

CSE 468 Course Intro

Computer Network Security

Jed Crandall

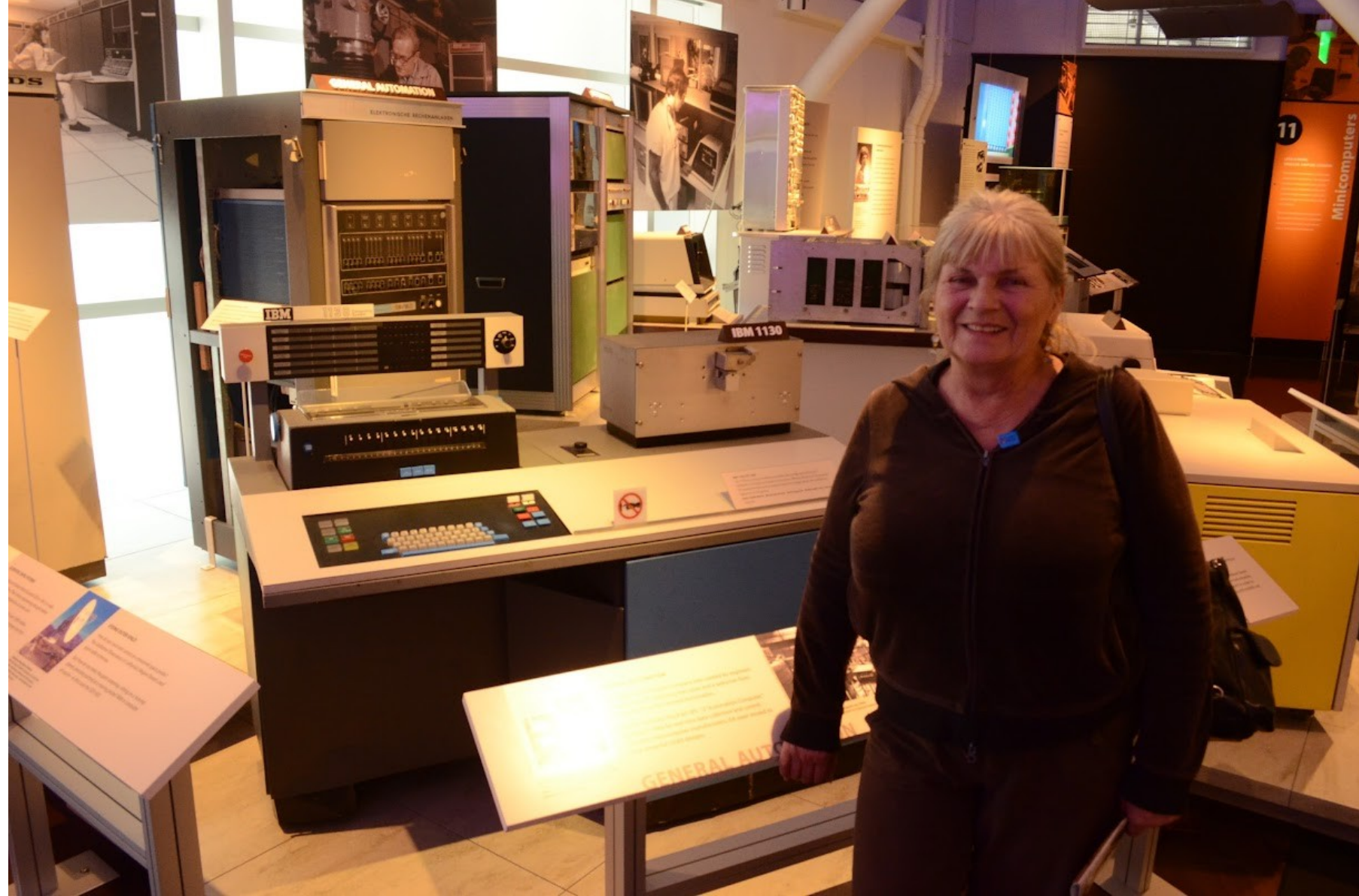
jedimaestro@asu.edu

Syllabus in a nutshell

- Attendance not recorded
- Midterm 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 and censorship evasion
 - Machine-in-the-middle attacks, adversarial networking
 - 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 64 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!

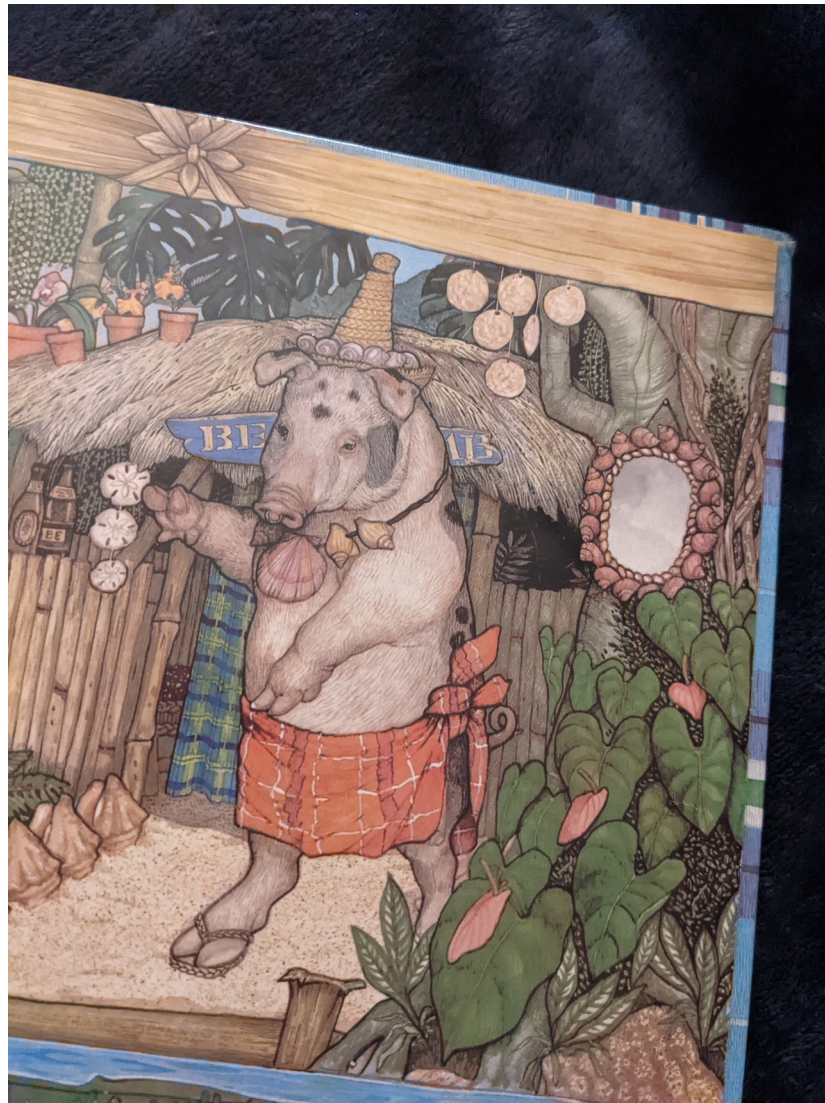
boot: _

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

UNIX, C, and the Internet...

- UNIX was developed to run on anything
 - Bell Labs, 1969 (Thompson and Ritchie)
 - Contrast with TOPS10
- C provides direct access to hardware, virtually no runtime environment
 - Bell Labs, 1972-1973 (Ritchie)
 - Contrast with COBOL

UNIX example...





```
jedi@mariposa:~$ cat /usr/share/dict/american-english | tr [a-z] [A-Z] | grep "MB$" | head -n 20  
COULOMB  
HOLCOMB  
LAMB  
LIPSCOMB  
MB  
MB  
APLOMB  
BENUMB  
BOMB  
CATACOMB  
CLIMB  
COCKSCOMB  
COMB  
COXCOMB  
CRUMB  
CURRYCOMB  
DUMB  
ENTOMB  
FIREBOMB  
HONEYCOMB  
jedi@mariposa:~$
```

TOPS10 example...

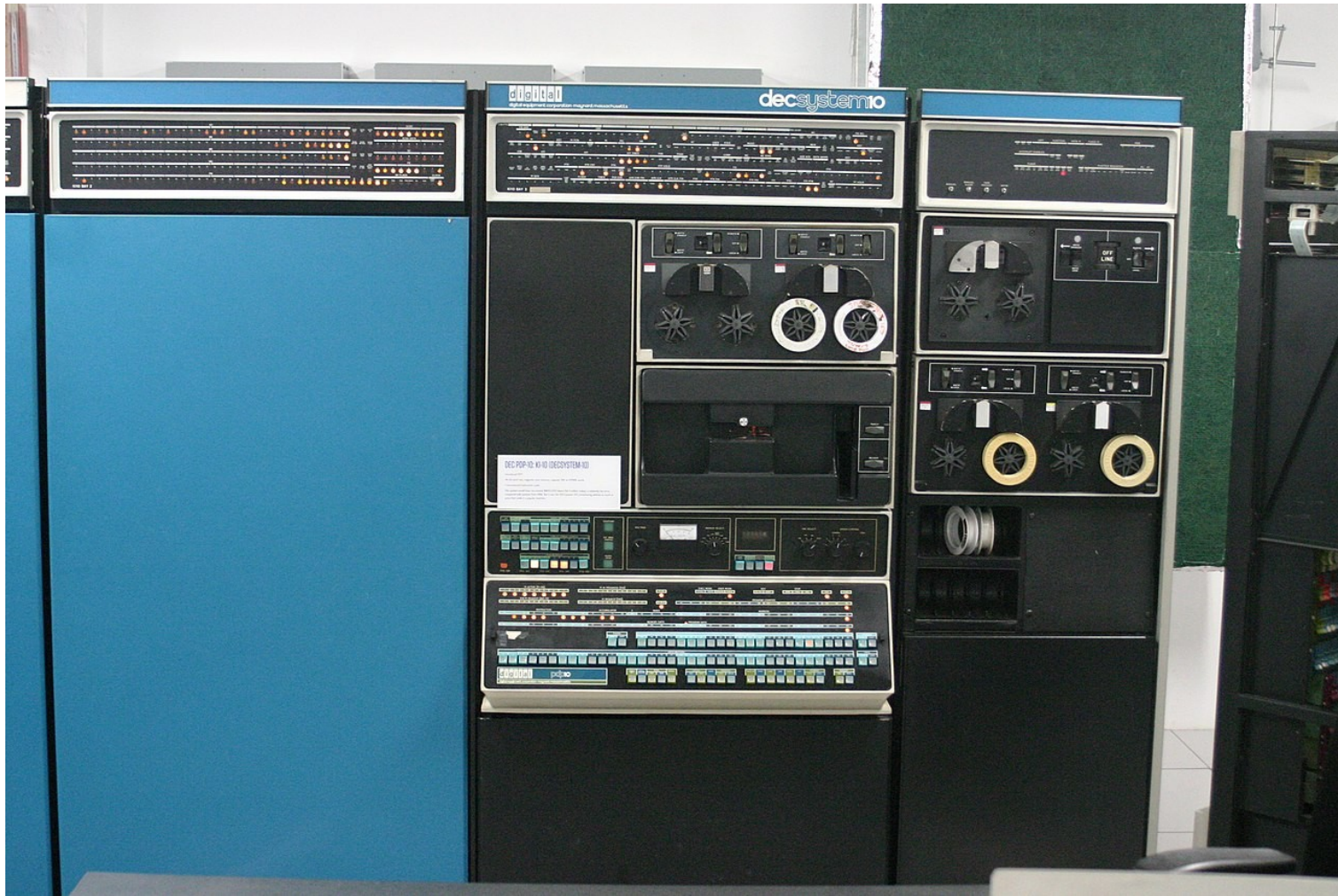
A TOPS-10 command primer

But

```
C:\> mkdir foo  
C:\> cd foo  
C:\FOO> dir
```

becomes:

```
.r credir  
Create directory: [,,foo]  
    Created DSKC0:[42,42,  
FOO].SFD/PROTECTION:775  
Create directory: ^Z  
  
.r setsrc  
*cp [,,foo]  
*^Z  
EXIT  
.dir  
%WLDDEM Directory is empty
```

<https://commons.wikimedia.org/wiki/File:DECSys10-KI10.JPG>

CP/M[®] GRAPHICS[™]

Your ticket to success.

Take the lead in microcomputer applications with powerful graphics software from Digital Research. CP/M and GSX are the keys to your graphic future. GSX is a logical extension of CP/M which many OEMs are adopting to standardize graphic device I/O. Computers with GSX allow your programs to take advantage of integrated graphic displays and peripherals like plotters, printers and CRT terminals. Together, CP/M and GSX deliver the same vital portability for your programs and data that has made CP/M the most accepted operating system in microcomputer history.

We also supply GSS-KERNEL[™] a library of graphic commands for drawing lines, polygons, and text according to the emerging ISO standard: GKS (Graphical Kernel System). We also offer GSS-PLOT[™] a library designed to let you create bar graphs, pie charts, histograms, and scatter plots. Both of these libraries can be linked with CBASIC[®] Compiler, Pascal/MT +[™] PL/I and FORTRAN on 8- and 16-bit systems. When you put it all together, the

Digital Research graphics family is the most complete system you can buy for development and execution of graphic-oriented applications. Whether you're an application developer, OEM or user of microcomputers, call Digital Research for your ticket to graphic success. (408) 649-5500, 160 Central Ave. Pacific Grove, California 93950.

Coming soon! CP/M 83 International Conference and Exposition in San Francisco, January 21-23, 1983. For more information about exhibiting call 617-739-2000.

DIGITAL RESEARCH[™]
The creators of CP/M[®]

CP/M GRAPHICS

GSS-KERNEL GSS-PLOT

©1982 Digital Research, Inc. All rights reserved. CP/M, GSS-KERNEL, GSS-PLOT, and the Digital Research logo are trademarks of Digital Research, Inc. The IBM logo and name are trademarks of International Business Machines Corporation. The name of IBM and its products are either registered trademarks or trademarks of International Business Machines Corporation.

https://commons.wikimedia.org/wiki/File:CP%E2%81%84M_Ad,_InfoWorld,_November_29,_1982.jpg



C example...

```
jedi@mariposa:/tmp$ cat cast.c
#include<stdio.h>

int main(int argc, char **argv)
{
    for (char *p = (char *) *argv; p < (char *) *argv + 20; p++)
        printf("%02x", *p);
    puts("\n");
    return 0;
}
jedi@mariposa:/tmp$ gcc cast.c -o cast
jedi@mariposa:/tmp$ ./cast AAAA BBBB
2e2f636173740041414141004242424200534845

jedi@mariposa:/tmp$ █
```

COBOL example...

```

000024
000025 PROCEDURE DIVISION.
000026 0001-MAIN.
000027     INSPECT FUNCTION REVERSE(STR-1)
000028         TALLYING WS-LEN1 FOR LEADING SPACES.
000029     COMPUTE WS-LEN = LENGTH OF STR-1 - WS-LEN1.
000030     DISPLAY WS-LEN.
000031     MOVE 1 TO I.
000032     MOVE WS-LEN TO J.
000033     PERFORM REV-PARA WS-LEN TIMES.
000034     DISPLAY STR-1.
000035     DISPLAY STR-2.
000036     GOBACK.
000037 REV-PARA.
000038     MOVE STR-1(J:1) TO STR-2(I:1).
000039     SUBTRACT 1 FROM J.
000040     ADD 1 TO I.
000041     EXIT.

```

***** Bottom of Data *****

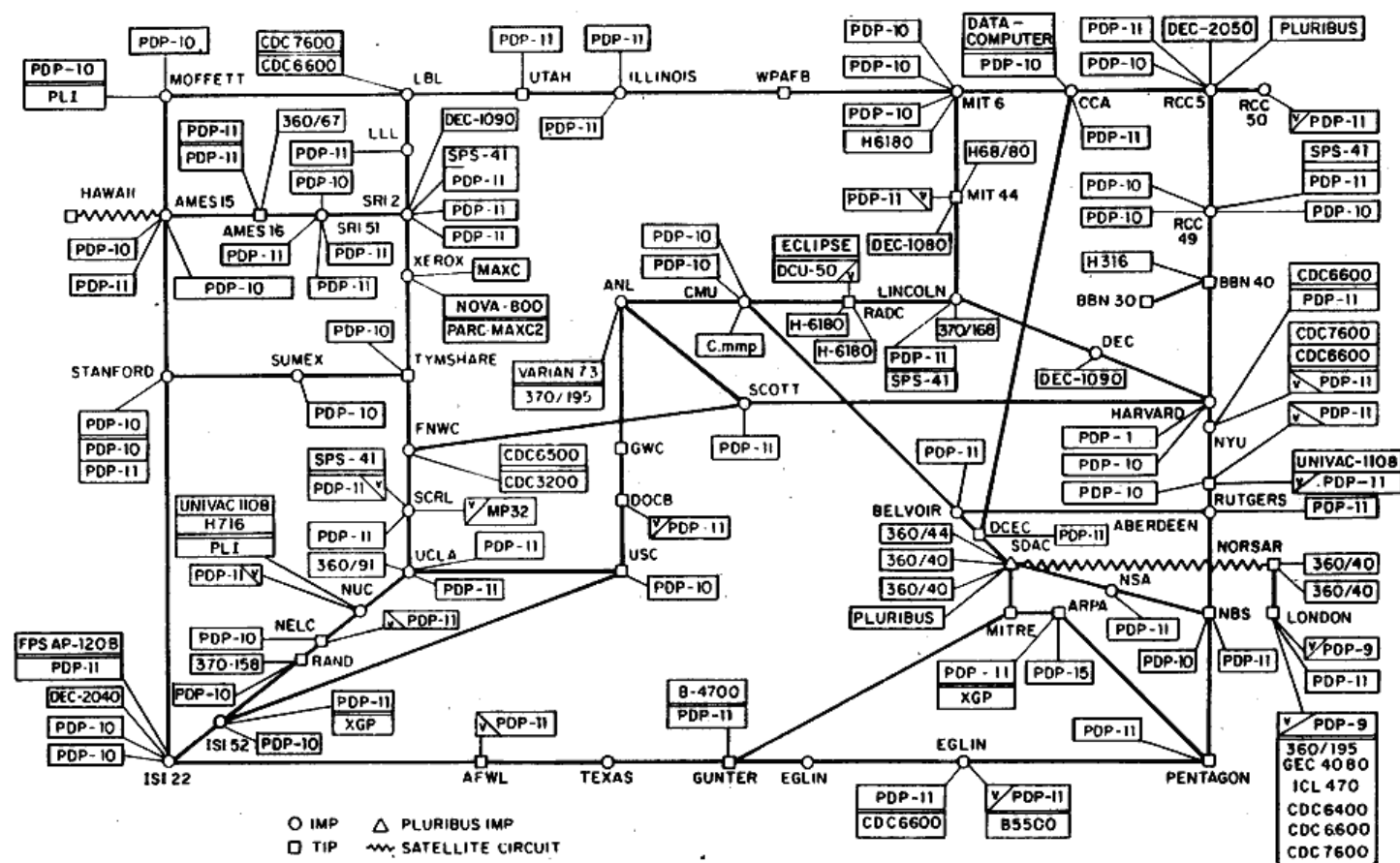
What does all this mean?

The Internet is more like UNIX and C than it is like TOPS-10 or COBOL. This means the smarts are in the end hosts, not the internal routing nodes, and it's really hard to tell what two machines are saying to each other even if you know the protocol.

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”

ARPANET LOGICAL MAP, MARCH 1977



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

Postel's Law

- “be conservative in what you do, be liberal in what you accept from others”
- https://en.wikipedia.org/wiki/Robustness_principle



End-to-end principle

- Put the smarts in the end nodes (security, reliability, QoS, *etc.*)
- https://en.wikipedia.org/wiki/End-to-end_principle



https://commons.wikimedia.org/wiki/File:ARPANET_first_router_2.jpg

Example: Congestion control

- Congestion collapse
- Van Jacobson
- TCP Tahoe, Reno, Vegas, CUBIC...
- Random Early Detection (RED)

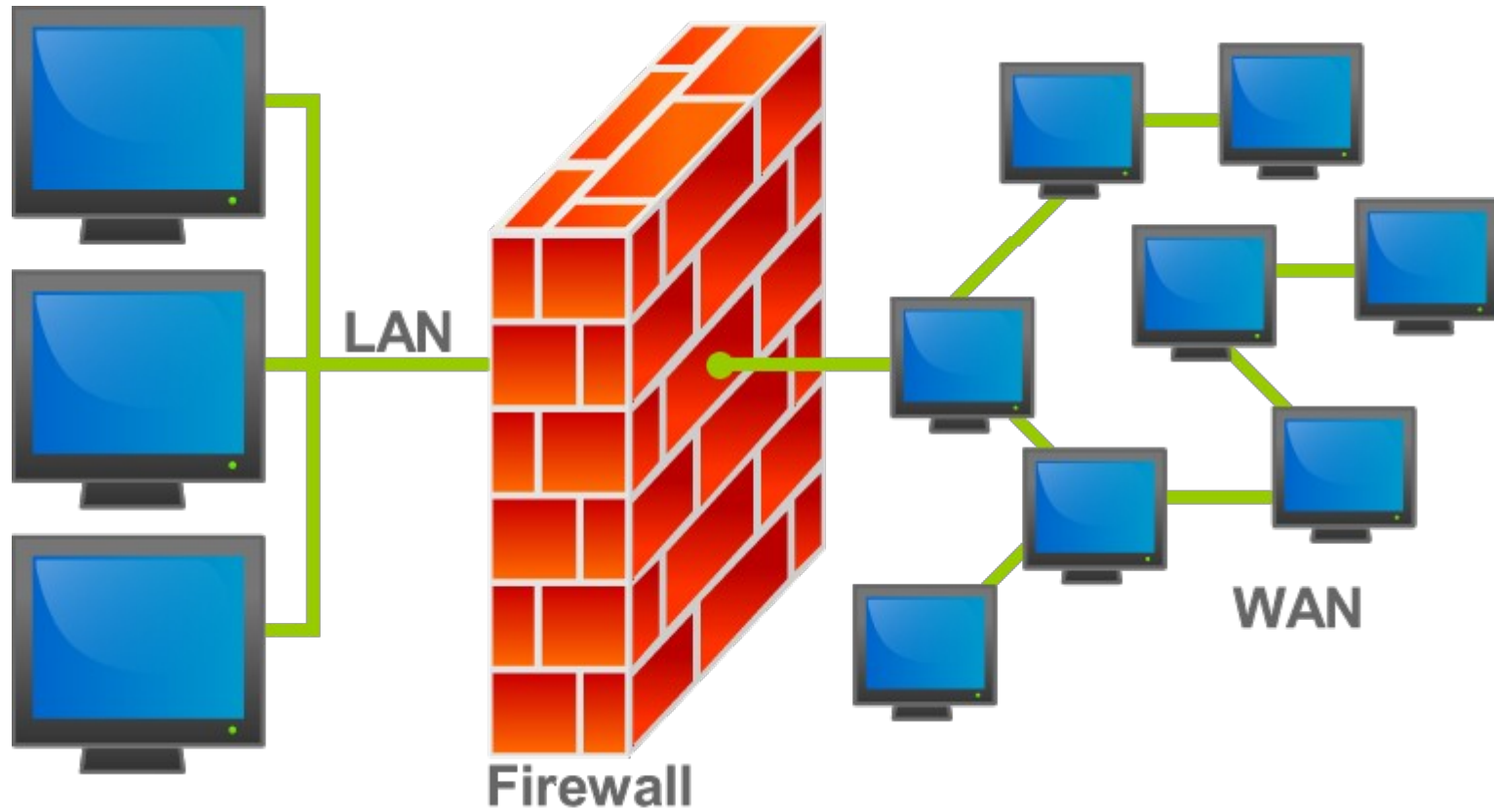


<https://alchetron.com/Sally-Floyd>

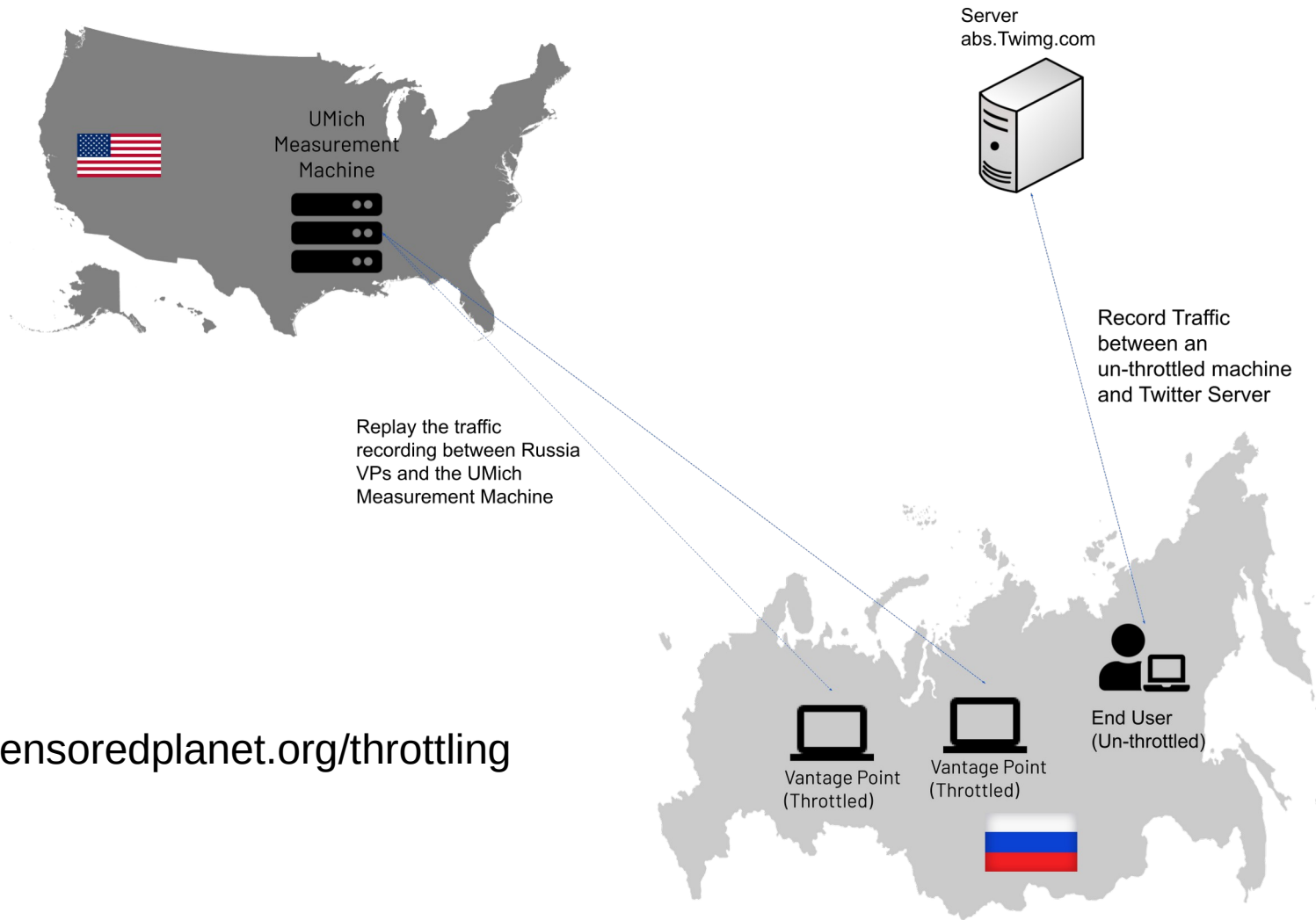
Good design, w/ consequences...

- Every device on the Internet is basically “doing its own thing” *w.r.t.* what packets it sends and how it interprets the packets it receives. (Postel’s Law)
- State is kept in many places without any explicit synchronization mechanisms. (End-to-end principle)

Why all this matters today...

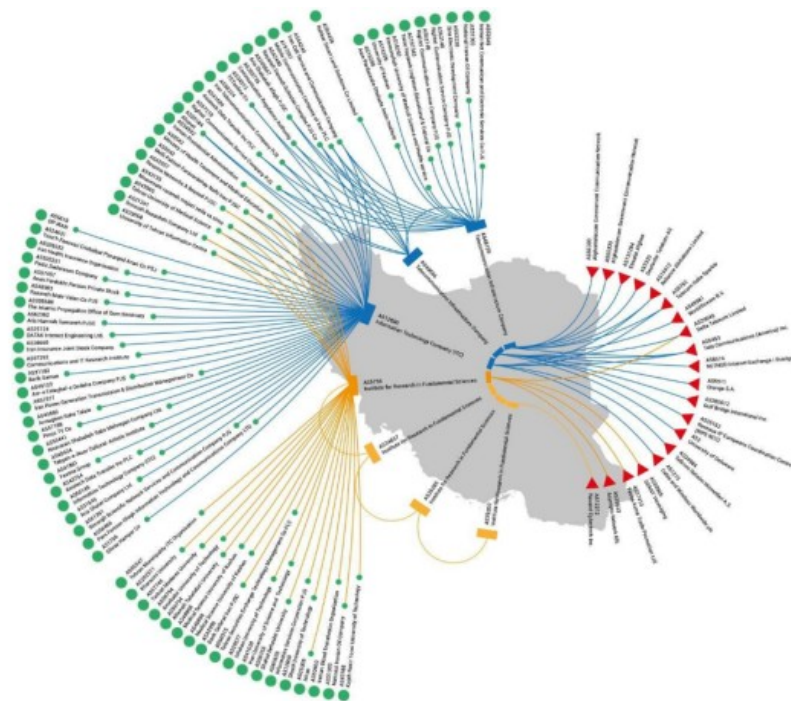
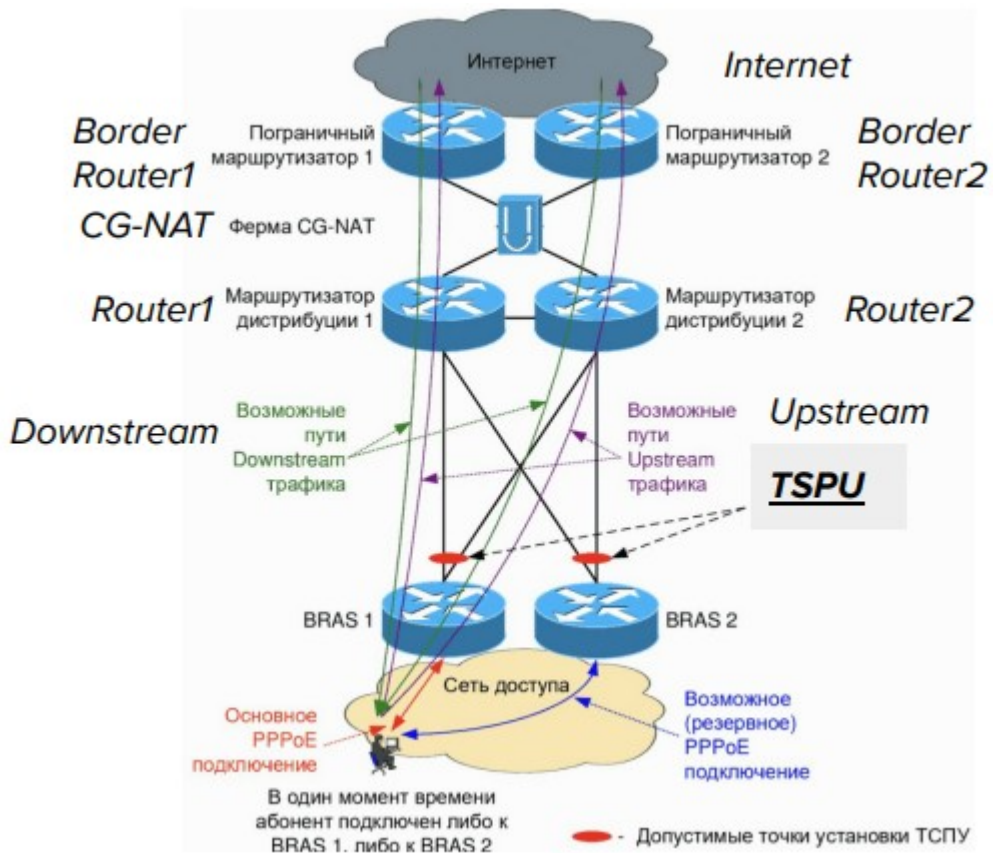


<https://commons.wikimedia.org/wiki/File:Firewall.png>



<https://censoredplanet.org/throttling>





Reproduced and cropped from <https://www.article19.org/ttn-iran-november-shutdown/>



Gmail

facebook



Hotmail

YAHOO!



skype

paltalk.com

YouTube

AOL mail

(TS//SI//NF) **FAA702 Operations**
Two Types of Collection



Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.
- (FAIRVIEW, [REDACTED], BLARNEY, [REDACTED])

**You
Should
Use Both**

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.

[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

Why does light “bend” when it goes through a medium (like a glass of water)?