SAND--95-8670C
Conf-950787--31

THE STRAIGHT-LINE INFORMATION SECURITY ARCHITECTURE

Curt Nilsen
Sandia National Laboratories
Livermore, California, USA

ABSTRACT

Comprehensive monitoring can provide a wealth of sensor data useful in enhancing the safety, security, and international accountability of stored nuclear material. However, care must be taken to distribute this type of data on a need to know basis to the various types of users. The following paper describes an exploratory effort on behalf of Sandia National Labs to integrate commercially available systems to securely disseminate (on a need to know basis) both classified and unclassified sensor information to a variety of users on the internet.

INTRODUCTION*

The Clinton Administration announced on September 27, 1993 that the United States would "... undertake a comprehensive approach to the growing accumulation of fissile material ... and ... ensure that where these materials already exist they are subject to the **highest standards of safety, security, and international accountability...**"[1] (emphasis added by author).

Continuous, 'round the clock' sensor monitoring of these materials would be valuable in enhancing the nation's ability to assure the "highest standards of safety, security, and international accountability". Sensors can be used to assure that the material is in place, unaltered, and stable. Comprehensive sensor monitoring would also reduce the risk, expense, and frequency of manual inspection of the material.

In the past, remote monitoring of stored nuclear material was done usually for one user. However, comprehensive sensor information that enhances safety, security, and international accountability will require a wide variety of sensors and a variety of users -- domestic and international. Moreover, significant amounts of Pu may reside in pit form[4] for several years. Providing sensor information is complicated by the fact that some of the sensor information may be classified.

Project Straight-Line is Sandia National Laboratories' effort at exploring and demonstrating the concept of integrated comprehensive remote monitoring. To provide for the distributed multi-level information security for Straight-Line and future programs, Sandia is investigating the integration of commercially available systems to securely disseminate on a need to know basis both classified and unclassified sensor information to a variety of users on the internet. This paper will describe the initial approach taken to provide this information security. Topics included in this paper are:

- An introduction to the Straight-Line architecture
- Protecting against eavesdropping
- Need-to-know information distribution
- Special protection for classified sensor information
- How secure is secure enough?
- Project Status

INTRODUCING STRAIGHT-LINE*

To understand the information security of Straight-Line, it is necessary to have an understanding of the overall Straight-Line architecture. The following section provides this overview.

At the heart of Straight-Line is the RF collection of sensor data. Figure 1 illustrates a Straight-Line equipped storage magazine. RF technology was selected to minimize installation costs and make Straight-Line as site independent as possible. (The only exception is the video camera -- it is connected by wire to the Magazine Data Unit (MDU)).

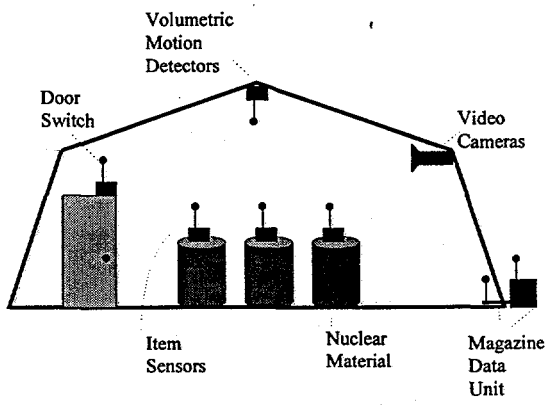

Figure 1 - RF collection of sensor information in the storage magazine

Straight-Line RF sensor packs transmit sensor data to the MDU at predetermined intervals and when "events" are

detected -- i.e. a motion detector detects motion. The MDU records this information and also sends it immediately to the Site Data Unit (SDU). Figure 3 illustrates this concept.

The Straight-Line RF unit is based on the AIMS unit. However, the Straight-Line unit incorporates several key changes. The AIMS unit used only "bi-level" sensors. However, the Straight-Line unit can use not only bi-level sensors, but analog sensors (i.e. sensors that return a voltage between 0 and 2.5 volts that could represent temperature, pressure, etc.). The Straight-Line units also accept a serial bit stream from sensors that provide digitized data. Moreover, the unit uses standard interfaces to facilitate incorporating a wide variety of sensors.

The digitized sensor data may also be encrypted (if the sensor creates classified sensor data) or authenticated (to assure the integrity of the data as it travels from the sensor to the user) per user requirements. The encryption occurs immediately at the sensor, thus turning the data into unclassified ciphertext. This ciphertext can then be safely transmitted over regular communication networks (the phone system or the internet) without risk of compromise.

Specific sensors used by Straight-Line currently include:

- Balanced Magnetic Door Switch (detects if the door is open or closed)
- Passive Infrared Volumetric Motion Detection (detects motion in the room)
- Item Motion (motion of a nuclear material container)
- Fiber Optic Seal (detects if seal is broken)
- Container and Ambient Temperature
- Radiation -- Gamma Spectrum
- Radiation -- Total Dose Gamma
- Tamper Detection (of the RF Unit)

Other sensors that produce standard bi-level, analog, or digital output can be added easily per user requirements.

Once the data is collected by the MDU, the system then needs to securely disseminate the information to users on and off the site. This process begins by the MDU transferring the information to the Site Data Units as shown in figure 2.

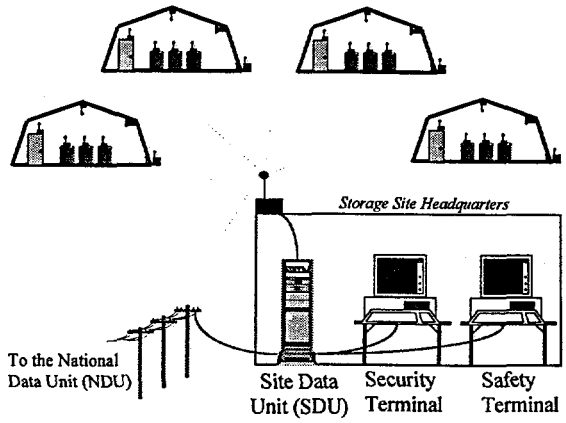

Figure 2 -- A typical Site Configuration

The Site Data Unit serves several functions. It provides sensor data to local users such as security and safety officials. The SDU then uses a high speed encryptor and transmits the data to the National Data Unit to facilitate dissemination of the sensor data to off-site users (see figure 3). Because the storage magazines may contain a wide variety of sensor information, it's important that the Straight-Line system provide data on a need-to-know basis. It is important also to prevent eavesdroppers from "listening in" on the data as it flows to the users.

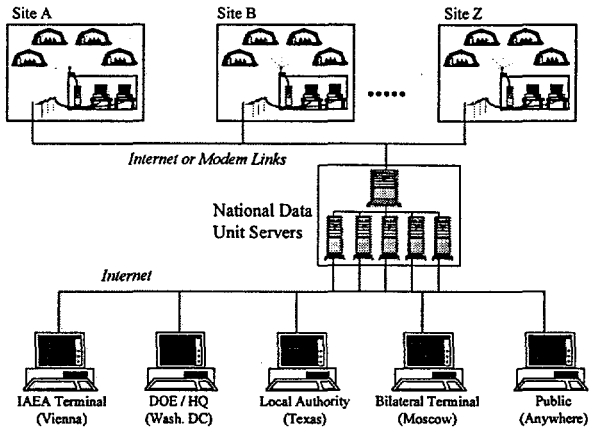

Figure 3 - Potential distribution of site information to off-site users

The off-site users are then able to access the appropriate information on a need-to-know basis. This is done by logging onto a specific "Web Page" on the internet's World Wide Web system. Straight-Line maintains a separate web page for each type of user. Special login and password procedures are also needed to access a web page. The protection and access to this information is described in the following sections.

For a more in-depth description of the Straight-Line architecture, see reference #2. Additional information regarding the initial installation of Straight-Line hardware at several facilities in the US can be found in reference #3.

PROTECTING AGAINST EAVESDROPPING

One of the pillars of the Straight-Line information security policy has been to protect the information from eavesdroppers. The philosophy has been to use encryption to encode all transmissions that traverse an unsecured system such as the internet or phone system.

This section will describe how the information will be protected as it flows from the storage site to the user. Figure 1 below shows these links.

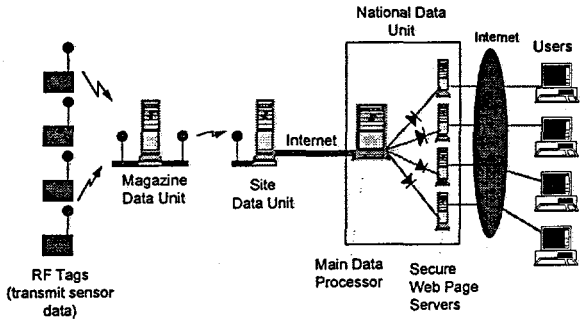

Figure 4, The flow of sensor information to the user

The MDU and SDU typically communicate via an RF LAN. If requested by the storage site, the communications over this LAN will be encrypted using features built into the RF LAN.

For SDU/NDU communications, high speed (ethernet), point to point encryptors will be used to communicate over the internet or phone lines. These encryptors are commercially available and will use the DES algorithm to encrypt the information. The initial Straight-Line prototype system will use the Semaphore Communication Corporation's NEU-WG Network encryption device (or equivalent). Semaphore states that the " ... Network Encryption Unit (NEU) family of products are high-speed, RISC-based hardware that have been engineered to provide authentication, access control, data integrity and encryption between nodes ... (on)... wide area networks." Thus not only is the information protected and authenticated as it traverses the internet, the NEU also prevents unauthorized access to the SDU and NDU main processor.

For internal NDU communications, no special protection is necessary. The NDU processors are all co-located and will be connected on a private network not accessible to the outside world.

Perhaps the most challenging aspect of the architecture was to provide encrypted communications to the user with a minimum of hassle. Straight-Line's approach has been to use commercially available software used for conducting commerce over the internet. Specifically, Straight-Line plans to use the Commerce Server software from the Netscape corporation. This software provides a very user friendly method of establishing encryption between the user and the web page server. Originally designed to maintain the privacy of credit card numbers and sensitive business documents, the Commerce Server should also protect sensor data. This software also provides server authentication. To provide the encryption and authentication, the software uses public key cryptographic technology from RSA Data Security Inc.

The only software the user needs is Netscape's Web Browser (or any other browser compatible with the Netscape commerce server). The combination of the browser and the server software integrates the key features needed to set up the encryption between the user and the server.

To log onto the web page, the user is authenticated by entering a ID name and a password. However, the password is only valid once. This is called a one-time password scheme. Every time the user logs onto the web page, the user is prompted for a new password (the next one on a list). The list of random passwords is distributed to users when they are enrolled into the system. The purpose of the one-time password scheme is to prevent someone from using a "snooped" password to gain access at a later time.

NEED-TO-KNOW INFORMATION DISTRIBUTION

As mentioned above, each web server is tailored exactly to the needs of the type of user it services. Access to this web page is based on user authentication provided by a one-time password implementation. Thus the key to assuring the system's need-to-know capability rests in the isolation of the web page servers from each other and the NDU main server.

To achieve this isolation, specially designed firewalls are used. The firewalls (shown as diodes between the web server and the NDU main processor in figure 1) provide several functions. The firewall assures that a user connected to web server cannot access the NDU main processor or "go through the back door" to reach another web page.

The firewall also performs another function. It provides an additional "need-to-know" check on the data being transferred between the web servers and main NDU processor. Specifically, all the data in the system is in the NDU main processor or easily accessed by the NDU (infrequently used data may stay at the SDU and be transferred only upon request by the NDU). The web pages communicate with the NDU main processor by

essentially issuing special database commands. When the NDU main processor receives this command, it immediately checks to determine if the web page server is authorized to make such a request. If the web page is authorized, then the request is granted. The firewall also double-checks these commands, making sure only the authorized commands and responses are sent and received by the web server. The firewall also insures that Straight-Line's custom message format is the only one allowed to cross over to the NDU main processor. All other messages and protocols are immediately stopped.

An additional feature of the current Straight-Line system allows fully cleared, on-site users to directly access sensor information on the SDU. Though the NDU provides sensor information in a timely manner, on-site safety or security officials may need real time sensor information. The SDU can provide this data with a minimum of delays.

Extra Measures for Protecting Classified Sensor Data

The system described above is appropriate for protecting sensitive unclassified information. However, protecting classified information requires additional measures. These are described below.

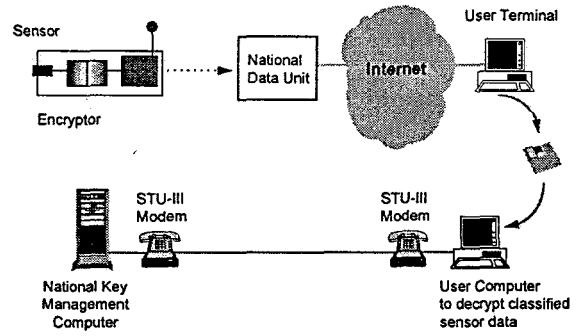

Figure 5, The flow of classified sensor information

As noted earlier, classified information created by a sensor is encrypted immediately at the sensor by special hardware encryptors. This cipher text then flows through the MDU, SDU, and NDU and out to the user. However, when the user loads the information onto their computer, it is still encrypted.

The user must then transfer the file to a floppy disk. The floppy then makes a one way trip to a computer approved for classified use. The classified computer then uses a STU-III modem to connect to the Straight-Line National Key Management computer. Based on the contents of the floppy drive, the correct keys are then transferred to the user's classified computer. The files can then be decrypted.

In addition to the natural protection a STU-III provides, special caller identification and additional encryption techniques are used to protect the transfer of the decryption keys.

How Secure is Secure Enough?

This is a very important question to ask when designing an information security architecture. Unfortunately, it is very hard to give a quantifiable answer. However, Straight-Line's approach has been to rely on existing precedents as being "secure enough". Specifically, the system is designed to protect sensitive unclassified information to a level consistent with standard methods used by industry and government to protect their sensitive information . This shall include using specially designed firewalls, one-time password schemes, etc. For the protection of classified information, appropriate hardware encryption is used immediately at the sensor to assure the data is protected. This is similar to the STU-III approach -- encrypted sufficiently well at the source, ciphertext can be safely transported across open, unsecured communication channels.

Another approach the Straight-Line team looked into is using an emailed enabled system. This would allow users to email requests for an update, and the system would email back a response as an html (hyper-text markup language) document. The NDU would then analyze the request. If the user has the correct authorization, then the document would be sent to the user and then viewed using a web browser. The Privacy Enhanced Mail (PIM) system would also be utilized, thus providing convenient encryption and authentication.

An emailed enabled system is simpler and provides fewer potential vulnerabilities for hackers to exploit. However, email can be easily delayed, and users may have to wait hours to view an updated report. Because of these delays, the Straight-Line team decided to explore first the concept of a secure web page. Moreover, there is a large effort within the US and other countries to use the internet for commercial transactions. Thus many companies will continually develop new security products to fill security holes as they develop.

Project Status

The Straight-Line team has installed prototype hardware to collect sensor information at three sites in the US (see reference #3). This installation was completed in June 1995. The prototype hardware and software used to provide dissemination of this information over the internet on a need-to-know basis (the secure web pages as described in this paper) will be operational in September of 1995. A limited security analysis will also be performed. With regards to sensors producing classified

information, the algorithms for encryption are being identified this summer.

In 1996, the Straight-Line team will be exercising and testing the system to determine ways to improve the performance, security, and cost effectiveness. Hardware encryptors for sensors producing classified data will also be built. Moreover, in depth security analyses will be performed to assure the system meets or surpasses all applicable regulations regarding the protection of sensitive and classified information.

It should be noted that Straight-Line has not and will not use "real" classified sensor data until after all necessary government approvals are obtained.

SUMMARY

The purpose of Straight-Line project is to explore and demonstrate the concept of comprehensive monitoring -- to provide the right sensor information to the right user in order to enhance the safety, security, and international accountability of stored nuclear material. Because the sensor data will be needed by several types of users, the Straight-Line team is exploring the use of secure web pages to provide convenient, need-to-know access to this information. The incorporation of commercially available encryption devices and internet security products will provide security consistent with that used in government and industry for the protection of sensitive data. Additional encryption of classified sensor information and off-line decryption (using appropriate algorithms) will provide the extra protection required US and DOE policy.

NOTES

* Most of the *Introduction* and the *Straight-Line Background* sections were taken from reference #2.

Funding for the research and development of the information security features described in this document was provided by the Office of Research and Development, Office of Nonproliferation and National Security, Department of Energy.

REFERENCES

1. "FACT SHEET - NONPROLIFERATION AND EXPORT CONTROL POLICY", September 27, 1993, Office of the Press Secretary, The White House.

2. Curt Nilsen, Dennis Mangan "STRAIGHT-LINE -- A NUCLEAR MATERIAL STORAGE INFORMATION MANAGEMENT SYSTEM", INMM 36th Annual Proceedings, July 1995, Vol. XXIV. An earlier version of this paper was presented at the 4th Annual Defense Nuclear Agency International Conference on Controlling Arms on June 20, 1995 in Philadelphia, PA. USA, and will be published in the proceedings of this conference.

3. Brad Mickelsen, "FAST-TRACK DEMONSTRATION OF THE STRAIGHT-LINE SYSTEM ARCHITECTURE", INMM 36th Annual Proceedings, July 1995, Vol. XXIV.

4. National Academy of Sciences, "MANAGEMENT AND DISPOSITION OF EXCESS WEAPONS PLUTONIUM", National Academy Press, 1994, pp. 118-119, 137-138

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

Sandia National Laboratories