Roadblocks in Developing New Security Professionals: Missing Foundations

John A. Tesch, et al

Colorado Technical University
Colorado Springs, CO
jtesch@coloradotech.edu

Agenda

- Security Teaching Resources
- Traditional Approaches For Teaching Security
- Foundation Body of Knowledge
- New Age Teaching Tools
- Conclusions

Security Teaching Resources

Are our resource tools good enough?

- **Academic Texts?**
- **B&N Books?**
- **Vendor Courses?**
- **In-house Courses?**
- **University Courses – Bachelors?**
- **University Courses – Masters?**

But, are we effective? Another issue.

Problem Statement

We are not meeting our course objectives (teaching responsibilities) because many STUDENTS are not adequately prepared for the material we are presenting.

Problem Teaching Examples

Example #1

A student is enrolled in an intense one week CEH course.

Lesson objective : Trace the steps in a SQL Injection Attack.

Student did not complete objective. –

- **Did not understand basic architecture of a relational database**
- **Did not understand the structure of a SQL statement**
- **Did not understand resulting root level access**

Takeaway – Student follows the steps successfully in the lab manual but cannot apply the material to the work environment

Problem Teaching Examples

Example #2

A student is enrolled in basic digital forensic course.

Lesson objective : Examine the addresses on a FAT Table.

Student did not complete objective. –

- **Did not understand the architecture of a FAT file system**
- **Did not know how to use a hex editor**
- **Did not know how to use DOS/Linux/Unix commands**

Takeaway – Student cannot complete the lesson because of the amount of background knowledge required

Problem Teaching Examples

Example #3

A student is enrolled in security network course.

Lesson objective : Examine the stages of a SYN attack

Student did not complete objective. –

- **Did not know how to locate and download a sniffer tool**
- **Did not know how to capture packets**
- **Did not know the format of the packets**

Takeaway – Student cannot complete the lesson because of the amount of background knowledge required

Traditional Approaches to Teaching Security

- Limit the classes to just qualified students
- Help the weak students “catch up”
- Ignore the weak students
- Blame the course designer for too difficult level of objectives
- Blame admissions for placing the students

Computer Body of Knowledge Areas

BS in Computer Science – Typical Courses

- **CS 104 Problem Solving Concepts with C++**
- **CS 115 Programming with C++**
- **CS 146 Introduction to Unix**
- **CS 215 Intermediate C++ Programming**
- **CS 230 Data Structures**
- **CS 242 Computer Architecture**
- **CS 250 Database Design**
- **CS 265 Algorithms**
- **CS 340 Operating Systems**

Security Body of Knowledge Areas

BS in Security – Typical Courses

- **CSS 150 Foundations in Security**
- **CSS 200 Principles of Network Security**
- **CSS 250 Security Risk Management**
- **CSS 300 Vulnerability Assessment and Management**
- **CSS 320 Process Engineering (Project Management)**
- **CSS 350 Forensics I**
- **CSS 351 Forensics II**
- **CSS 380 DRP/BCP**
- **CSS 440 Security Compliance and Ethics**
- **CSS 450 Security Capstone Course**

Foundation Body of Knowledge (FBK)

The Foundation Body of Knowledge is created by locating common elements in both the Security Body of Knowledge and the Computer Body of Knowledge

Process:

- **Find a mapping from the Security Body of Knowledge Areas to the Computer Body of Knowledge Areas (or other disciplines)**
- **Limit the mapping to the least amount of information (learning objects)**
- **Verify the learning objects to the lesson objectives**
- **Repeat for all Security Body of Knowledge Areas**

FBK Process

SBK – Security Body of Knowledge

CBK – Computer Body of Knowledge

FBK - Foundation Body of Knowledge

LO – Learning Objects

$$FBK_i(SBK_i, CBK_i, LO_i)$$

Create security foundation courses based on the FBK

Problem Teaching Example

A student is enrolled in an intense one week CEH course.

Lesson objective : Trace the steps in a SQL Injection Attack.

Student did not complete objective. –

- **Did not understand basic architecture of a relational database**
- **Did not understand the structure of a SQL statement**
- **Did not understand resulting root level access**

Takeaway – Student follows the steps successfully in the lab manual but cannot apply the material to the work environment

FBK Process – Example

Lesson objective : Trace the steps in a SQL Injection Attack.

Student did not complete objective. –

- **Did not understand basic architecture of a relational database**
- **Did not understand the structure of a SQL statement**
- **Did not understand resulting root level access**

Find the <u>minimal</u> amount of computer information needed to teach a security topic and build a Foundation Body of Knowledge learning object. Incorporate the learning object into a foundation course.

$FBK_i(CBK_i,SBK_i,LO_i)$

- **FBK_i=Relational Database Architecture**
- **CBK_i=Relational Databases**
- **SBK_i=Database Attacks**
- **LO_i=Tables, Rows, Columns, Format**

Case Examples

Case Study #1 – BS in Computer Security

- **CSS 150 Foundations in Security**
- **CSS 200 Principles of Network Security**
- **CSS 250 Security Risk Management**
- **CSS 300 Vulnerability Assessment and Management**
- **CSS 320 Process Engineering (Project Management)**
- **CSS 350 Forensics I**
- **CSS 351 Forensics II**
- **CSS 380 DRP/BCP**
- **CSS 440 Security Compliance and Ethics**
- **CSS 450 Security Capstone Course**

Case Study #1

Problem – In the CSS 350 course (Forensics I) , instructors are not completing objectives due to time spent teaching file system architecture.

Solution – Create required FBK objects. Change the content of the CSS 150 course to include FAT, NTFS, UFS, Ext2 and Ext3 file system learning objects.

Case Examples

Expanded Solution –

Disk Analyzer
File System Architecture
File Systems
Address Calculation
DOS Commands
Linux/Unix Commands
File Navigation
C Programming, ASM
C++/Java
Dump Analysis
Binary Number System
Hexidecimal Notation

Case Examples

Expanded Solution –

HTML
Network Protocols
Network Layers
Relational Databases
SQL
VPN
IPSec
Authentication
Email
Cryptography

Case Examples

Case #2 – NSA Community College Initiative (Colorado)

Required Core Courses

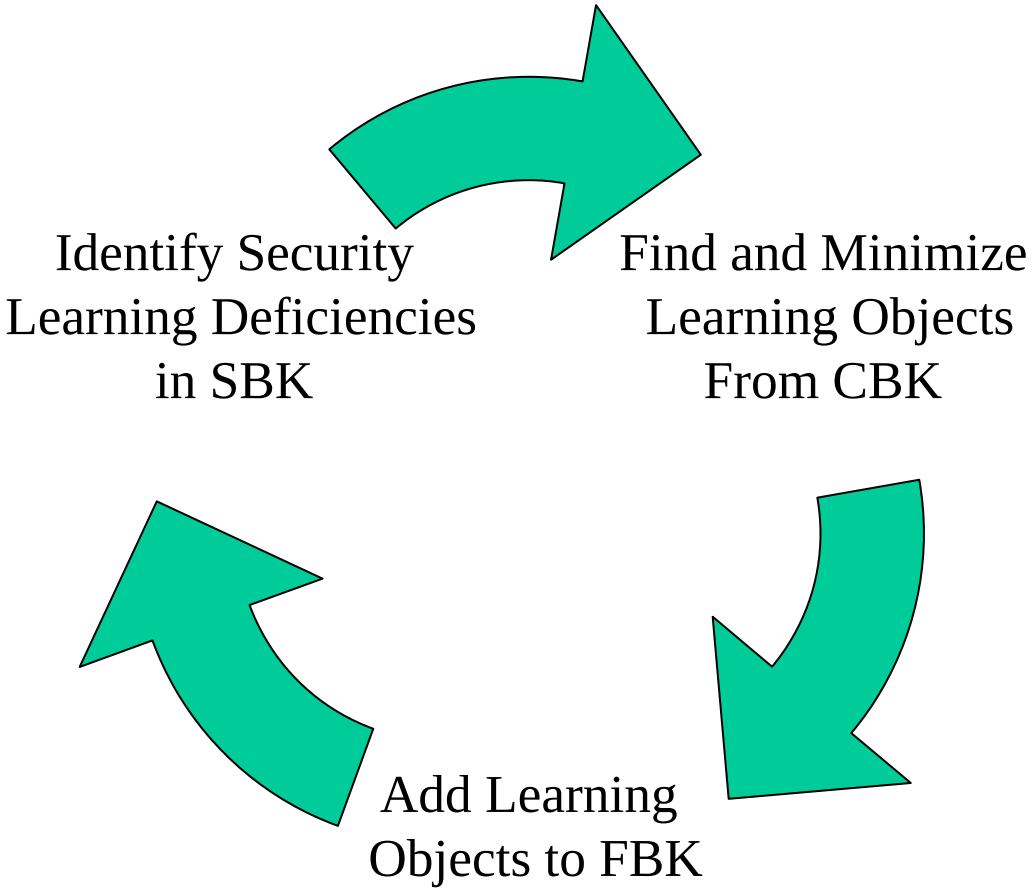
- Enterprise Security
- Secure Electronic Commerce
- Principles of Information Assurance
- Network Security

Case Examples

Problem – All courses will be offered at the community college level. Entry level students may find the material too advanced.

Solution – Using the framework, find the necessary learning objects. Create a course, Foundations in Security, with these learning objects. Make the course a prerequisite for the other courses.

FBK Process


Identify Security Learning Deficiencies in SBK
Find and Minimize Learning Objects From CBK
Add Learning Objects to FBK

New Age Tools

- **Free Software – Knoppix STD, Ubuntu, WinHex, Book Disks, Open Source, etc.**

  Look out for trojans, using evaluation copies and book disks in classroom, versioning, patching, etc.

- **VMware – It is a must. Now there are competitors. It just gets better.**

- **Remote Access – Teaching of the future, but what about the labs?**

New Age Tools

- **Internet Sites – CERT, CyberCeige, NTO Hackme, etc.**
- **Government Sites – NIST (Great for many things, especially class materials), INFRAGARD(FBI), NSA(CNSS, CAE), etc.**
- **Military – DoD 8570. Prepare for the future.**
- **ACM and IEEE access – Here is where things are happening (conference proceedings).**

New Age Tools

- **Industry/Vendor emails – How many do you review each day? How many do your students review each day?**
- **Websites – How about your favorites? Are you guiding student to create their own?**
- **Have you come to terms with certifications?**

New Age Tools

What does your Release of Liability Statement look like?

Conclusions

- You cannot expect to be effective if the student is not adequately prepared
- It is up to you to prepare the student
- Find the minimal amount of computer information needed to teach a security topic and build a Foundation Body of Knowledge.
- Design your security foundation courses based on your FBK. Make these courses a prerequisite for your security courses.
- Take advantage of the teaching resources that are available
- Constantly update your content and teaching method with new techniques