

MIS 3507: Defending Against Cybercrime

October 16, 2018

Fall 2018

Room Alter A603 on Tuesdays and Thursday from 3:30pm-4:50pm

Instructor Info

Name: Dr. Anthony Vance

Office Location: Speakman 207E

Office Phone: 801-361-2531

Office Hours: Tuesday, Thursday 2-3:15pm; or by appointment

Email: anthony@vance.name

Web: <https://anthonyvance.com>

Course Information

Description

This course is a broad introduction to the managerial issues of information security. Because security is multifaceted, the topics of the class range widely, including technical (e.g., cryptography), managerial (e.g., policy compliance), physical (e.g., door locks), and psychological (e.g., social engineering) issues. A key objective of the class is to develop a security mindset, in which one learns to think like an attacker for ways to exploit a system.

Learning Outcomes

Develop a security mindset

Learn to think like a security professional—how to identify threats like an attacker, and how to model and mitigate those threats.

Gain a working knowledge of methods of protecting data

Gain a working knowledge of modern methods of protecting data: encryption, hashing, confidentiality, authentication, integrity, non-repudiation, certificates, and IP security.

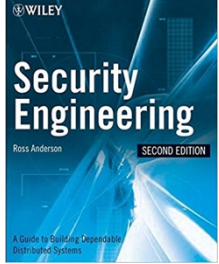

Learn methods of attack and defense

Learn methods of attacking systems and how to protect against those methods of attacks.

Appreciate the broad disciplines required for IS security

Appreciate the broad disciplines required for information security to work. We'll cover subjects as diverse as cryptology, physical security, psychology, and management.

Course Textbook

	<p>Required textbook: "Security Engineering: A Guide to Building Dependable Distributed Systems 2nd Edition," by Ross Anderson.</p> <p>Free PDF of the book: http://www.cl.cam.ac.uk/~rja14/book.html</p> <p>Amazon: http://a.co/9bzf6zP</p>
	<p>Optional: "Secrets and Lies: Digital Security in a Networked World," by Bruce Schneier.</p> <p>Excellent overview of information security, from cryptography to authentication, and to the human factor.</p> <p>Available online via Temple Library: https://goo.gl/ty5y2Z</p> <p>Amazon: https://amzn.com/0471453803</p>

Participation Policy

Contribution will account for 5% of your final grade. Most students will earn 80% of these points. Students who are exceptional and go above and beyond in enhancing the classroom experience may receive a higher score.

The following list is not comprehensive, but rather an example of items weighted in the contribution category:

- Providing feedback on the class via the course evaluation
- Treating others with respect
- Showing courtesy for presenters (guest speakers, instructor, students)
- Participating in class discussions
- Arriving on time and not leaving early
- Not using technology inappropriately (distracting yourself or others)

Classroom Procedures

It is alright to use your laptop to take notes, but do not use it for non-class related activities. Not only does this diminish your learning experience, but it distracts those around you.

Out of respect for our guest speakers, do not use electronic devices (e.g., laptops and cell phones) during their presentations. If you want to take notes, please do so on paper.

Assignments

Midterm Project Report

This is a group project. The midterm will be a vulnerability and penetration assessment report of a server. On Friday, October 5th, Teams of students will be given an IP address of a server to assess for security weaknesses. The midterm report will be due two weeks later on Friday, October 19th.

Readings Quizzes

Most readings and videos on the schedule have associated quizzes. Quizzes are **open book, open Internet** and must be completed within 30 minutes. You can take these on Canvas. Quizzes are due by **2:30pm** on the date due.

Labs

Labs are hands-on learning activities that will be begun in class and completed outside of class. Labs are typically due one week after they are introduced in class.

Threat Assessment Project

This is a group project. Teams will choose a recent security incident, summarize what happened, and give recommendations for how the threat could have been better managed. The report will also include a risk assessment of other potential threats the chosen organization faces, along with recommendations for mitigating each identified threat. Deliverables include a written report due on December 6th.



Required Reading

You are required to read one of the books on the "Security Readings" list at the end of this document by the last day of class, December 6th. To receive credit, submit your report via a quiz posted on Canvas. Indicate which book you read, whether you read the whole book, and give your brief reaction to it.


For **extra credit**, you may read an additional security book from the list of security books or one approved by Dr. Vance to replace your lowest lab score. If you choose this option, submit your report through this quiz by the last day of class, December 6th.


Required Security Films

Two films are required viewing for this course: "Zeros Days" and "Citizenfour." To receive credit, watch each film and simply indicate that you watched the whole film and give your brief reaction to the film on a quiz posted on Canvas.

	<p>"Citizenfour" by Laura Poitras</p> <p>The 2015 Academy Award winner for Best Documentary Feature, this film tells the story of Edward Snowden and the NSA spying disclosures of 2013.</p> <p>Availability: https://www.justwatch.com/us/movie/citizen-four</p> <p>Rated R. Edited version available on Vidangel.com.</p>
	<p>"Zero Days" by Alex Gibney</p> <p>A 2016 documentary about Stuxnet and the advent of cyberwarfare.</p> <p>Availability: https://www.justwatch.com/us/movie/zero-days</p> <p>Rated PG-13. Edited version available on Vidangel.com.</p>

For **extra credit**, you may watch either "The Lives of Others" or "The Conversation" to replaced one missed quiz. To receive credit, complete this quiz by the last day of class, December 6th.

	<p>"The Lives of Others" by F. Henckel von Donnersmarck</p> <p>The 2007 Oscar winner of Best Foreign Language Film of the Year, this film tells the story of a secret police agent in East Berlin in 1984 who surveils a writer and becomes increasingly absorbed in his life.</p> <p>Availability: https://www.justwatch.com/us/movie/the-lives-of-others</p> <p>Rated R. Edited version available on Vidangel.com.</p>
---	---

	<p>"The Conversation" by Francis Ford Coppola</p> <p>A classic 1974 film psychological thriller starring Gene Hackman that revolves around surveillance. It is more relevant today than when it debuted.</p> <p>Availability: https://www.justwatch.com/us/movie/the-conversation</p> <p>Rated PG. Edited version available on Vidangel.com.</p>
---	--

Late Work

All assignments and projects are to be submitted on time or early, so plan accordingly. If you have to miss class please submit your assignment early. On rare occasions, an exception may be granted, allowing the student to submit the work late with a 20% penalty. Under no circumstances will anything be accepted more than a week late.

Certification Option

As an option, students seeking certification may replace the final exam by passing the Security+ certification or another certification approved by the instructor. You can substitute your score on the certification (plus an adjustment–5% for the Security+) for the final. For example, if you received an 85% on the Security+ exam you would receive a 90% for your final exam score.

To receive credit for the certification, a student must show evidence of having taken the certification exam by the last day of class (5/1). If a student doesn't show the instructor evidence of passing the certification by this date, then he/she will be required to take the final exam.

Point Breakdown

Category	Points
Labs	300
Final exam	200
Midterm	150
Quizzes	100
Security book quiz	75
Threat assessment project	75
Security films quizzes	50
Participation	40
Course evaluation	10
Total	1000

Grading Scale

Grades	Scaled Points
A	930 points
A-	900 points
B+	870 points
B	830 points
B-	800 points
C+	770 points
C	730 points
C-	700 points
D+	670 points
D	630 points
D-	600 points
E	599 points or less

Schedule

Date	Topic	Assignments
Tuesday, 8/28/2018	Introduction to the Course	Anderson, Ch. 1
Thursday, 8/30/2018	Threat modeling	Read the beginning of each chapter, skim the rest of the chapter: "Threat Modeling," by Adam Shostack, Introduction , Chapter 1 , Chapter 4 Optional: Schneier, Chapter 21
Tuesday, 9/4/2018	Introduction to Cryptography	

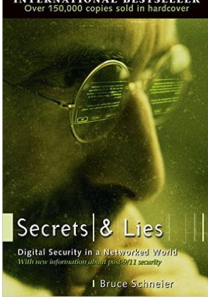
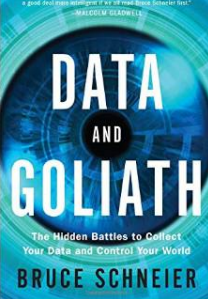
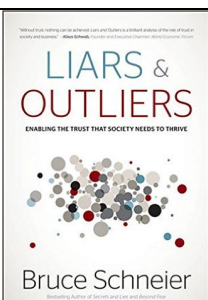
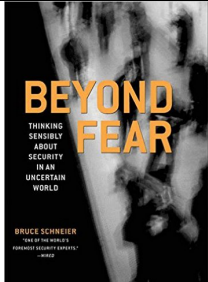
Thursday, 9/6/2018	Symmetric Cryptography	Quiz: Anderson, Ch. 5, pp. 129- 149
Saturday, 9/8/2018	Deadline to submit Lab 1: Threat Modeling	Lab 1: Threat Modeling
Tuesday, 9/11/2018	Asymmetric Cryptography	
Thursday, 9/13/2018	In-class video: "Codes," History Chanel episode of "Modern Marvels"	
Saturday, 9/15/2018	Deadline to email your PGP public key to Dr. Vance at anthony@vance.name.	
Tuesday, 9/18/2018	Digital Certificates and PKI	
Thursday, 9/20/2018	Authentication and Passwords	Anderson Ch. 2, pp. 31-39, 56-58 Lab 2: Symmetric Cryptography
Tuesday, 9/25/2018	Password Cracking	Gosney, " How LinkedIn's password sloppiness hurts us all " Goodin, " Why passwords have never been weaker " Quiz: Goodin, "Why passwords have never been weaker" Lab 3: Asymmetric Cryptography
Thursday, 9/27/2018	Dr. Vance is out of town. Watch three of the following: Enigma 2017 talk: " The Paper Ballot Is Not Enough ," Ben Adida, VP of Engineering, Clever. Slides .	Lab 4: Digital Certificates and PKI

	<p>Enigma 2017 talk: "Inside "MOAR TLS:" How We Think about Encouraging External HTTPS Adoption on the Web." Emily Schechter, Google. Slides.</p> <p>Enigma 2017 talk: "What Cybersecurity Can Learn from the Secret Service," Nathaniel Gleicher, Head of Cybersecurity Strategy, Illumio. Slides.</p> <p>Enigma 2017 talk: "Drawing the Foul: Operation of a DDoS Honeygot," Damian Menscher, Security Reliability Engineer, Google. Slides.</p> <p>Enigma 2016 talk: "Why Is Usable Security Hard, and What Should We Do about It?" Adrienne Porter Felt, Staff Software Engineer, Google Chrome. Slides.</p> <p>Enigma 2016 talk: "Disrupting Nation State Hackers," Rob Joyce, Chief, Tailored Access Operations, National Security Agency. Slides.</p>	
Tuesday, 10/2/2018	Introduction to Linux	
Thursday, 10/4/2018	Vulnerability Scanning	
Saturday, 10/6/2018		Lab 5: Password Cracking
Tuesday, 10/9/2018	Vulnerability Exploitation	
Thursday, 10/11/2018	In-class Lab	Lab 6: Vulnerability Scanning
Tuesday, 10/16/2018	Midterm begins No class, work on midterm	
Thursday, 10/18/2018	Optional: Exploitation tutorial	Lab 7: Exploitation
Tuesday, 10/23/2018	Physical security Midterm report due	Quiz: Anderson, Chapter 11
Thursday, 10/25/2018	The Human Element of Security	Online video: Bruce Schneier, The Security Mirage

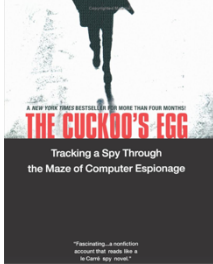
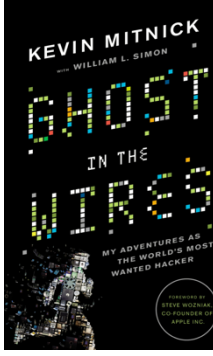
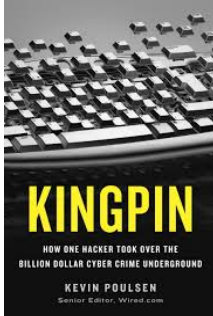
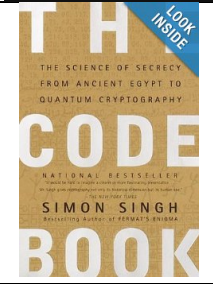
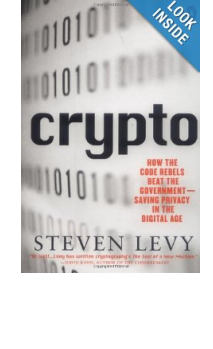
		"Cosmo, the Hacker 'God' Who Fell to Earth," by Mat Honan.
Tuesday, 10/30/2018	TBA	Lab 8: Physical Security
Thursday, 11/1/2018	Information Privacy	Lab 9: Social Engineering
Tuesday, 11/6/2018	Elections security	
Thursday, 11/8/2018	Network Security Monitoring and Incident Response	"Network Security Monitoring," by Richard Bejtlich, Chapter 1 Lab 10: Online Privacy
Tuesday, 11/13/2018	Network Security Monitoring In-class Lab	
Thursday, 11/15/2018	Information Security in Organizations	
Tuesday, 11/20/2018	Fall break, no class	
Thursday, 11/22/2018	Thanksgiving	
Tuesday, 11/27/2018	Malware Analysis	Introduction and Chapter 0 of Practical Malware Analysis by Sikorski and Honig. Lab 11: Network Security Monitoring
Thursday, 11/29/2018	Security and Terrorism	
Tuesday, 12/4/2018	TBA	Lab 12: Malware Analysis
Thursday, 12/6/2018	Course wrap-up	

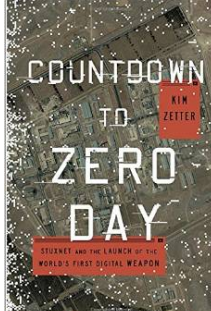
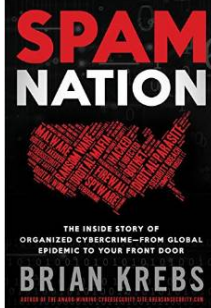
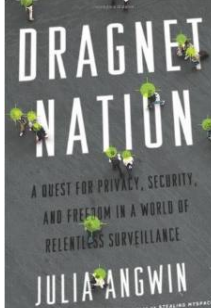
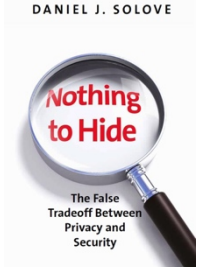
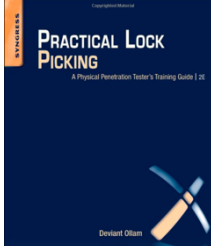
Thursday, 12/11/2018	Study day	
Tuesday, 12/13/2018	Final exams begin	
Wednesday, 12/19/2018	Last day of final exams	

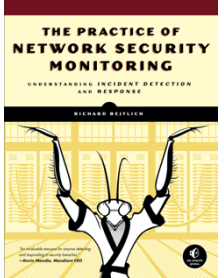
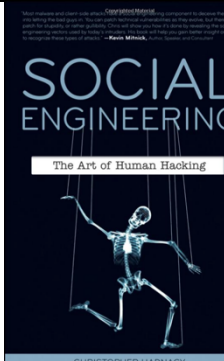
Selected Security Books by Bruce Schneier

	<p>“Secrets and Lies: Digital Security in a Networked World,” by Bruce Schneier.</p> <p>Excellent overview of information security, from cryptography to authentication to the human factor.</p> <p>Available online via Temple Library: https://goo.gl/ty5y2Z Amazon: https://amzn.com/0471453803</p>
	<p>“Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World,” by Bruce Schneier.</p> <p>Great book about the threats of surveillance to society, and what we can do about it. After reading the book, you probably won’t view surveillance the same way again.</p> <p>Available at Temple Library Amazon: http://amzn.com/0393244814</p>
	<p>“Liars and Outliers: Enabling the Trust that Society Needs to Thrive,” by Bruce Schneier.</p> <p>Interesting book about how security enables trust that society needs to function.</p> <p>Available online via Temple Library Amazon: https://amzn.com/1118143302</p>
	<p>“Beyond Fear,” by Bruce Schneier.</p> <p>This book is about national security, terrorism, and how to think sensibly about whether security measures are worth the cost to society.</p> <p>Available at Temple Library Amazon: https://amzn.com/1475781199</p>

Other Excellent Security Books

	<p>The Cuckoo's Egg</p> <p>Classic security novel—the true story of how a network admin got caught up in global computer espionage using network security monitoring. Reads like a thriller.</p> <p>Available at Temple Library Amazon: http://amzn.com/1416507787</p>
	<p>“The Ghost in the Wires” by Kevin Mitnick</p> <p>Autobiography of Kevin Mitnick, famed computer hacker and social engineer. In addition to being a very entertaining and fascinating read, you'll learn a lot about social engineering techniques from the accounts of his experiences.</p> <p>Available at Temple Library Amazon: http://amzn.com/0316037729</p>
	<p>“Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground,” by Kevin Poulsen.</p> <p>Amazon: http://amzn.com/0307588696</p>
	<p>“The Code Book” by Simon Singh.</p> <p>This is a very interesting and gripping book about the history and intrigue of cryptography and cryptanalysis.</p> <p>Available at Temple Library Amazon: http://amzn.com/0470474246</p>
	<p>“Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age” by Steven Levy.</p> <p>A very engaging look at the modern history of cryptography, including the development of DES, RSA, and PGP. Also, it describes the fight in the 1990's to legalize the use of strong cryptography.</p> <p>Available at Temple Library Amazon: http://amzn.com/0140244328</p>

	<p>"Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon," by Kim Zetter.</p> <p>Interesting and compelling read about the discovery of Stuxnet and how it changed the world.</p> <p>Available at Temple Library Amazon: http://amzn.com/077043617X</p>
	<p>"Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door," by Brian Krebs.</p> <p>In <i>Spam Nation</i>, investigative journalist Brian Krebs unmasks the criminal masterminds driving some of the biggest spam and hacker operations targeting Americans and their bank accounts. Tracing the rise, fall, and alarming resurrection of the digital mafia behind the two largest spam pharmacies-and countless viruses, phishing, and spyware attacks-he delivers the first definitive narrative of the global spam problem and its threat to consumers everywhere.</p> <p>Amazon: http://amzn.com/1402295618</p>
	<p>"Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance," by Julia Angwin</p> <p>Award-winning journalist Julia Angwin reports from the front lines of America's surveillance economy, offering a revelatory and unsettling look at how the government, private companies, and even criminals use technology to indiscriminately sweep up vast amounts of our personal data.</p> <p>Available at Temple Library Amazon: http://amzn.com/0805098070</p>
	<p>"Nothing to Hide" by Daniel Solove</p> <p>A book that debunks the most common attack to privacy arguments.</p> <p>Available online via Temple Library Amazon: http://amzn.com/0674035070</p>
	<p>"Practical Lock Picking, Second Edition: A Physical Penetration Tester's Training Guide" by Deviant Ollam</p> <p>The best book available to learn lock-picking.</p> <p>Available online via Temple Library Amazon: http://amzn.com/1597499897</p>

	<p>“Keys to the Kingdom: Impressioning, Privilege Escalation, Bumping, and Other Key-Based Attacks Against Physical Locks” by Deviant Ollam</p> <p>Another great and accessible book on more advanced lock-picking by Deviant Ollam.</p> <p>ScienceDirect (free through Temple): https://www.sciencedirect.com/science/article/pii/B9781597499835000105</p> <p>Amazon: http://amzn.com/1597499838</p>
	<p>The Practice of Network Security Monitoring by Richard Bejtlich</p> <p>Excellent book on the principles of NSM and how to get started with Security Onion.</p> <p>Available online via Temple Library</p> <p>Amazon: http://amzn.com/1593275099</p>
	<p>“The Art of Deception” by Kevin Mitnick</p> <p>In-depth discussion of the techniques of social engineering and how to educate your organization to be less susceptible to these attacks.</p> <p>Available at Temple Library</p> <p>Amazon: http://amzn.com/076454280X</p>
	<p>“Social Engineering” by Christopher Hadnagy</p> <p>Another well-regarded book on social engineering, from the organization that operates the Social Engineer Village at DEFCON.</p> <p>Available online via Temple Library</p> <p>Amazon: http://amzn.com/0470639539</p>
	<p>“Unmasking the Social Engineer,” by Chris Hadnagy.</p> <p>From the publisher: “<i>Unmasking the Social Engineer: The Human Element of Security</i> focuses on combining the science of understanding non-verbal communications with the knowledge of how social engineers, scam artists and con men use these skills to build feelings of trust and rapport in their targets.”</p> <p>Available online via Temple Library</p>

	Amazon: http://a.co/d1A6C17
--	---