**International Studies 4702**

**Case Studies in Information Security**

Spring 2019

Short Description

# Instructor

Steve Romig, Office of the CIO

Mount Hall

[romig.1@osu.edu](mailto:romig.1@osu.edu)

(614) 688-3412

Office Hours: TBD

Class Time: T/Th 5:30-6:50PM, 160 minutes per week

Location/Room: TBD

This course will provide students with a deeper understanding of core elements of Information Security through review and analysis of real-world case studies, security frameworks, annual trend/survey reports and related materials.

# Course Description

The goal of this course is to provide students who have taken an introductory Information Security course (such as CSE 4471) with a more advanced understanding of the background, terminology, and concepts of Information Security. This will prepare students to engage in deeper study of Information Security and to apply what they have learned in business and technical contexts.

This course will focus heavily on outcomes demonstrating the ability to use knowledge gained in an introductory course, such as developing security requirements from business use-cases, comparing security requirements against implementation reality, and conducting post-incident reviews.

Course material will be drawn from real world events such as Stuxnet, SONY Pictures, Target, and EquiFax; emerging information technologies such as Social Media, Cloud Computing, Big Data and the Internet of Things; and perennial concerns such as privacy, public safety and business considerations.

This is a 3 Credit Hour course, lasting 14 weeks, offered in Spring of each year. There is no assigned textbook: weekly readings are drawn from publicly available sources.

# Pre-Requisites

CSE 4471, “Introduction to Information Security”

International Studies 3702, “Herding Cyber Cats: Information Security Management”

# Course Goals

By the end of this course, you should have a deeper understanding of the following topics using case studies and real-world examples:

* The application of a variety of security controls to address risk based on real-world examples
* Threats, with a focus on organized crime and nation-states
* Intrusion detection, threat hunting and incident response/investigations
* Penetration testing
* The underground economy
* Vulnerability, patch and related service management areas
* Identity and access management
* Inside threats and user behavior analytics

# Course Assignments and Grading

## Reading

This course includes reading assignments in preparation for most of the lectures which are meant to give background material for the lectures. Students are encouraged to do some additional research on relevant current events to supplement in-class and on-line discussions and their writing assignments. Reading assignments listed in the schedule below are due on the day they are listed.

## Grading

Grades will be determined by attendance (10%), a Final Examination (30%), and through regular discussion and short writing assignments (12 papers, 42 pages total), which will account for the other 60% of your grade. The deadline for writing assignments is 5:00 PM on the Friday of the week of the assignment.

Each paper will count for 5.0% of the final grade. See weekly Class Schedule for additional details. Paper requirements will be fully explained in class.

Paper 1 4 Pages Week 2 Attack graph for “cookies” problem, mitigations, costs.

Paper 2 3 Pages Week 3 Internet services/data, restrictions/conditions.

Paper 3 3 Pages Week 5 Benchmarks, system hardening, budget constraints.

Paper 4 2 Pages Week 6 Ransomware, mitigation, prevention, attack response.

Paper 5 6 Pages Week 7 Response to malware attacks, response/patching.

Paper 6 3 Pages Week 8 Identity management, authentication, accountability.

Paper 7 3 Pages Week 10 Insider threats, detection/prevention/privacy.

Paper 8 4 Pages Week 10 Kill chains tactics/techniques. Mitigations of attacks.

Paper 9 4 Pages Week 11 Intrusion detection. Table top exercise analysis.

Paper 10 3 Pages Week 13 Cloud services. Securing/auditing/authentication.

Paper 11 3 Pages Week 14 The changing Information Security environment.

Paper 12 4 Pages Week 14 Reflection paper about what was learned in this class.

## Grading Scale

93-100% A

90-92% A-

87-89% B+

83-86% B

80-82% B-

77-79% C+

73-76% C

70-72% C-

67-69% D+

60-66% D

0-59% E

## Grade Disputes

I am happy to revisit grades and to discuss my evaluation of your work with you. Grade change requests can be made in-person or via email. Please be ready to outline where you believe you should have received additional points and how many points you should have received.

## Discussions/Participation

Students are expected to discuss the weekly readings and “current events” in class and on-line. Grading for these will be based on the relevance of your comments, the accuracy of your analysis and your application of common security principles and controls.

## Writing

I expect all assignments to be written in 12-point font with 1-inch margins. Everything should be double-spaced and should always include a title, your name, the date, and the course. Writing is a tool that allows us to express ourselves throughout our lives. If you need assistance, do not be afraid to ask me or consult a university resource, such as the Writing Center, which offers free tutorials on writing

## Attendance and Participation

Attendance will be recorded for each class meeting and one half of one point will be deducted for each class missed without good reason.

You must let me know before class or within 48 hours of missing the class (via email is fine). Additionally, if you miss a class you are responsible for getting notes and information missed from your fellow classmates.

# Course Policies

## Late Work

Assignments should be handed in on time. However, I do understand that situations occasionally come up that prevent this. I'm generally not concerned if an assignment is a few hours late, but if your assignment is more than a day late I will grade it for full credit only in situations where (1) the assignment was late due to unavoidable circumstances and (2) you let me know about your situation within 48 hours of missing the deadline. If you do not turn something in and you don't communicate with me within 48 hours of missing the deadline, you will receive zero points.

## Plagiarism

All work in this course is to be individually developed. Plagiarism includes using another person's writing without giving them credit, using large verbatim sections of the work of another person or online source (even a public source) or submitting something you have written for another class. If you unsure, please give credit to your source or talk to me about it. Students who plagiarize will be penalized and reported to university officials. You will also receive a grade of zero for the assignment where plagiarism occurred.

## Academic Misconduct

It is the responsibility of the Committee on Academic Misconduct to investigate or establish procedures for the investigation of all reported cases of student academic misconduct. The term "academic misconduct" includes all forms of student academic misconduct wherever committed; illustrated by, but not limited to, cases of plagiarism and dishonest practices in connection with examinations. Instructors shall report all instances of alleged academic misconduct to the committee (Faculty Rule 3335-5-487). For additional information, see the Code of Student Conduct (http:l j studentaffairs.osu.edu/info for students/csc.asp).

## Disability Services

**The University strives to make all learning experiences as accessible as possible. If you anticipate or experience academic barriers based on your disability (including mental health,chronic or temporary medical conditions), please let me know immediately so that we can**

**privately discuss options. To establish reasonable accommodations, I may request that you register with Student Life Disability Services. After registration, make arrangements with me as soon as possible to discuss your accommodations so that they may be implemented in a timely fashion. SLDS contact information: slds@osu.edu; 614-292-3307; slds.osu.edu; 098 Baker Hall, 113 W. 12th Avenue**.

## Statement on Diversity

The Ohio State University embraces and maintains an environment that respects diverse traditions, heritages, experiences, and people. Our commitment to diversity moves beyond mere tolerance to recognizing, understanding, and welcoming the contributions of diverse groups and the value group members possess as individuals. The faculty, students, and staff are dedicated to building a tradition of diversity with principles of equal opportunity, personal respect, and the intellectual interests of those who comprise diverse cultures.

## Class Schedule

This schedule includes a tentative list of topics, readings and assignment due dates. Reading assignments should be completed before the class session they are listed in, discussion and writing assignments are due a week or two later (details below).

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Day** | **Details** | **Assignments** |
| Course Overview | 1 | Course Overview; syllabus review; beyond the CIA triad; privacy, anonymity, attribution, repudiation | Read: “Beyond the CIA Triad”, Jim West (<https://isc2usmg.org/images/documents/Beyond_the_CIA_Triad.pdf>)  Read: “Dilemmas of the Internet Age: Privacy vs Security”, Deena Zaru (<http://www.cnn.com/2015/02/04/politics/deena-zaru-internet-privacy-security-al-franken/index.html>)  Discussion: Privacy and security: how do you define these?  What’s the relationship between the two?  (1 week) |
| Course Overview | 2 | Concepts and Terminology | Read: “An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants”, Paxson et al (<http://www.icir.org/vern/papers/miscreant-wealth.ccs07.pdf>)  Read: “Show Me the Money: Characterizing Spam Advertised Revenue” (<http://www.icir.org/vern/papers/ppair-usesec11.pdf>)  Discussion: Find an example of something security related being shared or sold on the Internet, share it with the class (1 week) |
| Tools for Thinking About Security | 3 | Attack trees, attack graphs | Read: Attack Trees, Shneier (<https://www.schneier.com/academic/archives/1999/12/attack_trees.html>)  Read: Attack Graphs (<https://blogs.technet.microsoft.com/johnla/2015/04/26/defenders-think-in-lists-attackers-think-in-graphs-as-long-as-this-is-true-attackers-win/>)  Discussion: What costs are associated with risks and the security controls we use to address them? (1 week)  Writing: Create an attack graph for the “cookie” problem, indicate possible mitigations and relative costs. 4 pages (1 week) |
| Risk | 4 | Overview of  Risk | Read: Sample risk assessment, risk assessment template (to be provided) |
| OSU’s Security Policies and Framework | 5 | Security policies and standards | Read: OSU Responsible Use Policy : https://it.osu.edu/sites/default/files/files-1477502439/responsible-use-of-university-computing-and-network-resources-policy.pdf  Read: OSU Data Classification Policy: https://it.osu.edu/sites/default/files/files-1477502242/institutionaldata.pdf  Read: OSU Data Elements: <https://cybersecurity.osu.edu/system/files/2017/08/30/osuidp-dataelementclassificationassignments.pdf>  Read: OSU IT Security Policy: <https://it.osu.edu/sites/default/files/files-1477502296/itsecurity.pdf> |
| OSU’s Security Policies and Framework | 6 | Information Security Standards | Read: OSU Information Security Standard: <https://cybersecurity.osu.edu/system/files/osu.iss.v1.5.pdf>  Skim: OSU Information Security Control Requirements (ISCR): <https://cybersecurity.osu.edu/system/files/osu.iscr.v1.5.1.pdf>  Writing: classify a given list of data (to be provided), and for each list the services where it can be stored. Also, for a given list of Internet services and data (to be provided) indicate whether that service can be used for that data, under what restrictions/conditions it could be used, and what acceptable alternatives would be. 3 pages (1 week). |
| OSU’s Security Policies and Framework | 7 | Information Security Standards | Read: OSU ISCR IT1-IT9, selected sample evidence of implementation (to be provided) |
| OSU’s Security Policies and Framework | 8 | Information Security Standards | Read: OSU ISCR IT10-IT18, selected sample evidence of implementation (to be provided)  Discuss: Thoughts on the OSU policies and standards?  What is missing?  What would you remove?  Is there a better approach?  How might you go about answering these questions if you don’t know? (1 week) |
| System Security | 9 | System hardening: CIS and related benchmarks, guides | Read: CIS documentation, especially their Benchmarks.  <https://www.cisecurity.org/>  Read: Sample CIS scan of a Windows desktop (to be provided) |
| System Security | 10 | System hardening: CIS and related benchmarks, guides | Writing: Review a sample benchmark report, decide where to spend fake money to address the remaining issues, and get scored against revealed threats, 3 pages (1 week) |
| System Security | 11 | Malware case studies | Read: Understanding the Mirai Botnet (<https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf>)  Read: Lenovo (<https://www.sans.org/reading-room/whitepapers/casestudies/lenovo-terrible-horrible-good-bad-week-35965>)  Discussion: Do some research, discuss an example of malware, why you found it interesting, what vulnerabilities (if any) were associated with it. (1 week) |
| System Security | 12 | Anti-malware, host-based IDS, related topics | Read: Next Gen Security Software: Myths and Marketing (<https://www.welivesecurity.com/2017/02/13/next-gen-security-software-myths-marketing/>)  Writing: Research ransomware, write a brief summary of why it is a problem now (as opposed to 10 years ago), what mitigations help prevent/handle it, etc. 2 pages (1 week) |
| System Security | 13 | Vulnerabilities, scanning, management  CVSS, CVE | Read: Common Vulnerabilities and Exploits (CVE, <https://cve.mitre.org/>)  Read: Common Vulnerability Scoring System (CVSS, <https://www.first.org/cvss/>)  Writing: assess the risk of several fictional vulnerabilities (to be provided), including justification for the values chosen.  How would this guide your response to malware exploiting that vulnerability? What mitigations might be employed to counter these vulnerabilities if they couldn’t be patched right away? 6 pages (2 weeks) |
| System Security | 14 | Vulnerability case studies | Read: Everything You Know About the Vulnerabilities Equities Market is Wrong (<https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong> )  Read: Zero Days, Thousands of Nights… (<https://www.rand.org/pubs/research_reports/RR1751.html> )  Read: For Good Measure: To Burn or Not To Burn (<https://www.usenix.org/publications/login/summer2017/geer>)  Discuss: reflect on the readings - should the US expose or hide known vulnerabilities?  Can you find other relevant material on this question? (1 week) |
| System Security | 15 | Patch management; Asset management; Configuration management; Change management; File Integrity Management | Discussion: Between keystroke logging, session hijacking, password guessing, phishing: which presents the greatest risk to modern systems?  How do you protect against this?  Are there other authentication related threats? (1 week) |
| Identity and Access Management | 16 | Review and discussion of elements of Identity Management through a role playing exercise (exploring authentication, authorization, accountability, single sign-on, multi-factor, password management, access management, and privileged account management). | Read: Designing an Authentication System: A Dialogue in Four Scenes (<http://web.mit.edu/kerberos/dialogue.html>)  Writing: Give your reflections on the in-class “game”: what did you learn, what worked and didn’t work in the exercise, what changes would you make, etc. 3 pages (1 week) |
| Threats | 17 | Threats, Threat Agents | Read: The Landscape of Internet Threats (<http://www.icir.org/vern/talks/ThreatLandscape.Brazil.May15.pdf>)  Read: Recent CrowdStrike (or other) threat reports.  The 2013 report was especially interesting to me.  Discussion: why might someone want to “attack” OSU’s assets (systems, data, accounts…)?  How important is that we enumerate/understand \*all\* of these?  What’s the difference between defending against nation-state attackers and other threats, such as “hacktivists” or spammers? (1 week) |
| Threats | 18 | Nation-state threats | Read: Stuxnet: <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>  Watch: Stuxnet: Zero Days (the movie) (optional)  Read: Kaspersky: <https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html>  Discuss: Comment on the readings and find other examples of “nation-state” cyber attacks to compare/contrast with. |
| Threats | 19 | Insider Threat, User Behavior Analytics | Read: FBI’s Counterintelligence Vulnerability Assessment for Academia  Read: CERT Insider Threat readings (<https://www.cert.org/insider-threat/>)  Writing: reflect on Inside Threats.  What’s easy/hard about preventing and detecting these?  What’s the relationship between an Inside Threat program and security program? What privacy concerns does this generate? How might this differ between corporations and Universities? 3 pages (1 week) |
| Attacks, Intrusions, Intrusion Detection/Incident Response/Forensics | 20 | Kill chains; Tactics, Techniques and Procedures; | Read: Lockheed Martin “Kill Chain” (<https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>)  Read: Anything on TTP (Tactics, Techniques and Procedures)  Writing: Discuss mitigations for three attack patterns (to be provided) 4 pages (1 week) |
| Attacks, Intrusions, Intrusion Detection/Incident Response/Forensics | 21 | Security incident and data breach case studies. | Read: Case studies on security incidents (SONY, Target, Home Depot, Equifax)  Discuss: find other case studies (preferably not mentioned by others), compare/contrast (1 week) |
| Attacks, Intrusions, Intrusion Detection/Incident Response/Forensics | 22 | Intrusion Detection, Incident Response and Hunting table-top exercise | Read: Sample Incident Response Process (to be provided)  Writing: Intrusion Detection and Incident Response Tabletop post-mortem: your observations, what worked, what didn’t work, suggestions for improvement in the incident response process and in the exercise. 4 pages (1 week) |
| Attacks, Intrusions, Intrusion Detection/Incident Response/Forensics | 23 | Penetration Testing: Red, Blue and Purple Teams | Read: Sample pen-test scope document, template and report.  Discuss: what are the benefits and short-comings of penetration testing?  How can the Red and Blue teams help each other improve? (1 week) |
| Industrial Control Systems (ICS) | 24 | Industrial Control Systems, PERA Model | Read: Material from the PERA web site (<http://www.pera.net/>)  Research: Current ICS related incidents  Discussion: Reflections on reading/lecture, what’s the worst that could happen? (1 week) |
| Cloud | 25 | Cloud services and the challenges we face in securing them - assessments and auditing, authentication, monitoring, investigations… | Read: Cloud Security Alliance Guide (<https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf>)  Read: Security Operations Perspective on Cloud Services (OSU paper, to be provided)  Writing: in light of everything discussed so far, where are the challenges in adopting cloud solutions?  What Cloud Services are in use at OSU?  Any special challenges to the secure use of these services? 3 pages (1 week) |
| Internet of Things | 26 | The challenge of securing the Internet of Things. | Read: Zigbee Exploited (<https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf>)  Read: Dolphin Attack: Inaudible Voice Commands (<https://arxiv.org/abs/1708.09537>)  Read: This Doll May Be Recording What Children Say, Privacy Groups Charge (<https://www.npr.org/sections/alltechconsidered/2016/12/20/506208146/this-doll-may-be-recording-what-children-say-privacy-groups-charge>)  Discussion: In light of what we’ve discussed this semester and what you know about the Internet of Things, discuss what security controls should be applied to secure the IoT and what new controls might be needed. (1 week) |
| Trends, the future, roadmaps | 27 | The past and future of Information Security, with particular attention to what’s changing and what’s not and how well we can predict future trends. | Read: Verizon data breach report 2009, plus the current Verizon data breach report  Writing: pick two annual reports from the same source, three years apart (preferably one recent, one from three years ago).  For the predictions made in the older report, which have come true, which haven’t?  Reflect on this and the ramifications for making plans for future security needs. 3 pages (1 week) |
| Summing up, loose ends | 28 | TBD | Writing: reflect on the main things you learned from this class. 4 pages (1 week) |