A Curriculum Framework for the Emerging Discipline of Information Assurance

James A. Davis, PhD
Information Assurance Center
Department of E CPE
Iowa State University
Ames, Iowa
davis@iastate.edu

Melissa Dark, PhD
Center for Research in Information Assurance and Security
Purdue University
West Lafayette, Indiana
dark@cerias.purdue.edu

1. Introduction

In this paper, we describe a community effort to identify the common body of knowledge (CBK) for computer security curricula. Academicians and practitioners have been engaged in targeted workshops for the past two years, producing the results summarized here (see [1] for a more detailed description). The long-term objective for the project is to develop a curriculum framework for undergraduate and graduate programs in Information Assurance (IA). The framework includes: identification of broad areas of knowledge considered important for practicing professionals in information assurance, identification of key learning objectives for each of these areas, identification of a body of core knowledge and skills that all programs should contain, and a model curriculum including scope and sequence. The framework's development has been facilitated by workshops and working groups of leading information assurance educators. The goal is to produce a document similar to the Joint IEEE Computer Society/ACM Task Force document [2] "Model Curricula for Computing" (Computer Science Volume), which will then be widely distributed for comment and dissemination. We anticipate that the framework will be used to guide the development of shared instructional materials, classroom instruction, and the assessment of individuals and programs.

The focus for this paper is the design of the curriculum framework and the identification of the common body of knowledge. One of the interesting challenges is the breadth of the Information Assurance field. There is a tendency to view IA as strictly a subset of computer science, however many of the issues that IA professionals address requires knowledge and skills drawn from traditionally non-computer disciplines. IA is truly a multidisciplinary endeavor, blending topics that span the disciplines of computer science, computer engineering, mathematics, management information systems and business, political science, and law. Additionally, key

processes used by IA professionals (e.g., vulnerability assessment) require a deep understanding of how important concepts in each of these disciplines are connected to each other.

The rationale for the project is based in the need to develop a consensus on core IA skills and knowledge. The demand for Information Technology (IT) professionals stemming from turnover plus growth has been pegged in various references at around 600,000 open positions per year [3]. There is an urgent need to significantly increase the number of graduates who are prepared for careers in the IA fields. A major barrier to meeting this challenge is that few Universities currently offer a comprehensive IA educational program; furthermore, sufficient numbers of experienced faculty to ramp up such an effort does not exist. Given the growing need for graduates educated in computer security and the current lack of a capacity to meet that need, there is a premium placed on leveraging existing expertise by sharing instructional materials for core concepts. This will succeed on the scale needed only if there is an accepted IA curriculum framework in place.

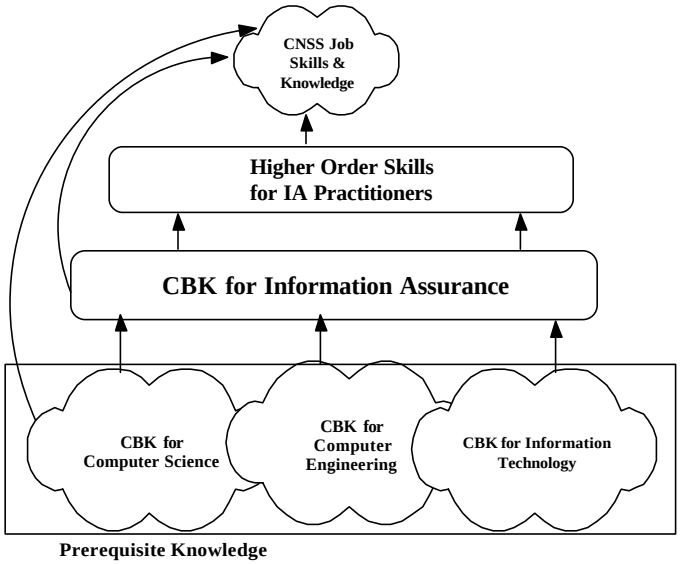

Figure 1. Curriculum Framework

2. Framework Structure

The overarching framework for connecting curricular entities is shown in Figure 1. There are four layers represented: the CBK for participating disciplines, the CBK for information assurance, higher order skills that graduates will develop as their education progresses (e.g.,

understanding the security implications of given combinations of software), and the accepted set of job skills (e.g., those specified in the Committee on National Systems Security (CNSS) Federal training and education standards for IA professionals [4]). The top layer could also contain the skills and knowledge needed for graduates to move on to postgraduate studies and engage in research in information assurance.

While the notion of layering knowledge implies a strictly hierarchical relationship between the layers, clearly some of the program outcomes rest directly on the CBK for information assurance or even prior knowledge brought in from the supporting disciplines. For example, CNSS 4011 requires that student have a familiarity with basic computer architecture concepts that would most likely be taught in a sophomore CS or Computer Engineering course.

While it is possible to infer sequence from the framework, we want to note that the way in which the IA curriculum is approached for instruction, i.e., in a bottom-up, top-down, or project-based manner, is an institutional decision. The hierarchical relationship suggested in Figure 1 is not meant to suggest that the material *should* be taught in a classic bottom-up fashion. In fact, we recognize that one of the most powerful paradigms for teaching computer security concepts is to embed appropriate topics in the context of a problem domain. For example, buffer overflow attacks (which account for the majority of network attacks) are easy to understand when added to a discussion about stack frames for high-level languages. When buffer overflows are studied is isolation in a security course, the discussion is more abstract. Similarly, the implementation of access control and reference monitors fits well with a study of the implementation of file systems in an operating systems course. It is our hope that the model proposed here when instantiated with skills and knowledge will help uncover opportunities to connect course content.

Each of the layers is described in the following sections. Once instantiated, we map backwards from the outcome down through the layers. The relation used is “needs to learn”. For example, in order to determine the fitness of a particular password scheme (which would be a higher order skill), we may need to understand how the password is stored and which cryptographic algorithm is used. In order to understand the strength of the cryptographic algorithm, we may need to understand basic number theory principles and algorithmic complexity. One interesting result when viewing the curriculum in this way is that we can identify outcomes that are not well supported by the curriculum. Additionally, we can easily identify taught material that does not directly support an outcome. The latter is not always undesirable, but this process at least

affords the opportunity to make an informed decision on the role of the topic in the curriculum. In the following sections, we will briefly describe the types of information in each layer.

Layer 1: Prerequisite Body of Knowledge

As noted earlier, information Assurance is a broad multidisciplinary field, drawing on knowledge from Computer Science, Computer Engineering, Mathematics, MIS, Political Science, Law, and many more. For this project, we chose to focus on students with a computer science and engineering background preparing to study computer security in a graduate program. As such, the information assurance topics rest squarely on the CS and CprE curricula, although they may use selected topics from other disciplines. The supporting disciplines of Computer Science and Computer Engineering each have an identified body of knowledge. Other disciplines, such as Information Technology, are under development. These are the topics thought to be essential for students study in their respective fields. The most mature project of this type is the Computing Curricula 2001. CC2001 defines fourteen content areas, each containing several sub areas. Sub areas are assigned the amount of time needed to cover the material, which provides an indication of the relative importance of the topic.

Layer 2: Information Assurance Body of Knowledge

The information assurance body of knowledge is comprised of disciplinary knowledge and skills from layer 1 as applied to the practice and advancement of information assurance needs, issues, and organizations. The information assurance body of knowledge is informed by all three levels of the curriculum framework and should be aligned to the other layers in a logical, coherent, and systematic manner. It is the technical “know how” and expertise that extends beyond what a typical computer science/computer engineer/information technology professional would need/be expected to know. For example, all computer science students might be expected to know operating system principles, concurrency, memory management, and so on (2). This would be considered a part of the layer 1 computer science core body of knowledge. The information assurance layer 2 skills that build on the computer science operating system knowledge might include concepts such as implementing the principle of least privilege, reference monitors, configuring and managing security tools, etc.

Layer 3: Higher Order Skills

The higher order skills layer depicted in figure two represents the skills and abilities that cut across the layer 1 and layer 2 topic areas. Regardless of the disciplinary foundation and the

articulation of that foundation to advanced technical IA knowledge, all IA professionals need higher order information assurance skills in the areas of risk assessment, modeling and mitigation; evaluation of the efficacy of competing security mechanisms, methodologies, and models, security requirements, standards, and legal implications and laws.

Layer 4: Job/Professional Level

The fourth and last layer at which we are considering information assurance knowledge and skills is at the job/profession level. This includes, but is not limited to, 1) job analyses provided by the CNSS [4], 2) skills recognized by given professional organizations for credentialing, e.g., the common body of knowledge for the Certified Information Systems Security Professional (CISSP) credential [5], and 3) skills needed in research and development.

3. Current Status

To date three workshops have been held, the outcome of which is a description of the general topics (equivalent to the "areas" level in the ACM/IEEE 2001 Computing Curricula). Four broad areas of knowledge have been identified, namely: cryptology, secure computing systems, network security, and management, policy and response. An example of one of the four content areas has been provided in Appendix A. We anticipate that the topics will now be reviewed by the broader community of information assurance educators to determine if the identified topics are sufficient. The next step in this project is to then flesh out body of knowledge with sub areas (equivalent to the "units" level in the ACM/IEEE 2001 Computing Curricula) and the relative importance of each unit as denoted by time.

4. References

[1] James A. Davis and Melissa Dark, "Defining a Curriculum Framework in Information Assurance and Security", Proceedings of the 2003 ASEE Annual Conference, Nashville, TN, June 22-25, 2003

[2] ACM/IEEE 2001 Computing Curricula. http://www.computer.org/education/cc2001/final/index.htm

[3] Information Technology Association of America survey, May 2002, http://www.itaa.org/news/pr/PressRelease.cfm?ReleaseID=1020695700

[4] The Committee on National Security Systems, National Training Standard for Information System Security Professionals 4011 http://www.nstissc.gov/html/library.html

[5] ISC^2 Common Body of Knowledge http://www.isc2.org/cgi/content.cgi?category=8

Appendix A: Example Topics in Cryptology

The development of cryptography
- First principles
  - Protecting confidentiality
  - Ensuring integrity
  - Guaranteeing authenticity
- Historical cryptography
  - Substitution ciphers
  - Transposition
  - Frequency-based cryptanalysis
  - Codes & Code machines

Fundamentals
- Block vs stream ciphers
- Chaining
- Threshold cryptography
- Zero-knowledge proofs
- Oblivious transfer
- Pseudo-random number generators
- Secret sharing
- Key management and key distribution
- Key space

Important symmetric algorithms
- DES
- AES
- Clipper / Skipjack
- RCn

Asymmetric algorithms
- Public key cryptography
- RSA
- Elliptic curve cryptosystem
- Digital Signature Algorithm

Cryptographic protocols
- Identification, authentication and authorization
- Role of encryption
- Frameworks for secure e-commerce
- Third-party certification authorities
- Single sign-on
- Electronic voting
- Electronic contracts & non-repudiation

Hardware implementations
- Cost/benefit analysis
- Enforcement
- Digital rights
- Vulnerabilities
- Crypto processors

Digital signatures
- Definitions & Benefits
- Mechanisms
- Certificates

Applications of cryptography
- Cryptography in the OSI model
  - IPv6
- IPSec
- Smartcards
- Biometrics

Public key infrastructure and certificate authorities
- Need for public key cryptosystem
- Need for public key infrastructure
- Public key certificate
- Key revocation
- Key recovery

Implementation issues
- Algorithmic weakness vs implementation weakness
- Secrecy of the algorithm is not a defense
- Types of attacks
- Overview of non-brute-force attacks
- Product certifications
  - Common Criteria
  - Commercial standards
- Key escrow

Cryptanalysis
- Strategies
  - Brute-force
  - Linear and differential cryptanalysis
  - Meet-in-the-middle/birthday attack
  - Timing analysis
  - Side-channel analysis
- Analysis of randomness
- Interception techniques
- Reverse engineering
- Hardware failures

Steganography
- Examples
- Analysis
- Defenses

Latest developments
- Chaffing and winnowing
- Recent algorithms
- New products
- Quantum computing effects on cryptanalysis
- Quantum cryptography