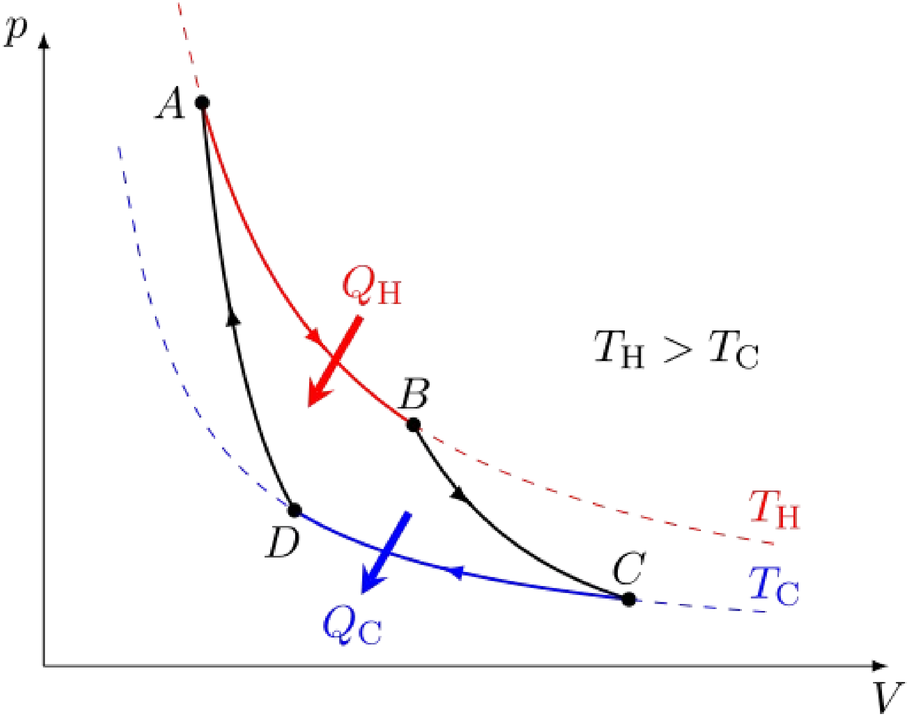
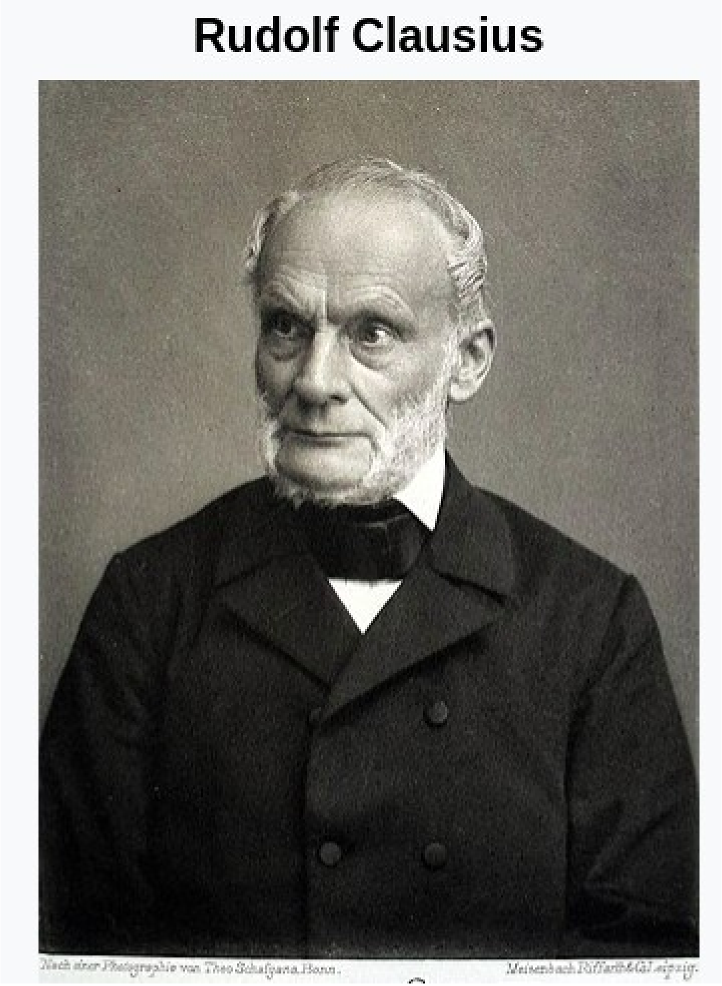
Port scanning and network side channels

CSE 548 Spring 2024

jedimaestro@asu.edu



https://en.wikipedia.org/wiki/Nicolas_L%C3%A9onard_Sadi_Carnot
https://en.wikipedia.org/wiki/Carnot_heat_engine



Rudolf Clausius

Nach einer Photographie von Theo Schafgans Bonn.
Meisenbach Riffarth & Co Leipzig.

“entropy”

(from Greek ἐν en "in" and τροπή tropē "transformation")

Like energy, but you can’t use it.

https://en.wikipedia.org/wiki/Rudolf_Clausius

Entropy

- Statistical foundation by Gibbs, Boltzmann, Maxwell, Planck, *etc.*
- Directly inspired the name of entropy in Shannon’s information theory

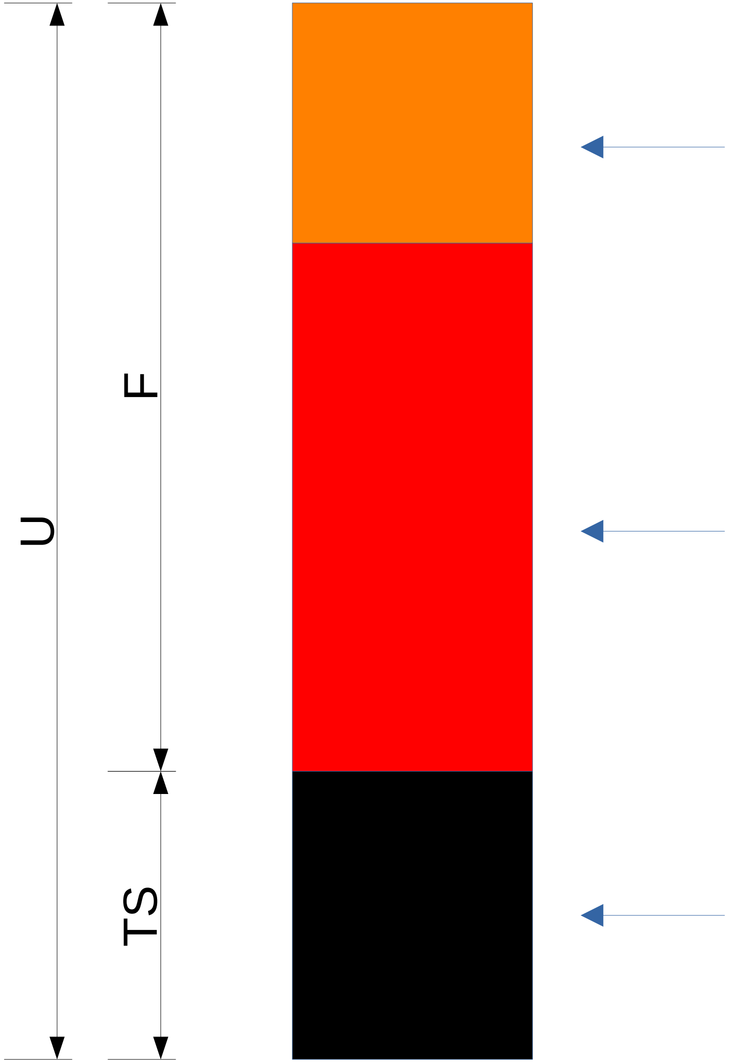
$$H = -\sum_i p_i \log_2(p_i)$$

Reality

- Real engines aren’t as efficient as a Carnot engine
  - Efficiency of 20% or less, compared to 37% Carnot efficiency limit
    - https://news.mit.edu/2010/explained-carnot-0519
- Real computing devices and algorithms don’t use the available energy with 100% efficiency, either
    - Where does that energy go?

$$F = U - TS$$

F = free energy
U = total energy
T = temperature
S = entropy



energy necessary for the computation

energy “wasted”

lost to entropy

How do we make computing faster, more efficient, and/or more reliable?

Harder, better, faster, stronger...

- Shared resources
- Data structures
- Caching
- Copy-on-write
- Divide-and-conquer
- Redundancy
- ...

- Cool the system down
- Don’t erase on deallocation
- Optimize for common case
- Branch prediction
- …

Harder, better, faster, stronger...

- Shared resources
- Data structures
- Caching
- Copy-on-write
- Divide-and-conquer
- Redundancy
- ...

- Cool the system down
- Don’t erase on deallocation
- Optimize for common case
- Branch prediction
- …

All of these make copies of the information being processed and/or decrease the entropy of the system

Definitions

- Covert channel: a channel two processes can use for communication that was not intended to be used for communication
  - Sender and receiver collude
- Side channel: a channel through which information leaks, but the sender is not sending the information intentionally
  - No collusion

Outline

- Review of port scanning, idle scans
- Examples of ***network*** side channels
  - SYN backlogs and DoS
  - RST rate limitation
  - Off-path TCP hijacking
  - Blind in/on-path attacks

TCP 3-way handshake (review)

- SYN: I'd like to open a connection with you, here's my initial sequence number (ISN)
- SYN/ACK: Okay, I acknowledge your ISN and here's mine
- I ACK your ISN

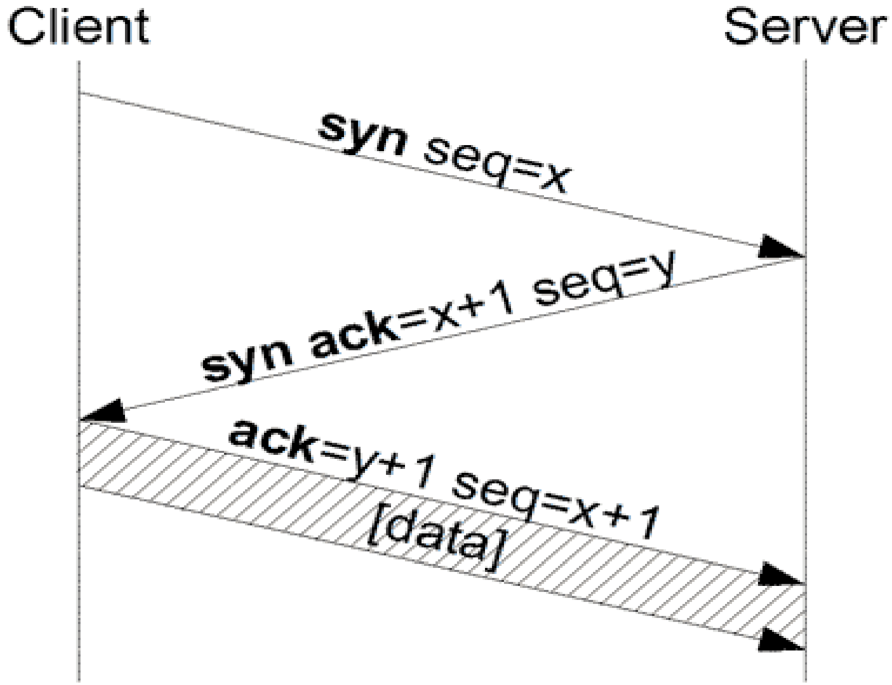


Image from Wikipedia

Open port == listening

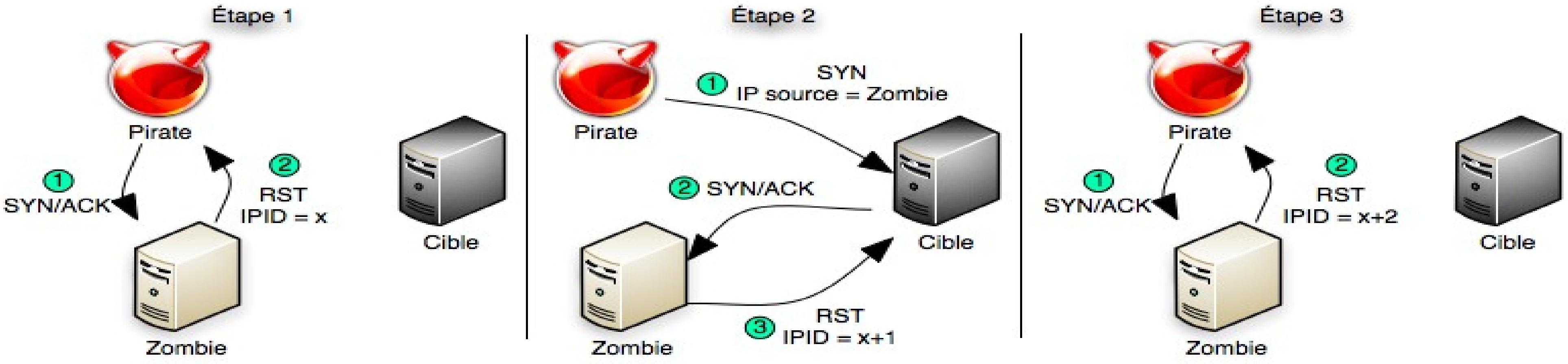
- If you send a SYN packet to port 80 (the HTTP port) on a remote host and that host replies with a SYN/ACK, then we say that port 80 on that machine is “open”
  - In this example, that probably means it's a web server
- If it responds with a RST, we say it's “closed”
- If there is evidence of filtering (no response or ICMP==Internet Control Message Protocol error), we say it's “filtered”
  - UDP is more complicated: open|filtered *vs.* closed

Things nmap can do

- Is a port open? Closed? Filtered?
  - Many ports on one machine is a “vertical scan”
- For a /24 network, which machines are up? Which machines have port 80 open?
  - One port for a range of machines is a “horizontal scan”
- OS detection (research on your own)
- Stealth, info about middleboxes, etc.

Idle scan

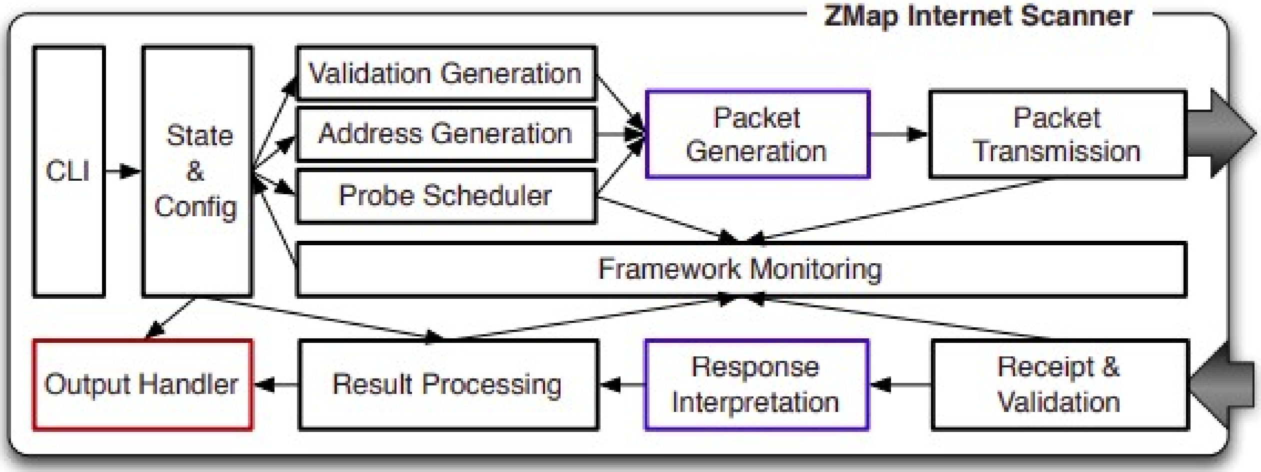
- Every IP packet sent has an IP identifier
  - In case it gets fragmented along the way
- Old and/or stupid machines use a globally incrementing IPID that is shared state for all destinations



Par Shiningfm — Travail personnel, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=8273541

Zmap

- https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_durumeric.pdf
- https://zmap.io/



Theme

- Attacker wants to find out (*i.e.*, copy) certain information while doing the least amount of work possible
  - – Are hackers lazy, or do they just respect the 2nd law of thermodynamics?
    - Yes, both
  - – Copying information is the simplest computation you can do, and is what reversible molecular computers use as a benchmark
  - – Side channels (like the idle scan) are the same thing, just more indirect...

Examples of network side channels

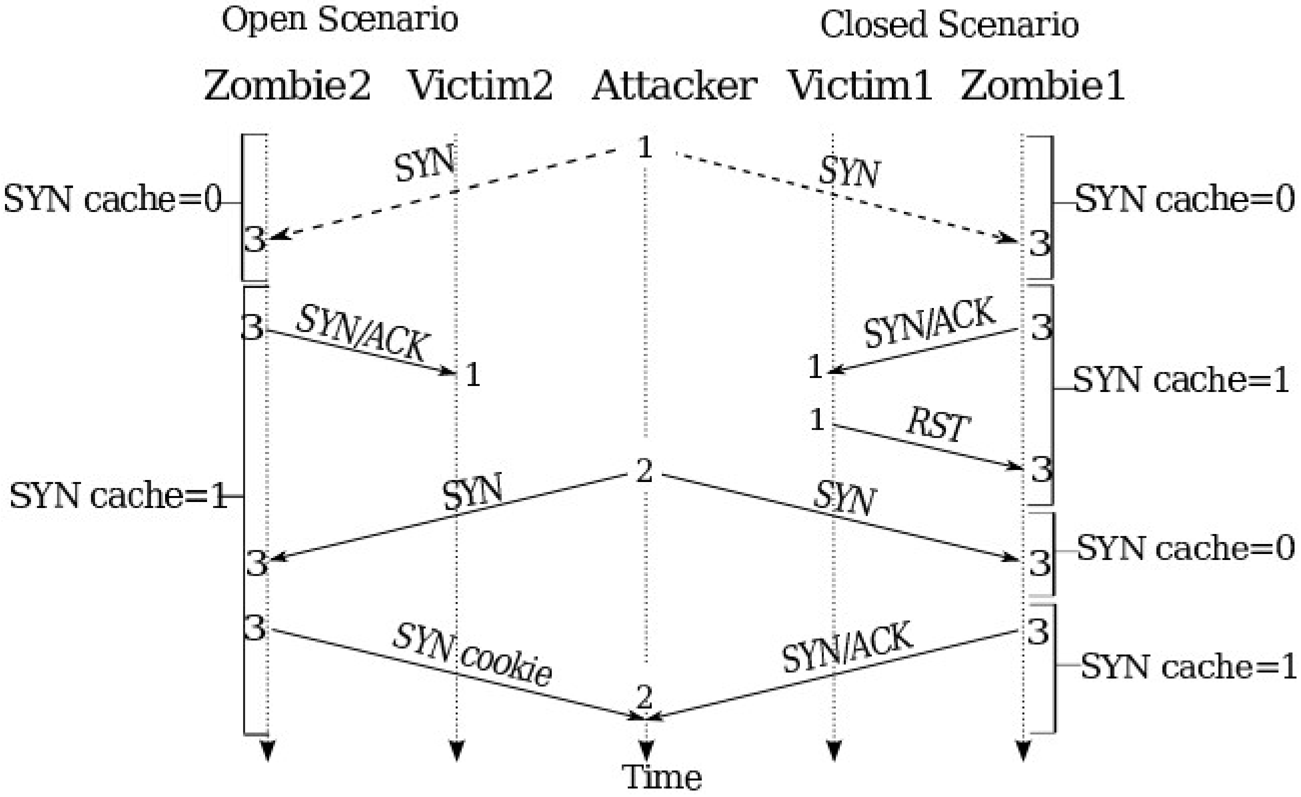
- DoS and SYN backlog basics
  - A side channel based on the SYN backlog
- Blind off-path TCP hijacking
- Blind in/on-path DNS and TCP hijacking

DoS in general

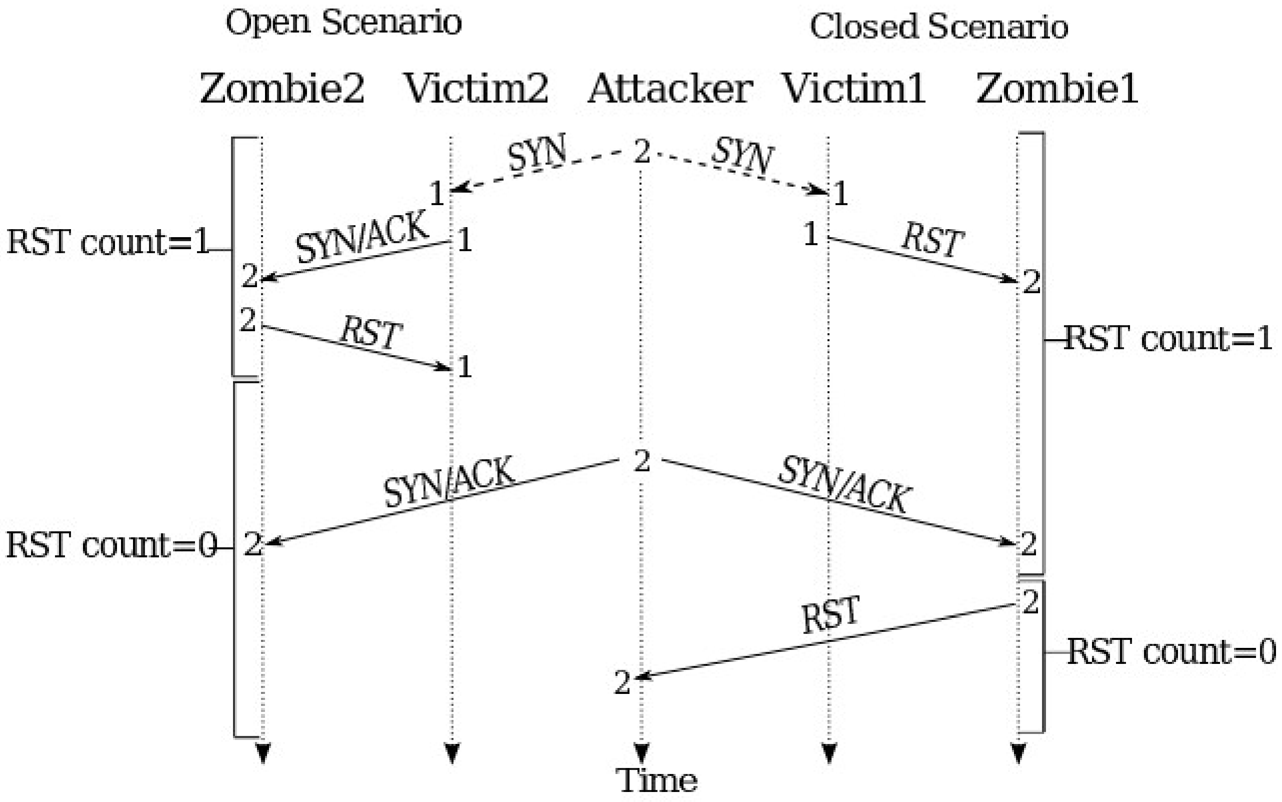
- Exhaust some kind of resource, *e.g.*:
  - Optimistic ACK to exhaust bandwidth
    - See https://homes.cs.washington.edu/~tom/pubs/CCR99.pdf
  - PING of death (*e.g.*, large PING) causes crash
  - Exhaust CPU in layer 7
  - More examples: http://www.isi.edu/~mirkovic/bench/attacks.html
  - SYN flood: Older hosts had either a fixed amount of half-open connections they could keep track of or no limitations at all; attack is to send lots of SYNs and never ACK or RST
    - Defenses: SYN backlog policies and SYN cookies

SYN cookies and SYN backlogs

- SYN cookies
  - Special kind of SYN/ACK
  - See https://cr.yp.to/syncookies.html
  - Can confirm ACK number and reconstruct the necessary state for a connection without having kept any state after sending the SYN cookie
- SYN backlog examples
  - Linux reserves ½, ¼, 1/8th, and so on for successively older SYNs, prunes 5 times a second
  - FreeBSD has 512 buckets of 30, you can't predict what bucket you fall into (in theory)



From… https://jedcrandall.github.io/usenix10.pdf



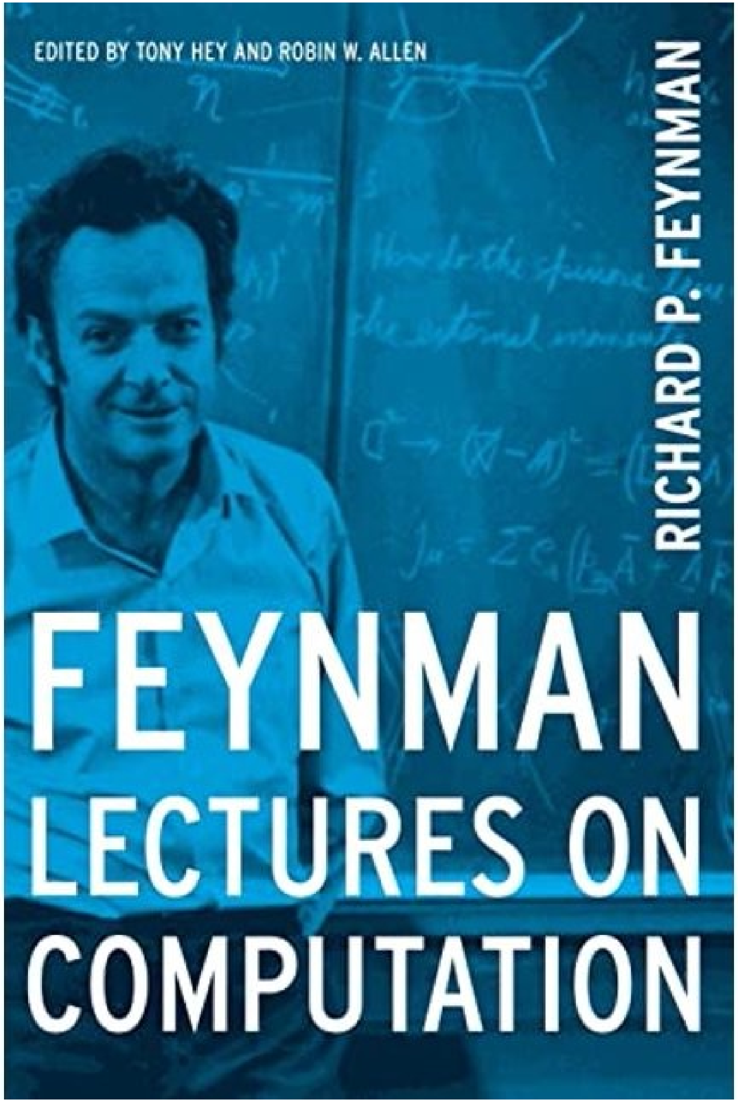
From… https://jedcrandall.github.io/usenix10.pdf

USENIX Securtiy 2016 Cao *et al.* Slides...

USENIX Security 2021 Tolley *et al.* slides...

References

- *NMAP NETWORK SCANNING*, by Gordon “Fyodor” Lyon
- Google “nmap”, “idle scan”, etc.
- Other references were linked to inline



EDITED BY TONY HEY AND ROBIN W. ALLEN

RICHARD P. FEYNMAN

FEYNMAN LECTURES ON COMPUTATION