Recitation 25 — Mirai

Overview

- Mirai is a botnet made up primarily of IoT (Internet of Things) devices
- Botnets in general have changed the landscape of attacks. They allow adversaries to send lots of traffic from many different places, and in many cases they can evolve as older attacks are thwarted.

Basic infrastructure

- Figure 2 in the paper gives a good explanation of the architecture of Mirai
- Mirai creates new bots by exploiting the default passwords on IoT devices
- It compromises *many* machines

Attacks

- Many IoT devices can't actually send much traffic. But Mirai is a *huge* botnet.
    - Many different types of attacks
    - Many of these attacks try to exhaust compute/memory/storage resources rather than network bandwidth
- Mirai, like many botnets, evolved new attacks (one example is mentioned in Section 4.2)

Possible Mitigations

- Section 7 suggests many improvements
- Random default passwords would've made it much more difficult for Mirai to compromise machines; why not do this?
    - Many answers, but the complexity of installing random default passwords, making sure users know how to find them, what to do if a user loses the password, etc.
- Automatic updates would have allowed the security flaws that Mirai exploited to be patched more quickly, but many IoT devices don't do automatic updates