CSE227 – Graduate Computer Security

The Final Showdown

UC San Diego

Housekeeping

General course things to know

- Final presentations are scheduled: https://tinyurl.com/cse227schedule
- Presentation Details
  - 10 minutes for presentation, 2 mins for questions (I will cut you off @ 10mins)
  - Talk should include introduction to the problem, your research questions, your methodology (including data collection), and your results
  - All team members must speak approximately an even amount
- **Expectation is you come to all sessions next week**

Housekeeping

General course things to know

- Final report is due **6/9** — via Gradescope
  - Spec is on course webpage: https://kumarde.com/cse227-sp26/spec.pdf
  - 5 page document — USENIX Security template (please follow the instructions)
  - Most details in the spec — this should basically **look like a paper**
- **If you need more space, you can put things in an Appendix**; but five pages is a strict limit
- Remember, this is 25% of your grade

Today's lecture

Learning Objectives

- SETs (~10 minutes)
- SECURITY DEBATE DAY
- Final thoughts :)

SETs

Attendance

https://tinyurl.com/cse227-attend

Codeword:
Fight!

Debate Day

Debate Structure

- I will present a “security take” informed by everything we read together this quarter
  - We will take a *blind vote* about how we feel collectively about this
  - I’ll cold call two people, and they will offer an opening argument for each side of the argument
  - Then, we’ll ping pong throughout the class; cold calling for responses to what was previously just said, until the conversation feels “over”
  - We’ll take another vote, and I can tell you how we shifted over the course of the class

Application security is no longer an computer security concern

Internet centralization is a desirable outcome

Network censorship is not bad, it’s just a different culture

Spam is an inherently unsolvable problem

Web surveillance is an acceptable cost for better ads

AI safety research is a waste of time

AI's impact on scams and e-crime is overblown

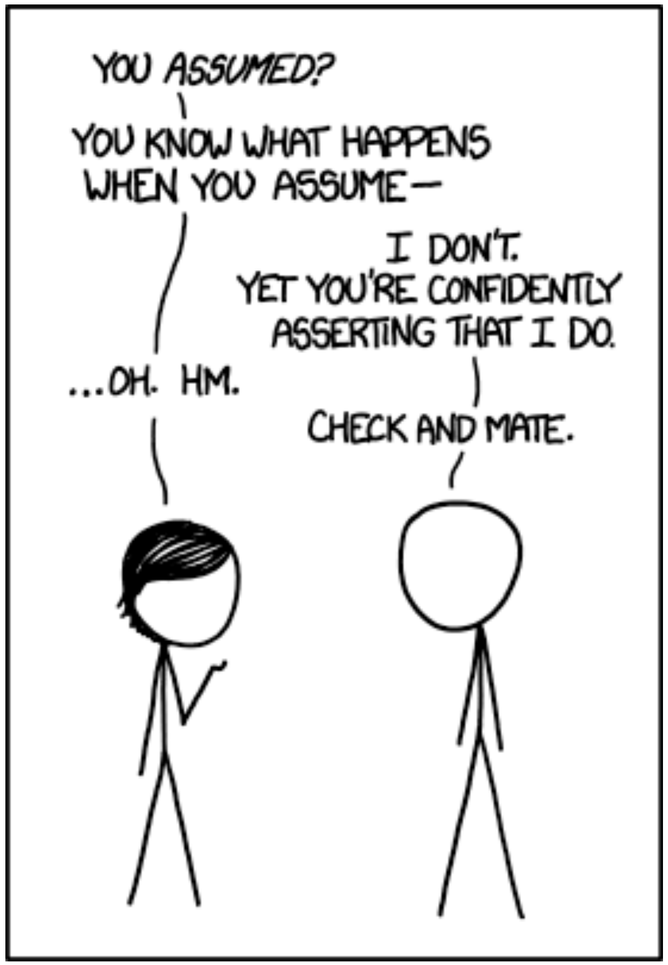
Final Thoughts

Computer security is all about trust

- If you were to take one thing away from this class, it's that **trust is a first-class citizen** in all of computer security
  - Who do I trust, and why do I trust them to do X…. this is the fundamental question you must always ask yourself in security (and probably in life too)
- You can chart out *trust* in almost every single topic area we discussed

Computer security is all about assumptions

- You know what they say about assumptions…
- The attackers job is to **interrogate the assumptions made by the developers** to break the system
- The defenders job is to **enumerate the assumptions they are making** and ensure proper protections don't break invariants
  - This is the cat and mouse struggle



https://xkcd.com/1339/

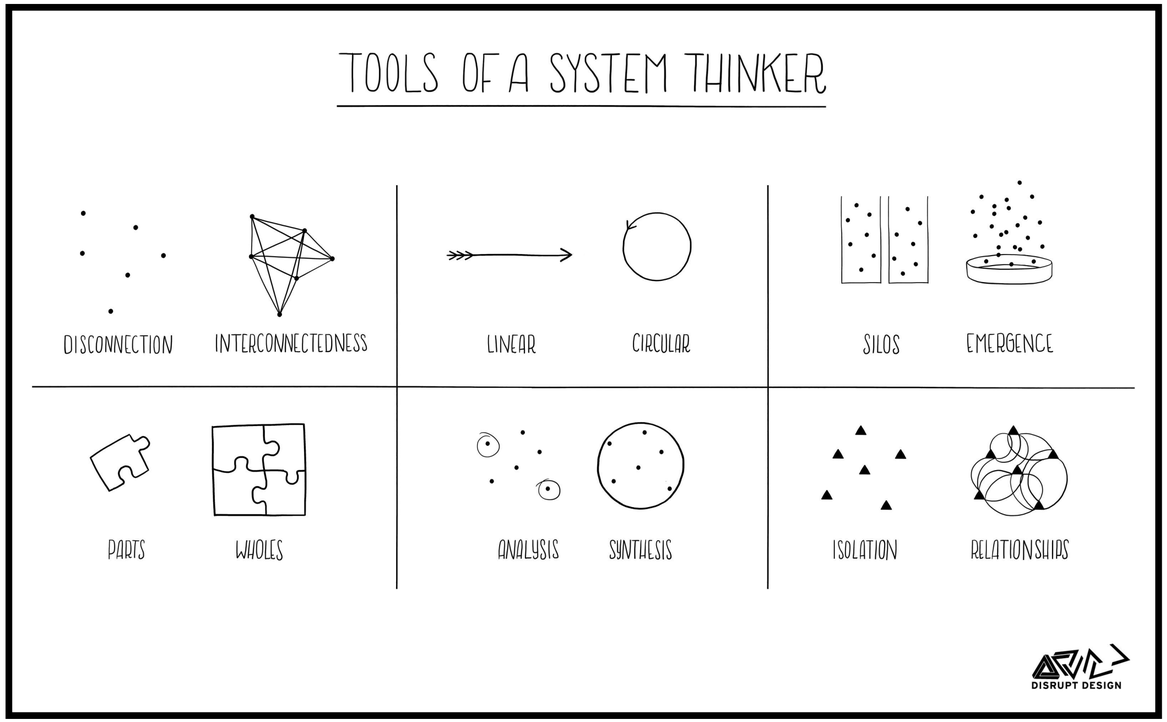
Computer security is about *system thinking*

- "System thinking is simply thinking about something a *system* — the existence of entities, the parts, the chunks, the pieces, and the relationships between them." – Edward Crawley, MIT

- Computer scientists like to think about the world in units and chunks

  - But security people like to think about the whole picture

- Systems include: software, hardware, and *people*….



Computer security research is all about creativity

- Many people think CS is strictly technical…
  - But actually, research is an *inherently* creative field
- You are constantly *generating* new ideas and *creating* knowledge… most of your time is spent thinking rather than coding / technical stuff
  - Security research marries deep technical knowledge with curiosity and creativity

Meta-Discussion

- What are something new that you took away from the class this quarter?
- What surprised you about research (doing it or otherwise?) during this quarter?
- Any final takeaways?

Next time…

- Final presentations… Good luck!