CDSE Center for Development of Security Excellence

"Your Fridge is Spying on you!" Understanding the Internet of Things (IOT)

LEARN. PERFORM. PROTECT.

What is the IoT?

The extension of internet connectivity beyond standard devices to traditionally "dumb" devices…

…by embedding electronics, software, sensors, and connectivity…

…enabling those things to exchange data.

MIT Coke Machine
1982

Kevin Ashton
1999

Today

CDSE 2

Over 8 billion devices…

Grantoswell, Flickr

Patrick Pelletier, Flickr

Google

Medical: medical devices, emergency notification, hospitals
Agriculture: farming, waste management, temperature sensing
Environmental: air and water quality, atmospheric conditions, wildlife
Large scale deployments: "smart cities"

CDSE 3

Over 8 billion devices…





Smart Clothes and Wearables



- Designed to be kept with the user during use
- Provides health and fitness feedback via internet or app
- Have been exploited / PoC to change dosages or track individuals
- Different type of risk

Benefits of IoT

By David Berkowitz - https://www.flickr.com/photos/davidberkowitz/5343789473/, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=32434601

- Asset management
- "Identification of Things"
- Use resources efficiency
- Monitoring / status checks
- Allows innovation (sensors, tags, analysis, manufacturing)

Case Study: Unnamed Casino

Casino hacked (through the fish tank) - 2017

- Attackers infiltrated the network through an internet-connected thermostat
- Traversed the network from that point
- Exfiltrated 10GB of sensitive data

Case Study: Cloudpets

Cloudpets - 2017

- Hackers gained access to user database
- Affected 800,000 users
- Included network access, voice recordings, etc
- Potentially allowed for remote surveillance

https://www.networkworld.com/article/3285968/internet-of-things/strange-and-scary-iot-hacks.html#slide3

Case Study: Jeep Cherokee

Jeep Hack - 2015

- Security researchers in a controlled proof of concept
- Controlled radio, vents, and brakes from 10 miles away
- Used a "0-day" exploit

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Case Study: Mirai Botnet

Mirai - 2016

- Scanned for open telnet ports in IoT and tried default password
- Originally created to attack competing Minecraft servers
- Reused by other attackers to attack DynDNS next month
- Currently in the wild and being modified
- Creators working with FBI and won't serve time

CDSE 10

Attacks Against IoT

service	% of attacks
Telnet	75.40%
SSH	11.59%
other	13.01%

#	downloaded malware	% of attacks
2	Trojan-Downloader.Linux.Hajime.a	5.89%
3	Trojan-Downloader.Linux.NyaDrop.b	3.34%
6	Trojan-Downloader.Shell.Agent.p	0.38%
7	Trojan-Downloader.Shell.Agent.as	0.27%
9	Backdoor.Linux.Gafgyt.ba	0.24%
10	Backdoor.Linux.Gafgyt.af	0.20%

KASPERSKY

CDSE 11

Risks and Vulnerabilities

Risks

- New attack surfaces
- Botnet recruitment
- Expanded aggregation of information

Vulnerabilities

- Can't always patch older devices
- Few security features
- Physical access = root
- Poor remote security

CDSE 12

Countermeasures

- Update firmware
- Change default passwords
- Do you REALLY need it?
- Don't share / show serial numbers
- Follow security feeds
- Use a router firewall and view devices

We need to secure our devices, or we might unknowingly be part of the next attack!

DoD Policy (Plagiarize accordingly)

1. Use appropriate contract vehicles
2. Use solutions you actually need
3. Encrypt when possible
4. Involve your ISSP (RMF impact?)
5. Manage the supply chain
6. Network operations
7. Search for unauthorized devices

Where we're going

Internet of Things Cybersecurity Improvement Act of 2017 (August 2017)
Requires companies with federal contracts to ensure that devices are patchable, use passwords that can be changed, and are free from "known vulnerabilities"
Status: "Read twice and referred to committee"

Securing IoT of 2017 (March 2017)
Amends the Communications Act of 1934 to require FCC to establish cybersecurity standards for IoT-type devices
Status: "Referred to subcommittee"

California Securing IoT of 2017 (March 2017)
Requires baseline standards for IoT devices. Requires but doesn't define "reasonable" security features
Status: Pending Governor signature (9/6/2018)

GAO Report: (July 2017)
"Enhanced assessments and guidance are needed to address security risks in DoD"

Conclusion

IoT is convenient, easy to use, and effective

But

There's risks to ourselves and our mission

So

We need to focus on security over convenience!