Term Information

Effective Term	Autumn 2018

General Information

Course Bulletin Listing/Subject Area	International Studies
Fiscal Unit/Academic Org	UG International Studies Prog - D0709
College/Academic Group	Arts and Sciences
Level/Career	Undergraduate
Course Number/Catalog	4702
Course Title	Case Studies in Information Security
Transcript Abbreviation	Case Stud Info Sec
Course Description	This course will provide students who have taken an introductory Information Security course a deeper understanding of the background, terminology and concepts of Information Security. The course will focus heavily of behavioral outcomes, such as developing security requirements from business use-cases, comparing security requirements against implementation reality.
Semester Credit Hours/Units	Fixed: 3

Offering Information

Length Of Course	14 Week, 12 Week, 8 Week, 7 Week, 6 Week, 4 Week
Flexibly Scheduled Course	Never
Does any section of this course have a distance education component?	No
Grading Basis	Letter Grade
Repeatable	No
Course Components	Lecture
Grade Roster Component	Lecture
Credit Available by Exam	No
Admission Condition Course	No
Off Campus	Never
Campus of Offering	Columbus

Prerequisites and Exclusions

Prerequisites/Corequisites	INTSTDS 3702 and CSE 4471
Exclusions	
Electronically Enforced	Yes

Cross-Listings

Cross-Listings	None

Subject/CIP Code

Subject/CIP Code	45.0901
Subsidy Level	Baccalaureate Course
Intended Rank	Sophomore, Junior, Senior

Requirement/Elective Designation

Required for this unit's degrees, majors, and/or minors

Course Details

Course goals or learning objectives/outcomes

- Students gain deeper understanding of the application of a variety of security controls to address risk based on real-world examples.
- Students gain knowledge of intrusion detection, threat hunting and incident response/investigations, identity and access management, inside threats and user behavior analytics.
- Students gain knowledge of information security threats with a focus on the underground economy, organized crime and nation-states.

Content Topic List

- Tools for thinking about security, examples of security-related programs being sold on the internet, costs and risks of security controls.
- Ohio State University security policies and framework.
- System Security: system hardening, malware case studies, vulnerabilities, scanning/patch/asset/file integrity management.
- Identity and access management.
- Threats from nation-states, insider threats, user behavior analytics.
- Attacks, intrusions and detection/incident response/forensics.
- The Cloud, Internet of Things, and future trends in information security.

Sought Concurrence

No

Attachments

- IS 4702_FinalSyllabus.docx

  (Syllabus. Owner: Meltz,Richard Lee)

Comments

- This course is submitted in conjunction with International Studies' proposal to establish a minor in Information Security. *(by Meltz,Richard Lee on 12/21/2017 02:22 PM)*

Workflow Information

Status	User(s)	Date/Time	Step
Submitted	Meltz,Richard Lee	12/21/2017 02:22 PM	Submitted for Approval
Approved	Mughan,Anthony	12/21/2017 02:41 PM	Unit Approval
Approved	Haddad,Deborah Moore	12/21/2017 04:07 PM	College Approval
Pending Approval	Nolen,Dawn Vankeerbergen,Bernadette Chantal Oldroyd,Shelby Quinn Hanlin,Deborah Kay Jenkins,Mary Ellen Bigler	12/21/2017 04:07 PM	ASCCAO Approval

International Studies 4702
Case Studies in Information Security
Spring 2019

Short Description

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 behavioral 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 drawn from publicly available sources.

Instructor

Steve Romig, Office of the CIO

Mount Hall

romig.1@osu.edu

(614) 688-3412

Office Hours: TBD

Class Time: T/Th

Location/Room: TBD

Pre-Requisites

CSE 4471, “Introduction to Information Security”

International Studies 3702, “Herding Cyber Cats”

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

Required Readings

See Schedule Below

Course Assignments and Grading

The course will require weekly reading, including identification of “current events” for discussion online and in class.

Grading for the course will be largely based on participation in on-line and in-class discussions and on four individual and group projects where students research, analyze and present case studies and other detailed analysis relating to the material discussed in class. This will include one or two short (15-20 minute) presentations in class.

Sample reading assignments:

- Ken Thompson, “Reflections on Trusting Trust”, Turing Award Lecture, Association for Computing Machinery, August 1984, http://dl.acm.org/citation.cfm?id=358210
- Jason Franklin, Adrian Perrig, Vern Paxson, Stefan Savage, “An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants”, CCS, 2007, http://www.icir.org/vern/papers/miscreant-wealth.ccs07.pdf
- Peter Loscocco, Stephen Smalley, Patrick Muckelbauer, Ruth Taylor, S. Jeff Turner, John Farrell, “The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments”, 21st National Information Systems Security Conference, October 1998, https://www.cs.utah.edu/flux/fluke/html/inevit-abs.html
- “Verizon’s 2017 Data Breach Investigations Report”, May 2017, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
- Center for Internet Security (CIS) Benchmark, https://www.cisecurity.org/cis-benchmarks (license required, available through OSU Enterprise Security)
- OSU Computer Security web site: https://cybersecurity.osu.edu/
- OSU Information Security Standard (ISS): https://go.osu.edu/infosec-iss (OSU login required)
- OSU Information Security Control Requirements (ISCR): https://go.osu.edu/infosec-iscr (OSU login required)
- Material on Stuxnet, such as the book “Countdown to Zero Day” by Kim Zetter or the documentary “Zero Days” directed by Alex Gibney.
- Material relating to security incidents such as the 2013 Target breach, the 2014 Home Depot breach, the 2014 Sony Pictures breach, the 2016 DNC breach and so on.

Papers/Presentations

Students will complete at least four writing assignments or presentations as individuals and in small groups (2-3 people). These assignments will generally involve some analysis and/or comparison involving “real world” scenarios and application of general security controls (most frequently using OSU’s Security Framework as a common base for comparison). Each of the 4 projects will account for 15% of the total grade, for a total of 60% of the grade.

Discussions/Participation

Students are expected to discuss the weekly readings and “current events” in class and on-line. Grading will be based on relevance, accuracy of analysis and application of common security principles and controls. This will make up 30% of the grade.

Attendance

With certain exceptions (exams or exam reviews), I will take attendance every class period using Top Hat. Top Hat is online system whereby you use your phone, tablet or phone to acknowledge your class attendance. Days that attendance will be taken are noted with an "a" on the course schedule. *You may miss up to TWO classes without a loss of attendance points. After that, you will lose FIVE points for every class (noted with an "a" on the course schedule) that you miss.* See course policies below for more specific information. Attendance will be 10% of the total grade.

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

Course Policies

Attendance and Participation

Attendance is *critical* in this class and will be taken daily. If you forget to check-in you could lose your attendance point for that day. Attendance will be taken every day, except where noted on the syllabus (e.g.,exam and review days).

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.

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

Make-up Presentations

Make-up presentations will be arranged for university-excused or unavoidable circumstances (e.g., deaths, personal/family illness and emergencies) with prior notification or written verification within 72 hours of your absence. If you are not present in a class during an exam or presentation, and you do not have the proper documentation, you will not be allowed to make it up.

Late Work

Assignments should be handed in on time. However, I do understand that situations occasionally come up. 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.

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.

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:lj studentaffairs.osu.edu/info for students/csc.asp).

Disability Statement

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. In addition, I have created a module for each class (by date and topic) in Canvas. The class module contains more detailed information about the topic, readings, activities and reflection assignments. Failure to review a class module may result in you missing a reflection assignment or reading, which could negatively influence your discussion participation score.

Topic	week	day	Topics	Reading	Assignment
Course Overview	1	1	Course Overview; syllabus review; beyond the CIA triad; privacy, anonymity, attribution, repudiation	"Beyond the CIA Triad", Jim West (https://isc2usmg.org/images/documents/Beyond_the_CIA_Triad.pdf) "Dilemas 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?
Course Overview	1	2	Concepts and Terminology	"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) "Show Me the Money: Characterizing Spame 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.
Tools for Thinking About Security	2	1	Attack trees, attack graphs	Attack Trees, Shneier (https://www.schneier.com/academic/archives/1999/12/attack_trees.html) 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?

Risk	2	2	Overview of Risk	Sample risk assessment, risk assessment template.(OSU)	Writing: create an attack tree; create an attack graph for attacks against cookies in a setting of your choosing.
OSU's Security Policies and Framework	3	1	Security policies and standards	Responsible Use: https://it.osu.edu/sites/default/files/files-1477502439/responsible-use-of-university-computing-and-network-resources-policy.pdf Data Classification: https://it.osu.edu/sites/default/files/files-1477502242/institutionaldata.pdf Data Elements: https://cybersecurity.osu.edu/system/files/2017/08/30/osuidp-dataelementclassificationassignments.pdf IT Security: https://it.osu.edu/sites/default/files/files-1477502296/itsecurity.pdf	None: focus on the reading for this week.
OSU's Security Policies and Framework	3	2	Information Security Standards	Information Security Standard: https://cybersecurity.osu.edu/system/files/osu.iss.v1.5.pdf Information Security Control Requirements (ISCR): https://cybersecurity.osu.edu/system/files/osu.iscr.v1.5.1.pdf	Writing: classify a given list of data, and for each list the services where it can be stored.
OSU's Security Policies and Framework	4	1	Information Security Standards	ISCR IT1-IT9, selected sample evidence of implementation	None: focus on the reading for this week.
OSU's Security Policies and Framework	4	2	Information Security Standards	ISCR IT10-IT18, selected sample evidence of implementation	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?
System Security	5	1	System hardening: CIS and related benchmarks, guides	CIS documentation, especially their Benchmarks. https://www.cisecurity.org/ Sample CIS scan of a Windows desktop	None: focus on the reading for this week.
System Security	5	2	System hardening: CIS and related benchmarks, guides	Review the benchmark spending assignment, discussion of how benchmarks are typically applied and managed.	Writing: Review a sample benchmark report, decide where to spend fake money to address the remaining issues, and get scored against revealed threats.

System Security	6	1	Malware case studies	Understanding the Mirai Botnet (https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf) 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.
System Security	6	2	Anti-malware, host-based IDS, related topics	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 its a problem now (as opposed to 10 years ago), what mitigations help prevent/handle it, etc.
System Security	7	1	Vulnerabilities, scanning, management CVSS, CVE	Common Vulnerabilities and Exploits (CVE, https://cve.mitre.org/) 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 software exploiting that vulnerability?
System Security	7	2	Vulnerability case studies	Everything You Know About the Vulnerabilities Equities Market is Wrong (Everything You Know About the Vulnerability Equities Process Is …) Zero Days, Thousands of Nights… (Zero Days, Thousands of Nights: The Life and ... - RAND Corporation) 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? Ca n you find other relevant material on this question?
System Security	8	1	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?

Identity and Access Management	8	2	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).	Designing an Authentication System: A Dialogue in Four Scenes (http://web.mit.edu/kerberos/dialogue.html)	Writing: reflections on the in-class "game"
Threats	9	1	Threats, Threat Agents	The Landscape of Internet Threats (http://www.icir.org/vern/talks/ThreatLandscape.Brazil.May15.pdf) 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?
Threats	9	2	Nation-state threats	Stuxnet: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ Stuxnet: Zero Days (the movie) (optional) Kaspersky: https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html	None: focus on the reading or watch the movie.
Threats	10	1	Insider Threat, User Behavior Analytics	FBI's Counterintelligence Vulnerability Assessment for Academia 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 privacy?

Attacks, Intrusions, Intrusion Detection/Incident Response/Forensics	10	2	Kill chains; Tactics, Techniques and Procedures;	Lockheed Martin “Kill Chain” (https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf) Anything on TTP	Writing: Discuss mitigations for three attack patterns (to be provided)
Attacks, Intrusions, Intrusion Detection/Incident Response/Forensics	11	1	Security incident and data breach case studies.	Case studies on security incidents (SONY, Target, Home Depot, Equifax)	Discuss: find other case studies (preferably not mentioned by others),
Attacks, Intrusions, Intrusion Detection/Incident Response/Forensics	11	2	Intrusion Detection, Incident Response and Hunting (with a tabletop exercise)	Intrusion Detection and Incident Response prep reading	Writing: Intrusion Detection and Incident Response Tabletop post-mortem
Attacks, Intrusions, Intrusion Detection/Incident Response/Forensics	12	1	Penetration Testing: Red, Blue and Purple Teams	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?
Industrial Control Systems (ICS)	12	2	Industrial Control Systems, PERA Model	PERA web site (http://www.pera.net/) Current ICS related incidents	Discussion: what’s the worst that could happen?
Cloud	13	1	Cloud services and the challenges we face in securing them - assessments and auditing, authentication, monitoring, investigations…	Cloud Security Alliance Guide (https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf) Romig: Security Operations Perspective on Cloud Services	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?
Internet of Things	13	2	The challenge of securing the Internet of Things.	Zigbee Exploited (https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf) DolphinAttack: Inaudible Voice Commands (https://arxiv.org/abs/1708.09537) 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.

Trends, the future, roadmaps	14	1	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.	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.
Summing up, loose ends	14	2	TBD		Writing: reflect on the main things you learned from this class (2-3 pages).