SAND82-1281C

PHYSICAL SECURITY WORKSHOP SUMMARY: ENTRY CONTROL

Michael J. Eaton

Sandia National Laboratories

Albuquerque, New Mexico 87185

ABSTRACT

Entry control hardware has been used extensively in the past to assist security forces in separating the authorized from the unauthorized at the plant perimeter. As more attention is being focused on the insider threat, these entry control elements are being used to extend the security inspectors' presence into the plant by compartmentalizing access and monitoring vital components. This paper summarizes the experiences expressed by the participants at the March 16-19, 1982 INMM Physical Protection Workshop in utilizing access control and contraband detection hardware for plant wide entry control applications.

This work was supported by the U.S. Department of Energy under Contract DE-AC04-76DP00789.

DISCLAIMER

This book 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

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.

INTRODUCTION

Entry control related topics were scattered throughout many of the workshop sessions. Two sessions were specifically devoted to access control and contraband detection; however, other sessions that dealt with federal rules, regulatory emphasis and maintenance had implications that pertained to the entry control areas. This presentation provides a brief overview of the salient items that were discussed in the areas of rules and regulations, access control, contraband detection, SNM detection, and maintenance.

RULES AND REGULATIONS

The keynote speaker from the Department of Energy, Mr. William Hagis, stated that until recently the DOE R&D emphasis had focused on physical security system designs that would counter attacks by terrorists groups -- the external threat. Now the DOE has broadened that emphasis to include concepts and equipment that would provide protection against people who are authorized to be in vital areas -- the internal or insider threat.

Mr. Hagis pointed out that the implementation of effective insider protection systems will be difficult because of the potential impact on facility operations. He enumerated the following list of new R&D development efforts in the entry control area that have been initiated by the DOE to address the insider problem: improved personnel identity verification equipment; a remotely read badge system that will be capable of authorizing and monitoring personnel movements with a minimum impact on facility operations; personnel screening explosive detectors that will extend the number of explosive compounds that can be detected; and nuclear material detectors that will significantly improve the capability to detect shielded material.

The keynote speaker from the NRC, Mr. Robert Burnett, also spoke about the growing emphasis on insider protection. He indicated that the NRC is currently preparing a set of rules, for commission review, that would govern personnel access authorization at nuclear power plants. In one of the workshop sessions that dealt with the review of NRC rules, regulations, and inspections, it was concluded that one of the major initiatives of NRC safeguards programs and regulation development in the next several years will be to improve protection against the insider threat.

ACCESS CONTROL

The access control session dealt specifically with credential and personnel identity verification. Throughput, or more broadly, operational impact, was the most significant concern expressed by the participants. Most of the facilities represented by the session attendees utilize some form of a picture badge system that requires security guards to match facial features. For high security applications, the double badge or badge exchange system is the preferred technique. Difficulties establishing the right motivational atmosphere for guards to consistently perform the badge exchange role were discussed, as well as the throughput problems that develop once the population exceeds a few tens of people. The lack of quantified data relating to the human performance in this role was noted. This led to a discussion of the Type I (false rejection) and Type II (false acceptance) error rates used to compare different access control techniques. The badge exchange system was judged to have an acceptably low false acceptance rate and reasonable efficiency for populations of 10 to 20 people, but developed a high false acceptance rate and low efficiency when the population reached 100 or more.

The use of positive personnel identity verification (PPIV) equipment was discussed as a possible solution for high security large population applications. There was some confusion about the difference between identity verification and identification. Identity verification systems compare the features that are presented for access to an enrolled set of features in storage, and verifies that they are the same. Identification typically refers to the forensic process of searching through a number of stored features attempting to find a match.

In a review of the state-of-the-art in the PPIV area, it was concluded that only four techniques seemed to have real potential: fingerprint, hand geometry, hand writing, and voice. Only a very few of these units, principally hand geometry, and to a lesser extent, voice, have been utilized in operational situations. The other units are developmental in nature. The reason for the low utilization to date principally seemed due to the initial emphasis being directed toward the external threat. Cost was also a consideration. Now that most of the external systems are in place or under construction and the upgrade emphasis is shifting to the insider threat, PPIV systems may receive much more attention. The only way to predictably achieve low false acceptance rates for large population access control systems, will be to utilize some form of automated personnel feature matching.

The use of a PPIV system in a guard supervised mode was discussed. With this configuration the routine transactions are handled by the identity verifier, with a guard close by to discourage overt attempts to defeat the system, and to resolve anamolies. This system combines the best features of both access control techniques and eliminates their weaknesses.

A number of different credential systems are being utilized at the various facilities represented by the group. The coding mediums include magnetic stripe, magnetic spot, optical, tuned circuits, and Wiegand effect. One of the serious limitations of a credential-only based security systems is that the card rather than the individual is being identified and therefore a high false acceptance rate can result. Use of memorized personnel identification numbers can significantly increase the security afforded credential-based systems by adding a low form of identify verification.

An interesting mixture of experiences concerning use of various credential systems were related. A number of problems with breaking credentials were mentioned. The problem was particularly acute in cold climates when polyvinyl chloride (PVC) badges were used. The polyester based plastic badges did not seem to be as prone to this problem. Magnetic systems had frequent problems when used in a shop-type environment due to misreading of greasy badges and accelerated badge reader wear. When abrasive materials get into the read heads, they wear out after a few hundred badge insertions. All of the systems need frequent preventive maintenance to work satisfactorily. Most of the problems occurred during the introductory phase and were eventually resolved as experience with the various systems was gained. The most common mistake was underestimating the preventative maintenance required.

No credential system was identified that was clearly superior for all applications. The major factors influencing the selection of a preferred system are the physical operating environment and the amount of information needed for coding.

CONTRABAND AND SNM DETECTION

Discussions revealed that the introduction of contraband detection equipment causes more resentment by facility operators than any other piece of physical security hardware. This presents a difficult internal public relations problem.

Metal detectors used for weapons search were discussed first. Attempts to use portable weapons detectors on vehicles were unanimously unsuccessful. Visual search by a guard is the only way to accomplish this task today. Walk-through weapons detectors employed for personnel search are capable of effective attended operation if the operational location is carefully selected and the initial adjustments and calibrations are properly completed. A number of bad experiences were associated with poor planning and calibration.

The state-of-the-art for personnel screening detectors needs to be advanced to cover the complete range of explosive materials available. Explosive detectors are available in hand-held form that will detect the most prevalent materials utilized in terrorist bombs. These detectors are being packaged in a form more suitable for personnel screening applications. Experiences utilizing dogs as explosive detectors were shared. It was concluded that dogs are not suited for routine personnel screening applications, but are effective in conducting limited duration searches. One facility indicated that they were spending $2000 per year in veterinary bills for their dogs.

Experiences with available walk-through SNM detectors indicate that they detect bare material adequately but are vulnerable to shielded material. Complaints were also expressed about high false alarm rates. These problems should be corrected by the next generation walk-through detectors to be introduced on the market early next year. At one of the facilities located in a cold climate, the liquid scintillator detectors become cloudy at lower temperatures, resulting in a significantly reduced sensitivity.

Facilities with large populations have found that it is necessary to install multiple entrance lanes to accomplish contraband detection while maintaining adequate throughput. This can be a special consideration when explosive detectors are used because of the 10-15 second sample and process time.

MAINTENANCE

The maintenance session covered all physical protection equipment, as well as entry control. Many pitfalls were discussed that have direct application in the entry control area. The concensus of opinion was that maintenance is handled more efficiently by on-site people rather than by contractors. Response time and frequent employee turnover were cited as major problems with contract maintenance. A major stumbling block with on-site maintenance is union jurisdictional problems. At one site, approximately $300,000 per year is spent on maintenance costs. The facility representative indicated that cost could be cut in half if it were possible to remove the duplication created by overlapping union trades. Two suggestions were presented to minimize this problem: 1) before the hardware arrives on site, management should determine, through negotiation, the responsibilities of each trade; and 2) the designers and installers must create clean hardware interfaces when more than one trade union is involved. Many instances were pointed out where decisions had been made to save a few hundred dollars in the installation phase that caused many thousands of dollars to be wasted in reoccurring maintenance expenses. Closed circuit TV systems seem to be the highest cost maintenance item at most sites.

CONCLUSION

Attendees at the workshop represented all disciplines in the physical protection area, thus providing a valuable opportunity for interaction among people sharing the common goal of adequately deterring or countering potential malevolent acts at nuclear facilities. Two types of constructive discussion occurred. The first was the vertical interaction which gave the rule makers, designers, installers, operators, and maintainers the opportunity to view the physical protection problem from different perspectives and to gain an appreciation of the problem from various veiwpoints. The second was the horizontal interaction of individuals sharing common roles in physical protection. These interactions should lead to improved productivity in all aspects of physical protection programs.