

AC 2007-826: SECURITY EDUCATION IN THE 21ST CENTURY: THE ROLE OF ENGINEERING

Bradley Rogers, Arizona State University

Dale Palmgren, Arizona State University

Dennis Giever, Indiana University of Pennsylvania

Mary Lynn Garcia, Sandia National Laboratories

Security Education in the 21st Century: The Role of Engineering

Introduction

Higher education bears the primary responsibility for the development of the nation's human resources in all fields, and security is no exception. However, the 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. A typical high-level security team consists of a wide range of individual specialists, including scientists and engineers, applied social scientists, and those educated in the liberal arts. At the same time, effective solutions to security problems require that the varied specialists comprising the security team communicate effectively and strive toward a common goal. For example, an intelligence specialist with a background in languages and cultures needs to understand the type of specific threat information needed by an engineer that is designing a system to protect an embassy. Consequently, coupled with a need for discipline specific knowledge, there is a need for all members of the security team to have broad exposure to other disciplines and ways of approaching problems so that the security team can more effectively work together toward a common goal.

In the aftermath of September 11 2001, reducing the considerable vulnerabilities to terrorist attacks faced by open and democratic societies has become a priority throughout the world. In the United States this has led to a major reorganization of the federal government, the financing of two wars, and major paradigm shifts throughout the criminal justice, intelligence, diplomatic, military and educational infrastructures of the nation¹. These changes were undertaken with the specific goal of focusing the nation's resources on *security*, which is defined in this context as the protection of assets from malevolent human attacks. Resources that can be focused on security include hardware and technology, but, most importantly, they include the nation's human resources. Higher education contributes to the nation's security, both through focused research projects that develop hardware and technology and through the development of educational programs to produce a generation of leaders that can develop, articulate and implement solutions to increasingly complex security problems. The availability of funding has led to an extensive development of research capabilities within universities over the last five years. However, the development of rigorous academic curricula and standards in the security field has lagged behind.

Since September 2001, more than 100 academic institutions in the United States have developed curricula dedicated to the education of security professionals². The development of rigorous educational programs in the field of security is made more difficult by the lack of an accepted body of knowledge in the field, and the proliferation of programs offering courses, certificates and degrees in "security" or "homeland security" with no vetting process to determine the quality or legitimacy of the conferred credentials. Furthermore, in practice the security profession includes specialists from a variety of almost autonomous backgrounds that often work in isolation. The result is that the degree programs listed in [2] tend to focus on particular aspects of security, the majority being non-technical in nature, and with resemblance between the curricula coincidental.^{2,3} The most effective programs will be those that embrace the interdisciplinary nature of the field and educate professionals in the fundamental broad methodologies of security, and yet support all the specializations of individual members of the security team, including those that have less mathematical maturity than scientists and engineers.

The field of security as an academic discipline is in its infancy, and will require the melding of many disciplines. Successful programs will embrace the philosophy of liberal education with the goal that future leaders be able to integrate contributions from many specialties to design and implement broad and effective solutions to security problems. This paper will discuss a joint program involving engineering and applied social science that addresses many of the issues discussed above. Specifically, Arizona State University at the Polytechnic Campus (ASU Polytechnic), Indiana University of Pennsylvania (IUP) and Sandia National Laboratories (SNL) are developing curricula in which engineering faculty and members of the technical staff at SNL will deliver technical portions of the curricula to graduate students in the Criminology department at IUP that are specializing in critical asset protection. In the technical portion of the coursework, the Sandia methodology for security system design and evaluation will be emphasized. The Sandia methodology is a rigorous and scientific systems engineering approach to security that embraces the unique contributions from varied specialists on the security team, while maintaining focus on the overarching goal of effective security. The result will be that students will develop a more complete, broader way of approaching the problem of security, and understand the unforeseen problems that can be induced by poorly conceived and implemented solutions. Graduates will better appreciate the contributions of individual experts in the security team, understand the role and importance of their own specialty, and, as their careers evolve and expand into management, they will have knowledge and appreciation of the complete process.

Program Foundations – The Sandia Methodology

Engineering has a great deal to contribute to the field security, including a wide range of specific technological innovations. However, engineering also makes an extremely important contribution through the application of systems engineering principles to the problems of security. In fact, the interdisciplinary nature of security is easily illustrated when the security is viewed from a systems perspective^{4,5}. At Sandia National Laboratories, these systems engineering principles have led to the development of a systematic methodology for the development, design, and evaluation of security systems, known as the Sandia methodology. The methodology, for the specific case of physical security, is illustrated in figure 1 below:

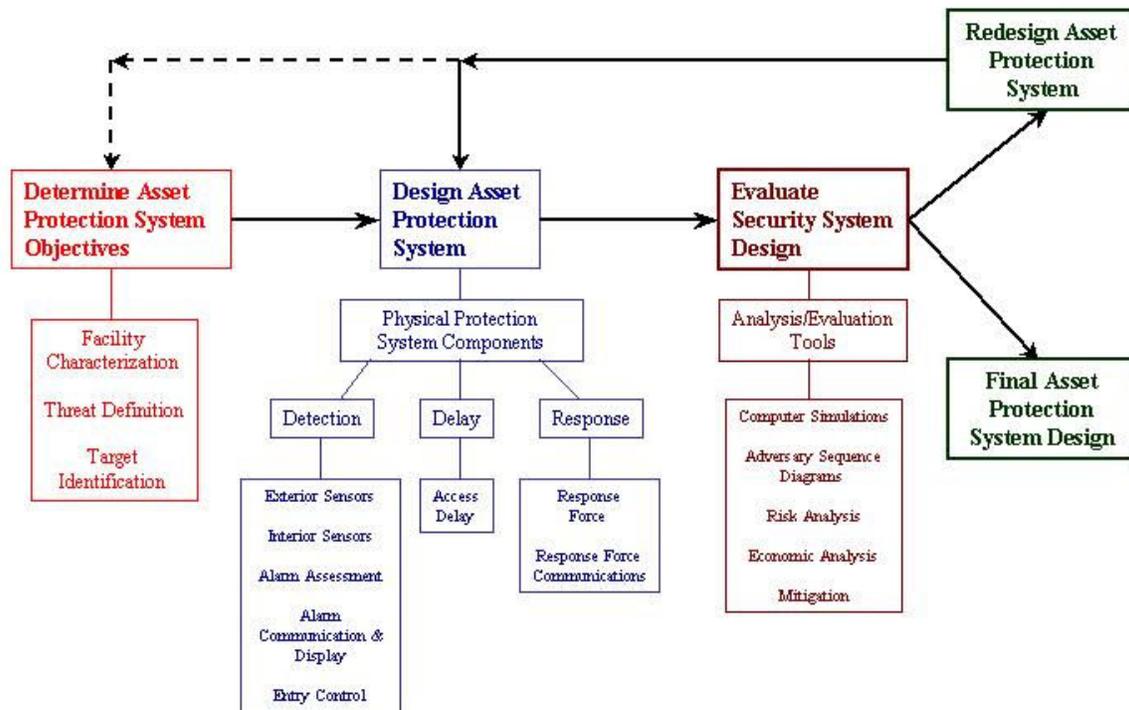


Figure 1. The Sandia Methodology for Physical Security³

Figure 1 outlines a systems engineering approach to physical security. The determination of objective phase serves to define the problem. The design phase develops a proposed solution to the problem based on the objectives. Finally, the system evaluation phase seeks to determine if the proposed solution meets the original objectives. In all phases, an overall systems viewpoint is critical – the system will be developed to respond to an input (an attack) and work to produce a specific output (a defeated adversary and an intact asset.) From a management perspective, the technologies and human resources utilized to produce this desired outcome must be viewed in context to their contribution to the global system behavior. For example, a decision to upgrade equipment with new technology may actually degrade the performance of the system if the new equipment is difficult to integrate into the existing system. Therefore, individuals responsible for the development of security systems need to understand the systems viewpoint, whatever their educational background.

Details of each of the tasks identified in figure 1 can be can be complex, as discussed in reference 4. On the other hand, this figure does illustrate that the individual tasks laid out in the methodology require teams of specialists from very different backgrounds, including disciplines that have not traditionally worked together. Facility characterization and target identification, for example, will usually require integration of knowledge and experience from the facility management into the system design. The response force, which, depending on the threat and the value of the asset, can vary from unarmed security guards to a military style assault force, requires expertise in offensive and defensive tactics and procedures. The evaluation and simulation of system performance requires modeling expertise, involving personnel with backgrounds in mathematics, statistics and general system analysis. Economic and risk

evaluations are critical to ensure available resources are concentrated on protecting the most important assets, which are those with the highest consequence of loss.

As an example of the interplay between different disciplines, consider the fundamental problem of identifying the threat. The system designers and analysts can do absolutely nothing until the capabilities of the threat have been defined. At the same time, threat identification is an intelligence specialty, and may be assigned, for example, to experts in information analysis, law enforcement, and languages and cultures. The result from this group will be the production of a design basis threat, to which the security system will be designed, or to which an existing system will be evaluated by a team of system engineers. However, the design basis threat must contain specific information so that a system can be engineered to defeat the threat. Therefore, the threat definition team must understand the type of information needed by the system engineers so that an effective countermeasure can be produced. Examples of specific information to which an engineer can design includes items such as insider vs. outsider threats, sabotage vs. theft, numbers of adversaries, training levels, weapons, tactics and equipment, and so on⁶.

The programs that will be discussed in this paper are based on the principle that each specialist on the security team should be educated in the overall security systems engineering methodology so that they understand where their particular expertise fits into this general picture. This is true not only for engineers, but for other team members as well. This will become especially important as the careers of individuals progress and their responsibilities evolve into management of security projects, which will require a knowledge and appreciation of the complete process. Consequently, the education of security experts also requires an interdisciplinary team. Depending on the specialty, engineering faculty will have many roles. However, in all specialties a firm foundation in the principles of systems engineering is important, and this is one of the most important contributions that engineering faculty can deliver to the development of the security field.

It is worthwhile to point out that the methodology discussed above (and the educational philosophy based on the methodology) is a preventative approach – the system proactively seeks to prevent adversary success. A great deal of effort has also been undertaken on the reactive side, in which efforts are made to minimize the effects of a successful attack. The distinction between proactive and reactive approaches to security is succinctly explained in the analogy by Fuller⁷ in which he states that the nation not only needs to park a fleet of ambulances at the base of the cliff (reactive), but erect a fence at the top as well (proactive). These programs are concentrating on the fence at the top of the cliff.

The Programs at ASU Polytechnic and Indiana University of Pennsylvania

In cooperation with Sandia National Laboratories, ASU Polytechnic and IUP have been involved in the education of security professionals since 1996. The approach at ASU Polytechnic has been in the field of security engineering, while that at IUP has concentrated in the field of criminology. Both programs are linked, however, through the common methodology described above, which forms the foundation of each program. Programs were offered at the graduate level so that undergraduate specializations could be built upon with advanced and concentrated study of security topics to provide an avenue for working professionals to gain expertise within the security field, and to provide a measure of control over students entering the programs.

Cooperative programs are under development with the goal that specialized coursework delivered by each institution will be available to students from both institutions, and mechanisms will be in place to encourage faculty to serve on graduate committees at the partner institution. The programs that have been developed at each university are briefly described below.

ASU Polytechnic 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. Two of the core courses were consecutive security systems engineering courses based on the Sandia methodology. These courses were supplemented by courses in Security Technology and Instrumentation, and Security Risk Management. Additional courses offered specific to security include explosives, simulation and modeling, and cyber security. At the outset of the program, the security engineering courses were taught by personnel from Sandia National Laboratories. Subsequently, the courses have been offered on demand by ASU faculty.

Graduates of the program at ASU were all successful in obtaining employment in the security engineering field, including placement at Sandia National Laboratories, in private security engineering firms, in law enforcement, and in the military. Even with this successful track record, however, the program has suffered from lack of enrollment, and faculty resources to support the program on a continual basis are difficult to justify. There are several reasons for the lack of enrollment in the program. First, the ASU degree program was limited to students with technical backgrounds, but most of the interest in the program came from individuals that did not have an engineering or physical science background. Students that did not directly qualify for admission were asked to complete a normalization sequence. However, virtually all of these students opted for other programs that were not as mathematically rigorous. Second, the economy was such that most recent graduates of engineering programs 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 in the security engineering field. Substantial interest in the program was expressed by engineers employed in the security industry, but the resources have not been available to develop the program for online delivery.

At IUP, a Masters program is under development in critical asset protection services (CAPS). The program is designed for the large pool of students with a background in criminal justice or criminology, but is founded on the Sandia methodology for security systems engineering. The curriculum is designed to prepare graduates for leadership positions in the fields of homeland security and critical asset protection. Graduates will be equipped with a unique combination of depth in their specialization coupled with breadth due to their perspective of a systems view of security, so that they can make immediate and significant contributions to the field. The CAPS program is consistent with IUP's commitment to ensure that graduate programs encourage intellectual excellence, research and scholarship, provide in-depth study in each student's special field, and stimulate continued cultural and intellectual growth for faculty and students. The specific objectives for the CAPS program are listed below. Graduates of the program will be able to:

1. Identify, prioritize, and assure the protection of assets that are the most critical in terms of loss of life and property, public health, governance, economic vitality, national security, public confidence, and quality of life in accordance with the Sandia Methodology.
2. Detect, delay, and efficiently and effectively react to attacks on critical assets and infrastructures in accordance with the Sandia Methodology.
3. Explicate possible motivations behind and contributing factors to political violence and terrorist activities and incorporate this knowledge into prevention and intervention strategies.
4. Address challenges and issues that emerge in the field of critical asset protection through research, communication, structural design, policy creation, implementation, and evaluation.
5. Design physical and cyber protection systems that will minimize identified vulnerabilities of a variety of critical assets.

Program objectives 1 and 2, listed above, involve mastering the basic framework of the Sandia systems engineering methodology described earlier in this paper. This provides the opportunity for interdisciplinary cooperation between the fields on engineering and criminology – two fields that have traditionally been almost completely independent.

Students enrolled in the program at IUP have science and math backgrounds appropriate for students in analytical social sciences, including algebra and statistics, as well as basic courses in the natural sciences. The challenge is not to teach traditional engineering courses to these students, but rather to develop and deliver these materials in a manner consistent with their backgrounds. The educational model that will be followed is closely aligned with the problem based learning approach utilized by Sandia National Laboratories for delivery of physical security courses to a range of audiences, both within the federal government infrastructure and in private industry. In this approach, a security design project is developed by student teams paralleled with the delivery of lecture course so that theoretical concepts are continually reinforced.

Conclusions

A primary goal to the security educational initiatives at ASU Polytechnic and IUP has been to define and develop the field of security as a recognized academic and professional discipline. To accomplish this goal, consensus on the roles and contributions of individual academic disciplines to the field of security needs to be developed and articulated. This will require that students receive broad exposure to the body of knowledge while they are educated in their specialization. We believe that the systems engineering approach to security developed at Sandia National Laboratories provides a framework that can help to establish these principles. A large percentage of individuals involved in the security field, including those responsible for systems that protect the most critical assets, are often not engineers. Consequently, engineering faculty have the opportunity to provide a fundamental contribution to the nations security by developing and delivering coursework in the principles of security systems engineering to students in fields other than engineering.

References

1. Altiero, Nicholas (2002) Research - Zeroing in on Security Prism, V11, #6 Also Available at: prism-magazine.org/feb02/research.cfm (Accessed December 2006)
2. American Society for Industrial Security, "Academic Institutions Offering Degrees and/or Courses in Security", asisonline.org/education/universityPrograms/traditionalprograms.pdf (Accessed December 2006.)
3. Rogers, B., Palmgren, D., McHenry, A., Danielson, S. (2006) A Rigorous Foundation for Security Engineering Programs , ASEE Annual Conference Proceedings, Chicago, IL
4. Garcia, Mary Lynn (2001) The Design and Evaluation of Physical Security Systems, Butterworth/Heinemann.
5. Garcia, Mary Lynn (2006) Vulnerability Assessment of Physical Protection Systems, Butterworth/Heinemann.
6. Rogers, B (2006) Engineering Principles for Security Managers, The Handbook of Security, Ch. 3, Martin Gill Ed., Palgrave/Macmillan
7. 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/storyguestc0703.html (Accessed February 2007.)