2006-422: A RIGOROUS FOUNDATION FOR SECURITY ENGINEERING PROGRAMS

Bradley Rogers, Arizona State University

Dale Palmgren, Arizona State University

Albert McHenry, Arizona State University

Scott Danielson, Arizona State University

A Rigorous Foundation for Security Engineering Programs

Abstract

Security may be defined as the protection of an asset from a malevolent human attack. The development of a security system capable of preventing successful attacks requires integration of human resources, technologies, and policies and procedures. Therefore, the development of a security system to protect high value assets can be described as a complex systems engineering problem. In practice, however, security systems engineering presents challenges not normally faced in more traditional systems engineering problems. For example, the talent necessary to develop effective systems requires the assembly of teams of experts from very diverse fields, ranging from mathematicians to specialists in languages and cultures. In addition, security systems must be capable of continuous and rapid evolution to respond to changing scenarios caused by new and evolving threats. A systems engineering methodology developed and tested at the United States' national laboratories over the last forty years, known as the Sandia methodology, effectively addresses the unique aspects of security system development and evaluation.

ASU has developed a curriculum leading to a Master of Science degree focused on security systems and engineering and, in the process, faced many challenges. The experience demonstrates that a rigorous methodology, such as the Sandia methodology, can successfully form the foundation of a system engineering curriculum focused on security engineering education. In addition, such programs offer students an option for a scientifically rigorous education in the field, in contrast to the more typical criminal justice or policy-oriented approaches used in most educational programs focused on homeland security. This paper explains the Sandia methodology, briefly describes the courses developed, the types of master's projects done by students, and the graduates' post graduation accomplishments. In addition, the challenges and difficulties, the current status of the ASU program, and recommendations for further development in this area are presented.

Introduction

Terrorist attacks on the United States and other nations have profoundly affected the public consciousness, and reducing our considerable vulnerabilities to terrorist attack has become a priority throughout the world. Within the United States a enormous amount of resources have been, and continue to be, dedicated to homeland security related programs, including a major reorganization of the federal government and the funding of two wars. This developing national priority has had a considerable impact on higher education, both through a refocusing of federal research dollars and through the development of educational programs dedicated to Homeland Security. For example, the Department of Homeland Security (DHS) through the Research and Technology office has established University-based centers of excellence at several major research universities and the Homeland Security Advanced Research Projects Agency (HSARPA) supports fundamental and applied research within academia as well as the private sector[1].

On the educational side, the American Society of Industrial Security (ASIS) currently lists 113 Colleges and Universities within the United States that have programs dedicated to the education

of security professionals[2]. Development of educational programs in the security field is complicated by the fact that the practice of security does not fit into the traditional classification of a profession. For example, a partial list of individuals involved in critical aspects of security includes physical scientists and engineers, biological scientists and medical doctors, computer scientists and mathematicians, behavioral scientists, lawyers and legal experts, criminal justice professionals and criminologists, law enforcement personnel, military personnel, emergency response personnel, business and management specialists, and experts in languages and cultures. In fact, it is difficult to find a field that doesn't have particular specialized knowledge and skills to contribute to the security team. On the other hand, the degree programs listed by ASIS tend to focus on particular aspects of security. The majority are non-technical in nature, and resemblance between the programs is usually coincidental. As a consequence, establishing the value added by these programs is elusive.

A more effective approach to security education is one that embraces the interdisciplinary nature of the field, and seeks to identify the common threads and fundamental principles which bind individuals of diverse backgrounds together in the pursuit of security. This is accomplished when security is approached from the systems viewpoint, and treated as a complex systems engineering problem. This leads to a comprehensive methodology for approaching all security problems, and forms the basis for a rigorous scientific approach to security that produces measurable outcomes. Such an approach has been developed at the national laboratories over the last 50 years, and was driven by the need to protect the nation's nuclear infrastructure[3]. This articulation, known as the Sandia Methodology, serves as a roadmap to guide the effective design, analysis and implementation of security systems, and can form the foundation of educational programs in the field, including those in which scientific and mathematical maturity are not emphasized.

Security Systems and the Sandia Methodology

For our purposes, security is defined as the protection of an asset from a malevolent human attack. The possibility that an asset may be attacked and stolen or destroyed constitutes a security risk. There are several methods available for dealing with security risks, including buying insurance, or simply accepting the risk[4]. A security system functions to reduce the risk of loss of an asset, and the installation of a security system should be justified by a risk evaluation. However, in this paper it is assumed that the risk analyses has been completed, and the decision has already been made to protect assets through the development or improvement of a security system.

There are also reactive and proactive aspects of a security infrastructure, both of which are important and complimentary to each other. On the reactive side, measures are taken to mitigate the consequences of a terrorist attack, such as investments in first responder training and equipment. The proactive side is that of prevention, in which measures are taken to prevent a successful attack in the first place. The distinction between proactive and reactive approaches to security is succinctly explained in the analogy by Fuller[5] in which he states that the nation not only needs to park a fleet of ambulances at the base of the cliff, but erect a fence at the top as well. The proactive development of systems designed to prevent successful attacks is the subject of this paper.

The development of effective security measures involves the methodical solution of a complex systems engineering problem. The Sandia Methodology guides the effective design, analysis and implementation of security systems, are very robust, and forms a foundation that can be applied to the development of *all* security systems[3]. At ASU, this methodology formed the framework of the Master of Science degree in Security Engineering Technology.

The Sandia methodology is the articulation of a general security systems engineering technique involving a thorough and rational set of procedures guiding the conception, design, implementation and analysis of security systems. The following chart summarizes the Sandia approach.

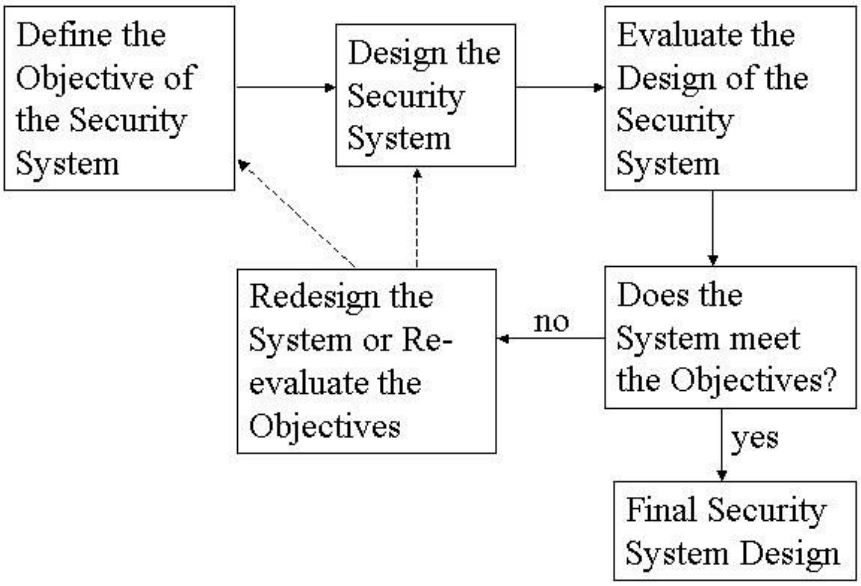

Figure 1 – The Sandia Methodology for Security Systems Engineering[3]

This diagram simply reflects sound and obvious problem-solving strategy, and reflects the framework of the principles and procedures for the design of security systems. When details of each of these fundamental tasks are identified, the talent and expertise necessary to accomplish the development and implementation of the security system becomes clear. To illustrate this conjecture, consider the following more detailed diagram, which Sandia has developed specifically for the problem of physical security.

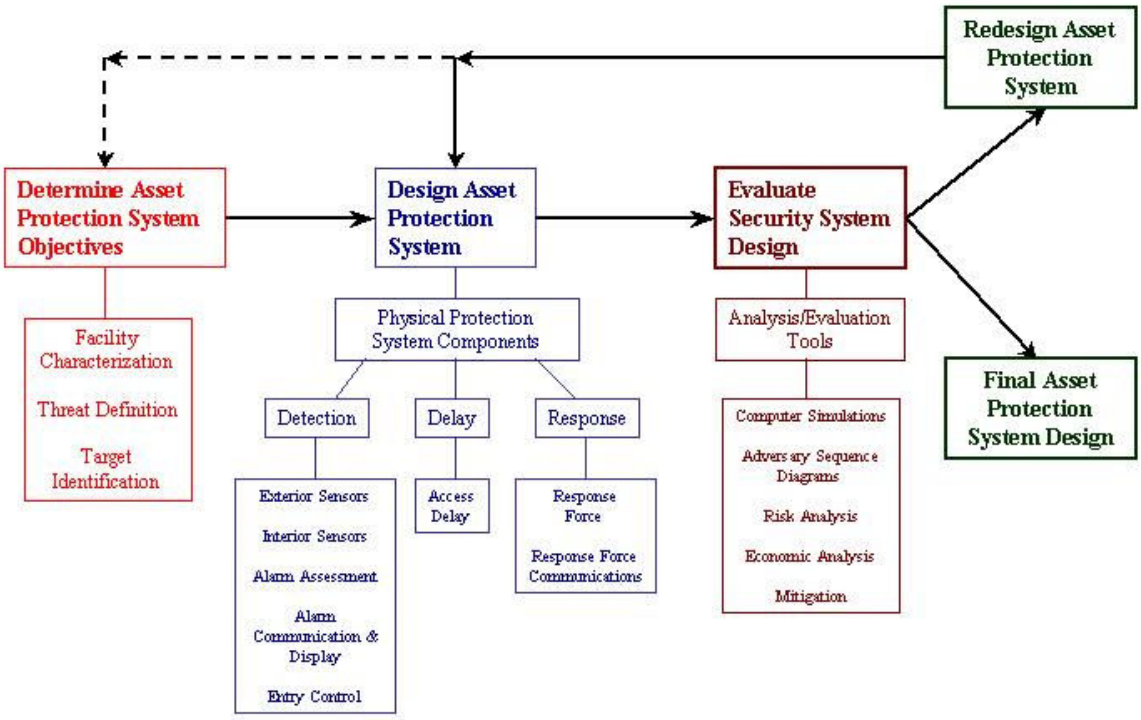

Figure 2 – Details of the Sandia Methodology for Physical Security[3]

Figure 2 includes details of the methodology for a particular aspect of security, that of physical protection systems, and illustrates the tasks that must be completed for the implementation of a successful physical security system. Other assets, such as personnel, a computer network, or a transportation system, will not include exactly the same details, but the systematic framework shown in figure 1 will be the same. Also revealed to some extent in figure 2, is the distinct nature of each of the subtasks, and the necessity of both interdisciplinary cooperation and a systematic approach to the problem to achieve effective security.

The methodology is separated into three parts. The first is the problem definition phase, in which the assets are identified, the surrounding infrastructure characterized, and the threat defined. After the problem has been defined, a system, consisting of detection, delay and response components working in tandem, is designed. Finally, the system is evaluated to determine if the proposed design meets the objectives identified in the problem definition phase.

The determination of objectives of a security system consists of three distinct subtasks, often requiring a team of diverse specialists. The identification of assets to be protected is based on the consequence of loss of the asset, and often requires specific operational expertise. For example, in the development of a system to protect a hydroelectric dam, the failure of seemingly innocuous components may lead to catastrophic system failure. An expert with a thorough understanding of the system operation is required to identify these components. The facility characterization identifies the constraints under which the security system must operate, including the facility layout, work practices, and legal issues, as well as identifying vulnerabilities.

The threat definition effort identifies the capabilities of the adversary. In many respects, the entire systems engineering process revolves around the capabilities of the threat, since no security system can be effective against all threats. (For example, equipping a facility with an highly instrumented triple perimeter fence and guarding it with a military style response force will provide essentially no protection against an insider threat.) Therefore, a threat description detailing the capabilities of the adversaries, called the design basis threat, is developed at this phase. This also illustrates a particular constraint on the design of security systems, in that a highly effective system must be flexible and able to respond to changing and evolving threats.

In most cases, the cost of protecting all assets will be prohibitive. Consequently, the final portion of the problem definition phase of the methodology is to identify assets that merit specific protection with a security system. Critical assets are identified not simply by their economic value, but by the consequence of their loss. For example, in many industrial situations the failure of a relatively inexpensive component may ultimately lead to a catastrophic failure sequence. The tools developed in the field of risk management can be of particular use in this effort.[6]

Physical security design components consist of detection, delay and response elements. A security system functions by detecting an attack, then delaying the adversary long enough for the response force to intercept and neutralize the attack. These components must be designed to work together. For example, adding a delay element before detection does nothing to improve the performance of the system since the response is not initiated until detection occurs. The performance of the system can be estimated by comparing the timelines of the adversaries as they attempt to complete their task with that of the response force, whose timeline begins as soon as detection is achieved.

A well designed physical security system consists of detection around the perimeter, with delay elements toward the target. Intrusion detection elements may consist of exterior and interior sensors, human observations, dogs, entry control technology and other subsystems. Delay mechanisms include any items that impede the adversaries progress to the target. A delay system can incorporate technologies such as barriers, physical distance, water, hardened walls, doors and windows, as well as active elements such as sticky thermoplastic foam and entanglement devices. The response element can vary from the local police to an expensive military style on-site response force. System improvement can be obtained through earlier detection, longer delay (after detection), and increased response capabilities.[3]

Security system analysis seeks to predict the performance of the security system against the design basis threat. A security system is a probabilistic system, and measures of system performance are based on statistical and probabilistic variables. For example, in a path analysis, the probability of interruption, P_I, is defined as the probability that an adversary will be interrupted before completion of their task, and the probability of neutralization, P_N, is the probability that given interruption, the response force will be able to neutralize the adversary. The system is successful if the adversary is interrupted and neutralized by the response force, and the probability of success is given by the product $P_I P_N$. The variables of P_I and P_N are determined by application of standard mathematical and statistical principles coupled with data detailing the capabilities of the adversary and the response force[3].

In this paper, security is being discussed from the viewpoint of systems engineering and a systems perspective, in which performance is measured only by the effectiveness of the system in producing the desired output. However, this can present a management problem because the development of an effective security system requires the integration of a large number of specialists with diverse backgrounds. For example, the threat definition effort is largely that of intelligence gathering, requiring a unique set of talents. The system design is an applied engineering effort. Sensors necessary for the detection of identified threats are developed by scientists and engineers working at a fundamental level, but before the system engineer can utilize them, new sensor technology developed in the laboratory must be field tested, characterized, and incorporated into working hardware. Computer simulations, developed by analytical engineers, scientists and mathematicians, must rely on such test data, as well as human performance capabilities quantified through human factors research. The response force must prepare for tactics and strategies likely to be employed by identified threats. In fact, in practice each of the subtasks is strongly intertwined with all other tasks, and weakness in any aspect of the system will lead to ultimate failure. At the same time, specialists tend to work in isolation, competing for resources with other team members whose tasks are equally critical.

Therefore, it is very important that all security educational programs at the college level, including those not based on technology, embrace the interdisciplinary nature of this field, and seek to define the common threads and fundamental principles which bind individuals of diverse backgrounds together in the pursuit of security. The Sandia methodology provides a convenient framework on which to establish this cooperation.

The Program at ASU

In cooperation with Sandia National Laboratories, ASU began offering a Master of Science degree in Security Engineering Technology in 1997. The program consisted of nine three credit courses and thesis credits for a total of 33 credits. Coursework specific to security engineering consisted of four courses, with the remaining five courses being related electives. The specific Security Courses in the core of the program, all of which are three credits, are:

SET 560 Principles of Security Methodology: Introduction to the systematic Sandia methodology for the development, design and analysis of asset protection systems;

SET 561 Analysis of Security Systems: Advanced modeling and design principles for security systems, path analysis, scenario analysis, computer modeling, and physical effects;

SET 570 Security Technology: Physical principles and design of security technology, including instrumentation, communications, delay elements and barriers, and force technologies; and

SET 598 Risk Management: General principles of security risk management, including methods of identifying, prioritizing, and dealing with all types of risk. Qualitative and quantitative risk assessment approaches are covered.

Additional courses offered specific to security include explosives, simulation and modeling, and cyber security. At the outset of the program in 1998, SET 560, 561 and 570 were taught by personnel from Sandia National laboratories, with the remainder of the coursework delivered by ASU faculty. Subsequently, the courses have been offered on demand by ASU faculty.

Program Outcomes

The SET program has produced positive outcomes and some disappointments. Accomplishments include 100% placements of graduates, including employment at Sandia National Laboratories, in private security engineering firms, in law enforcement, and in the military. Masters theses have included an economic model of investments in security systems, a computer simulation of security systems using Extend software, a vulnerability assessment of conventional power plants and a comparison of vulnerability assessment tools for computer systems.

There are two primary difficulties handicapping this program. First, it has suffered from a lack of enrollment, so that faculty resources to staff the program have not been justified. Second, the fact that the degree is in Security Engineering Technology rather than Security Engineering has led to limited opportunities for graduates within the federal government infrastructure, which does not recognize the Engineering Technology degree in this field.

We believe that the lack of enrollment is due to several factors. First, the program sought to recruit graduates from engineering, engineering technology, physical sciences and applied mathematics programs. Interested students from other disciplines were encouraged to apply, but some were asked to complete a normalization sequence. The program was advertised nationally, and specific recruitment efforts were made in Arizona and New Mexico. However, the target populations were either obtaining good jobs upon graduation with their Baccalaureate degree or had chosen other paths for their graduate education. It is worthwhile to note that these efforts were occurring in 1997 through 2000, but even after September 11, 2001 it was difficult to generate interest among young graduates for the security engineering field. Substantial interest in the program was expressed by engineers employed in the security industry, but the program was not available for distance delivery.

A significant amount of interest in the program came from those interested in the security field, but without the necessary technical background to complete the program. To try to increase enrollment and at the same time protect the integrity of the program, some of these students were offered an appropriate normalization sequence to improve their mathematical and scientific maturity so that they could gain admission. However, none of these students were able to complete this process.

The SET program at ASU was developed in partnership with Sandia National Laboratories and was specifically designed to produce graduates that could effectively work within the National Laboratory environment, as well as other positions within the federal infrastructure, and two of the graduates were hired by Sandia. Unfortunately, when other graduates applied for federal positions, they were informed that their engineering technology degree was not recognized and that they were ineligible for the positions. Ethically, it became necessary to inform students at the outset of the program that they may not be eligible for such jobs, which effectively brought enrollment in the program to a halt.

Conclusions and Recommendations

The experiences in the development and delivery of the SET program at ASU have led to the several conclusions.

- Such a program is best delivered as a Security Systems Engineering program.
- The Sandia methodology forms a foundation for such a Security Systems Engineering program and is appropriate not only for engineering students, but for students from other disciplines as well.
- Graduates of the systems-based engineering technology program have been successful in their subsequent careers.
- Security is a difficult field in which to develop highly technical educational programs because:
    - Young graduates of programs in engineering, engineering technology, mathematics and the physical sciences have not developed an interest in security as a career.
    - Experienced engineers whose careers have evolved into the security field are unable to devote the time needed to return to school and complete a Masters degree.
    - While the interest in security is higher among graduates of non-technical programs, few of these individuals are willing to develop the necessary mathematical and scientific maturity necessary to successfully complete a graduate program in security systems engineering.

The recommendations for further development of security systems engineering programs are as follows.

- As much as possible, the programs need to be offered in a distance education mode.
    - In some cases, it may be necessary for students to visit the institution for a short period for practical instruction in security technology and equipment.
- Any technical programs in security should result in an engineering degree recognized by the federal government civil service job classification system.
- The development of short courses and seminars leading to certificates is an attractive and potentially profitable option eliminating many of the difficulties associated with formal degree programs.

References

1. United States Department of Homeland Security Research and Technology Directorate: www.dhs.gov/dhspublic/theme_home5.jsp (Accessed January 2006.)

2. American Society for Industrial Security, "Academic Institutions Offering Degrees and/or Courses in Security", May 2005, www.asisonline.org/education/ universityPrograms/traditionalprograms.pdf (Accessed January 2006.)

3. Garcia, Mary Lynn, "The Design and Evaluation of Physical Security Systems," Butterworth/Heinemann, 2001

4. Garcia, Mary Lynn, "Vulnerability Assessment of Physical Protection Systems" Butterworth/Heinemann, 2005.

5. Fuller, Jeff "An Ambulance at the Bottom of the Cliff and a Fence on Top," ANSER Institute for Homeland Security, March 2003, www.homelandsecurityintelwatch.net/200307 (Accessed January 2006.)

6. Kumamoto, Hiromitsu and Henley, Ernest (1996) Probabilistic Risk Assessment and Management for Engineers and Scientists, 2nd edition, IEEE Press.