

Conf-9306/80--5

INSIDER PROTECTION

by

Ivan G. Waddoups
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185
(505) 8441649

JUL 27 1993
OSTI

ABSTRACT

The government community is broadly addressing the insider threat. The first section of this paper defines protection approaches and the latter sections present various applicable technology developments. The bulk of the paper discusses technology developments applied to 1) personnel and material tracking and inventory, 2) classified document protection, and 3) protecting security systems. The personnel and material tracking system uses a PC based-host to 1) collect information from proximity tags and material movement sensors, 2) apply rules to this input to assure that the ongoing activity meets the site selectable rules and, 3) forward the results to either an automated inventory system or an alarm system. The document protection system uses a PC network to efficiently and securely control classified material which is stored on write-once-read-mostly optical media. The protection of sensor to multiplexer communications in a security system is emphasized in the discussion of protecting security systems.

INTRODUCTION

Most industries provide some form of protection against insider malevolence. This is particularly true in the high value and/or sensitive industries involved with commodities such as precious metals, gems and nuclear materials. This paper is motivated by, and based upon, experience in insider protection in the nuclear industry.

The insider is an adversary with knowledge of facility operations and authorized access to such op-

This work was supported by the U. S. Department of energy under Contract DE-AC0476DP00789.

erations. An insider threat is formidable because many of the conventional forms of protection, such as barriers and access control, are routinely and necessarily bypassed by such individuals in the performance of their job responsibilities. There is evidence that suggests the need for increased protection against the insider threat. Societal conditions that increase white collar crime are also seem to be more prevalent today.

PROTECTION APPROACHES

Since the threat can be anyone in the facility, and most areas within the facility require a subset of employees to have access, a single protection approach is usually not adequate. The approaches generally applied have been administrative or procedural in nature. These include operational procedures, clearances, and special personnel security assurance programs. These approaches are the fundamental foundation of an insider protection program and should be continued. The goals of a protection system are to minimize the likelihood that an errant insider is employed, detect malevolent insider activity, prevent such activity, and mitigate the consequences of a successful attempt. These administrative and procedural approaches contribute to the minimization and detection goals.

Technological approaches can also be applied to detect, prevent and mitigate. This paper is directed at such technological approaches, but is based on the assumption that the current administrative and procedural approaches remain in place unless the technological can be shown to reduce the need for them.

Our evaluations to date have led us to conclude that significant enhancements to insider protection

MASTER

875

can occur through the monitoring and/or control of critical elements in the operation of concern. These critical elements to be monitored/controlled include information, people, material, system components and system status. The following sections define the rationale and approaches in each of these areas.

MONITOR AND CONTROL INFORMATION

Classified Document Control System - Current classified document management systems require a tremendous amount of space and extensive manpower to account for, inventory, and protect the documents against insider threats. Comprehensive analysis of current control and accountability procedures reveal that the main problem is the actual handling of the paper itself. The Classified Document Control System (CDOCS) eliminates paper by scanning and storing images of pages on a personal computer using "write once read mostly" (WORM) high density optical media. By saving images on the computer not only are manpower and space requirements reduced, but the chance of compromise is diminished. As an added benefit, the information is now more readily available to the authorized user.

The CDOCS system consists of a personal computer, displays, an optical drive, a high speed scanner, and a laser printer. It uses a two-display system: a VGA display for the menus and data, and a high-resolution dual-page 19" display for the actual scanned image. The dual-page display allows the option of rotating images into landscape mode (i.e., for viewgraphs). The image storage medium has a large capacity and assures that no one can alter the document. A single WORM disk can store 25,000 pages per side at 200 dpi. A user can transfer information into the system by using a high-speed scanner capable of handling approximately forty pages per minute. A laser printer provides hard copy output, and special circuitry scales the document image and prints the image at 300 dpi resolution. Experience has shown that the printed output is visually indiscernible from the original.

CDOCS uses many levels of checks to enhance security. The different security levels include a password system for log in, an operating system shell that restricts access to the operating system, multiple-level checking for data access, and a complete audit trail of all actions on classified documents and images. The user interface consists of a data window

with pull-down menus and appropriate data entry forms. A special key or mouse allows users to access the menu. A user can retrieve the scanned image by storing a programmable number of key words on the form, the user may search for the document on any single keyword or multiple keywords. In addition, the user may also assign a document control number, a file location, a type, and/or a status to any document, and then use any of the above criteria to search for a document image. The system provides extensive auditing or logging of events reports to management personnel. The manager may display the desired reports of transactions on the screen or provide a printout.

Although most of the paper is scanned and stored in the system, there will still be some paper left to manage. Human nature is to want a piece of paper to carry around or use as a reference when writing another document. The system also allows management of these paper documents through data records similar to those kept for scanned images.

Protected FAX - Recent technical innovations have made the transmittal of large amounts of information, a relatively simple process. Many of the systems and devices used to transmit this information from inside a security area are largely unprotected against misuse by insiders who have access to classified information. One such device is the facsimile (FAX) machine. A dishonest individual could potentially transmit a classified document anywhere in the world with little chance of being detected. Ideally, a FAX machine should: 1) be able to identify classified material, 2) prevent the attempted transmission, 3) identify the perpetrator(s), and 4) record the incriminating information. The limited scope of this task did not allow us to perform all these functions, but we developed a prototype to deter and detect the perpetrators. If the information that is transmitted on a FAX machine is classified, and if that information is correlated with the sender, an insider will not attempt to transmit classified information because the risk of detection (and its consequences) is too high. In this system, all of the essential information concerning a FAX transmission was recorded in real time, but was not analyzed until later. Thus, the system did not actually prevent insiders from transmitting classified information, but simply made it obvious that they had broken security regulations so that further action could be taken.

The prototype system utilized modified paper, an unmodified FAX machine and an analysis computer. The modified paper contained a fine mesh of black and white dots over which the document was printed. This mesh increased the run-length compression scheme a FAX machine uses such that the length of an optical image file becomes much longer, typically over 100,000 bytes. Using this approach, the analysis computer simply monitored FAX transmissions for the presence of unusually long files.

The analysis computer hardware and software was also developed. The hardware consists of an IBM-PC with two FAX boards and a laserjet printer. The FAX boards were capable of receiving incoming FAX transmissions and storing them on the hard disk in the computer. We developed software to analyze incoming FAX transmissions for long file lengths which indicate the presence of classified information. The software was developed in the Windows operating environment. The software logged all transmissions that exceeded a certain file length and generated an alarm report for each occurrence. The alarm report contained a hard copy of the suspect transmission.

MONITOR AND CONTROL PEOPLE

General Access Control - The primary reason for existing access control systems is to restrict presence in designated areas to authorized individuals. Therefore, when a facility uses access control, it is protecting against the insider if only to a minimal extent. The primary issue relates to the degree of accountability, monitorability, and compartmentation provided by the entry control system. In the vast majority of current situations, large numbers of people are admitted into large areas with little opportunity or capability to establish localized accounting or monitoring. The thrust of the development effort described below is to technologically enforce and monitor personnel presence and movements within specific sensitive areas such as nuclear material processing and storage.

Personnel Tracking System - The personnel tracking subsystem consists of a set of battery-powered, electrostatic proximity tags worn by the users, a number of exciter/receiver antenna pairs, an antenna reader for each exciter/receiver antenna pair, and a Tag Control Unit (TCU). Indala Corporation of San Jose, California, developed and manufactured the

tags, antennas and antenna readers. We designed and developed the TCU.

There are two types of antenna pairs: long-range and short-range. Long-range antennas reliably detect up to six tags simultaneously when they are within approximately eight to ten feet of the exciter antenna. Authorized personnel install the long-range exciter/receiver antenna pairs in strategic locations throughout the facility. As users move about the facility, the antennas detect the tags that they are wearing and report the users' locations (via the antenna readers and TCU) to the Personnel and Material Tracking (PAMTRAK) System host. The PAMTRAK host uses this information to report unauthorized access to restricted areas and to enforce facility rules (such as the two-person rule). Short-range antennas provide limited read range of six inches, and PAMTRAK only requires that they detect one tag at a time. PAMTRAK uses the short-range antennas with the entry control subsystem to assign tags to users when they enter the facility.

The TCU is an IBM-compatible PC. The TCU can be a stand-alone system or a subsystem of the PAMTRAK system. The TCU gathers data and records events within a facility. The TCU stores this data in files on the controller's hard disk and downloads the data for review or for permanent storage. Each TCU can handle one to thirty antenna pairs. Access to the TCU's control menus and base operating system is protected by built-in security.

MONITOR AND CONTROL MATERIAL MOVEMENT

General Overview of Material Control Systems - Material control, as used in this paper, is defined as the means by which the loss of material is prevented or detected in order to maintain accountability. This is usually accomplished by monitoring access to, use of, and transfer of material in order to determine the physical status and location of all material in the inventory. Currently, most facilities use administratively controlled access, paperwork to document material activity, and human-conducted inventories. Technological approaches are being developed to accomplish these functions and thus 1) reduce insider exposure to material, 2) obtain real time indication of material activity and 3) rapidly detect anomolous conditions. Several other organizations are involved in developing approaches to this need, but this paper only discusses Sandia's

developments. A shelf monitoring system was developed in the early 1980's and has been implemented and is operational at Westinghouse Hanford. The system described below is currently in the beta-testing phase.

Material Monitoring System - The material monitoring subsystem consists of a number of wireless, battery-powered WATCH (Wireless Alarm Transmission of Container Handling), at least one WATCH receiver, and a WATCH Controller Unit (WCU). Inovonics Corporation in Boulder, Colorado, manufactures the WATCHs and receivers. We designed and developed the WCU.

The WATCH units are small electronic devices that transmit status messages via radio frequency (RF) to the WATCH receivers. The devices detect and report movement, tampers, and low batteries. Each device contains a switch that generates a tamper when it is opened. It also periodically sends state-of-health (SOH) messages so PAMTRAK can detect attempts to shield or destroy it.

There are two types of WATCH devices. The first type senses and reports motion. This type contains adjustable mercury switches that detect small movements of the device. The second type reports the closure of a balanced magnetic switch (BMS). Users place motion devices on parts or material to report unauthorized attempts to move the material. They attach BMS devices to doors to report unauthorized attempts to enter rooms.

The WCU is an IBM-compatible PC. The WCU can be a stand-alone system or a subsystem of the PAMTRAK system. The WCU gathers data and records events within a facility. The WCU stores this data in files on the controller's hard disk and downloads the data for review or for permanent storage. Each WCU can handle one to 256 WATCHs. Access to the WCU's control menus and base operating system is protected by built-in security.

Integrated Personnel and Material Tracking (PAMTRAK) System - PAMTRAK consists of a host, an entry control subsystem, and the personnel tracking and material monitoring systems discussed above. A facility can configure PAMTRAK to use any combination or any number of material monitoring, personnel tracking, or entry control subsystems with the PAMTRAK host subsystem.

The Entry Control Subsystem consists of one or more Positive Identity Verifiers (PIVs). PIV is the general term for a device that uses some physical characteristic to identify a person. PAMTRAK uses a hand geometry unit, however there are units available that measure different physical characteristics. Each PIV communicates with the PAMTRAK host via a serial communications link. It reports successful and unsuccessful identification attempts as well as tampers to the PAMTRAK host. A PIV can also control physical barriers such as doors or turnstiles.

The PAMTRAK host subsystem consists of a host computer, system terminal, a number of barcode readers, a serial printer for reporting alarms, and a laser printer for printing barcodes and reports. The PAMTRAK host receives authorized access and movement information from the users (via the system terminal and barcode readers) and from the other subsystems. It uses this information to maintain an internal representation of the state of the facility and compares the state with the rules specified for the facility. Any time the state of the facility violates the rules, PAMTRAK reports an alarm. When PAMTRAK reports an alarm it displays it on the monitor, prints it, logs it, sounds a horn, and if appropriate, sends it to another system.

HARDEN COMPONENTS/TAMPER PROTECT SYSTEM

General - We conducted an analysis to ascertain the elements of a security system which could be compromised by an insider. Some of the results are applicable to other computer-based data collection systems. The vulnerability category groups identified are:

1. Change device settings, adjustments, calibration, and internal components.
2. Change device alignment, detection coverage, shielding of passive devices.
3. Substitute for an element or deactivate it with a local switch.
4. Disable a device physically, electrically, or via other means.
5. Disable tamper-indicating devices.
6. Neglect to check container contents or compromise container seals.
7. Allow unauthorized personnel or material through a portal.
8. Falsely report or ignore alarm condition.
9. Disable backup systems.

10. Provide false credentials or unauthorized access by the computerized access control system.
11. Alter alarm processing or data transmission.

Seven of the eleven groups listed above could conceivably fit under the heading of alarm detection/communications system (1-5, 9, 11). This major component of the physical security system includes the device/sensor, control panels, communications lines, and the central processing unit (CPU). The remaining four vulnerability groups (6-8, 10) concern specific areas within the physical security system.

Security System ELS - The alarm communications system can be thought of as consisting of five major areas: alarm transmission, alarm displays and stations, alarm processing and software, line supervision and miscellaneous other components (e.g. enclosure protection, backup power). Each of these areas has some deficiencies with respect to the insider tampering threat. This paper focuses on the components of alarm transmission and line supervision.

The alarm communications system has been compared to a linked chain where the system is no stronger than its weakest link. One of the weaknesses against the relatively unsophisticated adversary occurs in the area between the sensor and the multiplexer (MUX). The development of the enhanced line security (ELS) system is intended to provide additional protection for this critical link.

The ELS system will be a part of the alarm communications system. It consists of modules which interface with the sensors and MUXs and a key transfer device (KTD) for providing initial keying information to the modules. The module at the sensor transmits data to the receiving module located at the MUX. The modules can be used as individual transmitting/receiving pairs, or several transmitting modules could communicate with one receiving module at the MUX. The sensor data is digitized and encrypted by the transmitting module and sent to the receiving module where it is converted to analog data. This puts it back in the form commonly seen by existing systems. Both alarm and tamper data can be transmitted. The ELS system will be transparent to the existing alarm communication system.

SUMMARY AND CONCLUSION

The insider threat is difficult to protect against due to its pervasive nature. The administrative and procedure protection approaches commonly used are directed at minimizing the likelihood of an errant insider and serve as a good foundation for a comprehensive insider protection scheme. Technological approaches are available to detect, prevent and mitigate malevolent activities. Systems have been developed to monitor and control information, material, people, components and systems. The combination of administrative, procedural, and technological elements can result in an effective protection approach which significantly reduces the risk from many potential insider threats.

BIBLIOGRAPHY

- Anspach, DeNise A., and Jonathan P. Anspach, PAMTRAK: A Personnel and Material Tracking System, INMM 33rd Annual Meeting Proceedings, Orlando, FL, 1992, pp. 673682.
- Crawford, David W., New Strategies for Protecting SNM, INMM 33rd Annual Meeting Proceedings, Orlando, FL, 1992, pp. 339341.
- Desonier, Lawrence, Classified Document Control System, INMM 31st Annual Meeting Proceedings, Los Angeles, CA, 1990, pp. 2830.
- Espinoza, Juan, Jr., and Raul R. Rivas, Alarm Communication Systems and the Insider Threat, Sandia National Laboratories, 1991.
- Jaeger, C. D., Insider Tamper Detection Alarm Communications, INMM 32nd Annual Meeting Proceedings, New Orleans, LA, 1991, pp. 681685.
- Liang, Alan Y., and Calvin D. Jaeger, Line Security Upgrade Considerations Alarm Communications, INMM 33rd Annual Meeting Proceedings, Orlando, FL, 1992, pp. 700705.
- Sandia National Laboratories, Insider Protection Technology Transfer Manual.
- Trujillo, Amado A., and Ivan G. Waddoups, Designing Physical Protection Technology for Insider Protection, Sandia National Laboratories, 1986.
- Waddoups, Ivan G., and Mark D. Tucker, The Protection of the Facsimile (FAX) Machine Against the Insider Threat, INMM 33rd Annual Meeting Proceedings, Orlando, FL, 1992, pp. 711715.
- Waddoups, Ivan G., Amado A. Trujillo, and Stephen Ortiz, Technology Development for Insider Protection, Sandia National Laboratories, 1987.