Proceedings of the 9th Colloquium for Information Systems Security Education
Georgia Institute of Technology
Atlanta, Georgia, 6-9, June 2005

A Methodology for Developing and Disseminating Curriculum Resource Material in Information Security

Melissa Dark, Linda Morales, Connie Justice

Abstract *– This paper discusses the work at three collaborating institutions to develop, test, and disseminate educational materials on secure network protocols that can be used in both undergraduate and graduate studies. The materials will be developed in alignment with existing education/training standards in information assurance and security. In addition, the authors have created a set of requirements for development of the materials that enables their reuse by faculty at other institutions. This paper describes our methodology for creating reusable learning modules in secure protocols*[1].

Index terms – Secure protocols, course and curriculum development.

I. Introduction

Educational institutions across the country have experienced a rapid growth in the discipline of information security and assurance (IAS). Due to a scarcity of faculty experienced in the IAS field, many faculty members with little training in the discipline find themselves preparing to teach courses in the area. These faculty can spend a considerable amount of time creating their own resource materials and thereby duplicating work done by many others in similar situations. While the number of textbooks dealing with information assurance and security has proliferated, there is a shortage of appropriate, high quality instructor support material and the time commitment required of instructors who are teaching a course in information security for the first time is considerable. This start-up time will be shortened if high quality, reusable resource materials are developed and become available. We feel that the classroom experience for the instructor and the students can be greatly enhanced with the use of such high quality, reusable support materials.

This paper describes a project aimed at mitigating the shortage of curriculum resource material in information security and assurance. The primary goal of the project is to provide standards-based instructional resources of high quality that in turn facilitate the teaching of information security and assurance, specifically in the area of secure protocols. These materials are for use at the home institutions of the authors (Purdue University, Indiana University-Purdue University at Indianapolis, and Texas A&M University-Commerce). In addition, we intend the materials to be usable by faculty at other institutions. To enable reuse, we have created a methodology for developing instructional materials and associated teaching resources. We call this methodology *Course Mentor*. The methodology identifies the components of a successful instructor resource package. The methodology also calls for internal and external evaluation of the materials to assure uniformity and quality in materials produced by the project. The remainder of this paper 1) describes the Course Mentor methodology and the associated evaluation, and 2) provides an example of work to date.

II. Course Mentor

The primary objective of Course Mentor is to provide resources that emulate the mentoring provided by an experienced faculty member. We have identified a number of design requirements to promote the effectiveness of Course Mentor materials. Among the requirements are:

- Course Mentor materials will be reusable and easily adoptable by faculty members at other institutions.
- Course Mentor materials will be developed in a modular fashion to allow adopters to create a custom-designed resource package suited to the needs of their curriculum, courses, and students.
- Learning objectives will be included in each Course Mentor module.
- Learning objectives will be clearly articulated as outcome statements.
- Learning objectives will be mapped to relevant standards, such as CNSSI [2] and ISC^2 [3].

[1] *This work is supported by the National Science Foundation SFS-0416901 and SFS-0423803, however, any opinions, findings, and conclusions or recommendations expressed in this material are those of the panel and do not necessarily reflect the views of the National Science Foundation.*

- Assessments to evaluate the realization of the learning outcomes will be included with each Course Mentor module.
- Assessment will be aligned with associated learning objectives.
- Materials developed for each Course Mentor module will be aligned with the associated learning objectives.
- Course Mentor materials will be developed according to a uniform template.
- The Course Mentor methodology will identify a minimum set of resource materials required for easy adoption.
- Course Mentor materials will undergo a rigorous evaluation process including peer review and evaluation led by a trained evaluator.

The components for a Course Mentor module are listed in Table 1 below.

Course Mentor Module Components
1. Title
2. CNSSI mapping
3. ISC^2 mapping
4. Length of Instruction
5. Learner Analysis
• Description of target audience including:
- Stable similarities
- Stable differences
- Changing differences
6. Learning Task Analysis
• Identification of declarative knowledge
• Identification of procedural knowledge
• Identification of principle knowledge
• Identification of procedural knowledge
- Annotation regarding the position of the learning tasks in a curriculum roadmap (both for undergraduate and graduate programs of study)
- Prerequisite modules (sequencing information that suggests an order in which to teach the modules)
- Prerequisite knowledge (outside the scope of the modules)
7. Instructional Strategy
• Module objective
• Learning outcomes (include mapping to assessment questions)
• Suggested readings
• Suggested learning activities (mapped to learning task analysis/learning outcomes)
8. Assessment
• Assessment mapping (mapping to learning objectives)
• Assessment
- Questions
- Answer key
- Grading rubric
• Homework
- Questions
- Answer key
- Grading rubric
9. Instructional Material (Depending on whether this is a lecture module or lab module, we will develop either Instructor Material or Lab Material).
• Instructor's Guide
- Story line (progression of topics, with rationale for the sequence)
- Instructor tips
▪ What do students typically have trouble with
▪ What I do in these situations
▪ Metaphors
- One or two worked-out examples to present in class. (If applicable, include a sequence for writing things on the board)
• Lab Material (if applicable)
- Scenario
▪ Abstract
▪ Problem
▪ Analysis
▪ Actions taken
▪ Recommendation
- Answer key
- Grading rubric
• Slides for lecture
• Slides of figures

Table 1 Course Mentor Module Components

Table 1 lists all of the components of a completed Course Mentor package. The sequence of events to develop the Course Mentor package differs from the order of the components in the final package.

The first step in the development of a Course Mentor module is to clearly articulate the learning objectives as outcome statements [1]. Outcome statements are statements of what learners should know and be able to do at the end of instruction. The learning objectives will be peer-reviewed by project collaborators and also validated using the CNSSI and ISC^2 education/training standards. Modifications will be made based on peer review. After learning objectives have been finalized, then assessment items will be developed for each learning outcome. While assessment items are usually used for purposes of determining student grades, in the context of this project we will use student performance data to measure the effectiveness of the Course Mentor-facilitated materials.

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

The next step is to develop other components including; 1) an instructor's guide with a progression of topics and their rationale, 2) a commentary describing concepts students typically have trouble with and suggestions for what to do in these situations, metaphors, worked-out examples, and 3) lecture notes. In addition, there will be an extensive collection of homework problems and solutions, together with practice problems and solutions in the style of guided exercises.

Course Mentor will also include information about target audience and length of instruction. During development we will conduct learning analysis and provide a description of the target audience for the collaborating schools. We feel it is important to describe the target audience so that potential adopters can determine the extent to which their audience is similar/dissimilar. During peer review we will ask other faculty to determine if the materials would be appropriate for their students. Therefore, prior to completion of the project, learner analysis will be updated to reflect peer review. Adopters will also want to know the approximate length of instructional time the module is expected to require. Therefore, an instructor will be able to see what the module of instruction is, the target audience and the approximate length of time it will take to present the material.

Course Mentor will also include a learning task analysis for each module. The purpose of conducting a learning task analysis is to qualify the nature of the learning task. Learning task analysis will be done after the topical content has been determined in full. The aim of the learning task analysis is qualify the type of learning that is to occur, e.g. are students to learn 1) facts, 2) concepts, 3) principles, 4) how to apply principles, 5) how to analyze problems, etc. Once the nature of the learning task is determined, instructional strategies can be selected based on appropriateness for the learning task. In addition, learning task analysis can often help sequence learning in a way that progresses from lower to higher level thinking. Course Mentor will include the strategy of instruction that includes suggested readings, worked out examples, metaphors, lecture notes, homework assignment (instructional tools if you will), as well as the learning and module objectives. The instructional strategy will revisit the nature of the learning task at hand (derived from the learning task analysis), elaborate on why particular instructional tools were selected given the nature of the learning task, and suggest sequencing when appropriate.

The assessment component of the module will aid the instructor in measuring students' understanding of the material presented and is an essential part of the success of the course. The assessment component will include possible test questions and/or performance assessment that can be used along with an answer key and grading rubric. During the development of the assessment items and instruments, we will utilize as an assessment blueprint and item analysis to test the validity of the assessment items/instruments. In this project, we will strive for content and construct validity meaning that the assessment items should reflect both the content as well as the nature of the learning task.

Course Mentor requirements were developed using a focus group of the collaborating faculty. By developing materials in this manner, we believe that Course Mentor will promote ease of adoption, and help the students, and the instructors who prepare them, for the professional environment and professional credentials.

III. EVALUATION

The evaluation of this project will be essential to assuring that the instructional materials are reusable. The evaluation protocol is depicted in Figure 1.

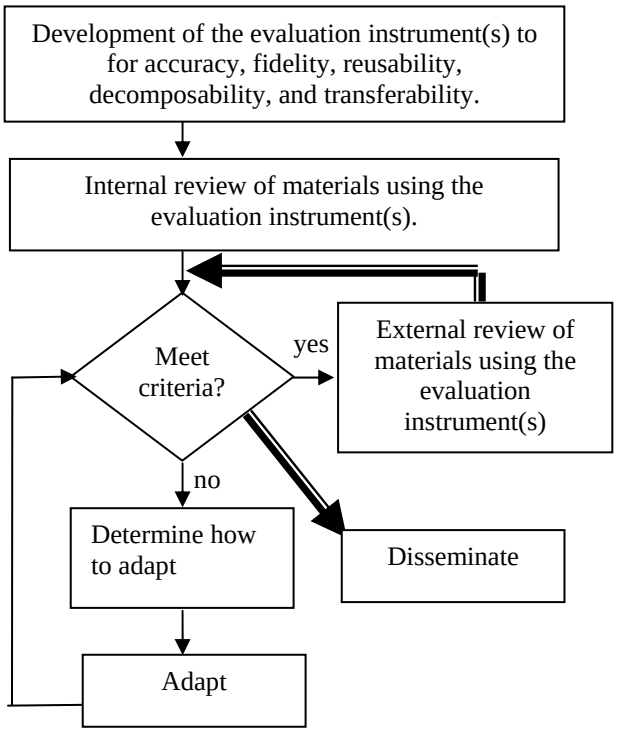

Figure 1 Course Mentor Evaluation Protocol

As has already been stated, the idea behind this project is to be able to provide high-quality reusable teaching material to faculty who need to teach a unit/course in secure protocols and have limited experience teaching the topic. Therefore, the evaluation focused on the extent to which the materials meet this goal.

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

The second box is Figure 1 is the review of the materials. We plan to develop an evaluation instrument(s) that will determine the extent to which the materials have the following criteria of merit: accuracy, fidelity, reusability, decomposability, and transferability. Each of these is further defined in Table 2.

Accuracy	the degree to which the materials reflect technical accuracy
Fidelity	the degree to which the materials are aligned to the learning objective(s) the degree to which the test items are aligned with learning objectives and curriculum materials
Reusability	the degree to which the materials can be reused by faculty at other institutions where learning objectives are held constant
Decomposability	the degree to which the materials are modularized, so that they can be decomposed and pieces can be reused where learning objectives are held constant
Transferability	the degree to which the materials represent areas of greater need and will therefore be more transferable

Table 2 Criteria of Merit for Evaluation of Curriculum Materials

We will use both internal and external peer review to evaluate the materials based on the criteria listed in Table 2. Internal review will be designed by the evaluator and conducted by the collaborating faculty. Each participant will apply the evaluation process to his/her own work as well as to the work produced by other collaborators. The evaluators will work through the evaluation model as depicted in Figure 1. First the internal evaluators will review their own materials and then each others' materials to evaluate fidelity, reusability, decomposability and transferability. For example in the area of fidelity, reviewers will identify where materials fail to align to the learning objectives so that corrections can be made.

Once the materials meet the criteria, then they will be forwarded to external reviewers. We plan to use two types of external reviewers 1) subject matter experts, and 2) potential adopters. The subject matter experts will be selected for a) content expertise in secure protocols, and b) for curriculum design expertise. We plan to select external subject matter experts from both academe and well as industry. The potential adopters will be purposively selected to represent different institutions, different levels (undergraduate and graduate), and different program types (computer science and information technology). External reviewers will play different roles to provide a comprehensive review of the materials for accuracy as well as fidelity, reusability, decomposability, and transferability.

IV. A Course Mentor Example

To date development for the applied secure protocols course includes the module definitions, learning outcomes and mapping to the CNSSI [2] and ISC^2 [3] standards. While developing the modules for the secure protocols course we examined essential topical areas. We collectively came up with 6 key areas that were critical [4, 5,6]. The key areas are: 1) background of security, 2) cryptography basics, 3) basic protocol building blocks, 4) applied protocols, 5) secure protocol applications, and 6) key management. Each of these key areas will represent one or more module(s). Each module includes multiple subtopics. The following list shows subtopics for each of the modules.

1. Background
    a. Security Goals
    b. Security Model
2. Cryptography Basics
    a. Symmetric Key Cryptography
    b. Public/Private Key Cryptography
    c. Hash Functions
3. Basic Protocol Building Blocks
    a. Digital Signatures
    b. Certificates
    c. Fair coin flips
    d. Mental poker
    e. Zero-Knowledge Proofs
    f. Blind signatures
    g. Oblivious transfer/signatures
    h. Authentication
    i. Time stamping
    j. Non repudiation
    k. Bit commitment
    l. Electronic voting
    m. Digital Cash
    n. Digital Certified Mail
4. Applied Protocols
    a. Kerberos
    b. PKI
    c. Digital Signatures
    d. Certificates
    e. RADIUS
    f. Authentication Protocols
5. Secure Protocol Applications
    a. IPsec
    b. PGP
    c. Virtual Private Networks
    d. SSL/https

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

e. Secure email protocols
f. Wireless secure protocols
g. SSH/sftp

6. Key Management
   a. Key creation
   b. Key distribution
   c. Key disposal
   d. Key revocation

At this time we are not mapping to the ISC^2 standards because they are undergoing significant change. We have mapped to CNSSI 4014 (Information Systems Security Officer) [2] as represented by Table 3 below.

4014	Develop Certification and Accreditation Posture	
	Implement Site Security Policy	X
	Enforce and Verify System Security Policy	X
	Report on Site Security Status	
	Support Certification and Accreditation	

Table 3 Initial CNSSI Mappings

One of the subtopics in the Basic Protocol Building Blocks module is Digital Certificates. One of the subtopics for the Applied Protocols module is PKI. One of the subtopics in the Secure Protocol Applications is secure email protocols. Here we provide sample learning outcomes for these subtopics respectively:

Digital Certificates

Upon completion of this module students will be able to:

- Describe digital certificates
- Describe a scenario that illustrates the need for digital certificates
- List some applications that use digital certificates
- Describe the function of a Certificate Authority (CA)
- Describe how a digital certificate is created
- Describe how a digital certificate is used
- Describe how a user can determine if a digital certificate is revoked
- List some reasons for revoking a digital certificate

Public Key Infrastructure (PKI)

Upon completion of this module students will be able to:

- Define Public Key Infrastructure (PKI)
- Define components of PKI
  - Trust hierarchy
  - Issuing and revoking certificates
- Identify the applications of PKI:
  - SSL/HTTPS
  - Secure e-mail (signed and encrypted)
  - Digital signatures
  - Data encryption
  - Network data protection (VPN, wireless)
  - Secure instant messaging
- Define digital certificates
  - X.509
  - Trusted entity assets
  - Enforcing policies for issuing certificates.
- Analyze PKI to identify potential vulnerabilities

Secure e-mail

Upon completion of this module students will be able to:

- Implement Pretty Good Privacy (PGP) as a means to provide secure email
- Identify the vulnerabilities and limitations of Pretty Good Privacy (PGP)
- Analyze PGP to identify potential vulnerabilities
- Identify secure e-mail protocols and plan for use of each

A peer review between the authors was conducted for this initial stage and then we started the development of assessment items/instruments. The sample below includes some of the assessment questions that were written for Digital Certificates and PKI.

A. Assessment Questions – Digital Certificates

Learning objective: describe digital certificates.

Assessment question: describe digital certificates.

Answer key: The purpose of a digital certificate is to provide verification that a public key belongs to a particular user. Digital certificates are issued by a trusted certification authority. The public key and owner's identification data are stored in the digital certificate, along with a hash of this information which has been digitally signed by the certification authority. The certificate may contain additional information (such as version number, serial number, CA's unique identifier, period of validity, etc) as required by the protocol used for creating the certificate. Users contact the certification

ISBN 1-933510-99-4/05/$15.00

authority when they wish to retrieve public keys belonging to other users.

Learning objective: describe a scenario that illustrates the need for digital certificates.

Assessment questions: describe a scenario that illustrates the need for digital certificates.

Answer key: Bob and Alice want to exchange confidential messages. They do not trust each other, but they both trust Trent (a certification authority). Bob sends his public key to Trent who creates and stores Bob's digital certificate. Alice sends her public key to Trent who creates and stores Alice's digital certificate. Alice and Bob can communicate with Trent to retrieve each other's certificate. (They may instead communicate directly and send their certificates to each other). They may now verify that the public key they have received belongs to the correct individual. Once they have completed the verification, they can conduct their confidential communication. (For example, they may use the public keys to exchange a secret session key.)

Alice wants to open a secure account with e-widget.com. e-widget's system assigns secure password, uses Alice's public key to encrypt the password, and sends it to Alice via e-mail. To prevent Mallory from gaining access to secure passwords, e-widget requires anyone who wants to open secure account must have a digital certificate. Alice sends her public key to Trent who creates and stores Alice's digital certificate. e-widget obtains Alice's certificate from Trent, encrypts her secure password with her public key and sends the encrypted password to Alice.

Learning objective: list some applications that use digital certificates.

Assessment question: list some applications that use digital certificates.

Answer key:

a. Secure e-mail
b. Electronic banking
c. e-commerce

Learning objective: describe the function of a certification authority (CA).

Assessment question/answer key: a certification authority is a trusted entity that that creates and stores digital certificates. The CA also stores a list of revoked certificates. The CA services requests from users to:

a. Create new digital certificates
b. Send a copy of an existing digital certificate
c. Send a list of revoked certificates.

B. Assessment Questions – Public Key Infrastructure

Learning objective: define components of PKI

Assessment question: **Fill in the blank:** The PKI infrastructure is based on _____.

Answer key: trust models.

Learning objective: define components of PKI.

Assessment question: list the component of PKI.

Answer key: PKI consists of

- A Certificate Authority (CA) issues and verifies digital certificates.
- A Registration Authority verifies credentials of users requesting digital certificates.
- A certificate management system.

Learning objective: describe PKI's four trust models.

Assessment question: describe PKIs four trust models.

- hierarchical trust model : single root CA
- Distributed trust model: root CA's sign each others certificates
- Web-based trust model; users need to trust sites they are visiting
- User-centric trust model: Pretty Good Privacy (PGP)

V. NEXT STEPS

To date, learning objectives for Digital Certificate and PKI have been developed, peer reviewed internally, and revised. With that done, lectures notes and other materials are being prepared according to the Course Mentor module components. Internal peer review will be conducted during module development. After the module is complete it will be submitted to the external reviewers. Additional modules for a course in Secure Protocols will be developed. The course will be taught in fall 2005 at IUPUI and at Texas A&M University-Commerce using the Course Mentor materials. Student evaluations and assessments will be used to examine and revise the materials. The materials will be evaluated according to the evaluation protocol described in Section III.

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

VI. Conclusions

In this paper we have described a methodology to systematically develop instructional materials. By this we mean that we will translate principles of learning and instruction into instructional materials, activities and information resources. We will intentionally and thoroughly use evaluation to enhance the effectiveness of the materials and resources as they are developed to improve their integrity as well as at the end to render judgment for the broader community. Our goal is to design an instructional solution in the area of secure protocols that is functional and appealing for the end users; our students, other faculty, and their students. By accomplishing the above, we hope to contribute to information systems security education in a useful and meaningful manner.

VII. References

[1] How to Write and Use Instructional Objectives. 6th Edition. N. Gronlund, Prentice Hall, 2000.

[2] CNSSI. http://www.cnss.gov/full-index.html

[3] ISC^2. https://www.isc2.org

[4] Applied Cryptography, B. Schneier, 1996 John Wiley & Sons, Inc.

[5] Network Security Essentials, Applications and Standards, 2e. William Stallings. Prentice Hall 2003

[6] Corporate Computer and Network Security, Raymond R. Panko, Prentice Hall, 2004.

ISBN 1-933510-99-4/05/$15.00