SRA 111

Introduction to Security and Risk Analysis

(Spring Semester 2008)

Course Description:

SRA 111 is an introductory course with a broad focus, spanning the areas of security, risk and analysis. In addition to familiarizing the student with basic security terminology, it will also touch upon social and legal issues, risk analysis and mitigation, crime intelligence and forensics, and information warfare and assurance.

This course will motivate students to understand the requirements for security in any government agency or business organization through the use of case studies. Included in this segment are cases related to cyberterrorism, bioterrorism, and critical infrastructure protection. Some concepts to be covered in the area of information security are: confidentiality, integrity, availability, and non-repudiation. Various methods of safeguarding these security concerns will be discussed, such as: single- and multi-factor authentication, encryption, digital signatures, prevention of denial of service attacks, and so forth. This course also covers social and legal issues related to security, in particular identity theft and social engineering. Topics in this section include identity theft, spam, spyware, and adware. This course also covers the basic principles and the approaches to risk analysis. Here students study vulnerability analysis, crime and intelligence analysis, forensics, techniques for risk assessment and risk mitigation.

The course will prepare students for more in-depth courses such as SRA 211, SRA 221 and SRA 311.

This course will incorporate collaborative and action-learning experiences wherever appropriate. Emphasis will be placed on developing and practicing writing and speaking skills through application of the concepts that define the course.

Course Objectives:

Upon completion of the course, the student will:

- Understand basic security concepts, terminology and possible solutions.
- Develop an understanding of the social and legal issues of security and privacy.
- Understand the basics of crime intelligence and forensics analysis.
- Be able to apply risk analysis, evaluation and mitigation methods.
- Understand information warfare and information assurance.
- Have an awareness of current and future trends in information and cyber security.
SRA 111

Classes Information:

- **Section:** 021
- **Class Time:** W 6-8:45 PM
- **Class Room:** Frable 221

About the Instructor/TA:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instructor:</strong></td>
<td>Galen A. Grimes</td>
</tr>
<tr>
<td><strong>Office:</strong></td>
<td>Frable 213</td>
</tr>
<tr>
<td><strong>Office Hours:</strong></td>
<td>See faculty website</td>
</tr>
<tr>
<td><strong>Phone/Fax:</strong></td>
<td>412-675-9479</td>
</tr>
<tr>
<td><strong>e-mail:</strong></td>
<td><a href="mailto:gagrimes@psu.edu">gagrimes@psu.edu</a></td>
</tr>
<tr>
<td><strong>Web Site:</strong></td>
<td><a href="http://www.personal.psu.edu/faculty/g/a/gag5/">http://www.personal.psu.edu/faculty/g/a/gag5/</a></td>
</tr>
</tbody>
</table>

Course Materials:

- Supplement reading materials. (See Appendix A for the attached reading lists).

Course Policies:

- **(Any policies implemented by the instructor or campus).**
- Quizzes will be given throughout the semester, at a rate of approximately 1 per chapter. Quizzes will always cover the material covered since the last Quiz or Exam. The quizzes will be combinations of objective and/or short-answer questions. Makeup quizzes will not be given. Any class material missed by the student is the student's responsibility to acquire.
- **Students with disabilities.** It is Penn State's policy to not discriminate against qualified students with documented disabilities. If you have a disability-related need for modifying your exam or test environment, notify your instructor during the first week of classes so that your needs can be accommodated. You will be asked to present documentation from the Office of Disability Services (located in 105 Boucke Building) that describes the nature of your disability and the recommended remedy. You may refer to the Nondiscrimination Policy in the Student Guide to University Policies and Rules.
- **Americans with Disabilities Act.** The College of Information Sciences and Technology (IST) welcomes persons with disabilities to all of its classes, programs, and events. If you need accommodations, or have questions about access to buildings where IST activities are held, please contact the Dean's Office (814) 865-3528 in advance of your participation or visit. If you need assistance during a class, program, or event, please contact any member of our staff or faculty in charge.
- **PSU Statement on Academic Integrity.** According to the University Advising Handbook: "Academic integrity is the pursuit of scholarly activity free from fraud and deception, and is
the educational objective of this institution. Academic dishonesty includes, but is not limited to cheating, plagiarism, fabrication of information or citations, facilitating acts of academic dishonesty by others, unauthorized possession of examinations, submitting work of another person, or work previously used without informing the instructor, or tampering with the academic work of other students. Any violation of academic integrity will be thoroughly investigated, and where warranted, punitive action will be taken." Students should be aware that standards for documentation and intellectual contribution may depend on the course content and method of teaching, and should consult instructors for guidance.

**Tentative Schedule:**

<table>
<thead>
<tr>
<th>Week</th>
<th>Topics</th>
<th>Readings</th>
<th>Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction to the course</td>
<td>Syllabus; M1-1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Why Study Information Security?</td>
<td>Chap 2; M1-2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Why Study Information Security?</td>
<td>Chap 2; M1-3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Why Study Information Security?</td>
<td>Chap 2; M1-4</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Basic Concepts of Information Security (Security goals, the Orange book)</td>
<td>Chap 1; M2-1/2</td>
<td>Team project announcement</td>
</tr>
<tr>
<td></td>
<td>Basic Concepts of Information Security (The common criteria, multi-level security, Defense in depth)</td>
<td>M2-3/4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Authentication methods, encryption methods</td>
<td>Chap 7, 8</td>
<td>Hands-on #1</td>
</tr>
<tr>
<td></td>
<td>PKI, and Digital Signatures</td>
<td>Chap 8</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Logical vs. Physical Security</td>
<td>Chap 9, 11</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Operating Systems vs. Application Level Security</td>
<td>Chap 10, 12</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Social and Legal Issues of Security &amp; Privacy</td>
<td>Chap 3: M3-1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identity Theft</td>
<td>Chap 3</td>
<td>Hands-on #2</td>
</tr>
<tr>
<td>8</td>
<td>Spam, Spyware, and Adware</td>
<td>Chap 3; M3-2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Social Engineering</td>
<td>Chap 3; M3-3/4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What is the Legal Position?</td>
<td>Chap 3</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Analysis Methods - Vulnerability Assessment</td>
<td>Chap 6; M4-1/5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Analysis Methods – Crime and Intelligence</td>
<td>M4-9/10</td>
<td>Hands-on #3</td>
</tr>
<tr>
<td></td>
<td>Analysis Methods – Forensics Analysis</td>
<td>M4-6/8</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Analysis Methods - Risk Assessment</td>
<td>Chap 4; M4-11/12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Analysis Methods – Risk Mitigation</td>
<td>Chap 4</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Information Warfare – Footprinting; Scanning and Sniffing</td>
<td>M5-1/3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information Warfare – Intrusion Detection/Prevention</td>
<td>M5-4</td>
<td>Current Event</td>
</tr>
<tr>
<td>12</td>
<td>Information Assurance – DoS / Wardriving</td>
<td>M5-5/7</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Secure the Future</td>
<td>Chap 5; M6-1/2</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Secure the Future</td>
<td>M6-3/5</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Term project</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SRA 111

| Term Project Presentation (Poster session) |

* Chap x – Chapter from the textbook

**Course Development Committee:**

- John Bagby (jbagby@ist.psu.edu)
- Chao-Hsien Chu (chu@ist.psu.edu) - Chair
- Galen A Grimes (gag5@psu.edu)
- Gerry Santoro (gsantoro@ist.psu.edu)
- Heng Xu (hxu@ist.psu.edu)
Appendix A: Reading List

Module 1: Motivation

Module 2: Basic Concepts of Information Security
- Information Assurance Technical Framework, NSA. (M2-2) http://www.iatf.net/framework_docs/version-3_1/index.cfm
- The Orange Book, DoD (M2-3). http://www.fas.org/irp/nsa/rainbow/stdlib001.htm

Module 3: Social and Legal Issues
- A&T, A Social Engineering Example (M3-3). http://www.searchlores.org/social_1.htm
- LabMice.net, Social Engineering. (M3-4) http://labmice.techtarget.com/security/socialengineering.htm

Module 4: Analysis Methods
- SANS Top 20 Internet Vulnerabilities. (M4-1) http://www.sans.org/top20/#w1
- Jeffrey King, 10 Vulnerabilities a Scanner Might Not Find, SANS Institute, May 12, 2003. (M4-5). http://www.sans.org/rr/whitepapers/threats/1030.php
SRA 111

- Security Scanning is not Risk Analysis ([http://www.intranetjournal.com/articles/200207/pse_07_14_02a.html](http://www.intranetjournal.com/articles/200207/pse_07_14_02a.html)) (M4-12)

**Module 5: Information Warfare & IA**
- Whatis.Com, Denial of Service. (M5-5). [http://whatis.techtarget.com/definition/0,289893,sid9_gci213591,00.html]
- Denial of Service Attacks, CERT® Coordination Center. (M5-6). [http://www.cert.org/tech_tips/denial_of_service.html]

**Module 6: Securing the Future**
Appendix B: Video List

• Businessweek video library: http://feedroom.businessweek.com/
• Information Assurance Video, NIATEC, Idaho State University. http://niatec.info/videos.htm
• Security Awareness Program Contest.
  http://www.educause.edu/content.asp?page_id=7103&bhcp=1
• Security on ZDNet: Video and Audio:
• ZDNet Video at the Whiteboard: http://news.zdnet.com/2036-2_22-5718923.html

Appendix C: Selected Web Links

• Center for Information Assurance at Penn State. http://net1.ist.psu.edu/cica/
• CERT Coordination Center, Carnegie Mellon University. http://www.cert.org/
• CERT Virtual Training Environment. https://vte.cert.org/aboutvte.html
• CIA, Criminal Intelligence Analysis, Interpol. http://www.interpol.int/Public/cia/default.asp
• Computer Forensics, Cybercrime and Steganography Resources. http://www.forensics.nl/
• Computer Security Resources Center (CSRC), National Institute of Standard and Technology (NIST). http://csrc.nist.gov/
• Dan Farmer and Wietse Venema, Forensic Discovery, Addison-Wesley, http://www.porcupine.org/forensics/forensic-discovery/
• IAPP – International Association of Privacy Professionals: https://www.privacyassociation.org/
• ISACA: http://www.isaca.org/
• IT Audit – The Institute of Internal Auditors, http://www.theiia.org/ITAudit/
• IWS- The Information Warfare Site. http://www.iwar.org.uk/cip/
• National Coordination Office for Networking and Information Technology Research and Development (NITRD). http://www.nitrd.gov/pubs/
• Privacy.Org: http://privacy.org/
• Security and Risk Analysis (http://www.cert.org/octave/methodintro.html)
• Wireless LAN Security & Wardriving (http://www.wardrive.net/)