LIS 510
Information Security and Privacy

Information School
University of Wisconsin-Madison
Spring 2021

Instructor: Dorothea Salo (please call me "Dorothea")
Student hours: on BBCollaborate, 1-3PM Thursdays or by appointment
Special course attributes: Intermediate, Graduate, Digital Studies P
salo@wisc.edu
Canvas: https://canvas.wisc.edu/courses/244252
Instructional mode: Online asynchronous

Introduction

Course description

Students completing this course will earn three credit hours. This class meets for one 150-minute class period each week over the semester, and carries the expectation that students will work on course learning activities (reading, writing, problem sets, studying, etc) for about 6 hours out of the classroom for every class period.

This course requires sophomore standing, but has no specific prerequisites or co-requisites. No prior technology or computer-science experience is assumed.

Introduction to personal, social, organizational, and basic technical concepts, skills, and processes related to the digital security and privacy of individuals and organizations. Preparation to help individuals and organizations enhance their own security and privacy, especially but not exclusively online.

Phenomena to be examined include:

- individual and societal need for digital privacy, safety, and security; governmental, commercial, workplace, and (especially) educational surveillance
- privacy and security law; privacy and security ethics
- individual and organizational behavior with regard to digital privacy, safety and security:
  - usability of security measures,
  - impact of (lack of) usability on security
  - incentives (and lack thereof) for good security practices
- "open-source intelligence" (OSINT); Internet of Things security; workplace bring-your-own-device security; mobile security and privacy
- common attack types: social engineering attacks, insider attacks, contractor attacks, supply-chain attacks
- risk assessment and mitigation: threat assessment; attack surfaces; attack tactics, techniques, and procedures; MITRE ATT&CK Framework and the CyberKillChain
- authentication, authorization, access control, identity, and attacks against them; passwords and attacks on them; biometric authentication and attacks on it
- security technologies and practices: log analysis, network and storage monitoring, digital forensics, pentesting
- vulnerabilities, vulnerability disclosure; ethical hacking

Assignments in this course offer repeated practice in *communicating* about privacy and security. Why? Because communication skills (such as incident reporting, composing training materials, communicating with people in power, and technical communication aimed at layfolk) are commonly noted as *absolutely required* in job contexts involving online security—as well as commonly noted as lacking in too many information security and privacy professionals.

Course learning outcomes

1. Communicate clearly and effectively to non-expert audiences about security vulnerabilities and security-related incidents (both grad and undergrad).
2. Mitigate common risks to information security and privacy (both grad and undergrad).
3. Use common command-line Linux tools related to information security and privacy (both grad and undergrad).
4. Develop awareness of the structure of the information security and privacy fields, and career opportunities within them (both grad and undergrad).
5. Build strategies and sources for current awareness of security and privacy issues (both grad and undergrad).

6. Demonstrate understanding of professional competencies important for management of information organizations (graduate).
7. Demonstrate understanding of societal, legal, policy or ethical information issues (graduate).
8. Demonstrate understanding of issues surrounding marginalized communities and information (graduate).

Course Policies

I aim to make this course as accessible as possible to all students. Students seeking accommodations for lecture or assignments must obtain a McBurney Center VISA. For more information, see `https://mcburney.wisc.edu/apply-for-accommodations/`.

Preferred name/pronouns: It is sometimes the case that a student's legal name or gender assigned at birth are reported to me on official documents in a form not in keeping with that student's preferred name or gender expression. Please let me know, as you are comfortable, about your preferences. My pronouns are she/her/hers. UW-Madison also permits students to indicate a preferred name: `https://registrar.wisc.edu/preferred_name.htm` Canvas does as well: https://kb.wisc.edu/luwmad/page.php?id=108069

Contacting me

READ THE SYLLABUS before asking a question, please; the syllabus may answer it! For any difficulty with the course that is not private or confidential, please speak up in class; I *will not answer such questions by email*. Please also do your best to assist your classmates.

Should you see dead links (it does happen, usually with no notice), weird due dates, or other syllabus problems, please bring them up in the appropriate Canvas forum.

Textbooks and software

REQUIRED:

- Andress, Jason. *Foundations of Information Security: A Straightforward Introduction*. No Starch Press: 2019. Library ebook: `https://search.library.wisc.edu/catalog/9912897557802121`
- Schneier, Bruce. *Secrets and Lies*. Wiley, 2000 (updated edition 2015). Library ebook: `https://search.library.wisc.edu/catalog/9912219160102121` I encourage you to purchase your own; though its examples are admittedly dated, its explanations are classic. Either the original edition or the 2015 15th-anniversary edition is fine; we will generally be reading whole chapters, not page-specific segments.

Assignments

Grading scale

All final grades will be based on this scale:

A: 93.5-100, AB: 89.5-93.4, B: 83.5-89.4, BC: 79.5-83.4, C: 73.5-79.4, D: 64-73.4, F: anything below 64.

Due dates below are specified by module (mostly for my reference); exact due dates are listed on Canvas.

	Final-grade %	Due date
Jargon File questions	6%	Any time before the end of Module 7
In the News items	8%	Any time before the end of Module 7
Each one teach one!	5%	End of Module 4
Book review(s)	15%	Module 7; end of course for graduates' second review
Incident report presentation	10%	Module 10
Campus privacy report		
Module-specific assignments	26%	Due end of each module except Module 14
Final report	15%	Final day of course
Final communication artifact	15%	Final day of course

Jargon File questions

There is a "Jargon File" discussion forum on Canvas, available throughout the semester. It is where you ask questions about anything in readings or lecture that lost you, including but not limited to unfamiliar terminology. To normalize asking such

questions, I require that you make three posts, each post containing a question, in this forum before the end of Module 7. (One post containing three questions does not complete this assignment.) More questions are of course welcome and encouraged! As many as occur to you! Once you have finished posting your required questions, you may also ask questions related to privacy and/or security that are not specifically relevant to class.

To make my grading life easier, please leave a "grade this, please" note at the bottom of any question you are submitting for this grade. This is a do-the-thing, get-the-points assignment; I am not grading questions on any other criterion than their existence. Honor system, though: ask real questions, please!

Everyone is welcome to answer questions in the Jargon File forum as long as the answers are kind and helpful. Should I see condescension ("well actually" "everybody knows" "wow, what a basic question" and so on), insults, abuse, bias/hate, or other harmful speech in answers, I will immediately delete the answer, and the student responsible for that answer will receive an immediate and ineradicable zero for this assignment *no matter what question(s) they post*. I will not tolerate oneupsmanship or cruelty in this course; such behavior is unprofessional and immoral. I will also report incidents of bias and hate to the university through normal reporting channels.

In the News

There is an "In the News" discussion forum on Canvas. Before the end of Module 7, post links and brief (3-5 sentence) summaries for at least (undergraduates: two; graduates: four) just-published news items about privacy and/or security. Please prefer stories relevant to higher education (and libraries/archives/records/data, MA/LIS students). Stories can come from:

- mainstream general news outlets (such as the *Wisconsin State Journal*, the *New York Times*),
- information-technology or information-security news outlets (such as *Ars Technica*, *The Verge*, *Hacker News*),
- higher-education news outlets (such as *Chronicle of Higher Education*, *Inside Higher Ed*, *Educause Review*),
- well-known and respected weblogs (such as Troy Hunt's, Bruce Schneier's, Becky Yoose's, ALA's Choose Privacy Every Day), or
- (**MA/LIS students only**) library/archives news outlets (such as *American Libraries*, *Library Journal*)

You may post more stories once you have completed the ones I will grade, but please wait a day or two so that your classmates have a chance to read and post them! (I don't mind if folks share stories with classmates who haven't posted theirs yet. What you're really practicing here, besides current awareness, is the important communication skill of boiling down complicated information into a brief, helpful summary!) Beyond the summary, you are also welcome (but not required) to post your own reactions to and questions about the story.

As with your Jargon Files questions, please put a "grade this, please" note at the end of each post I need to give you points for, also reminding me whether you are a graduate or undergraduate student. I will only remove points for excruciatingly poorly-written summaries. (If English is not your first language, you get leeway on mechanical errors. I still expect your summary to be concise and helpful, however!)

By all means use Twitter to look for stories to post (I'll happily suggest accounts to follow!), but a tweet or tweet thread does not count for this assignment; same for a Facebook or LinkedIn post. (Don't rules-lawyer, please. The spirit of this rule is "social media can lead you to stories, but can't be the story.") You may post news stories covering novel research, but please do not post new research publications directly — stick to news, please.

Book review(s)

Read and review a book! A good book review is no more (ideally much less) than 1000 words long (I am giving you a breather here; many review venues insist on half that or less, and *shorter does not mean easier to write*) and engagingly written. It often includes (but need not be limited to!) a BRIEF summary of the book's argument(s), a summary of the book's strengths and weaknesses, and a recommendation (or not) for reading or purchase along with a statement of appropriate audiences for the book.

For more reviewing advice, I strongly suggest perusing the "First-Time Reviewer" suggestions at the *LSE Review* website: `http://blogs.lse.ac.uk/lsereviewofbooks/guidelines-and-examples/` I would specifically like you to evaluate *how well the book communicates* its arguments about privacy/security: for whom is it written? is it clear to that audience? understandable to them? persuasive? dismissive or otherwise offputting? scaremongering? complete, or suspiciously incomplete? How might it improve its approach? Do you agree with its arguments?

UNDERGRADUATES: One book review, written as for a newspaper, magazine, or news website. You may, if you wish, specify the targeted publication.

GRADUATES: Two book reviews, each book from a different category in the categorized list below, written as for a scholarly or professional journal. (*College and Research Libraries* has a review section, as do quite a few other LIS journals.) You may, if

you wish, specify the targeted publication, and I encourage you to contact journals that carry relevant reviews to volunteer to review one of the more recent publications on the list!

Post your review to the Book Reviews forum on Canvas by the day it is due. The forum is open throughout the course; you are welcome and encouraged to post reviews early. Do NOT attach your review as a Word file or PDF, please; this will mean an automatic zero! You are not required to read all posted reviews, but I do recommend that you read reviews for as many of the different books/collections as possible.

BOOK LIST:

N.b. I don't approve of all the books below; I haven't even *read* all of them! Do not write a positive review just because you think I want one. You can be honest! I want to know what I should and shouldn't read!

Fiction

- Shumeet Baluja, *The Silicon Jungle*
- Cory Doctorow, *Attack Surface*
- Annie Jacobsen, *First Platoon*
- Bruce Sterling, *The Zenith Angle*
- Connie Willis, *Crosstalk*

History, law, and ethics

- Sanjay Sharma, *Data Privacy and GDPR Handbook* (Recommended for those interested in privacy-related careers.)
- Sarah E. Igo, *The Known Citizen: a history of privacy in modern America*

Individual privacy and security

- Nora A. Draper: *The Identity Trade: selling privacy and reputation online*
- Brian Kernighan, *Understanding the Digital World*
- Bruce Schneier, *Beyond Fear*
- Marvin Waschke, *Personal Cybersecurity*
- Jacqueline Ryan Vickery, *Worried about the Wrong Things*

Society, privacy, and security

- Bruce Schneier, *Data and Goliath* or *Click Here to Kill Everybody* or *Liars and Outliers* or *We Have Root*
- Woodrow Hartzog, *Privacy's Blueprint: the battle to control the design of new technologies*
- Susan Athey, *The Digital Privacy Paradox*
- Shoshana Zuboff, *Surveillance Capitalism*

Digital security how-tos

Word to the wise: The technical content of books in this category varies widely. I recommend skimming a book before you choose it to review. Computer-science and software-engineering undergrads, MS/Info folks: I suggest you pick from this list!

- Adkins et al. *Building Secure and Reliable Systems* Open access from `https://static.googleusercontent.com/media/landing.google.com/en//sre/static/pdf/Building_Secure_and_Reliable_Systems.pdf`
- Arbuckle and El Emam, *Building an Anonymization Pipeline: creating safe data*
- Shancang Li, *Securing the Internet of Things*
- John Bandler, *Cybersecurity for the Home and Office*

Many books on the list are available electronically: on the open web, via UW-Madison library subscription, or for relatively-inexpensive purchase. You may be able to find some in local public libraries, but please observe all COVID-19-related precautions if you avail yourself of a print library book. If you would like to review a relevant book I haven't listed (one excellent source is Cybersecurity Canon at `https://icdt.osu.edu/cybercanon`), tell me about it by the end of the first week of class, so I can decide whether to allow it. (Usually I say yes, but one constraint: I do not want you reviewing tool-specific books, e.g. *Metasploit Unleashed*. It's a terrific book and I recommend it highly—but I want you to review books that take a broader view of privacy and/or security.)

Grading criteria: Writing suitable for the specified outlet (use the Writing Center if you need it!), appropriate structure, depth of analysis and critique of the book's arguments, savvy reading/purchase recommendations.

Each one teach one!

Write an email that teaches someone you care about (your choice: family member, friend, acquaintance, roommate, classmate, work colleague, fellow volunteer…) as kindly, clearly, and briefly as you can *why* and *how* to avoid falling prey to a specific privacy or security danger (again, your choice; list below, but you are not limited to it). Definitely consider dangers that the person has already experienced or is at high risk of experiencing. Honor system: pick a danger that's new to you, please. You may pretend that the person has already asked you for help.

If you would like a classmate to teach you something, that's great! Request it in the Canvas forum for this assignment. To pick up a request from a classmate, simply reply to claim it, then reply with your email text before the due date.

Tell us about the tech-savviness level of, known risks to, and privacy/security habits of the person you chose — if it's not a classmate, *do not give us their name or any other identifying information without obtaining their explicit and unforced consent*, though — and post the subject line and text of your email to the designated Canvas discussion forum.

Glance at a few of Bruce Schneier's analogies/explanations in *Secrets & Lies,* or posts on Troy Hunt's blog (e.g. `https://www.troyhunt.com/fixing-data-breaches-part-2-data-ownership-minimisation/`), for excellent examples of written explanations. Make it clear, make it kind, make it FUN, okay?

Some dangers you might warn the person you're teaching against (not an exhaustive list!):

- Phishing (but choose ONE modality: email, SMS, or social media)
- Identity theft (but choose a specific form of it, e.g. financial-account impersonation or social-media account theft)
- Credential stuffing and/or password spraying (that is, attacks based on password reuse across accounts)
- Account theft (but choose a specific account or account type you know the person has)
- Bad passwords
- Ransomware
- Stalkerware
- Account compromise via "secret questions"
- Social engineering (but choose a context plausibly relevant to the person you're teaching)

It's tempting to infodump. Don't. You're not writing this email to impress me, but to help the person you're writing to. You will lose points if I suspect (and I've been teaching for over a decade) that you've lost or intimidated or shamed this person.

Incident presentation

Pretend you are a security professional explaining a major higher-education security or privacy failure to *non-technical* college/university leadership. (If it helps, picture Chancellor Blank, Provost Scholz or the deans of your college.) Make a well-designed, well-organized, compelling slide deck with *no more than eight slides* (cover and concluding slide excluded; using fewer slides is fine) explaining *as clearly and concisely as possible* what happened before, during, and after the failure. **GRADUATES**: Also explain *how to avoid such failures in future.* (No, you do not have more slides to do this in! That absolutely makes this assignment more challenging for you!)

Record yourself presenting the deck; save the presentation as a movie. (Both PowerPoint and Apple Keynote allow you to do this; I will link to how-tos on Canvas.) I don't need to see your face as you present; just the slides will be fine. I don't need more than 360p or 480p resolution ("standard" rather than any flavor of hi-def or hi-res). You are welcome to use the UW-Madison-branded slide templates (ugly though I find them), as doing so would be perfectly reasonable in a real-life situation like this: `https://brand.wisc.edu/multimedia/powerpoint/`

You may choose among any of the K-12 or higher-education incidents listed in Audrey Watters's `http://2017trends.hackeducation.com/data.html` or my own `https://pinboard.in/u:dsalo/t:breaches/t:highered` and `https://pinboard.in/u:dsalo/t:breaches/t:k12` MA/LIS students may also choose from library-specific breaches: `https://pinboard.in/u:dsalo/t:breaches/t:libraries` If you wish to analyze a different incident, please clear it with me first.

I will evaluate the presentation for:

- narration quality appropriate to a workplace presentation for high-ranking people
- text and image legibility at a distance (i.e. don't try to get around the number-of-slides limit with teensy-tiny text; please also keep accessibility considerations in mind — my own eyes are aging!)
- clarity of narrative (that is, the whole presentation needs to make sense as more than just a collection of random tidbits of information)
- inclusion ONLY of clearly relevant, appropriate details (yes, this means infodumps will be penalized; I expect you to use good judgment about what college/university leadership needs to know!)
- work-appropriate impassivity (blame-and-shame is inappropriate)

Campus privacy report

You will work on this semesterlong project in pairs or trios. (Grad students with grad students, undergraduate students with undergraduate students, please. Grad students will have some extra requirements.) I strongly encourage up-front expectation setting via a project charter or Team Compact: `https://web.archive.org/web/20190802110347/https://www.leadingvirtually.com/virtual-team-tools-team-compact/` I've been using these in my courses for several years, so I can say with some authority that *they really do make projects go smoother*.

You will assess the privacy and security of a specific type of data about UW-Madison students, and make recommendations for its appropriate handling vis-à-vis privacy and security, in a report. (Undergraduates: 4-6 pages. Graduates: 7-10 pages. I will discuss how my expectations differ below. In past semesters, students have chosen to go well over this limit; that's fine, though not necessary.) You will also communicate your findings in a public-relations communication aimed at the UW-Madison student body. You may (and I encourage you to) **share documents and other information you find** with everyone; there will be a Canvas forum to facilitate this.

Module-specific assignments for this project are listed in this syllabus before each module's reading list. They are due at the end of the module under which they are listed.

First, you will choose a class of student data to investigate. (Spread the wealth! We'll share knowledge at course end, so the more topics chosen, the more we all learn about our data trails.) **Undergraduates** and **MS/Info** students may choose one of the following:

- Admissions data (consider data gathered *about* applicants as well as *from* them)
- Financial data (bursar, Wiscard-as-payment-card)
- Wiscard swipe data (excluding financial data)
- Health data and medical records (UHS, vaccination records and other on-matriculation data, any fitness data shared with the university from a tracker or app or health program, COVID-19-related data)
- Data from and about student use of Canvas
- Data from exam-proctoring applications (UW-Madison's is Honorlock, but others may be in use in parts of campus)
- Student data collected by or shared with third-party educational-technology vendors (for example, third-party Canvas plugins such as Piazza, Google Drive, or Pearson MyLab; I will make available a full screenshot of the instructor-viewable "Apps" Canvas setting page in our course space for your reference)
- Physical location data ("geolocation")
- Video surveillance data (limit to campus, please)
- Data about student use of UW-Madison computing resources (wifi, labs, university-provided software and apps, etc)

MA/LIS students may choose one of the following:

- Library circulation data for physical materials
- Proxy-server data from library-purchased e-resource use (excluding electronic textbooks)
- Data from e-textbook and e-assessment use (excluding exam-proctoring software, but including exams and assignments given by third-party vendors such as Pearson)
- Data from use of digitized/born-digital local collections (UWDC, MINDS@UW)
- Data about reference transactions (all modalities: in-person, chat, email, phone)
- Data about attendance at information-literacy instruction sessions (inside and outside courses)
- Data employed in library learning analytics research projects ("Library Value Agenda" is a good search term here; for this one, you are not limited to UW-Madison, and I strongly recommend you look throughout UW System at least)

If there's a different class of student data you and your project partner(s) would like to investigate, let me know in the first module's assignment. I will most likely say yes!

Final deliverables:

- A fully-compiled, well-written, well-structured, well-edited, well-designed journalistic-style report on your findings and your reaction to them. Yes, you are not only allowed but *expected* to editorialize and make recommendations. For examples of the kind of report I'd like to see, look at some of The Markup's writeups, e.g. on podcast tracking `https://themarkup.org/ask-the-markup/2020/10/08/podcast-privacy-tracking-listener-data` and social-media tracking `https://themarkup.org/ask-the-markup/2020/10/01/i-scanned-my-favorite-social-media-site-on-blacklight-and-it-came-up-pretty-clean-whats-going-on`
  - You will lose points if you turn in a bloodless, boring, infodumpy term paper. That's not what I want to read, or want you to write.

- A polished, persuasive, professional-quality communication artifact about your findings, targeted to the UW-Madison student body (graduate and undergraduate) or a subset thereof especially appropriate to the chosen class of data. Adroit use of memes and tropes encouraged! The communication artifact may be:
  - an infographic (a bit more than a meme retread, please, though you may incorporate visual memes),
  - a web page (ONE page, please, and no infinite scroll),
  - a short (five minutes maximum!) well-produced podcast or song,
  - a very short (one minute maximum!) public-service announcement (imagine it playing at WSUM),
  - a short (three minutes maximum!) well-produced video/screencast (think TikTok, and yes, you may use it), or
  - a newsy blog post OR news editorial (think Daily Cardinal, Badger Herald, or news.wisc.edu).
- **MS/Info** and **MS/LIS students only**: An ethics and contextual-integrity review of the collection, (re)use, storage, and disposal of your chosen class of data. Do they comport with the ethics codes of your profession? (If you don't know what those ethics codes are, ask me.) Do they respect contextual integrity (from the point of view of a student)? Are they equitable to minoritized and oppressed populations; do they further endanger these populations, and if so, how? What does the literature (academic and trade) around this class of data say about the ethical challenges of using it… and what does it not say that it should? Do current laws, policies, and processes around this class of data protect it adequately? If not, how should those laws, policies, and processes improve?

COURSE SCHEDULE AND READINGS

N.b. I give you my linklists to help you satisfy curiosity. Clicking on them is optional, and you are *certainly not* expected to read everything on them — I've been collecting links for years!

Unit 1: The human context of security and privacy

Module 1: Why digital privacy? How does digital security contribute?

Topics: Why individuals and organizations need privacy and security. Corrosive effects of widespread surveillance. Personal, social, financial, and reputational risks of poor security practices. Jobs in privacy and security.

Campus data report: Meet with partner(s); set expectations. Choose a class of data to work with.

Linklists: `https://pinboard.in/u:dsalo/t:510/t:jobs`, `https://pinboard.in/u:dsalo/t:surveillance`, `https://pinboard.in/u:dsalo/t:510/t:incentives`

Schneier. *Secrets & Lies* chapter 5 "Security needs."

Foundations chapter 1.

Rasch. "The symbiotic, parasitic relationship between privacy, security." `https://securityboulevard.com/2020/01/the-symbiotic-parasitic-relationship-between-privacy-security/`

Chisholm and Hartman-Caverly. "Vitamin P: Why privacy is good for you (and good for society, too)." `https://chooseprivacyeveryday.org/vitamin-p-why-privacy-is-good-for-you-and-good-for-society-too/`

Madden. "Privacy, security, and digital inequality." `https://datasociety.net/pubs/prv/DataAndSociety_PrivacySecurityandDigitalInequality.pdf` (Summary of Findings, pp. 1-13)

Rubel and Jones. "The temptation of data-enabled surveillance: are universities the next cautionary tale?" `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3559429`

Spitzner. "Getting started in cybersecurity with a non-technical background." `https://www.sans.org/security-awareness-training/blog/getting-started-cybersecurity-non-technical-background`

NICCS. "NICE cybersecurity workforce framework." `https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework` (Click on each category and skim the subcategories. There's a lot!)

Hughes. "Privacy 2019: we're not ready." `https://www.darkreading.com/risk/privacy-2019-were-not-ready/a/d-id/1335621` (With apologies for the militaristic tone, ugh.)

Module 2: Privacy and security law and ethics.

Topics: Basic ethics; ethical hacking. Surveillance capitalism (adtech, social media, personalization, recommender engines, data brokers). Social-media surveillance. Facial recognition. Learning analytics; educational surveillance. Responses to surveillance (personal, societal). The unsettled state of privacy and security law; why legal compliance is not the same as ethical treatment of the privacy and security of others. Contextual integrity theory.

Campus data report: Investigate state and federal law *and* university/System/local policy *applying to your chosen class of data. As best you can, perform the first four steps of Zimmer's nine-step heuristic for your chosen class of data. (Base this on your own beliefs and expectations. It's fine to change your mind and rewrite later!)*

Linklist(s): `https://pinboard.in/u:dsalo/t:surveillance/t:marketing`, `https://pinboard.in/u:dsalo/t:surveillancecapitalism`, `https://pinboard.in/u:dsalo/t:510/t:highered`, `https://pinboard.in/u:dsalo/t:gdpr`, `https://pinboard.in/u:dsalo/t:contextualintegrity`

Foundations chapter 6.

UW-Madison Institutional Data Policy. `https://data.wisc.edu/institutional-data-policy/`

Vallor, Raicu, Green. "Technology and engineering practice: ethical lenses to look through." `https://www.scu.edu/ethics-in-technology-practice/ethical-lenses/`

Jones and Kaminski. "An American's guide to the GDPR." `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3620198` (Introduction, Section II, and Conclusion only. This is a typical law review article: half footnotes. Ignore the footnotes!)

Zimmer. "How contextual integrity can help with research ethics in pervasive data." `https://medium.com/pervade-team/how-contextual-integrity-can-help-us-with-research-ethics-in-pervasive-data-ef633c974cc1` (pay special attention to the "nine-step decision heuristic" please)

Chuen. "Watched and not seen." `http://gutsmagazine.ca/watched-and-not-seen/`

O'Carroll. "How ads hijacked the dream of the Internet." `https://www.csmonitor.com/Technology/2018/1206/How-ads-hijacked-the-dream-of-the-internet.-Can-digital-citizens-fight-back`

Wrenn. "How does Brown University know where you are?" `https://jack.wrenn.fyi/blog/brown-location-surveillance/`

Greenberg and Newman. "How to protest safely in the age of surveillance." `https://www.wired.com/story/how-to-protest-safely-surveillance-digital-privacy/?mid=1#cid=1103629`

MA/LIS students only: Salo. "Physical-equivalent privacy." (Preprint on Canvas. If *Serials Review* publishes it before class starts, I'll replace this with an actual link on Canvas.)

Skim the following (meant as representative examples, not information you need to commit to memory):

Regan and Jesse. "Ethical challenges of edtech, big data and personalized learning." `https://doi.org/10.1007/s10676-018-9492-2`

Bauer-Wolf. "Big brother: college edition." `https://www.insidehighered.com/news/2017/12/21/georgia-techs-monitoring-students-social-media-causes-concern`

Darragh. "Here's why I'm campaigning against facial recognition in schools." `https://www.vice.com/en_us/article/z3bgpj/heres-why-im-campaigning-against-facial-recognition-in-schools`

Short. "Canvas exposed." `https://digitaltattoo.ubc.ca/2018/08/20/canvas-exposed-the-little-problem-with-ubcs-big-expensive-new-tool/` (N.b. UBC is in Canada, which has different law than the US. For more information on Short's struggle with UBC, see my Pinboard: `https://pinboard.in/search/u:dsalo?query=ubc`)

Gurley. "California police used military surveillance tech at grad student strike." `https://www.vice.com/en_us/article/7kppna/california-police-used-military-surveillance-tech-at-grad-student-strike`

Module 3: Protecting yourself and your loved ones

Topics: Threat modeling. Adversarial thinking. An introduction to OSINT. Phishing attacks; catfishing; smishing. Social engineering of individuals. Cyberbullying, doxxing, SWATting. Revenge porn. Intimate-partner abuse. Identity theft. Mobbing; Zoombombing. Political manipulation. Biometrics.

Campus data report: Start a threat model for your chosen class of data. (You will likely refine and expand it as you learn more; for now, just get started!) Research existing phenomena (including breaches) around your data class to inform this threat model. (Link what you find in your report draft, please.)

Linklist(s): `https://pinboard.in/u:dsalo/t:identitytheft`, `https://pinboard.in/u:dsalo/t:phishing`

Foundations chapter 7 (This chapter isn't entitled "Threat Modeling" but arguably should be!)

Schneier. *Secrets & Lies* chapter 2 "Digital threats," chapter 4 "Adversaries."

"Open source intelligence." `https://www.thecybersecurityexpert.com/open-source-intelligence-what-is-it-and-how-can-you-use-it-to-defend-your-organisation/`

Levy and Schneier. "Privacy threats in intimate relationships." `https://doi.org/10.1093/cybsec/tyaa006` (Content alert: non-graphic domestic abuse, elder abuse, and child abuse.)

Cole. "How to tell if your partner is spying on your phone." https://www.vice.com/en_us/article/bjepkm/how-to-tell-if-partner-is-spying-on-your-phone-stalkerware

Pompon. "Phishing for your information: how phishers bait their hooks." https://www.darkreading.com/partner-perspectives/f5/phishing-for-your-information-how-phishers-bait-their-hooks-/a/d-id/1329753

Malwarebytes. "Child identity theft." https://blog.malwarebytes.com/awareness/2020/03/child-identity-theft-part-1-on-familiar-fraud/ and https://blog.malwarebytes.com/awareness/2020/03/child-identity-theft-part-2-how-to-reclaim-your-childs-identity/ (Please protect the young people in your life!)

Cross. "From catfish to romance fraud." https://theconversation.com/from-catfish-to-romance-fraud-how-to-avoid-getting-caught-in-any-online-scam-115227

Fagone. "The serial SWATter." https://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html

Schneier. "The doxing trend." https://www.schneier.com/blog/archives/2015/10/the_doxing_tren.html

Elmer, Burton, and Neville. "Zoom-bombings disrupt online events with racist and misogynist attacks." https://theconversation.com/zoom-bombings-disrupt-online-events-with-racist-and-misogynist-attacks-138389

Hayden. "A guide to open source intelligence (OSINT)." https://www.cjr.org/tow_center_reports/guide-to-osint-and-hostile-communities.php

Optional but fascinating: "Finding McAfee: a case study on geoprofiling and imagery analysis." https://medium.com/@benjamindbrown/finding-mcafee-a-case-study-on-geoprofiling-and-imagery-analysis-6f16bbd5c219

Module 4: Protecting organizations you care about

Topics: Biometrics; facial recognition. Insider threat. Contractor threat. Supply-chain threat. Business-email compromise. Ransomware. Email surveillance. Business email compromise. How social engineering contributes to organizational hacks. Spearphishing. Educational surveillance. Workplace surveillance. Surveillance of public places.

Campus data report: As best you can, assess the vulnerability of your chosen data class to the threats discussed this module. Add insider threat, social engineering, and ransomware to your threat model from last module; as best you can, assess how the data collectors and maintainers protect against these threats. Assess as best you can what contractors and vendors (supply chain!) touch this class of data. Finally, make an initial determination of whether you believe the collection, storage, analysis, and other use of this class of data constitutes surveillance. Explain your answer and state your reaction to what you have learned.

Linklist(s): https://pinboard.in/u:dsalo/t:nsa, https://pinboard.in/u:dsalo/t:facialrecognition, https://pinboard.in/u:dsalo/t:biometrics, https://pinboard.in/u:dsalo/t:insiderthreat, https://pinboard.in/u:dsalo/t:supplychain

O'Donnell. "Silent Librarian retools phishing emails to hook student credentials." https://threatpost.com/silent-librarian-phishing-student-credentials/149249/

Cohney et al. "Virtual classrooms and real harms." https://arxiv.org/pdf/2012.05867.pdf (This is basically a supply-chain analysis of educational technology.)

Leyden. "Who's hacking into UK unis?" https://www.theregister.com/2018/09/17/cyber_attack_uk_universities/ (I am 100% sure it's no different here...)

Weise. "A hacker's best friend is a nice employee." https://www.usatoday.com/story/tech/news/2016/08/15/hacker-social-engineering-defcon-black-hat/88621412/

Gallagher. "Why you can't bank on backups to fight ransomware anymore." https://arstechnica.com/information-technology/2020/02/why-you-cant-bank-on-backups-to-fight-ransomware-anymore/

Vaas. "Florida city sends $742K to fraudsters as it bites the BEC hook." https://nakedsecurity.sophos.com/2019/11/05/florida-city-sends-742k-to-fraudsters-as-it-bites-the-bec-hook/

Cox. "How big companies spy on your emails." https://www.vice.com/en_us/article/pkekmb/free-email-apps-spying-on-you-edison-slice-cleanfox (What's preventing higher education from doing this? ... Nothing.)

Keppler. "A university stopped requiring biometric devices after students complained." https://www.vice.com/en/article/v7gxpy/a-university-stopped-requiring-biometric-devices-after-students-complained

Darragh. "Here's why I'm campaigning against facial recognition in schools." https://www.vice.com/en/article/z3bgpj/heres-why-im-campaigning-against-facial-recognition-in-schools (N.b. this is an outstanding example of a student-penned communicative piece; keep it in mind for your final project deliverables!)

Satariano. "How my boss monitors me while I work from home." https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html?smid=tw-share

Unit 2: How can this happen?

Module 5: Individuals are bad at managing security and privacy.

Topics: Security vs. usability. Security and risk awareness. Password practices. Security by obscurity. "Dark patterns;" exploiting human cognitive habits. Security and privacy balanced against other priorities. Authentication and authorization; multi-factor authentication.

Campus data report: Do your best to find out which people and organizations within UW-Madison collect, store, and have (nominally legitimate) access to your chosen data class. (You are likely to encounter dead ends. In this case, explain where you looked, what you did find, and what you didn't find that you hoped or expected to find.) Decide whether you believe existing policy and practice provide adequate security and privacy protection for the data in light of your threat model.

Linklist(s): `https://pinboard.in/u:dsalo/t:socialengineering`, `https://pinboard.in/u:dsalo/t:passwords`, `https://pinboard.in/u:dsalo/t:darkpatterns`

Foundations chapters 3 and 8

Schneier. *Secrets & Lies* chapter 17, "The human factor."

Ion et al. "'... no one can hack my mind': comparing expert and non-expert security practices." `https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf`

Check a few of your favorite passwords in Troy Hunt's `https://haveibeenpwned.com/Passwords`. IMMEDIATELY CHANGE ANY THAT HAVE BEEN PWNED. Also check your email addresses in `https://haveibeenpwned.com/` and change passwords on any accounts that come up that you didn't already know about and change the password for.

Take the quiz at `http://www.pewinternet.org/quiz/cybersecurity-knowledge/` and then read Olmstead and Smith "What Americans know about cybersecurity." `http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/`

Play "The Password Game" at `https://www.surveygizmo.com/s3/2758757/The-Password-Game-Carnegie-Mellon-University-website`

"Unmasked: what 10 million passwords reveal about the people who choose them." `https://wpengine.com/unmasked/`

Francis. "Vendors approve of NIST password draft." `https://www.csoonline.com/article/3195181/data-protection/vendors-approve-of-nist-password-draft.html`

McGregor et al. "Investigating the computer security practices and needs of journalists." `https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-mcgregor.pdf`

Greenberg. "High-stakes security setups are making remote work impossible." `https://arstechnica.com/information-technology/2020/03/high-stakes-security-setups-are-making-remote-work-impossible/`

Nield. "Dark patterns: the ways websites trick us into giving up our privacy." `https://fieldguide.gizmodo.com/dark-patterns-how-websites-are-tricking-you-into-givin-1794734134`

Module 6: Privacy, security, and safety out of sight, out of mind… until a crisis

Topics: Security practices within businesses; reporting lines. "Shadow IT," BYOD. Relationships between IT and information-security professionals. Security practices in software development. Why security is often ignored until a crisis happens. "The market" and security incentives. Vulnerability disclosure practices, vulnerability hoarding, CVEs, CISA, bug-bounty programs.

Campus data project: OSINT what you can about how administrators, IT professionals, instructors, advisors, third-party software/service providers, etc (as appropriate to your class of data) think about securing and keeping private your chosen class of data. I strongly recommend looking in the higher-education trade press (e.g. CHE, Educause, Inside Higher Ed) as well as in university and System web presences (for e.g. committee minutes). Decide whether you think their beliefs and practices adequate (keeping contextual integrity in mind).

Linklist(s): `https://pinboard.in/u:dsalo/t:vulnerabilities`, `https://pinboard.in/u:dsalo/t:510/t:orgbehavior`

Foundations chapters 4 and 12

Singer and Perlroth. "Zoom's security woes were no secret to business partners like Dropbox." `https://www.nytimes.com/2020/04/20/technology/zoom-security-dropbox-hackers.html`

Anderson and Moore. "The economics of information security." `http://science.sciencemag.org/content/314/5799/610.full`

Magee. "Who owns cybersecurity risk management?" `https://blog.gigamon.com/2017/05/26/owns-cybersecurity-risk-management/`

Baxter. "The risk of shadow IT to business continuity." https://www.csoonline.com/article/3237226/business-continuity/the-risk-of-shadow-it-to-business-continuity.html

Nather. "Four reasons why organizations can't 'just patch.'" https://duo.com/blog/opinion-4-reasons-why-organizations-cant-just-patch

Schneier. *Secrets & Lies* chapter 13 "Software reliability" and chapter 22 "Product testing and verification."

Krebs. "Supply-chain security is the whole enchilada..." https://krebsonsecurity.com/2018/10/supply-chain-security-is-the-whole-enchilada-but-whos-willing-to-pay-for-it/

Hunt. "The effectiveness of publicly shaming bad security." https://www.troyhunt.com/the-effectiveness-of-publicly-shaming-bad-security/ (Contrast this with my repeated "no blame" exhortations. Which is useful or appropriate in which situations? We will discuss this question in class!)

"Common Vulnerabilities and Exposures: About." http://cve.mitre.org/about/

Varmazis. "Good guys and bad guys race against time over disclosing vulnerabilities." https://nakedsecurity.sophos.com/2017/08/07/good-guys-and-bad-guys-race-against-time-over-disclosing-vulnerabilities/

Module 7: Attacks and incident response

Topics: How attacks typically proceed; MITRE ATT&CK and Cyber Kill Chain frameworks. Adversarial thinking, again. Tactics, techniques, and procedures (TTPs). Attribution, and why it is difficult. Good and bad incident-response practices. Incident reports ("post-mortems"). Planning for good incident response. Incident-response teams.

Campus data report: List known attacks/breaches (anywhere, not just UW-Madison) against the class of data you chose. Explain as best you can attacker motives and TTPs. Briefly describe what you can of the incident response, and assess its quality.

Linklist(s): https://pinboard.in/u:dsalo/t:incidentreponse

Equifax report, section IV, pp. 40-54.

Hospelhorn. "What is the Cyber Kill Chain." https://www.varonis.com/blog/cyber-kill-chain/

Strom. "ATT&CK 101." https://medium.com/mitre-attack/att-ck-101-17074d3bc62

"Best practices for victim response and reporting of cyber incidents." https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf

Hunt. "Data breach disclosure 101: How to succeed after you've failed." https://www.troyhunt.com/data-breach-disclosure-101-how-to-succeed-after-youve-failed/

Ruefle. "Defining computer security incident response teams." https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

Aucsmith. "The technology and policy of attribution." https://cyberbelli.com/papers/attribution/

Cooper. "The day after: your first response to a security breach." https://technet.microsoft.com/en-us/library/2005.01.incidentresponse.aspx

McLaughlin. "Post Mortem: Death Star data breach by ROGUE ONE." https://www.threatstack.com/blog/post-mortem-death-star-data-breach-by-rogue-one/ (Humor, but also a solid, if brief, example of an incident report!)

Tilbury. "How not to build a digital archive: lessons from the dark side of the force." https://preservica.com/blog/how-not-to-build-a-digital-archive-lessons-from-the-dark-side-of-the-force/ (Likewise.) Unit 3: Nuts and bolts

Unit 3: Information security fundamentals

Module 8: Cryptography and encryption

Topics: Encryption algorithms. Hashing, salts/nonces, passwords, password stretching. Password attacks: brute-force, rainbow tables, dictionary attack. Public-key infrastructure: public and private keys, certificates, (root) authorities, certificate checking, certificate revocation. Digital signatures, digests. Non-repudiation. "Key escrow," "backdoors," and why they are a bad idea.

Campus data report: Based on what you have learned so far and what else you are able to find out, create a comprehensive, granular list of the datapoints belonging to your chosen data class. (I will have examples of what I mean on Canvas.) Explain what people or systems collect which datapoints, where and how long they are kept, and who is responsible for their security and privacy/confidentiality.

Linklist(s): `https://pinboard.in/u:dsalo/t:cryptography`

Foundations chapter 5

Newman. "What is steganography?" `https://www.wired.com/story/steganography-hacker-lexicon`

Gallagher. "What the government should've learned about backdoors from the Clipper chip." `https://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/`

Ducklin. "Serious security: how to store your users' passwords safely." `https://nakedsecurity.sophos.com/2013/11/20/serious-security-how-to-store-your-users-passwords-safely/` (Make sure you understand the ATTACKS as well as the techniques that guard against them.)

Gibbs. "Passwords and hacking: the jargon of hashing, salting, and SHA-2 explained." `https://www.theguardian.com/technology/2016/dec/15/passwords-hacking-hashing-salting-sha-2`

"EFF introduces actual encryption experts to US Senate staff." `https://www.eff.org/deeplinks/2018/05/bring-nerds-eff-introduces-actual-encryption-experts-us-senate-staff`

Module 9: Forensics

Topics: Storage-device forensics; filesystems and forensics. Memory forensics. Remanence. Ethics, the Fourth Amendment, and forensics. Sunshine laws; FOIA requests.

Campus data report: Explain whether students, as the data originators, can see the data collected and stored about them from your chosen class of data. If they can, what do they have to do to see that data? Write a sunshine-law request related to your chosen data class to the appropriate state entity. (I will link examples of real-world requests on Canvas for you to work from.)

Linklist(s): `https://pinboard.in/u:dsalo/t:digitalforensics`, `https://pinboard.in/u:dsalo/t:attacksteps`

Strickland. "How computer forensics works." `http://computer.howstuffworks.com/computer-forensic.htm` (Pages 1-6.)

US Department of Justice. "Digital forensic analysis methodology." `https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/03/26/forensics_chart.pdf`

Wade. "Memory forensics: where to start." `https://www.forensicmag.com/article/2011/06/memory-forensics-where-start`

Sartin. "Network postmortem: forensic analysis after a compromise." `https://www.computerworld.com/article/2573728/security0/network-postmortem--forensic-analysis-after-a-compromise.html`

Wilson. "Legal issues with cloud forensics." `https://www.forensicmag.com/article/2015/05/legal-issues-cloud-forensics`

Module 10: Software security. Malware and malware detection.

Topics: Malware. Ransomware. Vulnerabilities in code libraries. Malware detection techniques; reversing binaries. Prevention techniques; fuzzing; vulnerability-detection tools. Bug-bounty programs. Vulnerability disclosure. Open-source software and (lack of) incentives to fix vulnerabilities. Why software in higher-ed is difficult to secure. Image metadata and individual privacy.

Campus data report: Spend this week revising the previous weeks' work into a draft of your report. Start working on your persuasive communication if you haven't already. Turn in the report draft; you don't have to turn in a draft of the persuasive communication, but please feel free to do so if you'd like my feedback on it.

Linklist(s): `https://pinboard.in/u:dsalo/t:malware, https://pinboard.in/u:dsalo/t:ransomware`

Foundations chapter 11.

Brodkin. "Viruses, Trojans, and worms, oh my: the basics on malware." `https://arstechnica.com/information-technology/2013/02/viruses-trojans-and-worms-oh-my-the-basics-on-malware/`

Fruhlinger. "What is ransomware? How it works and how to remove it." `https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html`

the grugq. "Ransomware changed the rules." `https://medium.com/@thegrugq/ransomware-changed-the-rules-2f9346197663`

Hughes. "Open-source developers say securing their code is a soul-withering waste of time." https://www.techrepublic.com/article/open-source-developers-say-securing-their-code-is-a-soul-withering-waste-of-time/

Godefroid. "Fuzzing: hack, art, and science." https://patricegodefroid.github.io/public_psfiles/Fuzzing-101-CACM2020.pdf

Keshet. "A guide to malware detection techniques." https://www.cynet.com/blog/a-guide-to-malware-detection-techniques-av-ngav-and-beyond/

Williamson. "Going deeper on behavioral detection." http://www.securityweek.com/going-deeper-behavioral-detection

Johnson. "MSU won't pay ransom to hacker who stole financial documents, personal information." https://www.lansingstatejournal.com/story/news/2020/06/03/msu-not-paying-hackers-ransom-after-personal-financial-info-theft/3134507001/

MA/LIS students: "They paid nearly a half million in ransom. Where's the data?" https://www.news18.com/news/world/lake-city-they-paid-nearly-a-half-million-in-ransom-wheres-the-data-2220743.html (Secure and back up records and unique digital collections, please!)

Module 11: Server and web-application security

Topics: HTTPS and its implementations; SSL/TLS. Cloud security. DDOS attacks. Typosquatting/homograph/IDN attacks. Common web application attacks; application security. More on logging/log analysis. Authentication and authorization; two/multi-factor authentication.

Campus data report: Is your chosen class of data available (to any authorized person) over the web? If so, evaluate its security and privacy/confidentiality as best you can. Definitely use a browser privacy plugin! If not, do your best to learn what software is used for data access and assess its security/privacy.

Linklist(s): https://pinboard.in/u:dsalo/t:cybersecurity/t:webapps

Foundations chapter 13

Elliott. "Two-factor authentication: how and why to use it." https://www.cnet.com/how-to/how-and-why-to-use-two-factor-authentication/

Apache. "SSL/TLS Strong Encryption: An Introduction." https://httpd.apache.org/docs/current/ssl/ssl_intro.html (Don't worry about the technical details unless you want to.)

Wilson. "Our apathy toward privacy will destroy us. Designers can help." https://www.fastcodesign.com/3067094/our-apathy-toward-privacy-will-destroy-us-designers-can-help

Starr. "Fridge caught sending spam emails in botnet attack." https://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/

Arciszewski. "A gentle introduction to application security." https://paragonie.com/blog/2015/08/gentle-introduction-application-security

Cluley. "£120,000 fine for university after details of 20,000 staff and students exposed in data breach." https://www.welivesecurity.com/2018/05/23/120000-fine-university-staff-students-data-breach/

Bright. "Can a DDoS break the Internet?" https://arstechnica.com/information-technology/2013/04/can-a-ddos-break-the-internet-sure-just-not-all-of-it/

Ponemon. "Breaking bad: the risk of insecure file sharing." https://img.en25.com/Web/IntraLinks/%7B6988b757-8c9f-4d09-9dd6-da59f4083f1f%7D_Intralinks_Ponemon_Research_Report_Q4_2014%5B1%5D.pdf (Ignore the appendix.)

"Out of character: Homonym attacks explained." https://blog.malwarebytes.com/101/2017/10/out-of-character-homograph-attacks-explained/

Module 12: Individual device security and privacy

Topics: Computer, tablet, and phone security and privacy. Internet of Things security and privacy. Side-channel attacks. Botnets. Privacy from ad-tech and law enforcement on mobile.

Campus data report: Describe whether, when, and how student consent was sought for the collection, storage, analysis, and (re)use/sharing of your chosen class of data. Exchange your report so far with another team for feedback.

Foundations chapter 12

Schneier. *Secrets & Lies* chapter 14 "Secure hardware."

Griffey. "Personal international infosec." http://jasongriffey.net/wp/2017/03/14/personal-international-infosec/

Fairfield. "The 'internet of things' is sending us back to the Middle Ages." https://theconversation.com/the-internet-of-things-is-sending-us-back-to-the-middle-ages-81435

Feamster. "Who will secure the Internet of Things?" https://freedom-to-tinker.com/2016/01/19/who-will-secure-the-internet-of-things/

Koepke et al. "Mass extraction: the widespread power of US law enforcement to search mobile phones." https://www.upturn.org/reports/2020/mass-extraction/ (Undergraduates: executive summary only.)

Hollister. "US colleges are trying to install location tracking apps on students' phones." https://www.theverge.com/2020/1/28/21112456/spotteredu-degree-analytics-student-location-tracking-app-attendance

"Apple's privacy changes represent 'tectonic shift' for digital ad industry." https://adage.com/article/digital/apples-privacy-changes-represent-tectonic-shift-digital-ad-industry/2263841

Cunningham. "Phone and laptop encryption guide." https://arstechnica.com/gadgets/2015/08/phone-and-laptop-encryption-guide-protect-your-stuff-and-yourself/ (Do these things. Do them!)

Hornby. "Side-channel attacks." http://www.cryptofails.com/post/70097430253/crypto-noobs-2-side-channel-attacks

Module 13: Network security and privacy

Topics: Switches, routers, network segmentation. DMZs. Firewall basics. Packet analysis basics. Intrusion-detection systems. DNS-poisoning attacks; DNSSEC. Distributed denial-of-service attacks. VPNs. Even more on logging/log analysis (including in real time): IDS/IPS systems, SIEM systems. Broken network standards and how they happen; BGP, TLS.

Campus data report: Work on your final deliverables. Turn in drafts of both report and persuasive communication for my feedback.

Foundations chapter 10

Schneier. *Secrets & Lies* chapter 11, "Network security."

"What is a packet?" http://computer.howstuffworks.com/question525.htm

"Data encapsulation and the TCP/IP protocol stack." https://docs.oracle.com/cd/E19455-01/806-0916/ipov-32/

Bradley. "Introduction to packet sniffing." https://www.lifewire.com/introduction-to-packet-sniffing-2486803

Timberg. "The long life of a quick fix." http://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/

Davis. "NSA shares guide to eliminating obsolete TLS protocol configurations." https://healthitsecurity.com/news/nsa-shares-guide-to-eliminating-obsolete-tls-protocol-configurations

Shinder. "SolutionBase: Strengthen network defenses by using a DMZ." http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/

Andrus. "Network security: three keys to effective network segmentation in a world of targeted cyber-attacks." https://www.bradfordnetworks.com/network-security-three-keys-effective-network-segmentation-world-targeted-cyber-attacks/

Arntz. "How a VPN can protect your online privacy." https://blog.malwarebytes.com/privacy-2/2021/01/how-a-vpn-can-protect-your-online-privacy/

Module 14: Security auditing

Topics: Vulnerability scans. Penetration testing; white/gray/black box testing. Physical penetration testing and security exploits. Red teams/blue teams. Ethics of certain pentesting techniques deployed against local staff.

Linklist(s): https://pinboard.in/u:dsalo/t:osint, https://pinboard.in/u:dsalo/t:pentesting

Foundations chapters 9 and 14

"Information supplement: penetration testing guidance." https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf (Sections 1-4.)

McLaughlin. "Using open-source intelligence software for cybersecurity intelligence." http://www.computerweekly.com/tip/Using-open-source-intelligence-software-for-cybersecurity-intelligence

Drinkwater and Zurkus. "Red team versus blue team." https://www.csoonline.com/article/2122440/disaster-recovery/emergency-preparedness-red-team-versus-blue-team-how-to-run-an-effective-simulation.html

Murdoch and Sasse. "Should you really phish your own employees?" http://tech.newstatesman.com/guest-opinion/phishing-employees

"Jek" Hyde. "Smiling your way past the guard." https://twitter.com/i/moments/886241619992862720 (Jargon alert: read about Bash Bunnies at https://wiki.bashbunny.com/ and Rubber Duckies at http://usbrubberducky.com/)

Daniel. "How I socially engineer my way into high security facilities." https://motherboard.vice.com/en_us/article/qv34zb/how-i-socially-engineer-myself-into-high-security-facilities

iSchool learning outcomes

MA/LIS learning outcomes	Assignments measuring outcomes
1. Students demonstrate understanding of societal, legal, policy, or ethical information issues.	Campus data report requires MA/LIS students to do an ethics analysis of data collection, use, and retention.
4. Students demonstrate understanding of professional competencies important for management of information organizations.	Campus data report requires MA/LIS students to assess and suggest changes to library and campus policies vis-a-vis data governance, privacy, and security. It also acquaints students with sunshine laws and responding to sunshine-law requests.
7. Students demonstrate understanding of issues surrounding marginalized communities and information.	Campus data report requires MA/LIS students to do an ethics analysis of data collection, use, and retention. Each-one-teach-one may discuss attacks targeted at minoritized individuals.

Digital Studies Learning Outcomes

For Digital Studies students, this course fulfills the P requirement, and is designed to develop masteries related to the following program learning objectives:

Digital Studies Program Learning Objective	Course Material that Addresses LO
To understand key theories and concepts related to digital studies and the historical context surrounding the creation of digital technologies	Conceptual models of security and privacy (CIA model, contextual integrity) discussed and employed in the campus data report. Standards creation discussed.
To gain familiarity with methods, concepts and tools needed to research and evaluate information related to digital studies	OSINT as a research method employed throughout course.
To think critically about how digital technologies work and their impact on society	Each-one-teach-one assignment, campus data report require critical thinking about security and privacy.
To be able to create strategic communication content and self-expression using digital tools	One campus data report deliverable is a persuasive communication aimed at the student body.
To understand the professional and ethical principles related to the field of digital studies	Ethics introduced explicitly in first course module, referred to throughout rest of course.