INTERNATIONAL ATOMIC ENERGY AGENCY

SYMPOSIUM ON INTERNATIONAL SAFEGUARDS

Vienna, Austria, 13-17 October 1997

IAEA-SM-351/72

Information Security Implementations for Remote Monitoring

Curt A. Nilsen
Sandia National Laboratories
MS9201, PO Box 969
Livermore, California 94551-0969
United States of America

Email: curt_nilsen@sandia.gov

This is a reprint of a paper intended for presentation at a scientific meeting. Because of the provisional nature of its content and since changes of substance or detail may have to be made before publication, the preprint is made available on the understanding that it will not be cited in the literature or in any way be reproduced in its present form. The view expressed and the statements made remain the responsibility of the named authors(s); the views do not necessary reflect those of the government of the designating Member State(s) or of the designating organizations(s). In particular, neither the IAEA nor any other organization or body sponsoring this meeting can be held responsible for any material reproduced in this preprint.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Information Security Implementations for Remote Monitoring

IAEA-SM-351/72

1. Abstract

In September 1993, President Clinton stated the United States would ensure that its fissile material meet the "highest standards of safety, security, and international accountability." [1] Frequent human inspection of the material could be used to ensure these standards. However, it may be more effective and less expensive to replace these manual inspections with virtual inspections via remote monitoring technologies.

A successful implementation of a comprehensive remote monitoring system, however, requires significant attention to a variety of information security issues. In pursuing Project Straight-Line and the follow-on Storage Monitoring System, Sandia National Laboratories developed remote monitoring implementations that can satisfy a variety of information security requirements. Special emphasis was given to developing methods for using the Internet to disseminate the data securely.

This paper describes the various information security implementations applied to the Project Straight-Line and the Storage Monitoring System. Also included is a discussion of the security provided by the Windows NT operating system.

2.0 Introduction

An important advantage of a comprehensive remote monitoring systems is that physical (or on-site) inspections can be augmented or replaced by "virtual inspections." Personnel would no longer require physical access to the material to make needed measurements and inspections. The specific advantages of virtual inspections could include:

- Fewer intrusive on-site international and/or bilateral inspections.
- Reduced costs of hosting foreign inspections.
- Domestic inventory intervals are extended.
- Reduced radiation exposure to personnel.
- More timely notification of potential safety or security problems.

- Lower overall operational costs.

Moreover, preserving "protection in depth" can enhance physical security. Whenever a storage magazine is opened, several layers of protection (doors, locks, large concrete blocks, etc.) are removed. Though other layers are strengthened (i.e., more guards are present), it could be argued that the most secure state is when the magazine is fully locked. Remote monitoring systems can be used to minimize the times these protective layers are removed. [2]

One of the challenges is to design a system that can support multiple users, each of which has a different "need-to-know." In 1995, Sandia National Laboratories launched the "Project Straight-Line" effort to tackle the issues of providing a comprehensive nuclear material storage monitoring system and to provide the information security. [3] [4] [5]

3.0 Initial Challenges

No information system is absolutely secure. Vulnerabilities will always exist. The goal in assessing a system is to determine if it is secure enough. The challenge the Straight-Line team faced was a lack of requirements to determine what was secure enough. The Straight-Line team was not building a system for a particular customer. Rather, Straight-Line was an exploratory effort to develop ways to better manage nuclear materials.

With little requirements, the system design tended to become more conservative over the initial part of the design phase. In 1995, the Internet was still a relatively new and suspicious place for many in the nuclear material management community. Thus as the design became more and more conservative, it became more and more complicated. Reliability, usability, and cost also suffered. Fortunately, design reviews and wise counsel from Sandia's Information Systems Surety group and others led to a much more practical design approach.

An U.S. Post Office analogy is useful to explain the team's approach. A variety of options are available to send a document via the mail. For many types of documents, the easy to use, 32-cent "first class" stamp is the most appropriate. For documents requiring additional protection and assurance, "certified mail" may be best. Certified mail costs an additional $1.35, but can provide a mailing receipt and a record of delivery is kept at the recipients post office. For maximum security, "registered mail" is "the most secure option offered by the Postal Service. It provides added protection for valuable and important mail. Registered articles are placed under tight security from the point of mailing to the delivery office." [6] However, registered mail costs an additional $4.85 and additional effort is required (i.e., the sender must go to the post office, declare the value of the package, sign various forms, etc.)

Similarly, the design team came up with configurations at three different levels of security:

- Best Commercial Practices -- This configuration provides reasonable security through commercially available software designed primarily for conducting commerce on the Internet. The configuration is easy to use, relatively low cost, and adequate for many types of information -- just as first class mail is adequate for many types of documents.
- Pre-Encryption -- Some customers may not feel comfortable with the best commercial practices product. Pre-encryption provides another strong layer of protection and minimizes many vulnerabilities. For customers requiring extra assurance, this configuration may be the best -- just as certified mail is appropriate for postal customers wanting extra assurance for sending a document.
- Classified Information -- Although most of the information collected by the storage monitoring systems is unclassified, it may be necessary to provide this information to users on classified and unclassified local area networks (LANs). For customers requiring maximum security, this is the best choice -- just as registered mail is the best choice for maximum security when using U.S. mail.

These three configurations are described in the following sections. Note that these above configurations are primarily dissemination mechanisms. To collect the data, virtual private networks are used. Only properly authorized system administrators have access to this private network. This network can be made from dedicated lines, or can be created by using encrypting routers on an intranet or Internet. Moreover, it assumed that the site provides adequate physical security for the servers and firewalls.

4.0 Best Commercial Practices

In this configuration, the information is disseminated via the Internet's World Wide Web. Authorized users can connect to the remote monitoring web site and easily receive data via an encrypted link. Specifically, the web server used by Straight-Line is the Netscape Enterprise Server, version 2.0, running on a SGI Indy machine. The data is encrypted with SSL (secure socket layer) version 3, and can use a variety of encryption algorithms, including DES, Triple DES, RC4-128 bit key, RC4-40 bit key, and RC2. The web server can also be configured to allow only DES encryption (often required by U.S. federal organizations). For multiple groups of users, multiple web sites can be created. Each web site can be configured to the needs of the specific group. Moreover, the web site is only provided with information that the specific group has a need-to-know. Discretionary access controls on the database computer (the one feeding the web machine with data) help enforce these need-to-know policies.

To validate users, two methods are used. The first method is a standard password implementation. Because of SSL, the user identification and passwords are encrypted as they passed over the Internet. However, the use of simple passwords can present some vulnerabilities. The use of client certificates can reduce some of these vulnerabilities. (Distributing the client certificates and the certificate authorities verification key must be done with care, however.) Browsers such as Netscape version 3.0 or later readily support client certificates. The Straight-Line web server can now support either option.

For additional security, a firewall (a filtering router) was used to partially isolate the web server. Specifically, the firewall was used to only allow communication at specific ports with specific protocols. All other network communications are blocked. Moreover, the firewall provides a barrier between the Internet and the virtual private network that feeds data to the web server.

This configuration can be described as a "best commercial practice." It would be similar to a system used by a business to conduct secure sales via the web. The primary benefit of this configuration is its ease of use. Like a first class stamp, many users are familiar with web browsers and already maintain the software on their machine. From the data provider's viewpoint, it is very convenient and cost effective to not have to provide any software to the user. All updates, drivers, platform issues, etc. are taken care of by the browser manufacturer.

The major drawback of the configuration are the inherent web vulnerabilities. The hypertext transfer protocol (http) provides a powerful method to get data to the user. Unfortunately, the power and flexibility of http also increase its potential vulnerabilities. Another potential problem is managing the user certificates. Commercial vendors, such as Versign, Inc., offer a variety of certificate authority services, but there may be situations where a commercial vendor is not appropriate. Thus, a nuclear material management entity may have to act as the certificate authority. Depending on the size and diversity of the system users, the certificate authority task can become quite significant.

In summary, this configuration provides a powerful and very cost effective method to disseminate data. Adequate and easy to use encryption and user authentication are also provided. For many types of sensitive unclassified information, this configuration is likely the optimum choice -- just as first class mail is the best choice for sending a document. This configuration also generally meets the minimum standards required for many U.S. federal organizations to process sensitive unclassified information.

5.0 Pre-Encryption

"*New Netscape Software Flaw Is Discovered*" -- New York Times, May 18, 1996

"*Internet Explorer browser has security flaw*" -- CNN, March 4, 1997

"*Netscape Communications Corp. is fixing a security flaw*" -- USA Today, June 13, 1997

These headlines and statements cause worries, especially with management entrusted to protect sensitive nuclear material information. Moreover, the inherent openness of the web is likely to cause security related headlines to continue.

The approach the Straight-Line team took in creating this second configuration was to still use the World Wide Web to disseminate the information, but take extra measures to minimize the vulnerabilities inherent in web servers and http. Essentially, all data are encrypted before they are placed on the web server machine (i.e., pre-encryption). To be exact, data are encrypted using only the public keys of authorized users. The benefit of pre-encryption is that in the case where the web server or machine is compromised, the privacy of the data is still maintained.

To implement this configuration, the Straight-Line team used an encryption package from AT&T called "Secret Agent." This software implements a variety of encryption algorithms, including DES. The remote monitoring data are assembled into a html document, and then encrypted on an SGI machine. The file is then transferred through the firewall to the web server machine. The file is also given an unique file extension (.sa). Thus users can easily program their browsers to call a special helper application when these encrypted files are downloaded.

The helper application created by the Straight-Line team is essentially a batch file with a few DOS commands and a call to AT&T's secret agent program (currently the helper application works only on IBM-PC compatibles using DOS, Windows 3.x, and Windows 95 & NT). The helper application simply queries the user for the Secret Agent pass-phrase, and then decrypts and displays the data.

Although more secure than the best business practice configuration, the pre-encryption configuration is also more difficult to use and maintain. Every user must be provided a copy of the encryption software and a helper application. Maintaining this software for several platforms and issuing upgrades could require a significant investment. Moreover, key management can also become complicated, especially if the number of users becomes large. To ease some of the key management concerns, AT&T announced in October 1996 some Secret Agent enhancements to create a public key infrastructure. Even with these tools, a significant investment in time and money may be required.

In summary, this product is useful for those organizations that require a strong additional measure of security and are willing to pay the extra financial and usability costs.

6.0 Classified Information

A comprehensive, nuclear material monitoring system could be used by a variety of different users. In some situations, it is likely that some of these users may be on classified or secure, isolated LANs. The Straight-Line team faced a challenge of how to provide the remote monitoring information simultaneously to both Internet and isolated LAN users.

Several products in the U.S. are approved for the secure transfer of information from an unclassified LAN to a classified LAN. However, they are usually quite expensive, and are often export controlled. Because the Straight-Line team wanted to create a configuration that would be inexpensive and exportable, another solution was pursued.

The solution pursued was the "secure data mirror." The idea is for a disk drive on one computer (the source computer) to be "mirrored" (exactly replicated in near real-time) on a second computer (the target computer). The link between the source computer and the target computer also has to be absolutely and verifiably one-way. This provides assurance that classified information on an isolated LAN could never, ever leak back onto an unclassified system.

To create this one-way link, we constructed a secure infrared (IR) "data diode." The goal was to optically isolate the target computer. Thus, the data from the source computer was converted to IR signals, transmitted across a fiber optic cable, and then converted back to electronic signals at the target computer. With the source computer equipped only with IR transmitters (no receivers), and conversely, the target computer equipped only with receivers (no transmitters), absolute one-way flow of information was assured.

Unfortunately, absolute, one-way flow of information prevents the practice of "handshaking." When the source computer sends data, it really doesn't know if the target computer is ready to receive the data. Moreover, the source computer doesn't know if the data were corrupted during the transfer, and a re-transmission is required. The Straight-Line team has taken measures to mitigate this flow control problem, and are also working on methods to increase the bandwidth of the link. Initial results using data diode prototypes look promising, but extensive performance and reliability testing have yet to be done.

Another requirement that customers may require is the collection of classified sensor data. The Straight-Line approach is to immediately encrypt this information at the sensor. The unclassified ciphertext could then be handled as the rest of the plain-text unclassified sensor data. After the ciphertext is transferred to the classified LAN, the information can be decrypted and disseminated to authorized users on a trusted network. The Straight-Line team has built prototypes of a sensor encryptor using a federally approved algorithm to demonstrate the concept.

In summary, providing sensor information to classified and unclassified users is feasible. Although existing products can be used to transfer unclassified information to secure LANs, it is hoped that the secure data mirror will prove to be a reliable and acceptable product.

Although the above system can collect and disseminate both classified and unclassified sensor information and disseminate it on a need-to-know basis, it is not technically a "MLS" or "multilevel security" system. The term "MLS" is carefully described in the U.S. Department of Defense document “Trusted Network interpretation” (a.k.a. the Rainbow Series). Program requirements for Straight-Line prevented the adoption of an official "MLS" system.

7.0 Windows NT Security

According to the Microsoft Corporation, "Microsoft Windows NT Workstation has become a strong alternative to UNIX workstations because of its superior performance, lower total cost of ownership (TCO), application availability and support from leading workstation manufacturers. " [7] For these reasons, plus the familiarity of NT 4.0's Windows 95-like operating shell, Sandia's Storage Monitoring System is migrating to an all NT system. The security features built into NT were also a consideration. The specific security goals NT was designed to include:

- *"The owner of a resource (such as a file) must be able to control access to the resource. The operating system must protect objects so that other processes do not randomly reuse them. For example, the system protects memory so that its contents cannot be read after a process frees it. In addition, when a file is deleted, users must not be able to access the data from that file."*
- *"Each user must identify him or herself by typing a unique log on name and password before being allowed access to the system. The system must be able to use this unique identification to track the activities of the user."*
- *"System administrators must be able to audit security-related events. Access to this audit data must be limited to authorized administrators."*
- *"The system must protect itself from external interference or tampering, such as modification of the running system or of system files stored on disk." [8]*

NT is a reasonable operating system for the remote monitoring system computers. However, the operating system, *by itself*, does not provide two important security features:

- *Adequate File Encryption*: NT's Secure File Sharing and Remote Access Services (RAS) do not adequately encrypt a file to assure its privacy when traversing a network. For example, RAS uses only a 40-bit cipher. Typically, DES encryption or better is required in the U.S. for protecting sensitive unclassified information.
- *User Authentication*: NT's use of simple passwords is subject to a variety of vulnerabilities. For example, if a password is guessed or compromised (i.e., a user's password is also the

name of his pet dog, or the password is on a small piece of paper attached to the computer monitor), an unauthorized user will have easy and complete access to the account.

Fortunately, a variety of products work closely with NT to provide the above features. For example, Microsoft's Internet Information Server 3.0 provides SSL encryption, as well as user authentication via client certificates. Moreover, Microsoft claims that NT's "CryptoAPI provides an extensible architecture for developers to build exportable applications that take advantage of system-level certificate management and cryptography." [8] Thus NT, combined with additional software, provides a good system to support the secure dissemination of information to remote users.

7.0 Conclusion

Using primarily commercially available products, there is a reasonable set of configurations that can be used to disseminate storage monitoring information. The configurations described in this paper cannot meet all customer needs, but it is likely that many customers will find one of the configurations acceptable. However, regardless of the configuration implemented, security training and awareness will be essential at the user end. It does little good to securely deliver the information to a user's desktop if the user can be easily compromised.

8.0 References

[1] "Fact Sheet - Nonproliferation And Export Control Policy", September 27, 1993, Office of the Press Secretary, The White House.

[2] NILSEN, C., POLLOCK, R., "Storage Monitoring Systems For The Year 2000," Proceedings of the Institute of Nuclear Materials Management Annual Meeting, July 1997, Vol XXVI.

[3] NILSEN C., MANGAN D., "Straight-Line -- A Nuclear Material Storage Information Management System", Proceedings of the Institute of Nuclear Materials Management Annual Meeting, July 1995, Vol. XXIV.

[4] NILSEN, C., "Straight-Line Information Security", Proceedings of the Institute of Nuclear Materials Management Annual Meeting, July 1995, Vol. XXIV.

[5] NILSEN, C., JORTNER, J., DAMICO, J., FRIESEN, J., SCWEGEL, J., "Virtual Real-Time Inspection of Nuclear Material via VRML and Secure Web Pages," Proceedings of the Institute of Nuclear Materials Management Annual Meeting, July 1996, Vol. XXV.

[6] UNITED STATES POST OFFICE, "Using special mailing services," U.S. Post Office Web Site: http://www.usps.gov/busctr/welcome.htm, downloaded 8 August 1997, 9:50 am PDT.

[7] MICROSOFT CORPORATION, " Windows NT Workstation—A Strong Alternative to UNIX Workstations," Microsoft's web site: http://www.microsoft.com/ntserver/info/ntunix.htm, downloaded 8 August, 1997, 12:46pm, PDT.

[8] MICROSOFT CORPORATION, " Microsoft Windows NT -- Securing Windows NT Installation," Microsoft's web site: http://www.microsoft.com/security/, downloaded 8 August, 1997, 1:18pm, PDT.

This work was supported by the United States Department of Energy under contract DE-AC04-94AL85000.

Sandia
National
Laboratories