UCSD CSE 127: Intro to Computer Security

Scribe Notes Lecture 1

These lecture notes were originally scribed by students in CSE 127 Winter 2021. They have been lightly edited but may contain errors.

---

1) Course Overview

Topics Covered:

- The Security Mindset
- Systems/Software Security
- Web Security
- Network Security
- Cryptography
- Privacy, Anonymity, Ethics, Legal Issues

Course Goals:

- Critical Thinking
  - Think like an attacker, reason about threats and risks, balance security costs and benefits, etc.
- Technical Skills
  - Learn to protect yourself, manage and defend systems, understand how to design and implement secure systems, etc.
- Become a security-conscious citizen
- Become a proficient *and* ethical hacker

Course Resources:

- No official textbook. Optional books:
  - *Security Engineering* by Ross Anderson
  - *Hacking: The Art of Exploitation* by Jon Erikson

2) Ethics

The material we'll be learning in this class includes techniques that can enable real-world attacks. As such, using these techniques outside of the carefully constructed sandbox environments we construct in class for you to experiment with poses ethical issues and may violate university policies and even federal law. You must use the knowledge from this class responsibly and with human privacy and property rights in mind. To give some idea of the legal hazards, we will go over one poorly written law that using techniques from this class without authorization could violate.

18 U.S. CODE § 1030 - FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS (CFAA):

- Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer...
- The punishment for an offense:
  - a fine under this title or imprisonment for not more than one year, or both
  - a fine under this title or imprisonment for not more than 5 years, or both if:
    - the offense was committed for purposes of commercial advantage or private financial gain
    - the offense was committed in furtherance of any criminal or tortious act
    - the value of the information obtained exceeds $ 5,000

Examples of fraudulent activities that resulted in CFAA cases:

Exposing data of AT&T iPad users (United States v. Auernheimer):

In March 2013, Andrew "Weev" Auernheimer was sentenced to 41 months in federal prison after exposing the fact that AT&T servers revealed the unprotected email addresses of iPad users. He and a partner demonstrated the vulnerability by enumerating URLs containing a user ID on AT&T's servers to scrape email addresses. The prosecution made the case that guessing a URL parameter was accessing a protected computer resource without authorization. His conviction was vacated on appeal in 2013 in the Third Circuit on venue grounds, without the judges ruling whether the conviction itself was warranted. [1].

Teaching jailbreaking techniques for video game consoles (SCEA v. Hotz):

In January 2011, Sony Computer Entertainment America sued George Hotz for revealing methods about how to jailbreak and reverse engineer the Playstation 3 video game console, including civil charges under both the CFAA and the DMCA (Digital Millennium Copyright Act). A settlement agreement was later

reached between Hotz and Sony that included a clause that prevents Hotz from further hacking Sony products. [2].

Downloading academic articles on MIT network from JSTOR (United States v. Swartz):

Aaron Swartz used MIT's network to download a large number of academic articles from JSTOR, an online academic journal service, using several techniques to evade MIT's attempts to block his computer from the network. JSTOR reached a civil settlement with Swartz, and informed the US Attorney's Office that they did not want to press charges against him. Despite JSTOR's wishes, federal prosecutors indicted Swartz on multiple felony charges including wire fraud and the CFAA in July 2011. Swartz committed suicide in January 2013 [4].

Misusing license plate databases (Van Buren v. United States):

Nathan Van Buren was a police officer accused of looking up license plate information using a law enforcement database in exchange for money. Consequently, Van Buren was convicted of violating the CFAA for improper use of the database, despite the fact that he was granted permission to use the database for work purposes. The case was brought before the US Supreme Court in 2020. The main question of interest for computer security researchers was whether accessing a computer with authorization but for an improper purpose was a violation of the CFAA. If so, then violating the terms of service of any web site or online service might be a CFAA violation. The Supreme Court ruled that Van Buren accessing information he had authorization to but for an improper purpose was not a CFAA violation [3].

3) What is Security?

Computer security studies how systems behave in the presence of an **adversary**. An adversary is an entity that actively tries to cause the system to misbehave. For the past few decades, attackers and defenders have been engaged in a security arms race. Attackers are constantly probing system security measures, and defenders are constantly working to patch vulnerabilities. Being secure involves adopting a **security mindset**, thinking like both the attacker and the defender. When you interact with a system, think about what it means to be secure, and how it might be exploited.

To think like an attacker, you should always be on the lookout for ways in which security can break. Attackers want the system to misbehave—they identify the **weakest links** and the **assumptions that the system's security depends on**. Then, they attempt

to circumvent the security by interacting with the system in a way that was unforeseen by the system's designers. As a result, attackers must be able to think outside the box and have a strong understanding of what it means for a system to be secure, as well as the system itself.

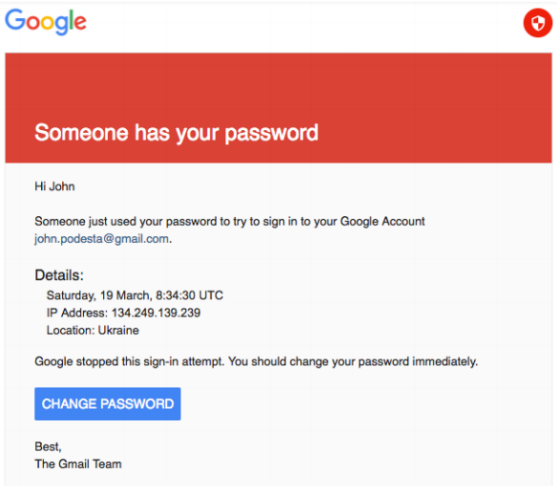
On the other hand, thinking like a defender requires you to know what you're defending and who you're defending it against. You should understand that not every system will be completely secure, and every security measure has its advantages and disadvantages. Hence, you should adopt a mindset of **rational paranoia**. Be paranoid of potential attacks but understand not every form of attack is likely to occur or worth the cost to defend from. Defenders should first establish a **security policy**. That policy should clearly outline what assets they wish to protect, and what properties they wish to enforce in the system (e.g. confidentiality, integrity, availability, privacy, and/or authenticity). Next, defenders should build a **threat model**. Understanding the background of the attackers, their capabilities, and their motivations can help defenders gauge which attacks will occur. Here are a couple examples of threat modeling:

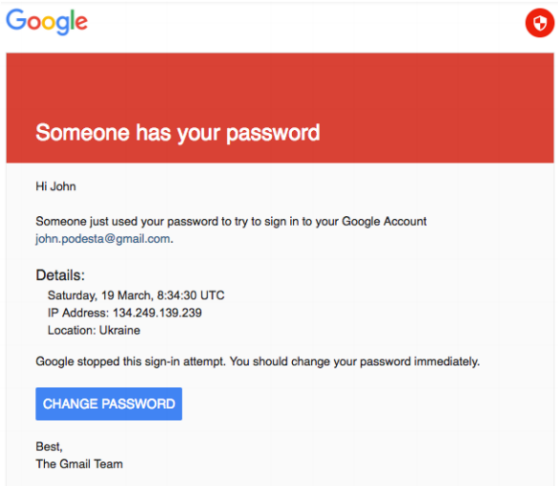
Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity	The Mossad doing Mossad things with your email account
Solution	Strong passwords	Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)	Magical amulets? Fake your own death, move into a submarine? YOU'RE STILL GONNA BE MOSSAD'ED UPON

Figure 1: Threat models

James Mickens "This World of Ours"

"This World of Ours" illustrates in a comical manner the importance of strong passwords, in addition to the futility of safeguarding sensitive computer data against a national intelligence agency





The above image demonstrates a real-life example of an email sent to Hilary Clinton's campaign manager, John Podesta, in the midst of the 2016 U.S. presidential election. This is an example of a spear-phishing attack, in which the attackers pose as a legitimate source using personalized information to target a specific individual. In this case, the fraudulent email masqueraded as a legitimate Google security alert. The perpetrators of this attack are thought to have been the Russian intelligence-linked hacker group "Fancy Bear". Following the breach, nearly 20,000 pages of Podesta's private emails were published to WikiLeaks, consequently stirring controversy during the election. This story highlighted a major cybersecurity threat in which foreign governments could influence U.S. politics [5, 6].

Now, defenders should perform **risk assessment**. This means understanding the weaknesses of the system and the cost associated with any predicted attacks. Costs may be direct (money, property, safety, etc.) or indirect (reputation, future business, well-being, etc.). Defenders can prioritize these attacks based on their severity and the likelihood of them occurring. Finally, defenders should develop appropriate **countermeasures.** They should weigh the costs of enacting a security measure against the cost of an attack that the security measure mitigates. There are many options available for countermeasures. They can either be technical (passwords, encryption, etc.) or non-technical (Law, policy, procedures, training, auditing, incentives, etc.) All of the principles mentioned here are cornerstones of adopting the secure mindset.

We also have to consider the various **security costs**. These costs include direct and indirect costs like lost productivity and increased complexity of systems. Rationally considering the tradeoffs between increased security and these costs to security mechanisms is part of a rigorous security evaulation. It may be rational for a system maintainer to forgo a security mechanism if the costs are high, the risk of exploitation is low, and the costs of a security breach are low.

It is important for us to have a good understanding of the **secure design**. First of all, we need to understand that secure design is a process, so it's very hard to add new features to the old systems we designed. In this class, while we design the system, we need to think like both an attacker and defender. Instead of trying to rationalize and argue that a system is secure, designers must try to understand and reason about possible attacks and forms of defenses. In special cases such as formal verification or cryptographic models, it is possible to have a formal proof of security. However, these types of formal proofs are impossible for many systems, and the proofs only work if attackers cannot violate the security model that the proof holds in.

When it comes to **designing your defense**, you must keep in mind that a system contains two components: **trusted components** and the **attack surface**. The trusted components are the parts that must function correctly for the system to be considered secure. The attack surface represents the components of the system that are exposed to the attacker. Finally, there are four general **security principles** to consider when designing defenses:

a) A simple open design that is maintainable

b) Privilege separation and least privilege

c) Defense-in-depth and diversity

d) Complete mediation and fail-safe

4) Exercises

The following exercises are meant to help you start developing a security mindset. In class, the students discussed them live.

Scenario # 1: How would you break into the CSE building?

Many of the initial responses were suggestions that require the least amount of resources/energy to accomplish such as asking someone to open the door, breaking a window, or trailing behind another student who is entering. Near the end of the discussion, more elaborate and expensive solutions were suggested including accessing the facility from the roof, becoming a university professor, and digging an underground tunnel.

Scenario # 2: How would you identify who was at a protest?

The student responses for this exercise included practical methods that are currently being used today. These methods include CCTV, facial recognition, and cell phone location data. Furthermore, many businesses are able to track their employees' whereabouts using less invasive methods such as public social media activity. Many protests are organized through social media outlets, and oftentimes these feeds include images of the participants and geolocation features.

Scenario # 3: How would you steal my (Nadia's) password?

The students suggested common password theft strategies such as keylogging and email phishing. The professor then asked the students to brainstorm specific phishing emails they would send that would likely be the most effective at grabbing her attention. These ideas included cut cat pictures, fake URLs, a fake Google form. Upon clicking these fake hyperlinks, a malicious script might execute granting the attacker root access to the system. Students also mentioned "shoulder surfing", an attacker physically looking at a victim's keyboard to observe key presses when the attacker is in the same room as the victim while the victim types her password.

Scenario # 4: What security systems do you interact with?

This exercise allowed students to think about ways they interact with all types of security measures, whether they are digital or not. Some of the suggestions provided in chat include two-factor security apps like Duo, car/home doors, badge readers, facial identification software, and password managers.

5) Bibliography

[1] Electronic Frontier Foundation. https://www.eff.org/cases/us-v-auernheimer, 29 Apr. 2015

[2] Electronic Frontier Foundation. https://www.eff.org/deeplinks/2011/01/sony-v-hotz-sony-sends-dangerous-message, 6 Oct. 2011

[3] Electronic Frontier Foundation. https://www.eff.org/cases/van-buren-v-united-states, 1 July 2020

[4] JSTOR. https://docs.jstor.org/, 30 July 2013

[5] Vox. https://www.vox.com/policy-and-politics/2016/10/20/13308108/wikileaks-podesta-hillary-clinton, 20 Oct. 2016

[6] Washington Post. https://www.washingtonpost.com/world/national-security/intelligence-chiefs-expected-in-new-york-to-brief-trump-on-russian-hacking/2017/01/06/5f591416-d41a-11e6-9cb0-54ab630851e8_story.html, 6 Jan. 2016