

CSE 548 Course Intro

Spring 2024

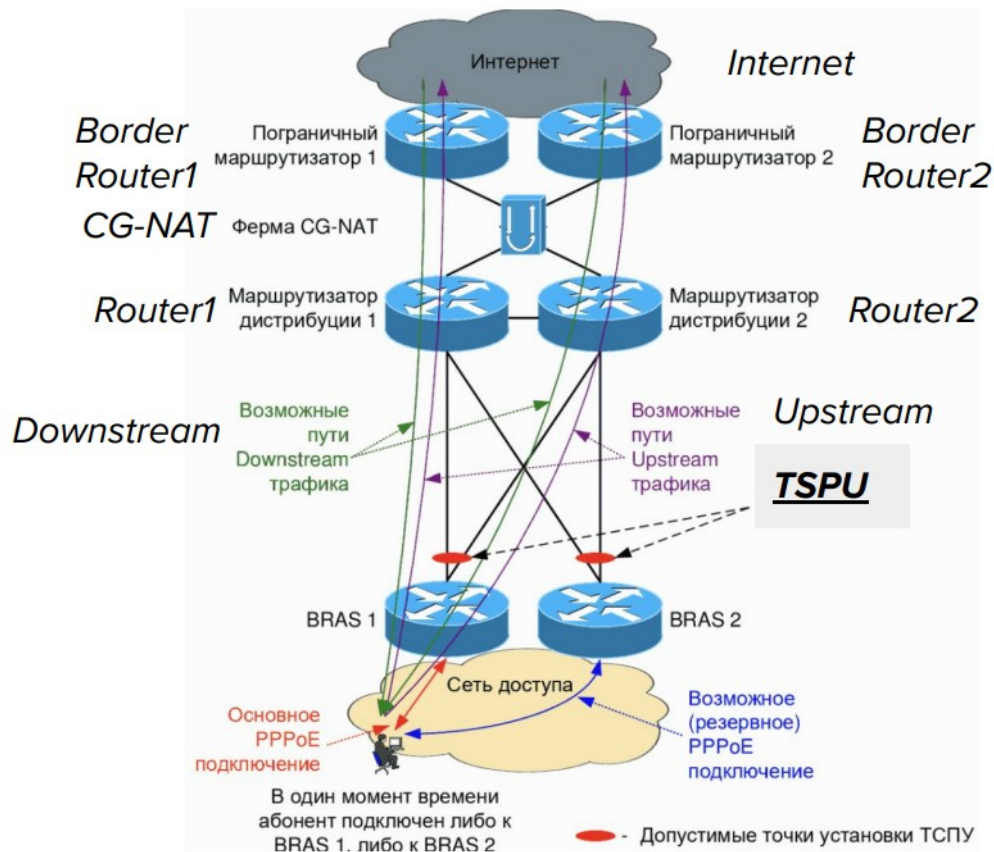
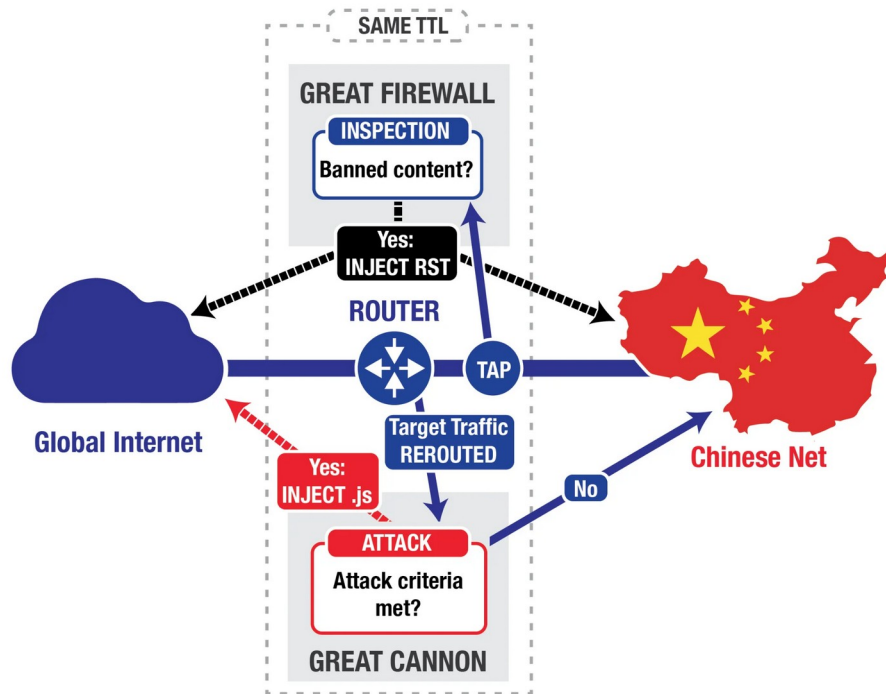
Advanced Computer Network Security

Jed Crandall

jedimaestro@asu.edu

Where are you from? In what ways are encryption and protocols restricted here, there, or in other places that matter to you?

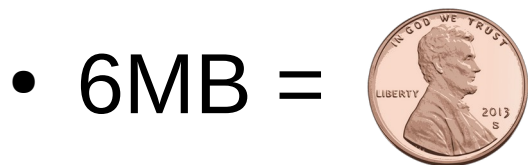
2015ish vs. 2025ish



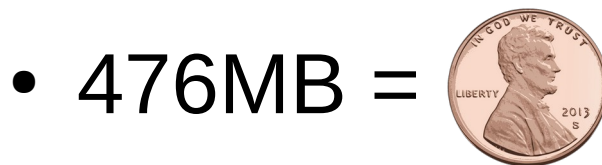
<https://citizenlab.ca/2015/04/chinas-great-cannon/>

https://diwenx.com/assets/files/TSPU_IMC-slides.pdf

2003ish vs. 2023ish



- 40,960.00 GFlop/s for about \$486 million (NEC EARTH-SIMULATOR)



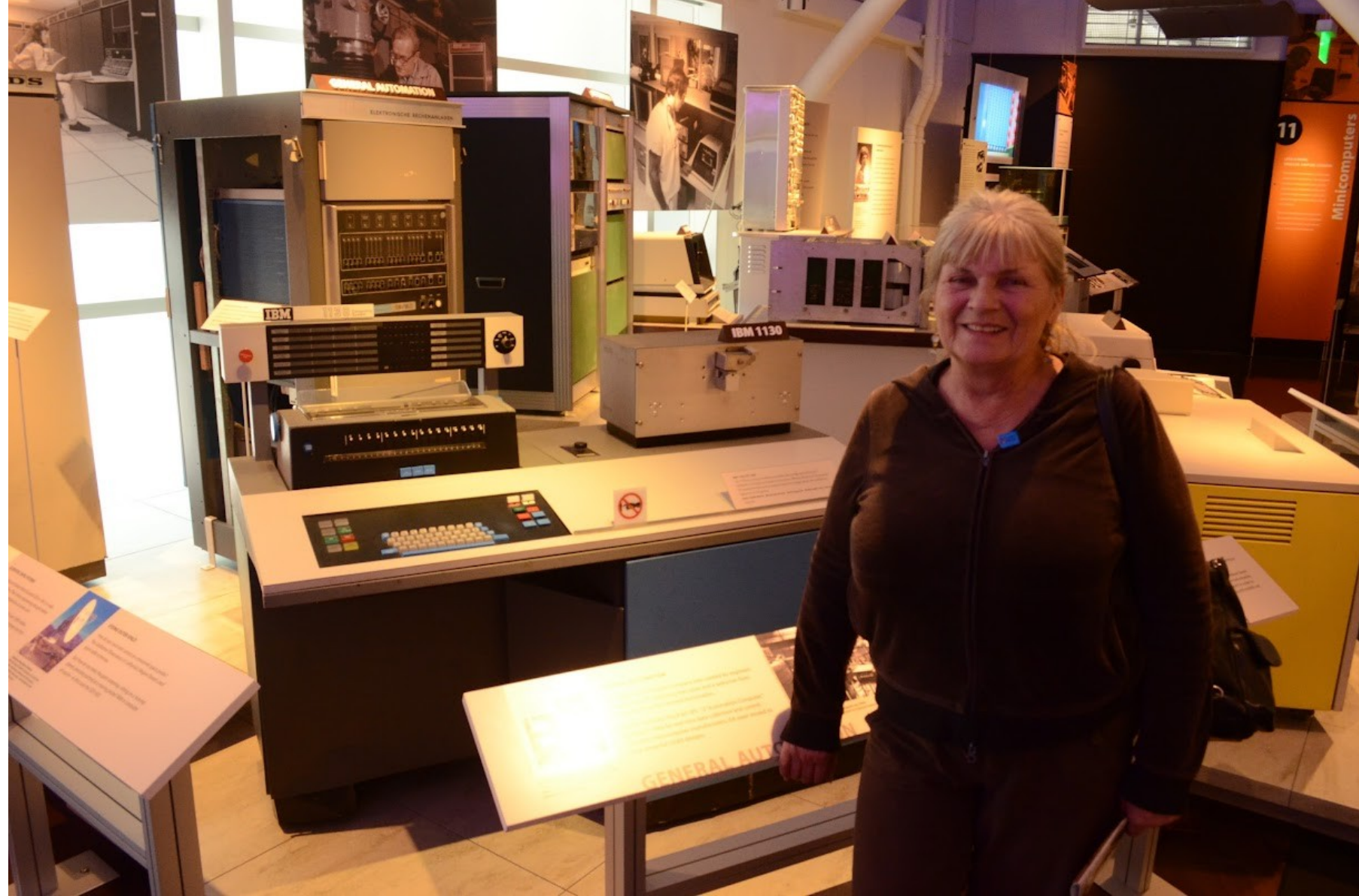
- 1,685.65 PFlop/s for \$600 million (FRONTIER)
 - 1.6 billion Gflop/s
 - **39000X as much**

Syllabus in a nutshell

- Attendance not recorded
- *Might* record lectures
 - Only me, the class, and the TA will have access
- Three exams and final are in-person
- Check both Canvas and the course website

A bit about me...

- Associate Professor, SCAI *and* Biodesign Center for Biocomputation, Security, and Society
- Research is about Internet Freedom, including:
 - Internet censorship (measurement and evasion)
 - Machine-in-the-middle attacks, adversarial networking, VPNs
 - Privacy, forensics, and a few other things





IBM 1130

IBM



IBM 1130, 1965
The 1130 was unusual in offering removable disk storage and a full line of peripherals including card readers and printers. IBM also offered over 50 for specialized tasks such as high-way alignment, bridge design, and auto layout for civil engineers.
Source: IBM 1130 Sales Kit. Memory size 16 words. Memory type Core. Memory width 16 bits.

GENERAL AUTOMATION

Not every minicomputer company was created by engineers jumping ship. A marketing executive and a salesperson at Honeywell founded General Automation.

https://commons.wikimedia.org/wiki/File:Apple_II_typical_configuration_1977.png



Welcome to Debian Linux 1.1!

This is the Debian Linux Boot Disk. On most systems, you can go ahead and press <ENTER> to begin installation. You will probably want to try doing that before you try anything else. If you run into trouble, or if you already have questions, press the function key <F1> for quick installation help.

WARNING: You should completely back up all of your hard disks before proceeding. The installation procedure can completely and irreversibly erase them! If you haven't made backups yet, remove the floppy from the disk drive and press <RESET> or <Control-Alt-Del> to get back to your old system.

Debian Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. For copyright information, press <F5>.

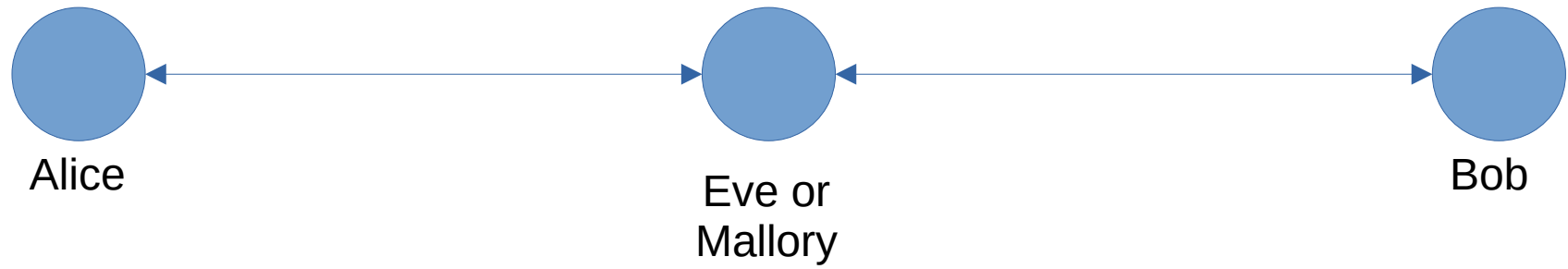
This boot floppy installs the Linux kernel version 2.0.0.

Press <F1> for help, or <ENTER> to boot!

boot: _

https://archive.org/details/debian_1.1

Why are you taking an advanced
network security class?



What to expect this semester

- You should be able to look at any PCAP and critically analyze it *w.r.t.* network security and privacy
 - So, we need to study crypto and physics (and build a quantum computer)
 - We need to understand the ways in which our tools (*e.g.*, Wireshark) can be wrong
 - *E.g.*, overlapping IP fragments
 - We need to think critically about what can make a bit pattern “malicious”

[Cypherpunks want] “a guarantee -- with physics and mathematics, not with laws -- that we can give ourselves real privacy of personal communications.”

“We are literally in a race between our ability to build and deploy technology, and their ability to build and deploy laws and treaties. Neither side is likely to back down or wise up until it has definitively lost the race.”

--John Gilmore

Grading/houses summary

- Divided into four houses (assigned, not chosen)
 - 2/3rds of exams/labs don't affect your individual grade, 1/3rd do
 - House with the most points at the end of the semester gets 100/100 on the final

Part 1: Crypto

- Three exams (no notes, book, calculator, *etc.*)
 - 1st is 100 points (25% of grade) individual effort, first half of RSA and Diffie-Hellman
 - 2nd not graded but for house points, second half of signature and key exchange
 - 3rd is not graded but for house points, attack crypto

Part 2: Network Intrusion Detection Systems (NIDS)

- Each student will individually create a Scapy script to obfuscate a TCP data transfer
 - 100 points, 25% of your grade
- Messages uploaded to a server that is keeping PCAPs for points
- Houses will be provided with the raw PCAPs
 - Take some points away for your own house if you can recover the raw message transferred

Part 3: Malware

- Each student will submit (100 points, 25% of your grade) a tar ball that compiles a “warrior”
 - Each student knows some secret about the build environment
 - Tar balls shared with entire class
- First round of house vs. house, randomly chosen warriors in Core Wars
- Each student gets to submit one more warrior for round 2

Calendar (Part 1 of 2)

- 1/15 – House assignments announced, read Diffie-Hellman paper carefully
- 1/20 – Read RSA paper carefully
- 1/22 – Read/skim Mini AES spec, LDC tutorial, and KRACK attacks and/or watch relevant YouTube videos
 - House names and number of bits for prime numbers due
- 1/27 – Read/skim MD5 collisions paper and WeChat Citizen Lab report
- 1/29 – Read OTR paper and watch CITIZEN FOUR

Calendar (Part 2 of 2)

- 2/3 – Read “Quantum Algorithms Revisited”
- 2/5 – In-person exam, individually graded
 - First half of RSA and Diffie-Hellman
- 2/10 – In-person exam for house points
 - Second half
- 2/12 – In-person exam for house points
 - Attack the Diffie-Hellman scheme of others

Do you *really* want to take this class?

- Your classmates will be depending on you
 - Not just the ones in your house
- 115/115 seats are full
- Instructor is unapologetically a cypherpunk and an academic