VULNERABILITY ASSESSMENT

Correctional Facilities Are Only as Secure as Their Weakest Point

Today's correctional security system is a complex configuration of personnel, procedures, detection, delay and response elements. Various tools and techniques are available to analyze a security system and evaluate its effectiveness. These total identity system deficiencies and vulnerabilities, evaluate possible improvements perform cost/benefit comparisons. To ensure effectiveness, systems must be designed to protect against security threats while maintaining efficient operations.

Correctional administrators should be cognizant of the need to perform vulnerability assessments, both at the design stage for new facilities and prior to planning a security upgrade for an existing facility. Failure to perform this assessment function means that the facility may have vulnerabilities that have not yet been addressed.

In the United States, prison systems are administered by each of the states, territories, the District of Columbia and the federal government. Many counties and municipalities also incarcerate misdemeanants. Few of these jurisdictions have defined threats to or requirements for security at correctional facilities, nor have many performed vulnerability assessments.

During the coming year, through sponsorship from the National Institute of Justice (NIJ) and in partnership with the National Law Enforcement and Corrections Technology Center-Southeast Region, Sandia National Laboratories in Albuquerque, N.M., will begin to assess vulnerability at selected correctional facilities and examine requirements for vulnerability assessment tools from the corrections community.

Determining Objectives

The design of an effective security system for a correctional facility requires a methodical approach in which the designer weighs the objectives, including efficient operations, safety and security, against available resources. The first step in the development of a security system design is to determine the system's objectives. Before formulating these objectives, the designer must: characterize (understand) the facility's operations and conditions; define the security threats at that facility; and identify escape scenarios and other targets of adversaries of the security system.

Adversaries of the security system at a correctional facility can be separated into four classes: inmates who wish to escape or wreak violence against facility personnel or other inmates, or who pose various other security threats to the system; facility insiders who may be a threat to security, such as a compromised employee smuggling in drugs; outsiders, such as families and friends of incarcerated offenders who might aid in an escape attempt or smuggle in contraband, or others with various agendas, such as members of organized crime or political activists; and outsiders acting in collusion with inmates or insiders.

For each class of adversary to the security system, the designer must understand tactics (such as deceit, force, stealth), capabilities and skills, level of motivation, speed with which the attack might be carried out, and ability to obtain, hide and carry tools and weapons.

Finally, all credible escape scenarios and other security targets should be considered. These considerations might include the defeat or bypassing of security system components or barriers, breaching of structural parts, use of such facility features as climbing or bridging aids, or the defeat of procedures by deceitful means such as forged identification.

As potential escape routes are identified, the facility's administrators must make decisions about the extent of vulnerability. The natural focus of security system design is to harden those features that are most likely to be used in an escape. Each improvement moves the attention of the potential adversary to the next easiest path of opportunity. The cost of a proposed improvement can be measured against the reduction in vulnerability to determine its worthiness for consideration. As the level of vulnerability decreases, a designer may reach the point of "acceptable risk" below which he is willing to accept the vulnerability because additional security is not worth the cost.

In addition to the primary responsibility of correctional institutions to protect the public by preventing the escape of convicted offenders, corrections officials also are responsible for the safety of inmates in their custody. The design objectives for the security system must therefore include measures to detect and counteract criminal activity by inmates who threaten the safety and well-being of other inmates and staff. These activities could include drug trafficking, trade in other types of contraband, prostitution and violence directed against other inmates or correctional officers.

Given the information obtained through facility characterization, threat definition and target identification, the designer can determine the security objectives of the security system. An example of a security objective might be to "interrupt a knowledgeable and motivated inmate before he can escape the confines of the facility."

Achieving Security Objectives

The next step in the process is determining how best to combine such elements as sensors, cameras, fences, barrier systems, contraband detection, entry control, control of interior movement, procedures, communication devices and response force personnel and weaponry into a security system. The resulting security system design should meet the system's objectives within the operational, safety and economic constraints of the facility. The primary functions of a security system are detection and assessment of any adversary, delay of that adversary, and response by correctional officers.

Certain general guidelines should be observed during the security system design. For example, a security system generally is more effective if detection is accomplished early in the breakout attempt, and if delay mechanisms are in place after the point of detection to interrupt the escapee's progress and expose him to a prompt response. In addition, there is close association between detection and assessment. Detection includes both some indication of an undesired act, plus an assessment of what caused the indication. Another close association is the relationship between response and communications. A response force cannot respond unless it receives a reliable communication request for a response.

These and many other particular features of a security system help ensure that the designer takes advantage of the strengths of each piece of equipment and uses the equipment in combinations that complement each other and protect against weaknesses.

Vulnerability Assessment

We do not recommend a checklist approach to the design of a security system. Rather, more sophisticated analysis and evaluation techniques should be used to better estimate the minimum performance levels achieved by a security system. Such techniques are most effective when they use test data.

An existing security system at an operational correctional facility cannot usually be fully tested. Drawing the attention of the inmate population to the various features of the security system, and demonstrating its strengths and weaknesses, can only provide inmates with information they have no need to know. Since full system tests are not practical, evaluation techniques are based on performance tests of component subsystems. Component performance estimates are combined into system performance estimates, based on a model of how the system operates using vulnerability assessment tools.

The end result of this phase of the design and analysis process is a system vulnerability assessment. Analysis of the security system design either will find that the design effectively achieved the security objectives or it will identify weaknesses, or both. If the security objectives are achieved, then the design and analysis process is completed. However, the security system should be analyzed periodically to ensure that the original security objectives remain valid, that the threat definition remains current, and that the security system continues to address those threats.

Adversary path: An adversary path is an ordered series of actions against a target which, if completed, results in successful accomplishment of adversary objectives. Protection elements along the path detect and delay the adversary.

Detection includes not only sensor activation but also alarm communication and assessment. Both the delay times associated with various security elements and the cumulative probability of detection along a specific path are needed to evaluate the effectiveness of the physical security system along that path. The identification and evaluation of adversary paths usually is a complex process.

Timely detection: One measure of effectiveness is timely detection. Timely detection translates into an acceptable cumulative probability of detecting the adversary while there is enough time remaining for the response force to interrupt him or her. Timely detection considers detection, delay and guard response times only. It does not consider engagement between the response force and adversaries; that is, it does not model neutralization.

Most critical path: To truly deduce the effectiveness of a total physical security system, one must consider the most critical path --the path with the lowest probability of interruption. The protection system is really only as effective as its protection of this path. The critical path characterizes the effectiveness of the protection system in detecting, delaying and interrupting the adversary.

Vulnerability Assessment Tools

Various tools are available for assessing vulnerabilities of a facility in general, although none that we are aware of have been created specifically for analyzing the vulnerabilities of a correctional facility. Sandia National Laboratories uses such tools and techniques as EASI, ASD, SAVI and ASSESS to measure the effectiveness and timeliness of detection. These tools were developed under sponsorship from the Department of Energy for the analysis of security at nuclear-related facilities.

EASI (Estimate of Adversary Sequence Interruption) was developed in the 1970s and models one path at a time, as selected by the user. EASI runs on a personal computer and uses specific detection, delay, response, and communication performance values to compute the probability of interrupting the adversary before he accomplishes his objective. It is able to perform sensitivity analyses and analyze physical protection system interactions and time trade-offs along the specified path.

ASD (Adversary Sequence Diagram) is a manual method of graphically modeling the security system at a facility. Once completed, it identifies paths which adversaries can follow to escape the facility. The most vulnerable path can be determined and used to measure the effectiveness of the entire security system.

There are three steps in developing an adversary sequence diagram for a specific facility. The first step is to model the facility by separating it into adjacent physical areas. Next, protection layers are defined between the adjacent areas.

Each protection layer includes one or more protection elements, such as doors, fences, surfaces and portals. Finally, path segments can be drawn between the areas through the protection elements. Both entry and exit paths can be modeled.

SAVI (Systematic Analysis of Vulnerability to Intrusion) was developed in the 1980s and contains an extensive database of representative detection probabilities and delay times, developed through years of testing at Sandia.

However, the analyst can change default times and probabilities to more accurately reflect the specific facility being modeled. SAVI models all paths using ASD methodology, graphically represents the paths and identifies the most critical path. An analysis using SAVI begins with constructing a site-specific

ASD for the given target. Input to the SAVI code includes the characteristics of the threat, response force deployment time, and delay and detection values for each protection element on the ASD. The code calculates the probability of interruption for each path. It lists the 10 most vulnerable paths and ranks them in order of their vulnerability. The analysis results are given in the form of graphs and path displays. One graph shows the distribution of the probability of interruption for all paths, given a specific response force time. A sensitivity graph provides information on the sensitivity of response force time. A vulnerability graph describes the probability of interruption before a successful escape and the time remaining after the interruption for the 10 most vulnerable paths, given a specific response force time. The interpretation of these results can suggest the need for sensitivity analysis of data that has been input to the code, as well as possible physical protection system upgrades to the most vulnerable paths.

ASSESS (Analytic System and Software for Evaluating Safeguards and Security) was developed in the early 1990s in coordination with Lawrence Livermore National Laboratories (LLNL) and is the most frequently used vulnerability tool for Sandia vulnerability analysts. ASSESS is a comprehensive approach for evaluating security effectiveness, but was developed primarily for theft or sabotage of nuclear materials. The code consists of six modules: manager, facility description, insider evaluation, outsider evaluation, neutralization and hand-off. Manager keeps track of analyses completed and in progress. Facility description allows the analyst to describe the facility targets and security components. Information gathered by facility description is used by the three evaluation modules. Insider includes extensive databases for insider adversary attributes and strategies and contains a reference detection

database. Outsider is an enhanced version of SAVI. Neutralization is based on the BATLE (Brief Adversary Threat Loss Estimator) program from LLNL. Hand-off considers collusion between an insider and an outsider.

Conclusion

A design and analysis procedure, together with appropriate physical security technology, provides the basis for good security. The design and analysis procedure consists of three phases: determine, design and evaluate. The first phase includes the determination of the system objectives, which involve facility characterization, threat definition and target identification. A good security system design provides detection, delay and response. Analysis of the security system design begins with a review and understanding of the objectives which the design must meet. Evaluation of the design normally requires the application of modeling techniques, such as EASI and SAVI. If the evaluation reveals weaknesses, the system is upgraded and another analysis on the redesigned system is performed.

DIAGRAM: Sample Facility Adjacent Physical Areas

REFERENCES

Gardner, B.H., W.K. Paulus and M.K. Snell. 1991. Determining system effectiveness against outsiders using ASSESS. Proceedings of the Institute of Nuclear Materials Management, July 28-31, New Orleans, La.

Sandia National Laboratories. 1998. Physical protection of nuclear facilities and material. Class notebooks for International Training Course, supported by the International Atomic Energy Agency, the U.S. Department of Energy, the U.S. Department of State, and the U.S. Nuclear Regulatory Commission. Albuquerque, N.M.

Sandia National Laboratories and Science and Engineering Associates. 1989. SAVI: Systematic analysis of vulnerability to intrusion. Unlimited Release Sandia National Laboratories Report. (December).

Snell, M.K. and Cal Jaegar. 1994. Using vulnerability assessments to design facility safeguard and security .systems. Proceedings of the Institute of Nuclear Materials Management, July 17-20, Naples, Fla.

Spencer, Debra and David Crist. 1996. Perimeter security for Minnesota correctional facilities. Proceedings of SPIE's First Annual Symposium on Enabling Technologies for Law Enforcement and Corrections, Nov. 19-21, Boston. SPIE -- The International Society for Optical Engineering.

~~~~~~~~

By Debra D. Spencer

Debra D. Spencer, Ph.D., M.B.A., is program manager at the National Institute of Justice Satellite Facility at Sandia National Laboratories. This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000.
~~~~~~~~

Copyright of Corrections Today is the property of American Correctional Association and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.