Recitation 24: Mirai
Plan

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

Logistics

* Check out the computer
* Exam 2 on 9/16 9-11am, Johnson Track
* Course evaluations open
  **Very important**
  * Feedback form - post course notes?

* AMA/Chilling outside 9/12 10am-noon
  Stata Amphitheatre
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

Tsunami of traffic
Technique:

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

The 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. stay at Stanford)
Things of note

* Different Mirai “flavors” after code leaked

* Mirai used to DDoS Mirai C2 servers

* Mirai competes against Mirai for hosts

Targets ....

Discuss in groups?
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?
    - End-of-life problem

- 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 ask it on 1st boot
- Mandate updates?
- Improve law enforcement / accountability?
- Eliminate payment channels?
For next time...

- Look at past papers, past exams

- Bring your questions.

- Is there anything particular you'd like us to cover?

henrycg.com/feedback.

Submit your subject evaluations, please please please!