SRA 111 is an introductory course with a broad focus, spanning primarily the areas of security, risk, and risk 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.
Classes Information

Section: 001  
Class Time: MWF 11:00-11:50am  
Class Room: Frable 227

About the Instructor

Instructor: Galen A. Grimes, Associate Professor of IST  
Office: Frable 213  
Office Hours: See faculty website  
Phone/Fax: 412-675-9479  
E-mail: gagrimes@psu.edu  
Web Site: http://www.personal.psu.edu/faculty/g/a/gag5/
Course Materials

• **Security Awareness—Applying Practical Security in Your World, 4th Ed.**
  Mark Ciampa
  Copyright © 2014 Course Technology

• **Computer Forensics And Cyber Crime, An Introduction, 3rd Ed.**
  Marjie Britz
  Copyright © 2013 Pearson/Prentice Hall

• Supplemental reading materials at the discretion of the instructor
• The New York Times (newspaper)
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. The Pennsylvania State University is committed to providing access to a quality education for all students. Penn State welcomes students with disabilities into the University's educational programs. If a student has a disability-related need for modifications or reasonable accommodations in this course, it is the responsibility of the student to first obtain a University accommodation letter confirming the disability and suggesting appropriate remedies. This letter should be obtained from the campus Disability Contact Liaison. The contact person at Penn State Greater Allegheny is Victoria Garwood (Frable 103, 412-675-9070, vkg2@psu.edu). Students from other Penn State campuses can find their contact person at http://www.equity.psu.edu/ods/dcl.asp. It is encouraged that students request their accommodation needs early in the semester, and once identified, a reasonable accommodation will be implemented in a timely manner. Students may also access the web site for the Office of Disability Services at University Park for more information: http://www.equity.psu.edu/ods/.

- 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/Tests</th>
</tr>
</thead>
</table>
<br>***Labor Day***<br>2 | | | | |
| 3    | **Introduction to Security** | Chapter 1— Ciampa | Discussion Activity 2— Malicious Code |


Chapter Review Questions—Chapter 1—Ciampa

4 Introduction and Overview of Computer Forensics and Cybercrime

Discussion Questions—Chapter 1 (Britz)


Discussion Activity 3—Security Access Controls

Discussion Questions 1-5, p.22

Quiz—Chapter 1 (Ciampa)

5 Desktop Security


Chapter 2—Ciampa

Discussion Activity 4—Security Policy

60 Minutes: Cyber War, JUN 13 2010, http://www.cbsnews.com/video/watch/?id=6578069n&tag=mncol;lst;1


Chapter Review Questions—Chapter 2 (Ciampa)
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Text</th>
</tr>
</thead>
</table>
| 6 | Contemporary Computer Crime | Discussion Question—Chapter 4 (Britz)  
Discussion Activity 5—Risk Assessment |
| 7 | Internet Security | Chapter 3—Ciampa  
Discussion Activity 6—Encryption  
Chapter Review Questions—Chapter 3 (Ciampa) |
| 8 | The Fourth Amendment and Other Legal Issues | Chapter 9—Britz  
ABC News Tracks Missing iPad to Florida Home of TSA Officer, Discussion Activity 7—Spam |
<table>
<thead>
<tr>
<th><strong>9</strong></th>
<th><strong>Personal Security</strong></th>
<th>Chapter 4—Ciampa</th>
<th>Discussion Activity 8—Network Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Authentication—1FA and 2FA</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>VIDEO</strong>: Nigerian 419 Scam</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chapter</td>
<td>Section</td>
<td>Text</td>
<td>Resources</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>------------------------------------------</td>
<td>------------</td>
</tr>
</tbody>
</table>
| 10      | Identity Theft and Identity Fraud | CBS 60 Minutes, “Biggest IRS Scam Around: Identity Tax Refund Fraud”, [link](http://www.cbsnews.com/videos/biggest-irs-scam-around-identity-tax-refund-fraud/) | Discussion—Case Studies Chapter 4  
VIDEO: NBC Dateline, “To Catch and ID Thief” (YouTube)  
VIDEO: NBC Dateline, “Putting a Face on ID Theft” (YouTube) |
|         |         | Chapter 5—Britz  
Discussion Activity 9—Mitigation of Risks and Threats |
|         |         | Discussion Questions 1-5, p.143 |
|         |         | Quiz—Chapter 4 |
DD-WRT [link](http://dd-wrt.com/site/index) | Chapter 5—Ciampa  
Discussion Activity 10—Policies and Laws |
<p>|         |         | Chapter Review Questions—Chapter 5 (Ciampa) |</p>
<table>
<thead>
<tr>
<th>13</th>
<th><strong>Enterprise Security</strong></th>
<th>Chapter 6—Ciampa</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VIDEO</strong>: To Catch a Con Man—(YouTube)</td>
<td>Chapter Review Questions—Chapter 6 (Ciampa)</td>
<td></td>
</tr>
<tr>
<td><strong>VIDEO</strong>: To Catch an ID Thief—(YouTube)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>VIDEO</strong>: To Catch a Lotto Scammer—(YouTube)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td><strong>Computer Forensics: Terminology and Requirements</strong></td>
<td>Chapter 10—Britz</td>
</tr>
<tr>
<td><strong>Video</strong>: To Catch a Predator -&lt;br&gt;<a href="http://www.msnbc.msn.com/id/21134540/vp/22412084/#22424498">http://www.msnbc.msn.com/id/21134540/vp/22412084/#22424498</a>&lt;br&gt;To Catch a Predator—YouTube&lt;br&gt;<a href="http://www.youtube.com/results?search_query=dateline+nbc+to+catch+a+predator&amp;aq=1">http://www.youtube.com/results?search_query=dateline+nbc+to+catch+a+predator&amp;aq=1</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Discussion Questions 1-5, p.299</strong></td>
<td>Quiz—Chapter 6 (Ciampa)</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Semester Project Presentations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Final Exam—Chapters 1-6 (Ciampa); Chapters 1, 4, 5, 7, 9, 10 (Britz)</td>
</tr>
</tbody>
</table>
NOTE: Syllabus subject to change without notice.

**Grading**

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>100.0%—93.0%</td>
</tr>
<tr>
<td>A-</td>
<td>92.9%—90.0%</td>
</tr>
<tr>
<td>B+</td>
<td>89.9%—88.0%</td>
</tr>
<tr>
<td>B</td>
<td>87.9%—82.0%</td>
</tr>
<tr>
<td>B-</td>
<td>81.9%—80.0%</td>
</tr>
<tr>
<td>C+</td>
<td>79.9%—78.0%</td>
</tr>
<tr>
<td>C</td>
<td>77.9%—70.0%</td>
</tr>
<tr>
<td>D</td>
<td>69.9%—60.0%</td>
</tr>
<tr>
<td>F</td>
<td>59.9%—00.0%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assignments</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter Review Questions</td>
<td>120 (20 points/each x 6)</td>
</tr>
<tr>
<td>Quizzes</td>
<td>180-300 (30-50 points/each x 6)</td>
</tr>
<tr>
<td>Lab participation</td>
<td>120 (20 points/each x 6)</td>
</tr>
<tr>
<td>Discussion Activities</td>
<td>100 (10 points/each x 10)</td>
</tr>
<tr>
<td>Risk Assessment Project</td>
<td>150</td>
</tr>
<tr>
<td>Group Video Project</td>
<td>150</td>
</tr>
<tr>
<td>In Class Discussion/Participation</td>
<td>15%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>100</td>
</tr>
</tbody>
</table>

Assignments are due the Sunday evening of the week they are assigned.
Use the following advice to receive maximum learning benefits from your participation in this course:

<table>
<thead>
<tr>
<th>DO</th>
<th>DON’T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do take a proactive learning approach</td>
<td>Don’t assume there is only one correct answer to a question</td>
</tr>
<tr>
<td>Do share your thoughts on critical issues and potential problem solutions</td>
<td>Don’t be afraid to share your perspective on the issues analyzed in the course</td>
</tr>
<tr>
<td>Do plan your course work in advance</td>
<td>Don’t be negative towards points of view that are different from yours</td>
</tr>
<tr>
<td>Do explore a variety of learning resources in addition to the textbook</td>
<td>Don’t underestimate the impact of collaboration on your learning</td>
</tr>
<tr>
<td>Do offer relevant examples from your experience</td>
<td>Don’t limit your course experience to reading the textbook</td>
</tr>
<tr>
<td>Do make an effort to understand different points of view</td>
<td>Don’t postpone your work on the course deliverables – work on small assignment components every day</td>
</tr>
<tr>
<td>Do connect concepts explored in this course to real-life professional situations and your own experiences</td>
<td></td>
</tr>
</tbody>
</table>

**Appendix A: Reading List**

**Module 1: Motivation**

**Module 2: Basic Concepts of Information Security**
• Kevin D. Mitnick, “Are You the Weak Link?” Harvard Business Review, April 2003, pp. 18-20. (M2-1)
• 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/std001.htm
• Common Criteria Documentation. (M2-4). http://niap.bahialab.com/cc-scheme/cc_docs/index.cfm

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
• Michael Potaczala, Computer Forensics, Term Paper, 2001. (M4-8). http://chantry.acs.ucf.edu/~mikey/cf/CHS5937-
TermPaper.pdf
• Security Scanning is not Risk Analysis (http://www.intranetjournal.com/articles/200207/pse_07_14_02a.html) (M4-12)/

Module 5: Information Warfare & IA
• Tony Bradley, Introduction to Packet Sniffing. (M5-2). http://netsecurity.about.com/cs/hackertools/a/aa121403.htm
• Tony Bradley, Introduction to Port Scanning. (M5-3). http://netsecurity.about.com/cs/hackertools/a/aa121303.htm
• 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
• Mark Lum, Offshore Outsourcing and Information Confidentiality, SANS Institute, April 2004. (M6-3). http://www.sans.org/rr/whitepapers/legal/1438.php

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
• 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/
- CIA, Criminal Intelligence Analysis, Interpol. http://www.interpol.int/Public/cia/default.asp
- 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/
- 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/)