Recitation 22: Mirai

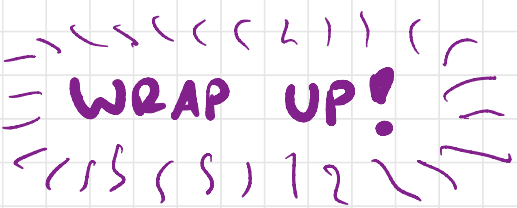
MIT - 6.033

Spring 2021

Henry Corrigan-Gibbs

Plan

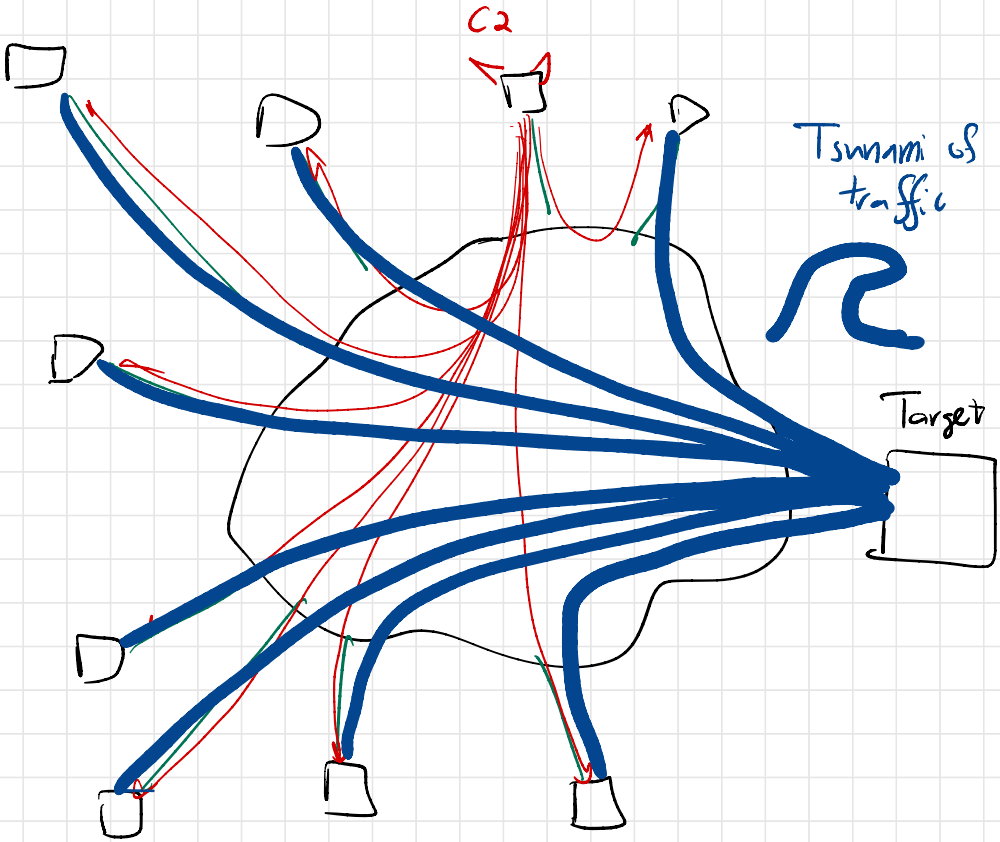
* What was Mirai?
* How did it work?
* Why did it work & what do we do about it?



Logistics

* This is the LAST RECITATION!
* Course evaluations open
  ↳ Very important
* Feedback form — post course notes?
* Office hours / AMA 5/20
  ↳ sign up if you want to join

What was the Mirai botnet?



Botnet = large fleet of hijacked machines that one entity controls.

Purpose: $$$! → Distributed DoS { political, business, gaming
→ Ad fraud
→ Spam mail

Technique:

1) Infected machines scan IPv4 space
2) Try common user/pass pairs
   ↳ Very common!?
3) Once logged in, infect machine

This attack is simple enough that any of us could do it.
↳ SHOW CODE

DO NOT TRY THIS AT HOME!?
↳ Bad karma and also illegal... many stories

Scanning like this is very common
↳ show market logs
↳ show country analysis
↳ show nmap

Be careful if you have a machine w/ a public IP (e.g. story at Stanford)

Why did it work?

- No one thought that these were security critical
  - → Unsafe defaults
- Devices are not patched
  - → How often do you update your TV / router / doorbell / toaster?
- Devices on open Internet — open by default

Also:

Incentive problem!

- → Cost of security paid by you and toaster vendor
- → benefit of security accrues to people getting DDoS'd.

... Remember back to our first paper

"We did nothing wrong" ...

What do we do about it?

(Similar to preventing bank robberies?)

- Mandate safe defaults? (CA law)
  - "connected device" has to have unique pass or asked on 1st boot
- Mandate updates?
- Improve law enforcement / accountability?
- Eliminate payment channels?

Wrap up

Take ≈ 3 mins to look at the 6.033 web site and refresh your memory on the papers we read this semester.

- What was one idea that you really liked?
- A paper that changed the way you think about computers or computation?

Submit your subject evaluations, pleaw plese plese!

Finally...

This has been an exceptionally difficult semester in an exceptionally difficult year.

THANK YOU for being such excellent students.

I have looked forward to spending time with you + Amir every week.
Let's keep in touch!

In computer systems, we often take inspiration from non-digital processes (USPS → internet?)

Now that you are experts on computer systems, I hope that you can take lessons you've learned in 6.033 and apply them to your life.

* May you be tolerant of faults in yourself and others.
* May you have high-bandwidth communication channels with your most important peers.
* May your ambitions, your success, and most of all your happiness, scale without bound.

Have a wonderful summer! ☺