Information Assurance Technology Forum, September 14, 2001, Johns Hopkins APL

IATF Academic Education – A Different Perspective

Dr. Bruce Gabrielson, NCE

Booz Allen & Hamilton
900 Elkridge Landing Road
Linthicum, Maryland 21090
gabrielson_bruce@bah.com

Introduction

The theme of this forum is "Blending IATF, CC, C&A, IA Policy, & NSTISSP #11". These documents have not been prepared as educational documents, nor are they intended as such. They are intended to give information systems developers, operators, and testers practical ways to implement primarily the technology component of Defense-in-Depth (DiD). However, DiD has three components— people, technology, and operations. This presentation will deal with the people issues, how to educate people to implement DiD.

Presentations we normally get at this forum are focused on the DoD side. This presentation will be different in that it will focus on the academic side. I could have addressed this subject from why we need material like this in the colleges and universities and why the IATF is a good document to use to education purposes. I felt to do so would have been preaching to the choir. The IATF has the subject material and has been accepted by the DoD and industry. It is also written in a way that professionals can understand it. The worthiness of the IATF is a given to this audience. However, using this approach would have missed the practical side and the lessons I learned form trying to move the IATF to the academic environment. Preparing the IATF so that it can maximize its benefits to the schools and students is a little different from maximizing benefits to governments, vendors, companies in general, and it yields different results.

In order to effectively understand and implement all the academic issues, one must first understand how students with varied backgrounds can learn to apply the entire systems engineering process to specify, develop, test, field, and operate secure systems. How can we push the entire systems engineering process into the academic mainstream of computer science thinking?

Motivation

Many organizations today are struggling with how to distill the myriad of security guidance and policy into a manageable process. Furthermore, vendors of information assurance (IA) solutions demand a strong business case for complying with product certification requirements as set forth in Government policy documents. The business case exists for increasing the knowledge level and availability of security professionals. I believe one method of addressing this need is transforming the IATF to satisfy requirements for the academic environment.

With many years teaching and training course experience plus the advantage of a formal teaching credential under my belt, I approached development of an academic course based on the IATF by asking myself eight specific questions.

1. What's an acceptable academic forum to present a course based on the IATF?
2. Who are the projected students?
3. How do I determine the how marketable the course would be and how do I market it to students?
4. What are the basic knowledge skills necessary to understand the IATF material?
5. Will I have human relations issues?
6. What should I choose for my lesson unit delivery model?
7. What knowledge does the IATF author want to convey?
8. Can I develop a lesson unit from existing material?

The Approach

For the next few minutes we shall discuss some of the issues I faced and lessons learned in answering these questions.

Question 1 – What's an acceptable academic forum to present a course based on the IATF?

I began my quest by sending emails to two local four-year colleges and two community colleges early in the summer. Each of these institutions offered a "traditional" computer security course. On the surface you might think that local colleges, particularly ones I had dealt with in the past, would have been happy to hear my proposal. In reality, some department chairs didn't even have the courtesy to respond to my initial contacts, and I literally had to walk into their offices to get them to talk to me. Why would that be the case? After listening to their concerns, I realized that many CS departments simply choose to move slower than the rate of technology advances. A computer science course based on a four-year old textbook would need to be written at such a basic level that technology advances wouldn't matter. I'm not sure any college textbook written about technology implementation in the Information Assurance field would still be current after a few years. The IATF is nearer to current technology. The academic community likes to pride itself in being current, but I didn't see this at some of the schools I approached.

Therefore, my first lesson learned and my first advice to someone in a similar situation, is go visit the department chair with a hardcopy of the IATF in your hand. At least you will get your foot in the door.

Why would I contact department chairs at both junior colleges and four-year colleges? Think about the IATF itself for a moment.

Briefly, the IATF is based on the concept that the technology of an information infrastructure is comprised of communications networks, computers, databases, management, applications, and consumer electronics that all exist at the global, national, or local level. It describes information infrastructures, the information infrastructure boundaries, the information assurance framework areas, and general classes of threats. DiD is the general theme for approaching technical solutions. The DiD objectives are organized around the four Defense-in-Depth technology focus areas:

- Defend the Network and Infrastructure
- Defend the Enclave Boundary

- Defend the Computing Environment
- Supporting Infrastructures

Thus, the IATF is focused on the application of today's technology to correct current operational security needs.

In contrast, traditional computer security classes have tended to concentrate on the theoretical aspects so they can provide stable information flow to students over a multi-semester period. Unfortunately, technology has moved and continues to move quickly in the information assurance field. Four-year institutions often call classes that address applied engineering techniques as seminars. Community colleges pride themselves in offering courses that are of immediate benefit to practitioners who can apply what they learn. Their responses were much more positive than the responses I received from the four-year institutions.

To me, information in the IATF sounds more like applied class material rather then theoretical class material. Although I consider the IATF material more thorough and focused at higher knowledge level, the forum for my course was likely to be an undergraduate class (or classes) at a school where the student body had the most interest.

Question 2 - Who are the projected students?

Classes aren't offered unless they have acceptance by both the faculty and the students. My concern was that the IATF might be considered too difficult for undergraduate level students by their computer science department. Therefore, initial contacts were intended to identify a suitable academic environment for course presentation based on both student and department interest. Interestingly, the community colleges were the most supportive of the suggestion, an indication that they try to closely follow the immediate need interest of their local student body, and they indicated that the material would fit with their curriculum focus.

I also read this response as community colleges cater not only undergraduates but to individuals who have graduated and are interested in immediately applicable technical courses. These are the students who might take this course.

Because of my projected school environment, I decided that I needed to assess my potential student market in this environment before deciding on a college for the initial course offering.

Question 3 – How do I determine the how marketable the course would be and how do I market it to students?

This was a tricky question posed by nearly all college administrators. Classes aren't taught unless a minimum number of students sign up. In reality to be able to offer this course to the widest number of students who might sign up for it, I needed to present the course in a manner desirable to students who have only a basic understanding of computer science. Anything related to computer security is likely interesting to a student, but my textbook and lesson material must support this interest.

In this regard the IATF met my needs easily. Think about how contributors prepare material for the IATF. They know their target audience and write to it directly.

IATF customers include system users, managers, and security officers or administrators who must interact with security engineers and architects to design comprehensive IA solutions. The target audience includes:

- Operational personnel
- Decision makers
- Scientists and researchers
- Commercial product and service providers
- Standards bodies and consortia

The audience forced the IATF to be written for a widely diverse mix of background and knowledge levels. This audience has not been students. I needed to be sure the IATF could support a student audience so I looked a little closer at the knowledge background needs.

The current IATF is already targeted for a wide variety of typical users. I believe this audience can be expanded with minimal IATF repackaging to include typical computer science students.

Question 4 – What are the basic knowledge skills necessary to understand the IATF material?

College level courses are not training courses. You really can't approach a university department with a traditional training class and expect a positive response. To be successful, you need to first develop a delivery model of your subject matter consistent with traditional educational thinking.

An instructor needs to understand the existing body of knowledge the student requires in order to understand the material and the new knowledge needed to apply an IA program successfully. Looking at the actual background knowledge necessary to understand the material, primarily declarative knowledge enforcement with some procedural enforcement at both the awareness and learning level (or higher) as shown in Table I is indicated for the IATF.

Table I – Suggested Specific Knowledge Breakdown

Declarative Knowledge	Procedural Knowledge
IA Technology Concepts and Architectures O/S – UNIX/NT Protocols – TCP/IP System Administration Network Security Laws/Regulations/Policies Human Relations	Using Security Tools Interpreting Results Problem Solving

Have contributors to the IATF considered how much time should the audience take reviewing a section before achieving the desired level of understanding or taking the desired action? This is an important question since requiring the reader to absorb too much information without having the proper background can become an overload. Addressing this perspective forces IATF contributors to ensure they provide background material and keep their writing short and to the point. I've written four and read many other textbooks over the years and testify that very seldom is this the approach taken by an author after the first few chapters.

Contributors to the IATF are required to provide the necessary background material up front before addressing their specific technology or process area. Therefore, a class based on the IATF should be readily understood by students who have met the minimum prerequisites necessary for other similar advanced computer science or engineering classes at their college.

Question 5 - Will I have human relations issues?

Notice in Table 1 that I've included human relations. I previously mentioned that the field of computer security is interesting to students. One of my concerns with this interest is the glamour associated with computer hacking. I wouldn't want this course to help train and unleash an army of hackers on the world. Therefore, the material and delivery for an IA course must be presented is such a way that it reinforces its acceptable use, the ultimate dilemma of any IA course developer.

To prepare a strategy for IA course development, a little psychology theory related to affective conditioning might help. An individual's moral attitudes are often in a state of flux until their early twenties[1], with many hackers falling into this age group. However, once adulthood is reached, attitudes become firmly established. To attempt affective conditioning is an extremely difficult task in an adult, one well outside the scope of most traditional academic programs. Affective conditioning is also considered a moral issue because changing the way a person thinks about something is a very sensitive subject.

A pre-screening process for student selection is impossible. Incorporating a unit of laws and regulations instruction at the beginning of the course helps to "set the stage" for the following technical material. In addition, using a delivery model that would allow a conditioning format could potentially be used for further conditioning efforts.

The approach I investigated and that works in a traditional delivery model is to provide conditioning using the non-direct technique of describing the potential 'enemy' in terms of personality and motivations. In other words, present cases, examples, and homework or test problems using the good guy/bad guy approach. It's subtle but it is a proven conditioning approach.

Question 6 - What should I choose for my lesson unit delivery model?

This question is absolutely critical to course development for both instructors and students, but likely not of much interest to this body. I'm including an in-depth discussion here for the benefit of the academic community.

While some instructors focus on how to deliver, I personally was looking to satisfy two needs with a delivery model:

- How to get the material across and understood
- How to decrease the turn-around time that might be needed to deliver the new material to students with various experience levels.

---

[1] *McMahon, Frank, Psychology, The Hybrid Science, Prentice-Hall, New Jersey, 1974.*

Basing the delivery model on what is envisioned as the expected outcomes (learning, conditioning and structured thinking), the potential technical diversity of student population, and learning theory for adults lead me to select the Mastery Model for course structure and delivery. Mastery Learning is a teaching technique founded upon the assumption that given sufficient time and appropriate materials, most students, regardless of their previous knowledge level, can achieve the desired outcomes.

In this model, the objectives of each unit are first stated, and then existing student skills are assessed. By doing so, a determination is made if the student already has the requisite background to begin the unit of study, or to establish if the student has already mastered the unit's training objective. Following the unit of study, a post-assessment is also required. The pre-assessment/post-assessment scenario allows learning reinforcement to take place by using the recitation theory and programmed learning[2]. The recitation theory is repeating to yourself what you have just learned. In our case, an immediate final test following a block of instruction helps to reinforce the learned unit.

The traditional Mastery Model supports three learning tracks, the main line, the self-pacing enrichment, and the alternative (correctional) track. This approach also has the appeal of being multi-sensory in nature and provides instructional designers the vehicle to meet a variety of multi-modality[3] learning styles, particularly Individually Prescribed Instruction (IPI)[4] techniques. Individualization is promoted within two of the three tracks. In an adult course model, it is the student who decides, based on the pre- assessment, what training track should be chosen. Especially for alternative track self-study learning units, this technique allows for self-paced training and the use of additional learning materials as necessary[5].

The Mastery Model is suggested for lesson unit development. It allows for alternative student selected self-study tracks.

Question 7 – What knowledge does the IATF author want to convey?

How is it possible that I could get near the end of my study and finally start to look at the material itself? Here is the real test of using someone else's text for a course you deliver. The final part of my effort was to develop my lesson plans, alternative study/reading lists and the assessment techniques. I had to put myself in the Contributors place and ask: "What do I want a student to understand or do after it has read an IATF chapter or section?"

IATF contributors often provide data dumps rather then expected learning outcomes. The problem has been my interpretation of what the basic concepts the author of the chapter wanted to convey if it wasn't clearly stated. The reader should understand that the IATF contains numerous sections and subsections, most written by more then one author. Whatever I interpret

---

[2] *Programmed learning is presentation of material in an organized sequence that follows an overall program (model). It is essentially self-instructional. An example would be sentence/paragraph structure with fill in the blanks as you proceed through the training unit. However, by structuring the pre-assessment and post-assessment test with fill in the blank questions, reinforcement will take place.*

[3] *Multi-mode: various methods of teaching groups or individuals*

[4] *Individually Prescribed Instruction, Learning Research and Development Center of the University of Pittsburgh, 1966.*

[5] *Gabrielson, Bruce, Psychological Aspects of Sensitive Training Course Development, Federal Information Systems Educator's Association (FISSEA) Conference, February 15-16, 1995. Gaithersburg, MD.*

as important will likely be different than someone else's interpretation. One IATF lesson learned from my review is that the IATF needs a summary of important concepts paragraph developed by the author of each section.

The author's most important concept wasn't always stated in the IATF's introduction to the topic, but it should be reflected at some point in the text. It isn't always readily available.

Question 8 – Can I develop a lesson unit from the existing IATF material?

The alternative study/reading list required by the Mastery Model was not too difficult to develop. The IATF already lists references that fit well within my model.

Probably my hardest task, and one I haven't finished yet, is to go through each chapter or section of the IATF and pull out in words stating what the student should understand after the unit of study. This is called an evaluation statement in the model.

I've initially approached this task by developing a couple of paragraphs for each section or chapter and then simply listing the most important concepts I feel should be conveyed to a student. At the same time, I've developed an assessment question for each concept I've listed. My Mastery Model requires an outline that once completed, helps in the lesson unit development.

How I perceive the important points might not necessarily be what the author wanted, but at least it is a start. The final lesson unit for each delivery block evolves from each goal and evaluation statement.

Now I have a new question: Will my course succeed?

I can't answer this question yet.

Mastery Model Statements

Course Goal Statement

- States the goals the student will be able to meet after each lesson unit.

Course Evaluation Statement

- States in measurable terms specifically what each student will be able to use, convey or apply after each lesson unit.

Lesson Plan Summary - Main line is the primary training track

- Primary Training Blocks for each lesson unit with immediate feedback reviews of pre/post-assessments
- Suggested alternative tracks to include selected papers and sources