Security and Privacy Issues in Smarthomes

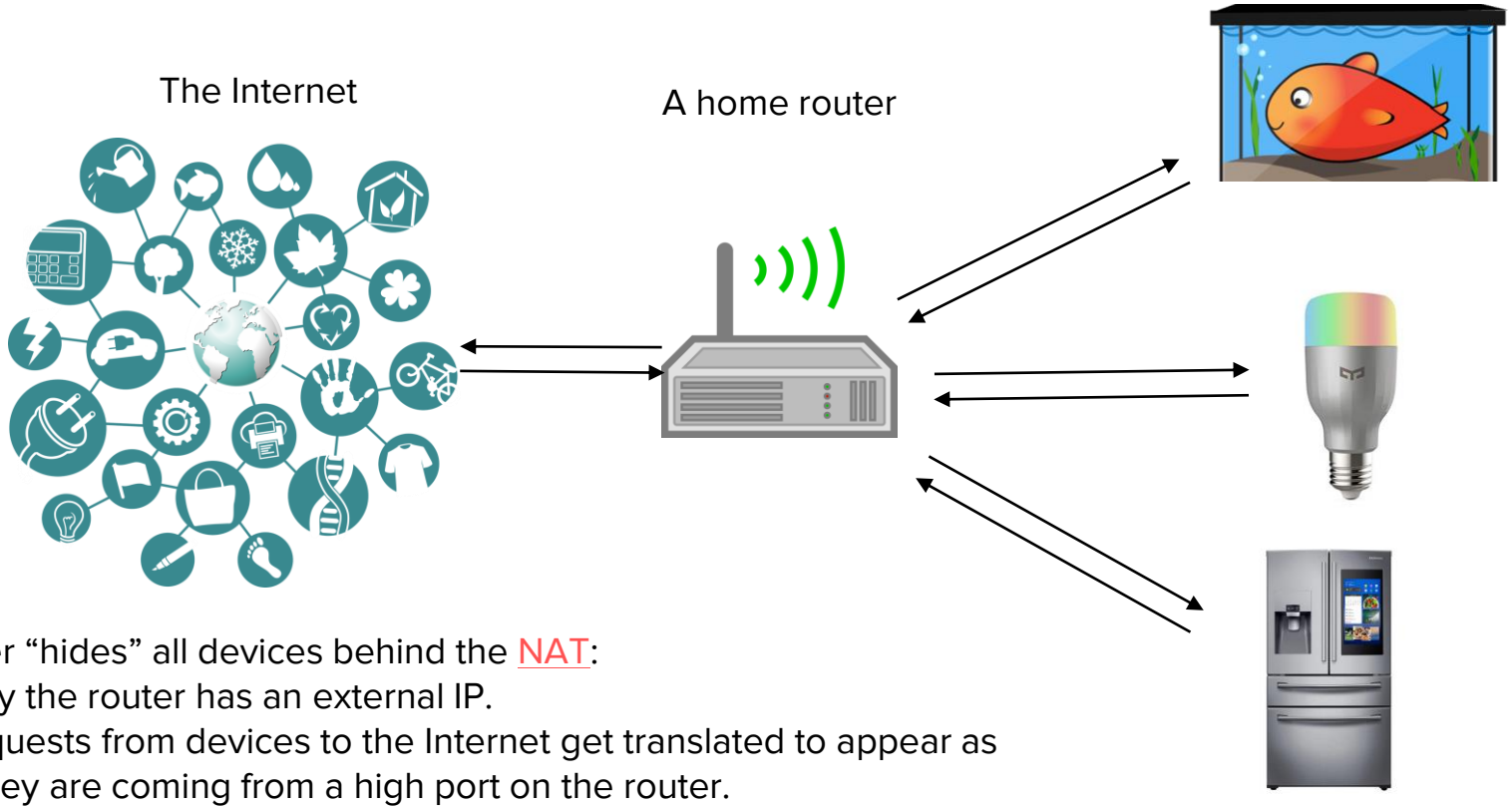
Earlence Fernandes, CS 642, UW Madison

Slides borrowed from Ivan Evtimov

General Notes

- One account on Nidan per group. Pick one email from the group to use.
- You will (probably) not be able to access the devices without a SOCKS5 proxy. Instructions on how to set that up and use it are in the spec.
- Re-read the spec: it is long but has many details

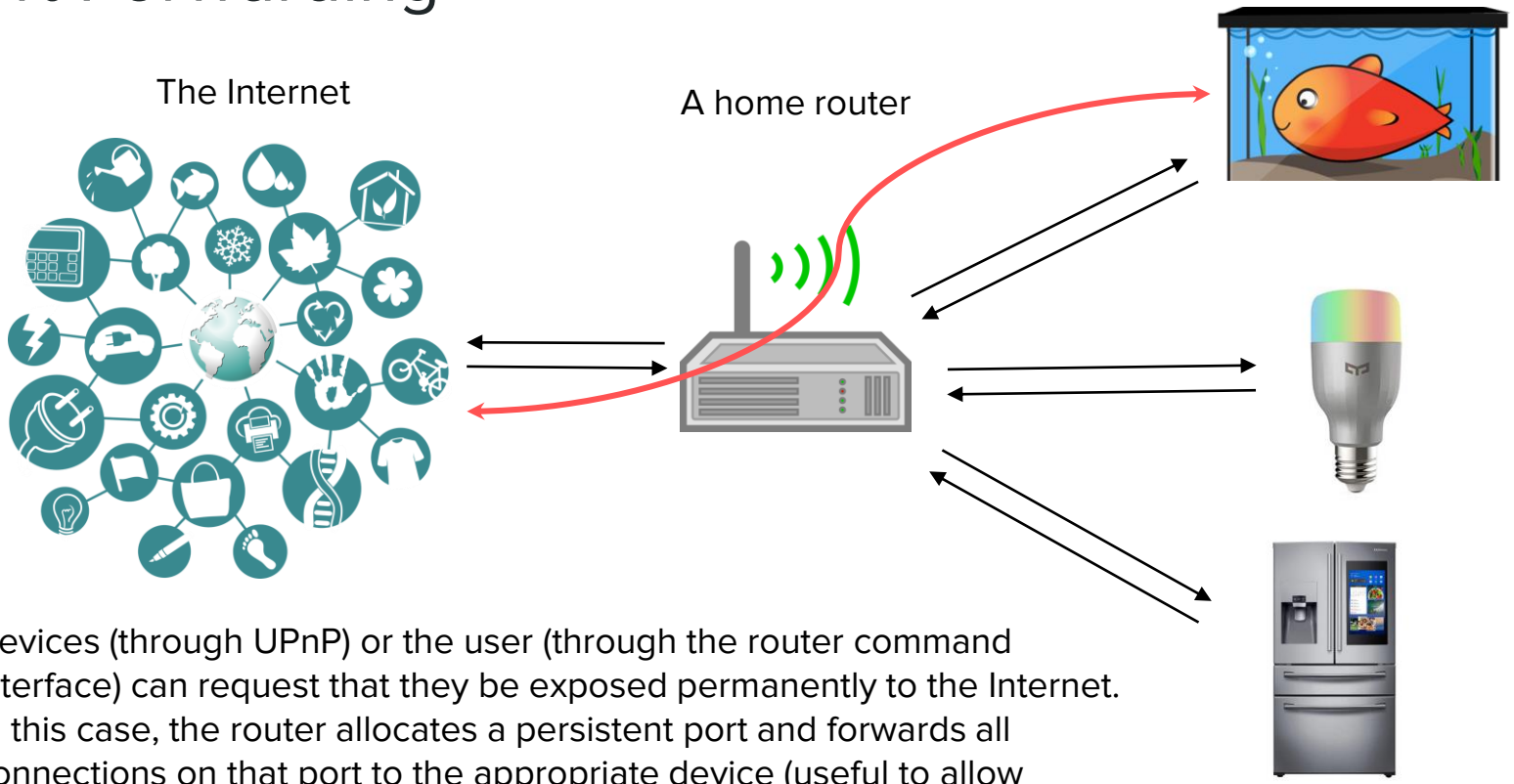
What does a smart home network look like?



The router “hides” all devices behind the NAT:

- Only the router has an external IP.
- Requests from devices to the Internet get translated to appear as if they are coming from a high port on the router.

Port Forwarding



- Devices (through UPnP) or the user (through the router command interface) can request that they be exposed permanently to the Internet.
- In this case, the router allocates a persistent port and forwards all connections on that port to the appropriate device (useful to allow external control).

Chaining Vulnerabilities

- Even one device with a security vulnerability can serve as an entry point to compromising the entire home.
  - Target Hackers Broke In Via HVAC Company (Krebs on Security)
  - How a Fish Tank Helped Hack a Casino (The Washington Post)

- You do not even need buffer overflows, web exploits or other highly technical vulnerabilities. Some very common pitfalls:
  - Default credentials
  - Trusting that the device is only accessible on a LAN
  - Failure to authenticate physical-channel commands (e.g., audio)
  - Authorization tokens embedded in the open-sourced code of a controlling app
  - Fallacies in programming automation rules

Smart home security and privacy is more than network security!

- Smart devices collect much more data than just web browsing history, thereby exposing potentially much more sensitive information
- No longer the case that one computer = one user = one impacted person, the privacy of every inhabitant is exposed
- People who set up the smart home have an outsized power (this can get ugly, e.g. NYT article on smart homes exacerbating domestic abuse situations)

Final words

- The exploits are not technically sophisticated (no buffer overflows, XSS, SQL injection)
- Web app vulnerabilities are out of scope
- Read the spec and ask questions.
- Have an idea on what else would be fun for this lab? Let us know!
- Have fun!