Global Information Assurance Certification Paper

Improving Defense in Depth for NASA's Mission Network

Introduction

NASA's Mission Network provides connectivity between all NASA mission sites, which span the entire world. NASA's Mission Network is used by NASA projects and NASA customers. Examples of NASA projects are Space Shuttle, the International Space Station, or satellites such as Hubble Space Telescope. NASA customers are U.S. government employees, international partners, contractor employees, experimenters, and scientists located both inside and outside the United States. NASA projects reside on the Mission Network as depicted in Figure 1. The Mission Network consists of both Wide Area Network (WAN) and Local Area Network (LAN) links. The Mission Network supports NASA projects on a 24-hour basis transferring operational real-time data (attitude, command, orbit, ephemeris, telemetry, state vectors, etc.) as well as non real-time data (on board experiment's data products, quick-look image data, etc). The network provides flexibility to satisfy a wide range of projects by providing an open side and a closed side and allowing the projects to choose which is appropriate for their requirements. This flexibility is provided through an open network for the non real-time projects and scientific data as well as real-time spacecraft command data for robotic satellite missions. The second side is the closed network, which is used for the command and control of robotic satellite missions and human spaceflight. The closed network resides behind a firewall. The open network resides behind filtering routers. The Mission Firewall is a combination of routers and firewalls to prevent penetration of hosts on the closed side from less secure networks including the open side. One major difference between the two sides is that Internet connectivity and remote access is allowed on the open Mission Network, but prohibited on the closed Mission Network.

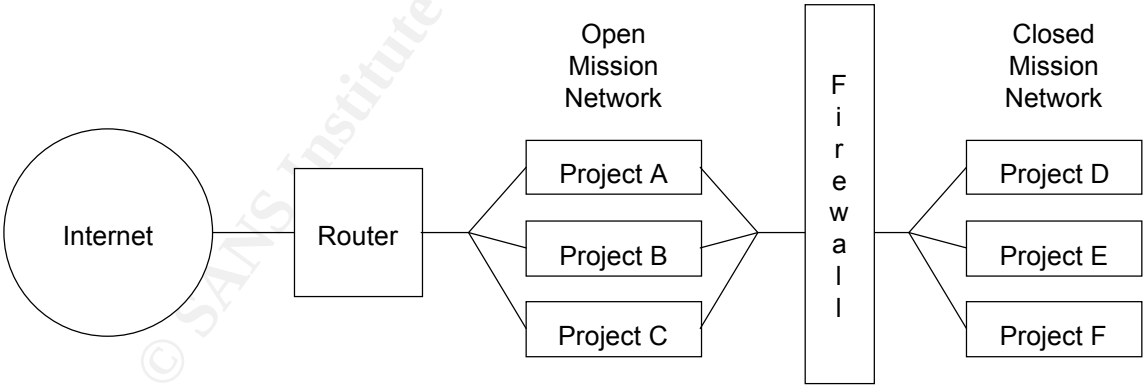

Figure 1. NASA Mission Network

The NASA mission security office has the responsibility for the security of the NASA Mission Network; therefore, there is a Mission Network security team to perform, evaluate and assist all projects connecting or connected to the Mission Network in developing defense in depth. This team ensures that projects comply with the policies and requirements of the Mission Network and NASA Procedures and Guidelines Security of

Information Technology. The team reports to and takes direction from the Network Security Officer (NSO).

The heart of NASA mission security is practicing defense in depth on the Mission Network. All the functions performed to ensure the security of the Mission Network are different building blocks to build a total security program. The different blocks NASA mission security uses include: security awareness programs, security plans and policies, business continuity, rules of behavior, firewalls, configuration management (CM), encryption, anti-virus, network architecture, host and network Intrusion Detection Systems (IDS), network and host based vulnerability assessment tools, network management (24x7), NASA independent investigations, NASA incident handling, and Center (e.g. GSFC) incident handling. This paper will discuss the security building blocks that were evaluated to improve the total security on the current Mission Network and areas for further research.

Defense in Depth for NASA Mission Networks.

Security Plans and Policies

NASA requires a security plan for all projects on the Mission Network. Security plans should provide information about: the system, the operational status, general description and purpose, information contacts, information identification, information processed, applicable laws, impact of loss of system and data, information sharing, risk assessment and analysis, technical controls, public access controls, rules of the system, personnel screening, training, contingency planning, incidence response, system interconnection, review of security controls and authorization to process.

To improve security a network mission statement should be developed for the Mission Network. There is a security goal for the Mission Network - to safeguard all NASA projects. A written mission statement should be developed and then all the security activities should be centered on that mission statement. To do this would entail organizing existing policies and building new policies. In addition, standards and policies for mission security should be more detailed than they have been. Mission Network security has policies that have evolved over the years, but with the leaps in the importance of security, and the number of security incidents encountered, more specific policies are needed. For example, one project workstation was found with a chat room on it. There needs to be a network policy for what process takes place when project workstations are encountered with non-mission programs on them. One of the SANS instructors presented (generally speaking) some of the policies that he had developed and put on the web. They appeared to be more organized than the existing Mission Network policies. After a mission statement is developed, and specific standards and policies are generated, the Mission Network security plan should be updated to meet the more exacting standards that have been developed.

Business Continuity

NASA projects have been responsible for business continuity for a long time but the importance has not been realized. The SANS class emphasized backups and contingency planning. Contingency planning is essential as many projects have critical

software (e.g. flight software) that must be backed up and preserved. Software such as flight software is much easier to protect by eliminating and mitigating the risks ahead of time than to restore it after an intruder has compromised it.

> Business continuity is a methodology primarily designed to avoid or mitigate risks to reduce the impact of a disaster condition and to reduce the time to restore an operation to "business as usual." Disaster recovery is an integral part of business continuity. Contingency planning is an integral part of business continuity. The primary difference between business continuity planning and disaster recovery and contingency planning is that business continuity seeks to eliminate or reduce the impact of a disaster condition before the condition occurs.[1]

In order for business continuity to be successful it has to be part of the overall plan for the projects. There are three steps to business continuity. The first step is the analysis of the risks. NASA projects need to analyze the risks and see which risks must be eliminated and which risks can be accepted. The Mission Network security team aids in this risk analysis. Examining a greater variety of risks and tying them to the actual project functions could improve risk analysis. For example, a project control room that commands a satellite must be able to withstand Denial of Service (DOS) attacks or the project could possibly lose the satellite, while a data processing facility can accept the DOS risks as the data can be resent later. Every project is required to perform a risk analysis on their own systems but most project personnel don't know a lot about it so they require additional expertise. The Mission Network security team evaluates the project risk assessments to see if they include: identifying the assets, identifying threats to the assets, identifying vulnerabilities, prioritizing the risks, identifying controls and processes, identifying uncorrected risks. If there is no vulnerability there is no risk. Risks without vulnerabilities do not have to be addressed. Vulnerabilities without associated threats or vulnerabilities that have controls which protect the project can be accepted or fixed on an extended timeline so the system administrator is not overwhelmed with additional work.

The second step in business continuity is compiling the disaster recovery processes into a contingency plan. The Mission Network security team does review these processes. Some of the issues to evaluate in the future are: does the contingency plan reflect the risks identified, does the plan contain the purpose for the project, could someone reading the plan execute the plan, does the plan explain what is the most critical function to recover first and prioritize the rest of the project functions, and are the key personnel updated regularly. The compilation of the team members, their job function, and letting the team members know what their recovery functions will be is critical for a successful disaster recovery.

The third step is testing the disaster recovery processes. If the projects do not test the processes they might not be able to implement the plan if/when a disaster occurs. Finally the three steps need to be reviewed and revised on a regular basis. Every NASA project needs business continuity.

Firewalls

The Mission Network contains all the various types of firewalls. The Mission Firewall that resides between the open Mission Network and the closed Mission Network is a group of systems that enforce an access control policy between the open and closed Mission Network. The Mission Firewall permits and stops traffic between both sides. At the perimeters of the open Mission Network there are border routers that separate the open Mission Network from the Internet. These border routers act as firewalls on the Mission Network. There are also routers and switches throughout the Mission Network, which act as firewalls.

There are two basic types of firewalls: network and application. Both types are used on the Mission Network. Network layer firewalls make their decisions based on the source, destination addresses, ports, services, etc. in individual IP packets. A network layer firewall can maintain internal information about the state of the connections passing through them and log traffic. Application layer firewalls run proxy servers that permit no traffic directly between networks and log and audit traffic passing through them. Proxy applications are software components running on the firewall that mediate traffic between a protected network and a less protected network. Proxies prevent traffic from passing directly between networks. Sometimes proxies can configure a specific protocol such as FTP. For example, FTP may be allowed out but not allowed into the network. There are screened subnet firewalls, which can be network or an application firewall. A firewall can be a bastion host that has highly defended and secured strong points that can resist attack. All these different types of firewalls are transparent to customers.

To improve network security ATM firewalls for use on the Mission Network should be researched. Some of the WANs use ATM now and some LANs may go to ATM in the next year so this is a place for research. One ATM network is a campus backbone network. The ATM backbone network only provides switched or soft permanent virtual paths (SPVPs) to its projects. SPVPs tunnel all information from the entrance side of the SPVP to the outlet side. ATM is a cell based telecommunications protocol that allows voice, video, and data streams to run seamlessly, end-to-end. All of these functions are planned to run over the NASA ATM WANs and LANs. The Mission Network can send traffic over the ATM backbone as if it were sending over copper cables. NASA projects on the ATM backbone are effectively all on the same network infrastructure. But logically ATM has channels for different networks. Unlike Ethernet, traffic on ATM can't be seen by other networks provided each network is on its own channel. So non-mission and mission traffic can run together on the same ATM network in different channels, mission traffic can be given priority to guarantee adequate throughput.

The ATM solution proposed by a study at the University of Maryland is to place firewalls at the borders of the ATM network where the access to the ATM network begins. The study examined what delays putting ATM firewalls at each border based on performance would experience. Marconi supports firewalls that will reach OC-3c and OC-12c speeds and these should be evaluated is where there is ATM connectivity to other sites (e.g.

university networks). A similar solution can be used to protect NASA ATM networks that the Mission Network uses.

In addition, the Mission Network security team members should have personal firewalls on their computers connected to the administrative networks. To improve security, personal firewalls should be installed on the PCs that contain sensitive data such as the various project security plans, network diagrams, risk analyzes, etc. Personal firewalls can help shield the PCs from network intruder attacks. While permitting connections to the Internet, they can stop unknown traffic. The team members can define their own rules that their personal firewall should follow. There are 3 types of personal firewalls: software-based standalone, hardware-based devices operating on the Internet connection's front end, and software-based agent-based which accept their security policy from a central server. Due to budget considerations, the most reasonable solution for the team is the standalone software based solution. The Mission Network security team should read evaluations of the software based solutions, pick the top 5 firewalls from literature comparisons and test each firewall on a personal PC and recommend the purchase of the best personal firewall for the whole Mission Network security team.

Configuration Management (CM)

CM is the discipline of establishing a known baseline condition, and then managing that condition.[2] When a project has many workstations, CM can be used to make sure that all the applicable patches have been applied on all the workstations and not just on some of them. It can be used to make sure that any changes made to one system do not adversely affect any of the other systems. It can be used to make sure than non-mission programs are not installed on NASA project workstations. CM gives stability to the Mission Network. NASA HQ requires that all changes to the operating system, including new releases and updates should be controlled and monitored. There must be tests and/or evaluations, and documentation of all operating system and application software. The project CM items that are verified by the Mission Network security team are: whether CM is part of the life cycle of a project, does CM ensure only authorized software and configurations are installed, are backups performed and how are the backups protected, are recoveries from backups performed, is COTS, public domain, or custom software used, are OS and security patches kept up to date, and have personnel been briefed on their responsibilities regarding the installation of licensed software on IT resources.

To improve security, NASA projects should perform more detailed auditing of the operational workstations on the Mission Network. Right now NASA project system administrators are required to read their logs at least once a week. SANS Security Essentials explained that reading logs once a week is not enough. What NASA projects really need are automated tools that can read the logs, and send alerts to a system administrator who can read the alerts and investigate and report the applicable alerts. The Mission Network security team is using such an automated tool in its lab, which needs to be refined and distributed to assist the project system administrators with their auditing. Also the Mission Network security team does not log on to a workstation during a security check and that needs to be improved. The Mission Network security team

should write procedures for auditing the project systems to verify what is configured on the project workstations.

Encryption

Encryption can be divided into three types. Symmetric encryption uses a secret key that is shared between two parties. The secret single key is used for both encrypting and decrypting the data. Both parties need to have the same key prior to sending the message. Asymmetric encryption uses two keys – a public key and a private key. The public key encrypts the message and the private key decrypts the message. Both parties do not have to have the same key prior to sending the message. Hash encryption is a one-way transformation of data that is irreversible. It can't be decrypted. (This last method is useful for passwords.) [3] All three types of encryption are implemented on the Mission Network.

To improve both Mission Network project and Mission Network security, NASA should go to Public Key Infrastructure (PKI) as soon as it can. NASA has been experimenting with PKI since 1992. NASA has explored such issues as secure email, secure web, secure desktop, secure file transfer, and secure networking. The plan is that NASA PKI will serve to provide authentication, data privacy, and data integrity for NASA's sensitive but unclassified information. One of the issues for the Mission Network is what customer information should be protected by PKI. For example commands should be protected by PKI but it is not clear that telemetry data should. Telemetry data is not that sensitive and the performance hit of using PKI with it could be impacting to the NASA customers. The rationale for implementing PKI by the NASA projects is based on requirements for authentication, encryption, access control, minimal impact to operations security, transparency, platform independence, multiple application support and scalability. In PKI, the Certificate Authority (CA) generates, revokes, publishes and archives certificates. In the project application it would employ a directory repository to make certificates available to certain project personnel. The CA generates its own key pairs and publishes its own certificates. The CA archives all transactions, including service requests and responses from and to other PKI components. The CA accredits the Registration Authority (RA) which vouches for the identity and other attributes of customers requesting certificates. The CA identifies certificate holders using X.509 distinguished names. The distinguished name uniquely identifies each certificate holder. The PKI provides certificate management functions for certificate holders. Certificate holders include CAs, RAs and other end mission entities. Project entities may include persons, computing systems (routers, firewalls, etc.) or applications. PKI provides the key management functions, services and policies supporting the use of these client digital certificates. There are still a lot of issues to be resolved before implementing PKI on the Mission Network. How the RA knows to whom they are giving the access codes; how the personnel "securely" receives the Registration codes; and whether it will be the customer's PC which will make the request/verification of the certificate initialization are all questions that still need to be addressed.

Network Architecture

All NASA Mission Network architecture designs must be secure to protect the NASA projects and the customer data on it. The networks must be designed in such a way that the networks protect the NASA resources, maintain operational support requirements and network connectivity at an acceptable level of risk. NASA projects on the closed Mission Network must be isolated from the Internet and cannot implement remote access. Protocols such as ICMP are not allowed on the closed Mission Network to help prevent intruders from finding out about the devices. Network management devices patrol the Mission Network 24x7. On the closed section of the Mission Network, all communication with scientists and/or principal investigators not on the closed Mission Network must go through the Mission Firewall. No back doors to the Mission Network are allowed and only authorized individuals have access.

Personnel managing the Mission Network are evaluating Juniper routers, which are new routers to the Mission Network. The routers are reported to be very fast - up to speeds of 5-10 Gbps. The routers are designed for many applications, such as high-speed access, and the ability to connect high performance interfaces from T1 though OC-48c/STM-16 could make designing the Mission Network for future growth easier. The advertised advantages of these routers are: custom software, route lookup rates in excess of 40 Mbps, throughput capacity exceeds 20 Gbps, redundant system and switch board, redundant routing engine, routing and forwarding performance clearly separated, and single-stage buffering. Apparently the network would be able to charge network customers according to their usage, improve performance of delay-sensitive applications, separate delay-sensitive and delay-tolerant traffic for more accurate planning, provide filter based forwarding, and offer VPNs.

To improve network security, security on the Juniper routers should be evaluated along with performance. (Cisco and Bay routers have been previously evaluated.) Evaluating a Juniper router to verify it is networking in a secure fashion is an immediate concern.

Host and Network Intrusion Detection Systems (IDS) –

Host based IDS

A host-based IDS looks at the communications traffic in and out of a single computer, and also checks the integrity of its system files and watches for suspicious processes. Host based IDS systems base their decisions on reading audit logs and getting other information from the host itself. The best known examples of host IDSs are TCPWrappers for UNIX and Nuke Nabber for Windows.

To improve Mission Network security, it is also critical that the Mission Network project know whether their files have been corrupted, modified or deleted by any intruder who enters a NASA project system. Some of the NASA projects develop flight software that is critical to a satellite. There is a freeware utility called FCheck that can be used to monitor changes to a file system. It is important that the files have been checked before

they have a chance to be hacked. The system administrator needs to know what the software looks like in a safe state. FCheck can take a snapshot of a project workstation, and then monitor the system and report when any differences occur in the files. FCheck can be configured to exclude log files. FCheck can be run on anything that can use a perl script, which means it can run on UNIX, Linux, and Windows workstations. This appears to be an alternative answer to Tripwire, which costs money. Tripwire is a commercial product that checks files to see if they have been changed. It is also important that Tripwire be used when the files are in a safe state. When run again, Tripwire and FCheck compare the existing state with the initial state and report any changes to the workstation. Unlike FCheck, Tripwire has a Tripwire Manager that allows system administrators to install Tripwire on all the workstations on a NASA project at the same time and then get reports from all the workstations sent to the manager. One of the best features of Tripwire is that it can now be used to monitor web pages. It can monitor web pages that leave the site and it can detect any changes to the pages. This feature also has logging capabilities. The Mission Network security team should evaluate FCheck and then compare it with Tripwire to see if it should be recommended or required on all project workstations.

To improve Network Mission project security the Mission Network team is also developing custom software IDS that contains snort, which is a freeware IDS. When implemented it might improve the security of Mission Network by analyzing collected logs and other input for potential security or reliability problems. The central logging facility should also collect configuration files, message digests, and other information about systems connected to Mission Network.

Network and host based Vulnerability assessment tools

Vulnerability assessment tools can uncover risks to a network. They can uncover risks caused by vendor software such as bugs, using default configurations, vulnerable services, and patches. They can uncover administration risks such as unacceptable passwords, etc. They can uncover insecure configurations such as sharing directories instead of limiting directories to necessary personnel, using modems, etc. Network scanners can analyze network devices detailing vulnerabilities and methods to correct those vulnerabilities quicker than could be accomplished by individual inspection. Network scanners can discover unknown devices or NIC cards connecting networks to other networks. Network scanners provide a summary of all operating systems and services and ports running on networks. Network scanners can be set up and run quickly as they do not have to be installed on the network. They uncover the vulnerabilities they find by simulating intruder attempts on the network. They are better than host based vulnerability tools because they can inspect devices on the network that can't support host-based tools such as routers, switches, etc. They can also perform brute force checks and denial-of-service attacks.[4] NASA uses multiple network-based and host based vulnerability assessment tools including some custom tools.

To improve Mission Network security, a telephone network scanner needs to be part of

the vulnerability assessment process. Evaluating a commercial telephone scanner to detect dial-in modems that are on the Mission Network could be helpful as nationally reported break-ins in recent years have come not just from the Internet, but through unauthorized dial-up modems. A product such as PhoneSweep could let Mission Network security team members find unauthorized modems (if there are any) and shut them down before an intruder used the same modem to break into a project system. PhoneSweep identifies 305 different dial-up systems, supports up to 12 modems, stores numbers to be called and call results. It replaces war dialing (which isn't recommended for the Mission Network). PhoneSweep will find misconfigured systems, undocumented systems, employee misuse, and fax machines. Telephone scanners should be evaluated and the best product put into use for the Mission Network.

To improve Mission Network project security, ISS has a system security scanner that will compliment a network scanner. (Mission Network security does use two network scanners.) This tool could assess individual host security on each workstation, detecting and report system security weaknesses. This tool works on both UNIX and NT workstations. System Security Scanner seeks out internal system vulnerabilities by working from the inside out. If IP filtering protects the exterior of the workstation, etc., a network scanner may not be able to see any vulnerabilities (there is a hard exterior). However, if an intruder can get into the project workstation, the network vulnerability tool did not see if the inside was configured properly. This is a host based security assessment and intrusion detection tool. The tool uses a policy to identify and report system weaknesses which the project would have to correct. The tool evaluates file permissions and ownership, network services, account setups, program authenticity, operating system configuration and common user-related security weaknesses such as unacceptable passwords to determine whether the security level is compliant with NASA policies. The tool can also identify previous system compromises. There is another commercial version of this tool – STAT and a freeware version of this tool – tiger. These tools should be evaluated for recommendation for Mission Network project security and Mission Network security use.

Summary

Defense in depth has been used by NASA's Mission Network in the past and will be used in the future to improve its security posture. These defense building blocks included increasing network capabilities, continued examination of network capabilities, assessment of new technologies and tools, increased security awareness for NASA non-security professionals, and training of the Mission Network security team members. Improvements in policy, business continuity, firewalls, CM, encryption, network architecture, host and network based IDS, host and network based vulnerability assessment tools should be developed. Classes, training and research provide new insight into security measures as NASA works to increase network capabilities while protecting its Mission Network and NASA projects.

[1] Glenn, p.1.

[2] Northcutt, p 19.

[3] SANS GIAC, p.5-15.

[4] Internet Security Scanner, p.3-4.

References

Carrozzi, Todd M., Jaeger, Robert F., Sanjour, Joseph, "ATM Firewall Performance Evaluation." URL: http://tebbit.eng.umd.edu/people/carrozzi/CMSC710.html (July 10, 2001).

Coast Intrusion Detection Pages, "Intrusion Detection," 3 Sept 2000. URL: http://www.cerias.purdue.edu/coast/intrusion-detection/detection.html (July 10, 2001).

Dalton, Curtis, "Getting Personal With Firewalls, "Jan 5, 2001, Network Magazine. URL: http://www.networkmagazine.com/article/NMG20010103S0010 July 10,2001).

Dalton, Curtis, "Strategies & Issues: Managing Remote Desktop Firewalls," Mar 5, 2001, Network Magazine. URL: http://www.networkmagazine.com/article/printableArticle?doc_id=NMG20010226S0002 (July 10, 2001).

Diversified Data Resources, Inc., "An Overview of SNMP," DDRI, Diversified Data Resources, Inc. URL: http://www.ddri.com/Doc/SNMP_Overview.html (July 10, 2001).

Gilbert Held, Managing TCP/IP Networks, New York, J. Wiley & Sons, 2000., 245-274.

Glenn, John, "BCP 103: Business Continuity Defined", June 2001. URL: http://www.contingencyplanning.com/article_index.cfm?article=380 (July 10, 2001).

Gumienny, Michael A., " Fcheck Intrusion Detection - Policy Enforcement." November 7, 2000. URL: http://www.geocities.com/fcheck2000/fcheck.html (July 10, 2001).

Guel, Michele, Building a Successful Security Infrastructure, 22 March 2000, SANS 2000.

Harris, "Security Threat Avoidance Technology (STAT) Scanner."
URL: http://www.statonline.com/products/scanner/features/scanner.pdf (July 10, 2001).

Internet Security Scanner, "Network and Host-based Vulnerability Assessment."
URL: http://documents.iss.net/whitepapers/nva.pdf (July 10, 2001).

Internet Security Systems, "System Scanner", 2000.
URL: http://www.iss.net/securing_e-business/security_products/security_assessment/system_scanner/index.php (July 10, 2001).

Juniper Networks, "Frequently Asked Questions," May 15, 2001.
URL: http://www.juniper.net/news/features/smart_ip/faq.html (July 10, 2001).

Kolodgy, Charles, Day, Roseann, Christiansen, Christian A., and Daly, John, "Data and Network Integrity (DNI) Technology to Invoke Trust in IT – The Tripwire Solution", 2001. URL:
http://www.tripwire.com/files/literature/white_papers/Technology_to_Invoke_Trust.pdf (July 10, 2001).

Marconi, SA-400 IP/ATM Firewalling for ATM Networks,
URL: http://www.marconi.com/media/sa-400_ds.pdf (July 10, 2001).

Mossy, Glenn, "Securing a Medical Information System at Federal Research Agency," 3 December 2000, SANS Information Security Reading Room.
URL: www.sans.org/infosecFAQ/securitybasics/med_info.htm (July 10, 2001).

NASA, IP Operational Network (IOnet) Access Protection Policy and Requirements Document, May 2001.
URL: http://forbin2.gsfc.nasa.gov/prodserv/security/secure.stm (July 10, 2001).

NASA, NASA Procedures and Guidelines Security of Information Technology, 26 August 1999. URL:
http://nodis3.gsfc.nasa.gov/library/displayDir.cfm?Internal_ID=N_PG_2810_0001_&page_name=main (July 10, 2001).

Nash, Andrew, Duane, William, Joseph, Celia, Brink, Derek, PKI Implementing and Managing E-Security, Berkely California, Osborne/McGraw-Hill, 2001.

Northcutt, Steven, "Information Assurance Foundations," SANS LevelOne Security Essentials, SANS 2001, Baltimore, Maryland, May 2001, 19.

Sandstorm Enterprises, Inc., " PhoneSweep Frequently Asked Questions," 2001.
URL: http://www.sandstorm.net/phonesweep/faq.shtml (July 10, 2001).

SANS GIAC, "Introduction to Encryption I," 1.2 LevelOne SANS Security Essentials,

© SANS Institute 2000 - 2005 Author retains full rights.

SANS 2001, Baltimore, Maryland, Part 2, May 2001, 5-15.

Stallings, William, Network Security Essentials, Upper Saddle River, NJ, Prentice Hall, 2000.

Swanson, Dan, "Identifying Early Plan Weaknesses: A Quick Questionnaire," November, 2000. URL: http://www.contingencyplanning.com/article_index.cfm?article=322 (July 10, 2001).

Tripwire, "Tripwire for Web Pages, Apache Edition Extending Data and Network Integrity to the Web," 2001. URL: http://www.tripwire.com/products/web_pages/ (July 10, 2001).