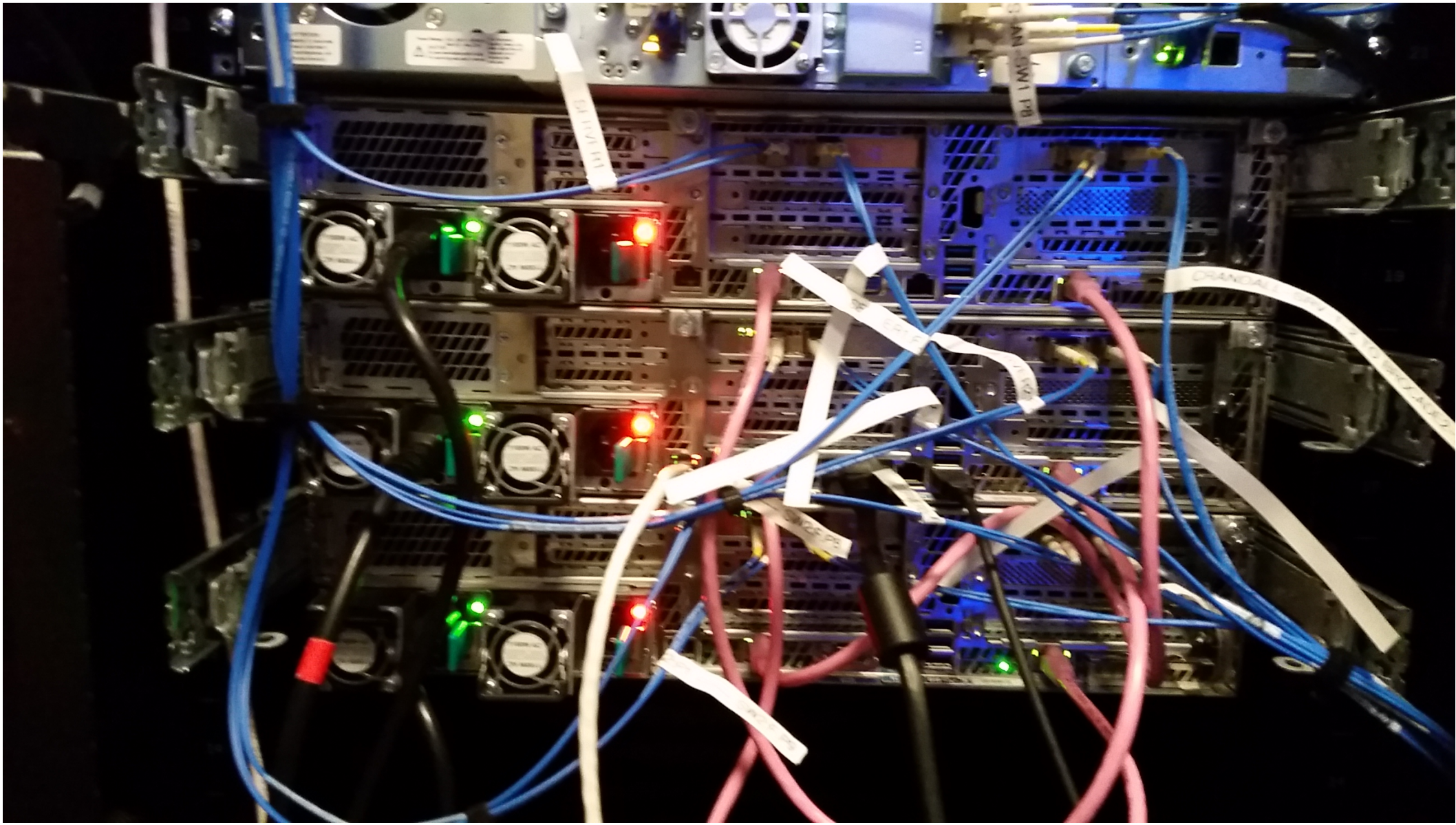
CS 444/544 Intro to Cybersecurity

Jed Crandall
crandall@cs.unm.edu

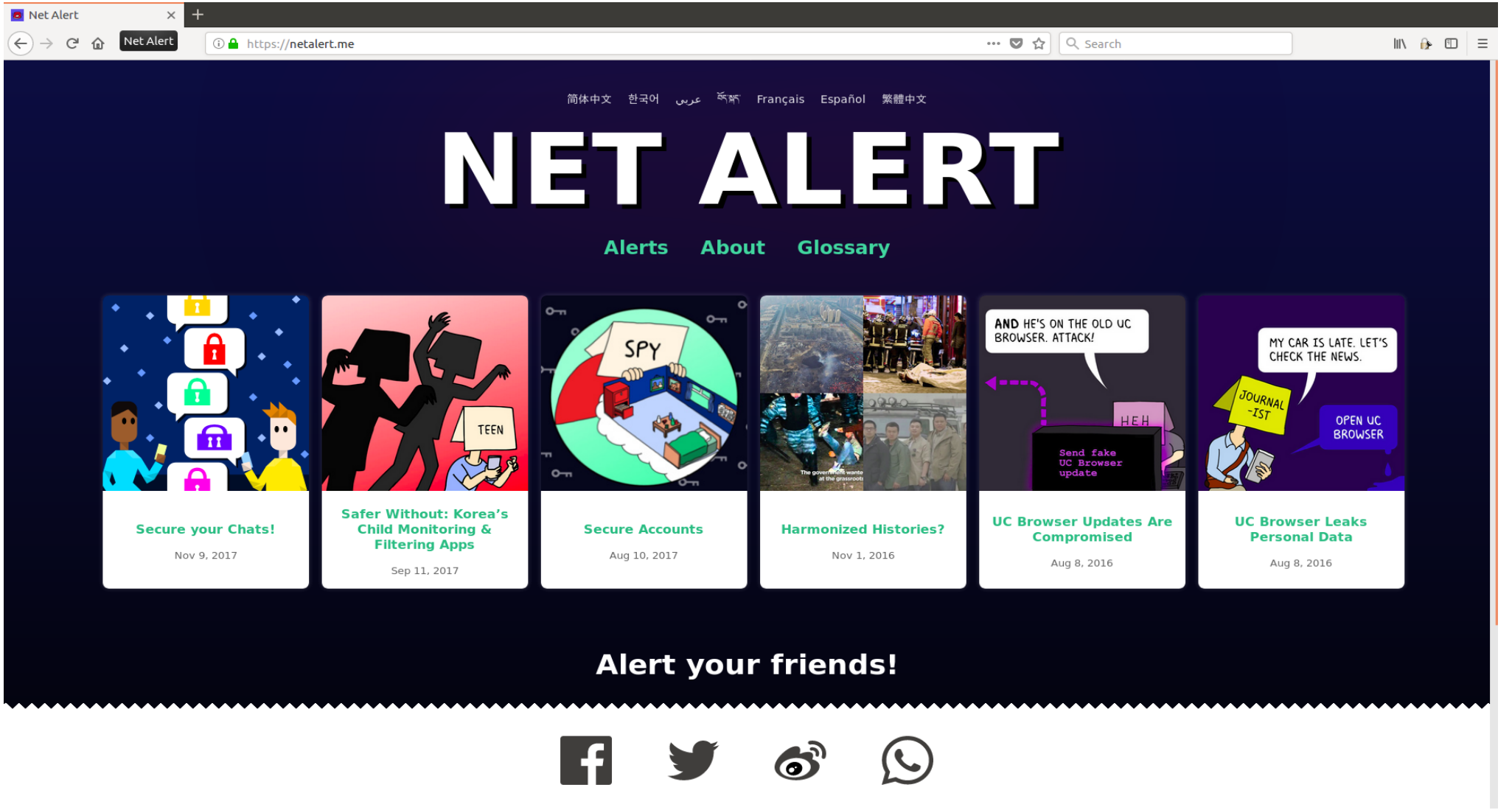
A little about me

- Associate Prof. in the Dept.of Computer Science
- Grew up in Northern California in Donner Party country
  - If you can't understand my spoken English, let me know
- Learned to program from my mom (and the Apple II BASIC manuals that were laying around the house)
- Undergrad from Embry-Riddle Aeronautical University in Prescott, Arizona
- Ph.D. from U.C. Davis, where the cybersecurity class covers classical topics (like Bell-LaPadula and the theory of information flow)
- General research area is Internet freedom
  - Background in computer architecture
  - Also have done research in operating systems and computer networks

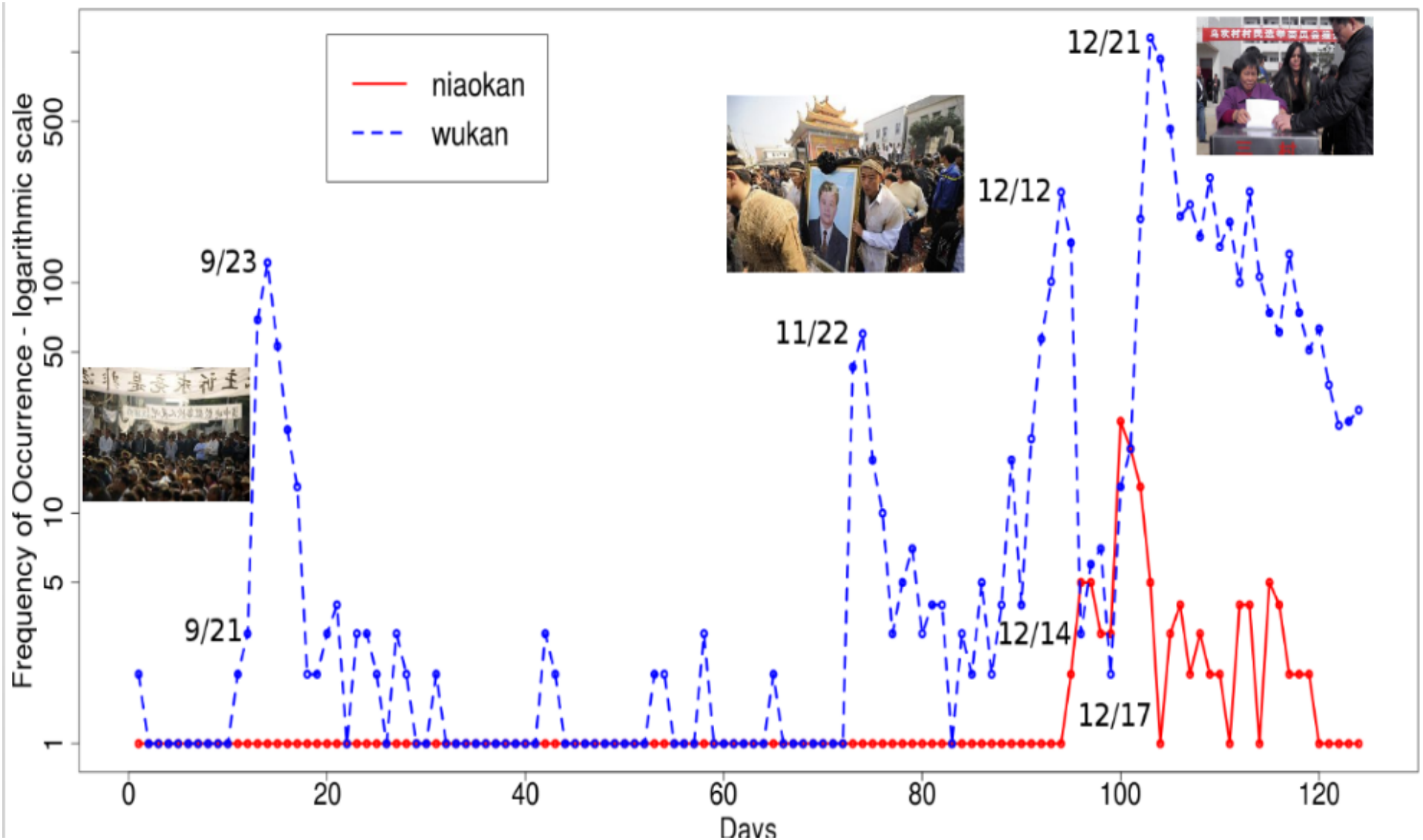
The Kraken



https://netalert.me



Weibo (wukan= 乌坎　niaokan= 乌坎)



Are you as excited as me?

- Cybersecurity is infinitely fascinating, you can spend a lifetime learning about it and still be surprised and amazed.
- This is my favorite class to teach (if you take another class from me in the future, forget I said that).

Empowerment

- Have you ever fantasized about being a Jedi, a wizard, a ninja, a pirate, *etc.*?
- You should think about how you hope to be empowered this semester.

Some administrative stuff...

- Course website (and syllabus) are easy to find
- My office is in no longer in CARC, I'm now back in the Farris Engineering Center
- Prereqs? (At a minimum, you should be a capable programmer)
- We do NOT have a TA
- No required textbooks
- ADA
- Title IX
  - TAs, GAs, and faculty are "responsible employees"
  - "Responsible employees" must report
  - Lots of campus resources I can help direct you to
- The rest of the syllabus is online (and we'll go over it in a bit)...

Grading

- 100% labs
- Labs may have flags
- Homeworks will be an email or presentation, not graded
- You losing your visa status or scholarship is not my problem

Cheating and collaboration

- Read the syllabus, this slide is not authoritative
- Do your own work
- When in doubt, ask
- In group assignments, don't do all the work yourself
- “If you're not cheating, you're not trying.”
  - A statement about my philosophical approach to teaching cybersecurity
  - <u>Not</u> an invitation to actually cheat, all policies in the syllabus or elsewhere still apply

My expectations of you

- Be studious
- Take responsibility for your own learning
- Take responsibility for others' learning
  - I have a tendency to be wrong, be misinformed, lie, and so on, hold me to the “show me” standard
- Do only excellent work
- Show leadership and be a mentor

Material to be covered

- We'll begin the semester with ethical disclosure issues, University policies, legal issues, research ethics, and ethical hacking
- Technical content
  - Cryptography and network security
  - Systems security and vulnerabilities
  - Digital forensics and privacy
- Also
  - New and emerging research areas
  - Societal impact

Some food for thought

- A genuine intellectual curiosity about cybersecurity is a very rare and very employable quality
- I'm interested in threats beyond the typical “criminal who wants to steal your credit card number”, the class material will inevitably reflect this
- Hackers are interested in how systems actually behave, not how they're supposed to work

Class advice

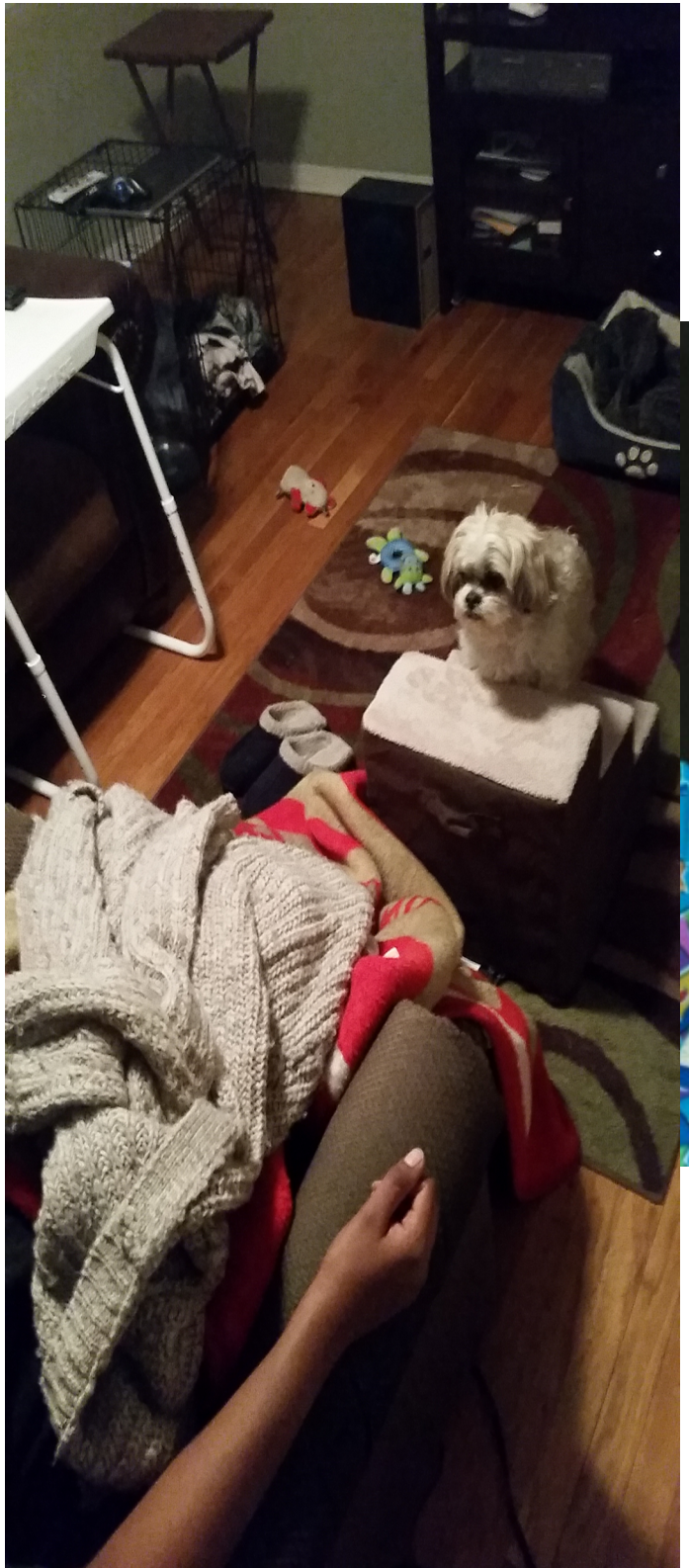
- Always question the interface presented to you
- Always think about how things *actually* work on the inside
  - *E.g.*, master combination locks
- Always think about things from multiple perspectives
- Program the weird machine
- If you see a button, push it
  - don't violate laws, class policies, University policies, ethical norms, and the like (not in the context of this class, anyway)


I'm the sweetest


HACK THE
PLANET

Class advice

- Information wants to be free
- Don't trust anyone, especially not authority
  - This includes textbook authors, experts, developers, lawyers, me...



Class advice

- In cybersecurity, timing is everything
- “Information only has meaning in that it is subject to interpretation” (quote from Fred Cohen)
- Cover your tracks, even when you don't think you need to