

Cyber Defense Organization

Fall 2020 - Internet of Things (IoT) Security



Attendance

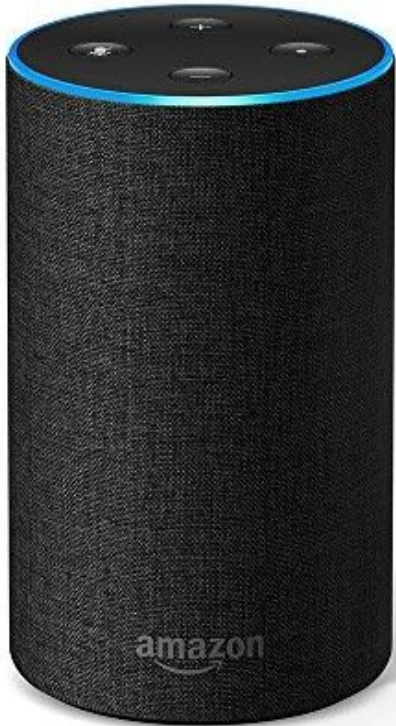
<https://forms.gle/hrQfSqmqHPMkAD2S7>

What is the 'Internet of Things'?

- The physical network of devices that can interact and exchange data with other devices.
- These devices commonly have some sort of sensor, such as voice activation, motion sensor, etc...
- Approximately 7 billion smart devices in the world!!



Examples of IoT Devices



What Data is collected through these devices??

- Medical Information
- Your Habits
- Your Voice
- Home information
- Personal Information
- Many more!!



All That Information is Safe....RIGHT??

- Like all information, IOT data it is stored somewhere
- Sometimes this data is stored on the devices themselves (Roomba).
- Other times data is periodically uploaded to a server, usually the company manufacturer (Amazon Echo.)
- Almost all of these devices are also connected to the internet in some manner, which means...
- THEY CAN BE HACKED!



IoT Devices are Vulnerable!

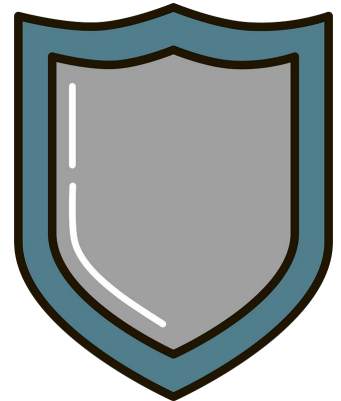
IoT devices can be breached through connection to the internet or other nearby devices that are also connected to it.

- Ransomware
- Arbitrary code execution
- Personal Information Theft
- Infect other devices



How IoT Influences Security

- A lot of data can be gathered by IoT sensors, some of it highly detailed.
- Connection of virtual and physical devices: These devices can have real physical implications if breached, IE somebody can control your smart home if given enough access
- IoT Architecture is Centralized. Most data goes to a 'base station' which can be used by thousands of devices, allowing a wider attack surface.



Example- The Mirai Botnet, October 2016

- Still one of the Highest ranking DDoS attacks ever.
- DSN Service Provider Dyn was targeted
- Dyn Servers were crippled and large sections of the internet went down
- How? A MEGA IoT device botnet connected through the Mirai malware using default passwords to gain access.
- Netflix, CNN, Twitter all had issues.



Example- What Did the World Learn?

- Smart devices can have a profound effect on our daily lives
- IoT devices can be linked together to form MASSIVE botnets to attack targets
- Regulations and laws passed to require stricter IoT device security.



What can we do to secure our IoT Devices?

1. Change Default Usernames & Passwords. This is how the Mirai Malware infected devices
2. Keep Device software up to date to ensure most updated security features
3. Enable Two-Step Authentication to ensure nobody else is logging in
4. Avoid connecting IoT devices to public Wi-Fi Networks
5. Ensure Privacy settings on device are what you want them to be



How Governments are Responding

- Mirai Botnet was a wake up call to many in the government
- There will only be more and more devices in the future
- IoT attack increase by 300% in 2019
- Oregon and California requiring “reasonable security features” to be added to IoT devices by companies
- United Kingdom to introduce mandatory security requirements for IoT device Manufacturers.



A Growing Field in IoT Security

Since IoT Security has become more of a prevalent issue in the world several organizations have released Frameworks, benchmarks, and guides on how to secure IoT devices in homes and multi-billion dollar corporations alike.

NIST- <https://www.nist.gov/topics/internet-things-iot> (2:00 Minutes)

OWASP- <https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf>

SCIOT- https://link.springer.com/chapter/10.1007/978-3-319-99073-6_29



Thank You For Watching!



Any Questions???



Coming up next week!

Tuesday: Blue Team Practice @ 7pm

Wednesday: Security + @ 5pm

Thursday: Red Team Practice @ 7:30pm

Friday: Insider Threats @ 3:30pm

*Times/Dates are subject to change.



Add us on Social Media!

Twitter: **@ualbanyCDO** 

Instagram: **ualbany_cdo** 

Website: **uacyber.org** 

Myinvolvement: **Cyber Defense Org**

We have a discord!

