developers are responsible for providing systems which are sound and which embody adequate security controls.

5. Users, service providers, and hardware and software vendors are responsible for cooperating to provide security.

6. Technical improvements in Internet security protocols should be sought on a continuing basis. At the same time, personnel developing new protocols, hardware or software for the Internet are expected to include security considerations as part of the design and development process.

It is challenging to attempt to comment usefully on how much worse the security problems have become in the intervening seventeen years.

Since 1991 there have been three National Academy of Sciences reports on cyber security: Computers at Risk: Safe Computing in the Information Age (1991), Trust in Cyberspace (1999), and Toward a Safer and More Secure Cyberspace (2007). The U.S. Government has been actively engaged with president directives (PDD-63, Critical Infrastructure Protection), creation of clones of the CERT, multiple cyber security research programs at DARPA, NSF, the Department of Homeland Security, and elsewhere around the world. Similar efforts continue, with the Center for International and Strategic Studies (CSIS) about to deliver its own report on cyber security in the form of advice to the 44th president.

Each of these reports has stated that the cyber security threat is real and growing. Each has emphasized the challenges created by the increasingly complex and interconnected nature of the Internet. The Internet is losing the voluntary cooperative environment that was the hallmark of its early days. For example a number of service providers refuse (or lack the knowledge) to handle routing issues that affect others but don't affect their own networks. There is little incentive to protect the commons.

Addressing security issues is hampered in a number of dimensions. "Security" means different things to different people. To some it's equated simply with spam, or hate speech, or protecting the intellectual property of copyright holders. To others the definition is very expansive and includes traditional attacks (e.g., DDOS), spam, hate speech, IP protection, child pornography, and others. Such a broad definition makes the problem too big and arguably intractable.

Another dimension to the security problem is the decreasing level of expertise together with increasing complexity of the task. Our first two pieces of advice were addressed to users, with the assumption that users should understand the systems they were using and also understand what they needed to protect. This probably wasn't feasible in 1991 and definitely isn't feasible now. Moore's law continues to provide ever more complex and powerful systems, but users remain limited in their capacity to handle complexity.

Our third piece of advice was addressed to service providers and computer system operators. As we said, PCs were not yet dominant, and most network users used shared machines. These machines were usually tended to by a system administrator who could assist, and, if necessary, discipline users. System administrators will exist in the corporate environments, but huge numbers of users are without the assistance or oversight of anyone competent to understand their usage.

Our fourth piece of advice was addressed to vendors, asking them to improve the security of their products. The results on this score are very mixed. Many products are indeed much better than they were many years ago. At the same time, we have observed repeatedly that usability trumps security, and whenever there is direct contention between the two, usability usually wins. The exceptions are in highly controlled environments, e.g. large corporations and sensitive government installations, and even in those environments the results are often mixed.

Our fifth piece of advice was addressed to users, service providers and vendors together, asking that they all cooperate to deal with whatever flaws were discovered. As the statistics from many companies and many CERTs show, though the level of cooperation has increased, the number of incidents continues to climb. The problems seem insurmountable.

Our last piece of advice was addressed to our own environment, the IETF and the rest of the technical community. We politely suggested security issues should be worked out at design time. The good news is that security protocols continue to be defined, but their deployment remains problematic. The most commonly used security protocol is SSL, but only in an asymmetric mode. The bare essentials of validation of end points at the address and domain name level, and validation of source addresses on incoming packets remain unimplemented except in the smallest proportion. The massive publicity surrounding the DNS flaws Dan Kaminsky discovered and publicized have finally generated some traction for the decade and half of work on adding signatures to the DNS system, i.e. DNSSEC, and yet it's still an uphill battle. (The U.S. Department of Commerce finally acceded to years of pressure to get the root signed and issued a Notice of Inquiry that starts with, "In terms of addressing cache poisoning and similar attacks on the DNS, are there alternatives to DNSSEC that should be considered prior to or in conjunction with consideration of signing the root?")

So where does this leave us in 2008? Providing a complete, comprehensive answer is beyond the scope of this paper and the capacity of the authors, but we can offer a few specifics that almost surely have to be included in any comprehensive plan going forward.

1. Traffic coming into the Internet must be identifiable according to its source.

2. Reliable identification and authentication of end points is essential.

3. Devices that are easily taken over by predators are inherently dangerous and need to be identified and given separate treatment.

4. Internet security is a global issue, not solely a national problem. The legal and law enforcement framework has to evolve to deal with threats and misbehavior from all quarters.

5. Solutions based on partitioning the Internet, and identification of selected "critical" resources are insufficient. Rather, solutions are needed that are applicable across the entire Internet and promote adoption through a virtuous cycle.

We look forward to reviewing this modest set of suggestions in another seventeen years and attempting to explain why we missed the mark so badly again.

Network Working Group
Request for Comments: 1281

R. Pethia
Software Engineering Institute
S. Crocker
Trusted Information Systems, Inc.
B. Fraser
Software Engineering Institute
November 1991

Guidelines for the Secure Operation of the Internet

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard. Distribution of this memo is unlimited.

Preamble

The purpose of this document is to provide a set of guidelines to aid in the secure operation of the Internet. During its history, the Internet has grown significantly and is now quite diverse. Its participants include government institutions and agencies, academic and research institutions, commercial network and electronic mailcarriers, non-profit research centers and an increasing array of industrial organizations who are primarily users of the technology. Despite this dramatic growth, the system is still operated on a purely collaborative basis. Each participating network takes responsibility for its own operation. Service providers, private network operators, users and vendors all cooperate to keep the system functioning.

It is important to recognize that the voluntary nature of the Internet system is both its strength and, perhaps, its most fragile aspect. Rules of operation, like the rules of etiquette, are voluntary and, largely, unenforceable, except where they happen to coincide with national laws, violation of which can lead to prosecution. A common set of rules for the successful and increasingly secure operation of the Internet can, at best, be voluntary, since the laws of various countries are not uniform regarding data networking. Indeed, the guidelines outlined below also can be only voluntary. However, since joining the Internet is optional, it is also fair to argue that any Internet rules of behavior are part of the bargain for joining and that failure to observe them, apart from any legal infrastructure available, are grounds for sanctions.

Introduction

These guidelines address the entire Internet community, consisting of users, hosts, local, regional, domestic and international backbone networks, and vendors who supply operating systems, routers, network management tools, workstations and other network components.

Security is understood to include protection of the privacy of information, protection of information against unauthorized modification, protection of systems against denial of service, and protection of systems against unauthorized access.

These guidelines encompass six main points. These points are repeated and elaborated in the next section. In addition, a bibliography of computer and network related references has been provided at the end of this document for use by the reader.

Security Guidelines

(1) Users are individually responsible for understanding and respecting the security policies of the systems (computers and networks) they are using. Users are individually accountable for their own behavior.

(2) Users have a responsibility to employ available security mechanisms and procedures for protecting their own data. They also have a responsibility for assisting in the protection of the systems they use.

(3) Computer and network service providers are responsible for maintaining the security of the systems they operate. They are further responsible for notifying users of their security policies and any changes to these policies.

(4) Vendors and system developers are responsible for providing systems which are sound and which embody adequate security controls.

(5) Users, service providers, and hardware and software vendors are responsible for cooperating to provide security.

(6) Technical improvements in Internet security protocols should be sought on a continuing basis. At the same time, personnel developing new protocols, hardware or software for the Internet are expected to include security considerations as part of the design and development process.

Elaboration

(1) Users are individually responsible for understanding and respecting the security policies of the systems (computers and networks) they are using. Users are individually accountable for their own behavior.

Users are responsible for their own behavior. Weaknesses in the security of a system are not a license to penetrate or abuse a system. Users are expected to be aware of the security policies of computers and networks which they access and to adhere to these policies. One clear consequence of this guideline is that unauthorized access to a computer or use of a network is explicitly a violation of Internet rules of conduct, no matter how weak the protection of those computers or networks.

There is growing international attention to legal prohibition against unauthorized access to computer systems, and several countries have recently passed legislation that addresses the area (e.g., United Kingdom, Australia). In the United States, the Computer Fraud and Abuse Act of 1986, Title 18 U.S.C. section 1030 makes it a crime, in certain situations, to access a Federal interest computer (federal government computers, financial institution computers, and a computer which is one of two or more computers used in committing the offense, not all of which are located in the same state) without authorization. Most of the 50 states in the U.S have similar laws.

Another aspect of this part of the policy is that users are individually responsible for all use of resources assigned to them, and hence sharing of accounts and access to resources is strongly discouraged. However, since access to resources is assigned by individual sites and network operators, the specific rules governing sharing of accounts and protection of access is necessarily a local matter.

(2)Users have a responsibility to employ available security mechanisms and procedures for protecting their own data. They also have a responsibility for assisting in the protection of the systems they use.

Users are expected to handle account privileges in a responsible manner and to follow site procedures for the security of their data as well as that of the system. For systems which rely upon password protection, users should select good passwords and periodically change them. Proper use of file protection mechanisms (e.g., access control lists) so as to define and maintain appropriate file access control is also part of this responsibility.

(3)Computer and network service providers are responsible for maintaining the security of the systems they operate. They are further responsible for notifying users of their security policies and any changes to these policies.

A computer or network service provider may manage resources on behalf of users within an organization (e.g., provision of network and computer services with a university) or it may provide services to a larger, external community (e.g., a regional network provider). These resources may include host computers employed by users, routers, terminal servers, personal computers or other devices that have access to the Internet.

Because the Internet itself is neither centrally managed nor operated, responsibility for security rests with the owners and operators of the subscriber components of the Internet. Moreover, even if there were a central authority for this infrastructure, security necessarily is the responsibility of the owners and operators of the systems which are the primary data and processing resources of the Internet.

There are tradeoffs between stringent security measures at a site and ease of use of systems (e.g., stringent security measures may complicate user access to the Internet). If a site elects to operate an unprotected, open system, it may be providing a platform for attacks on other Internet hosts while concealing the attacker's identity. Sites which do operate open systems are nonetheless responsible for the behavior of the systems' users and should be prepared to render assistance to other sites when needed. Whenever possible, sites should try to ensure authenticated Internet access. The readers are directed to appendix A for a brief descriptive list of elements of good security.

Sites (including network service providers) are encouraged to develop security policies. These policies should be clearly communicated to users and subscribers. The Site Security Handbook (FYI 8, RFC 1244) provides useful information and guidance on developing good security policies and procedures at both the site and network level.

(4)Vendors and system developers are responsible for providing systems which are sound and which embody adequate security controls.

A vendor or system developer should evaluate each system in terms of security controls prior to the introduction of the system into the Internet community. Each product (whether offered for sale or freely distributed) should describe the security features it incorporates.

Vendors and system developers have an obligation to repair flaws in the security relevant portions of the systems they sell (or freely provide) for use in the Internet. They are expected to cooperate with the Internet community in establishing mechanisms for the reporting of security flaws and in making security-related fixes available to the community in a timely fashion.

(5)Users, service providers, and hardware and software vendors are responsible for cooperating to provide security.

The Internet is a cooperative venture. The culture and practice in the Internet is to render assistance in security matters to other sites and networks. Each site is expected to notify other sites if it detects a penetration in progress at the other sites, and all sites are expected to help one another respond to security violations. This assistance may include tracing connections, tracking violators and assisting law enforcement efforts.

There is a growing appreciation within the Internet community that security violators should be identified and held accountable. This means that once a violation has been detected, sites are encouraged to cooperate in finding the violator and assisting in enforcement efforts. It is recognized that many sites will face a trade-off between securing their sites as rapidly as possible versus leaving their site open in the hopes of identifying the violator. Sites will also be faced with the dilemma of limiting the knowledge of a penetration versus exposing the fact that a penetration has occurred. This policy does not dictate that a site must expose either its system or its reputation if it decides not to, but sites are encouraged to render as much assistance as they can.

(6)Technical improvements in Internet security protocols should besought on a continuing basis. At the same time, personnel developing new protocols, hardware or software for the Internet are expected to include security considerations as part of the design and development process.

The points discussed above are all administrative in nature, but technical advances are also important. Existing protocols and operating systems do not provide the level of security that is desired and feasible today. Three types of advances are encouraged:

(a)Improvements should be made in the basic security mechanisms already in place. Password security is generally poor throughout the Internet and can be improved markedly through the use of tools to administer password assignment and through the use of better authentication technology. At the same time, the Internet user population is expanding to include a larger percentage of technically unsophisticated users. Security defaults on delivered systems and the controls for administering security must be geared to this growing population.

(b)Security extensions to the protocol suite are needed. Candidate protocols which should be augmented to improve security include network management, routing, file transfer, telnet, and mail.

(c)The design and implementation of operating systems should be improved to place more emphasis on security and pay more attention to the quality of the implementation of security within systems on the Internet.

APPENDIX A

Five areas should be addressed in improving local security:

(1)There must be a clear statement of the local security policy, and this policy must be communicated to the users and other relevant parties. The policy should be on file and available to users at all times, and should be communicated to users as part of providing access to the system.

(2)Adequate security controls must be implemented. At a minimum, this means controlling access to systems via passwords, instituting sound password management, and configuring the system to protect itself and the information within it.

(3)There must be a capability to monitor security compliance and respond to incidents involving violation of security. Logs of logins, attempted logins, and other security-relevant events are strongly advised, as well as regular audit of these logs. Also recommended is a capability to trace connections and other events in response to penetrations. However, it is important for service providers to have a well thought out and published policy about what information they gather, who has access to it and for what purposes. Maintaining the privacy of network users should be kept in mind when developing such a policy.

(4)There must be an established chain of communication and control to handle security matters. A responsible person should be identified as the security contact. The means for reaching the security contact should be made known to all users and should be registered in public directories, and it should be easy for computer emergency response centers to find contact information at any time.

The security contact should be familiar with the technology and configuration of all systems at the site or should be able to get in touch with those who have this knowledge at any time. Likewise, the security contact should be pre-authorized to makea best effort to deal with a security incident, or should be able to contact those with the authority at any time.

(5)Sites and networks which are notified of security incidents should respond in a timely and effective manner. In the case of penetrations or other violations, sites and networks should allocate resources and capabilities to identify the nature of the incident and limit the damage. A site or network cannot be considered to have good security if it does not respond to incidents in a timely and effective fashion.

If a violator can be identified, appropriate action should be taken to ensure that no further violations are caused. Exactly what sanctions should be brought against a violator depend on the nature of the incident and the site environment. For example, a university may choose to bring internal disciplinary action against a student violator.

Similarly, sites and networks should respond when notified of security flaws in their systems. Sites and networks have the responsibility to install fixes in their systems as they become available.

A Bibliography of Computer and Network Security Related Documents

United States Public Laws (PL) and Federal Policies

[1] P.L. 100-235, "The Computer Security Act of 1987", (Contained in Appendix C of Citation No. 12, Vol II.), Jan. 8, 1988.

[2] P.L. 99-474 (H.R. 4718), "Computer Fraud and Abuse Act of 1986", Oct. 16, 1986.

[3] P.L. 99-508 (H.R. 4952), "Electronic Communications Privacy Act of 1986", Oct. 21, 1986.

[4] P.L. 99-591, "Paperwork Reduction Reauthorization Act of 1986", Oct. 30, 1986.

[5] P.L. 93-579, "Privacy Act of 1984", Dec. 31, 1984.

[6] "National Security Decision Directive 145", (Contained in Appendix C of Citation No. 12, Vol II.).

[7] "Security of Federal Automated Information Systems", (Contained in Appendix C of Citation No. 12, Vol. II.), Appendix III of, Management of Federal Information Resources, Office of Management and Budget (OMB), Circular A-130.

[8] "Protection of Government Contractor Telecommunications" (Contained in Appendix C of Citation No. 12, Vol II.), National Communications Security Instruction (NACSI) 6002.

Other Documents

[9] Secure Systems Study Committee, "Computers at Risk: Safe Computing in the Information Age", Computer Science and Technology Board, National Research Council, 2101 Constitution Avenue, Washington, DC 20418, December 1990.

[10] Curry, D., "Improving the Security of Your UNIX System", Report No. ITSTD-721-FR-90-21, SRI International, 333 Ravenswood Ave., Menlo Park, CA, 94025-3493, April 1990.

[11] Holbrook P., and J. Reynolds, Editors, "Site Security Handbook", FYI 8, RFC 1244, CICNet, ISI, July 1991.

[12] “Industry Information Protection, Vols. I, II, III”, Industry Information Security Task Force, President's National Telecommunications Advisory Committee, June 1988.

[13] Jelen, G., “Information Security: An Elusive Goal”, Report No. P-85-8, Harvard University, Center for Information Policy Research, 200 Akin, Cambridge, MA. 02138, June 1985.

[14] “Electronic Record Systems and Individual Privacy”, OTA-CIT-296,Congress of the United States, Office of Technology Assessment, Washington, D.C. 20510, June 1986.

[15] “Defending Secrets, Sharing Data”, OTA-CIT-310, Congress of the United States, Office of Technology Assessment, Washington, D.C. 20510, October 1987.

[16] “Summary of General Legislation Relating to Privacy and Computer Security”, Appendix 1 of, COMPUTERS and PRIVACY: How the Government Obtains, Verifies, Uses and Protects Personal Data,GAO/IMTEC-90-70BR, United States General Accounting Office, Washington, DC 20548, pp. 36-40, August 1990.

[17] Stout, E., “U.S. Geological Survey System Security Plan – FY1990”, U.S. Geological Survey ISD, MS809, Reston, VA, 22092, May1990.

Security Considerations

If security considerations had not been so widely ignored in the Internet, this memo would not have been possible.

Authors' Addresses

Richard D. Pethia
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania 15213-3890

Phone: (412) 268-7739
FAX: (412) 268-6989

EMail: rdp@cert.sei.cmu.edu

Stephen D. Crocker
Trusted Information Systems, Inc.
3060 Washington Road
Glenwood, Maryland 21738

Phone: (301) 854-6889
FAX: (301) 854-5363

EMail: crocker@tis.com

Barbara Y. Fraser
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania 15213-3890

Phone: (412) 268-5010
FAX: (412) 268-6989

EMail: byf@cert.sei.cmu.edu