

ITSS Educational Framework Strategic Plan

BACKGROUND & SUMMARY

Since its establishment in 2006, IT Security Services has trained 116 IT professionals at UM in security methods to operate as a distributed security workforce. ITSS has also developed other supplemental educational materials to enable appropriate protection of University information technology resources and services. However, a need for ongoing education has emerged to address the ever-evolving IT security landscape and to continue building a culture of IT security awareness.

This plan is a strategy for organizing and further developing a broad security curriculum in support of the ITSS Security Program, to train and maintain a distributed workforce.

OBJECTIVES OF PLAN (GOALS)

The objectives of this strategy and communication plan are:

- To continue to train and maintain a distributed security workforce
- To create an educational framework that organizes, maintains, and interrelates the educational resources offered by ITSS
- To determine and deliver the content via the appropriate instructional method
- To raise the level of IT security awareness in the general user population
- Communicate the benefits and impacts of continuing education

MODES OF INSTRUCTIONAL DELIVERY & LOGISTICS

We aim for a flexible delivery method that allows materials to be delivered in multiple modes. Instruction will be delivered via one or more of the following methods, based on the content and objective.

- Traditional classroom/live lecture & lab
- Web-based materials with prompts (e.g. Captivate)
- Web-based materials with podcast
- Web-based materials

Each class will be offered 1-4 times per year, dependent on enrollment and instructor availability. For traditional instruction in the Boyer training lab, maximum class size is 36. Other venues will be determined as appropriate.

TARGET PARTICIPANTS

This instruction is intended for participants from the UM community, depending on their job responsibilities. These participants will fall into three overlapping categories: members of the campus community who are responsible for their own IT security; members of the professional IT community and research staff who are responsible for unit systems; and senior executives responsible for IT security investments.

EVALUATION METHODS

We will employ evaluation methods appropriate to each course, including online questionnaires, pre-examinations, course examinations, or interactive evaluations. Depending on the course, some evaluations may be optional or self-directed. Motivations for course evaluations include: measuring the effectiveness of the instruction, ensuring student engagement, and possibly providing credits toward certification. Evaluations will be shared with participant's management.

RISKS

- Web-based materials may attenuate learning
 - Staff doesn't follow through with self-paced courses due to prioritization issues
 - Staff may find it difficult to proceed through a self-paced curriculum without assistance
- Continued funding not available after two-year pilot

- Lack of formal evaluation may cause disengagement
- Insufficient attendance to sustain educational program
 - The information in the tracks may not be sufficiently individualized
 - Not enough interest in chosen topics
 - Lack of release time
 - Skills taught not applicable to students' jobs
- SMEs unavailable to create or deliver course content
- No time to refresh course material

PROPOSED CURRICULUM:

The curriculum is designed to provide basic training for members of the campus community, intermediate and advanced technical training for security administrators, and executive training for unit leaders. Training needs in other areas and for other constituencies are not directly addressed in this plan.

The curriculum supports several tracks, including:

- Members of the campus community
This track is designed for all members of the campus community who use computers in their daily activities.
- Security administrators
This track is for security administrators with responsibility for end-user systems.
- Senior security administrators
This track is for security administrators with broad responsibilities for server deployments, backup systems, network infrastructures, or departmental IT systems.
- Executives
This track is designed for senior departmental executives with responsibility for resource allocation, authorizing the implementation of security assessment recommendations, and managing the department's security investment.
- Research staff
This track is designed for junior and senior research and administrative staff with responsibility for procurement, installation, and operation of departmental research IT resources.

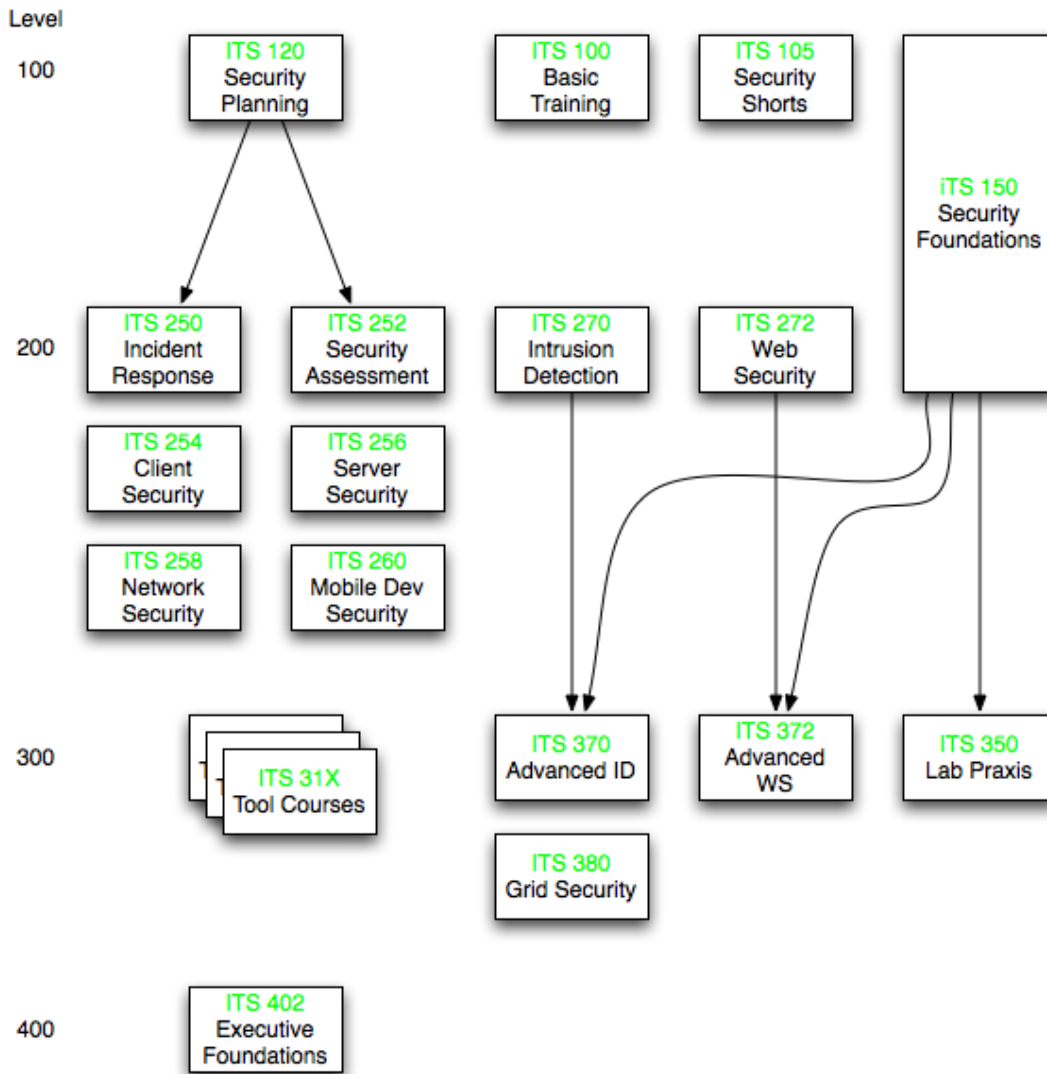
See Figure 1 for a diagram of the curriculum. Arrows on the diagram indicate a pre-requisite relationship. Suggested course sequences for each of the tracks are also listed on the diagram.

COURSE SEQUENCES:

- Campus Community: ITS 100, 105, 254, 260
- SecAdmin: ITS 120, 250, 252 (opt), 254, 260 (opt)
- SecAdmin Senior: ITS 150 or (120, 250-260), 350, 370, 372)
- Executives: ITS 402
- Research staff: ITS 254-260, 372, 380

Figure 1

DRAFT ITSS Security Training Curriculum



Course Sequences

Campus Community: ITS 100, 105, 254, 260

SecAdmin: ITS 120, 250, 252 (opt), 254, 260 (opt)

SecAdmin Senior: ITS 150 or (120, 250-260), 350, 370, 372)

Executive: ITS 402

Research: ITS 254-260, 372, 380

I. Full courses

These courses deal with major sets of topics, or provide advanced treatment of a single topic. They span multiple days, with a time commitment of four to eight hours per day. For the laboratory portion students are expected to bring an IA32-compatible laptop to class.

Advanced Web Security

Duration: 2 days, 16 hours total, lecture and lab

Pre-requisite: ITS 101, Security Foundations, Web Security, or permission of instructor

This course shows how to assess and secure your web infrastructure, using current open-source tools and techniques. Topics to be covered include: reconnaissance tools, shell & SQL injection, cross-site scripting & request forgery, secure coding practices, fuzzing, and U-M information security policies. Hands-on student experiments will comprise a significant portion of this course.

Security Foundations

Duration: 6 days, 24 hours total, lecture only

A compact and updated version of ITS101, this course is intended to establish a core set of security competencies in U-M IT staff members charged with security duties. Topics include: risk assessment, web security, networks, VPNs & wireless security, firewalls & VFW, logging and log file analysis, intrusion detection, scanning (Retina), incident response, forensics, security planning, and compliance, U-M security policies, laws, and ethics

Lab Praxis

Duration: 3 days, 12 hours total, lab

Pre-requisite: ITS 101, Security Foundations, or permission of instructor

The goal is to gain practical experience with the tools and methodologies discussed in the Security Refresher. Students will be guided through a set of self-paced labs. Labs focus primarily on defensive and reconnaissance skills and include packet sniffing and analysis, the dsniff tool suite, wireless attacks and defenses, advanced SSH, password cracking, botnet detection, phishing attacks and defenses, and a capture-the-flag session.

II. Basic Courses

Basic Training in IT Security

Duration: 1 hour, lecture

This course covers the fundamentals of IT security for unit staff, including threat awareness, basic procedures, password strategies, Web browsers including cookies and certificates, and resources.

Security Shorts

Available as documentation, Captivate video, or brown bag lunch presentations

- How to Browse the Internet and Read E-mail More Securely, or CYA: Cover Your Access
- How to Encrypt Documents in Microsoft Windows XP
- How to Encrypt Documents in Microsoft Windows Vista
- How to Secure Your Wireless Network
- How to Manage All Your Passwords
- Three Security Essentials for Your PC
- How to Encrypt Your Thumb drive
- How to Encrypt Documents with BitLocker

Security Planning

Duration: 2 hours, lecture

This course discusses the ITSS security planning framework.

III. Short Courses

These courses provide a focused treatment of a single security topic with some hands-on experience. For the laboratory portion students are expected to bring an IA32-compatible laptop to class.

Incident Response

Duration: 4 hours, lecture and lab
Pre-requisite: ITS 101, or Security Planning

This course provides an introduction to U-M's incident response goals, policies, guidelines, and procedures. This course invites student participation through sample scenarios.

Security assessments (RECON)

Duration: 4 hours, lecture
Pre-requisite: ITS 101, or Security Planning

This course provides an introduction to the RECON security assessment tool, including motivation, methodology, security tests, questionnaire, interpretation of tool outputs, report generation, and management follow-up. A case study will be examined. This course will prepare students to conduct a security assessment in their units.

Client Security

Duration: 4 hours, lecture and lab

This course provides intermediate training in securing a personal or client platform. Topics include authentication, administration of host-based firewalls, host intrusion detection systems, host-based scanning, use of secure networking protocols, Web browser security including cookies and certificates, and social computing challenges.

Server Security

Duration: 4 hours, lecture and lab

This course provides intermediate training in securing enterprise server platforms. This course will cover Windows, Linux, and Mac OS X servers and will be developed and taught by domain experts. (This course may be split into three courses.)

Network Security

Duration: 4 hours, lecture and lab

This course provides intermediate training in securing networked enterprise deployments, and covers network topologies, network firewalls and other middleboxes, VPNs, open-source and commercial network scanners and sniffers, distributed logging architectures, and configuration of secure network protocols.

Mobile Device Security

Duration: 4 hours, lecture and lab

This course provides intermediate training in securing information on mobile devices, and covers physical security, tools for discovering, encrypting, and remotely deleting sensitive information, U-M policies and procedures governing retention of sensitive information, and efficacy in the real world.

Intrusion Detection

Duration: 4 hours, lecture and lab

This course provides an overview of Intrusion Detection and Prevention systems, and discusses the architecture, implementation, and efficacy of such systems. Students will use the open source Snort IDS systems to create scripts for detecting network attacks, and will experiment with sampling of real or recorded network traffic.

Advanced Intrusion Detection

Duration 4 hours, lab

Pre-requisite: ITS 101, Security Foundations, Intrusion Detection, or permission of instructor

This course will put the concepts learned in the Intrusion Detection course into practice. Students will set up and appropriately configure an IDS system, examine a physical or virtual network for specified activity, and analyze the results.

Web Security

Duration: 4 hours, lecture and lab

This course provides intermediate training in Web security, and covers the HTTP protocol and its basic operation and authentication modes, an introduction to common attacks including SQL injection and cross-site scripting, overview of popular Web servers and security configurations, and basic defenses.

IV. Tool Training Courses

These courses provide a focused treatment of a single security tool or system.

Campus Virtual Firewall Training

Retina Training

PeakFlowX Training

V. Executive Courses

Security for Executives

Duration: 2 hours

This course summarizes security issues and recommends solutions for executive-level leaders. Topics include an overview of security metrics, evaluating cost and effectiveness of unit-level security procedures, leveraging centralized and departmental security resources, and a current threat briefing. A pilot version of this course will be conducted in a classroom setting, with future versions available using Web-based materials.

VI. Recommended Outside Resources

These resources offer skills supplemental to the foundational and advanced security classes offered by ITSS.

U-M Human Resource Development (HRD)

<http://www.umich.edu/~hrd/>

HRD offers more than one hundred professional development programs and courses designed to help career advancement at U-M.

The SANS (SysAdmin, Audit, Network, Security) Institute (SANS)

<http://www.sans.org/>

As the leading organization in computer security training, the SANS Institute provides intensive, immersion training designed to teach skills necessary for defending systems and networks.

Washtenaw Community College (WCC)

<http://www3.wccnet.edu/lifelong-learning/>

WCC offers non-credit lifelong learning courses on Information Technology topics, designed to help career advancement and meet professional requirements.