CSE 484/M584:
The end of
Computer Security (and Privacy)
Spring 2025

David Kohlbrenner

dkohlbre@cs

Admin

- Lab 4C and EC are due tonight
  - Please double check that you have both partners on exactly one submission.
  - EC versions are expecting a complete RCA and patch. Won't be graded without an RCA at least!

- No late days!

- Course feedback is now open, please fill it out!
  - https://uw.iasystem.org/survey/309432

Final Exam: Last questions/prep?

One last(?) time: Threat Modeling

- You have been placed in charge of threat modeling for the new subway system Neo Seattle will be building.

- No one has given you any good guidance about what exactly they mean by this!

- Consider:
  - Multiple types and definitions of "adversary" that might be relevant.
  - What those adversarial objectives might be.

One last(?) time: Threat Modeling

- Adversaries:

- Now:
  - Pick one and consider how we might approach defense.
  - Consider the costs of defense vs the asset being defended.

More security!

Looking for more security?

- CSE 490 Cryptography

- CSE 481S Security Capstone

- CSE 564 Graduate Computer Security

- CTFs – Competitive hacking
    - Batman's Kitchen is the UW team
    - Try https://picoctf.org/ (aimed at newcomers)
        - Includes a *non-competitive* verison

- Internships
    - Medium-size security companies are your best bet, maybe

Looking for more security?

- CSE 490 Cryptography

- CSE 481S Security Capstone

- CSE 564 Graduate Computer Security

- CTFs – Competitive hacking
  - Batman's Kitchen is the UW team
  - Try https://picoctf.org/ (aimed at newcomers)
    - Includes a *non-competitive* verison

- Internships
  - Medium-size security companies are your best bet, maybe

Many avenues in industry

- General software engineering

- Security engineering

- Incident response

- Network operations

- Penetration testing

- Misc security contracting

- Etc.

Many avenues in industry

- General software engineering

- Security engineering

- Incident response

- Network operations

- Penetration testing

- Misc security contracting

- Etc.

- Security research + academia!

Security Research

Research

- Usability of security tools

- Studies on security&privacy expectations

- Studies on abuse and misinformation

- Finding new types of vulnerabilities

- Building tools for safer systems

Learning more

Security-specific sources I use

- Risky Biz: long-running newsletters, podcasts, etc. about the security industry and state of security.
  - https://risky.biz/

- Security, Cryptography, Whatever: podcast more aimed at cryptography and cutting-edge applications.
  - https://securitycryptographywhatever.com/

- Lawfare: Articles, reporting, podcasts on national security ++
  - Notably, they cover a lot of cybersecurity: https://www.lawfaremedia.org/topics/cybersecurity-tech

Non-security-specific

- Ars Technica: High-quality tech news.
  - Notably, Dan Goodin writes about security work often: https://arstechnica.com/author/dan-goodin/

- The Register: Long-running IT/tech reporting.
  - Has a lot of security reporting: https://www.theregister.com/security/

People worth reading

- Molly White: Primarily cryptocurrency, but that includes a lot of security!
  - https://www.mollywhite.net/

- Chris Krebs: Independent security reporter for ~ever
  - https://krebsonsecurity.com/

- Bruce Schneier: Cryptographer and blogger for >20 years
  - https://www.schneier.com/

- More, obviously, but I ran out of time

Lots We Didn't Cover…

- Really deep dive into any of the above topics
- (Most) Network security
- (Most) Traditional OS security
- (Most) Recent attacks/vulnerabilities
- (Most) Specific protocols (e.g., SSL/TLS, Kerberos)
- Access control
- Spam
- ML Security/Privacy
- Malware / Bots / Worms
- Social engineering
- Cryptocurrencies (e.g., Bitcoin)
- Other emerging technologies
- …