

IOT SECURITY

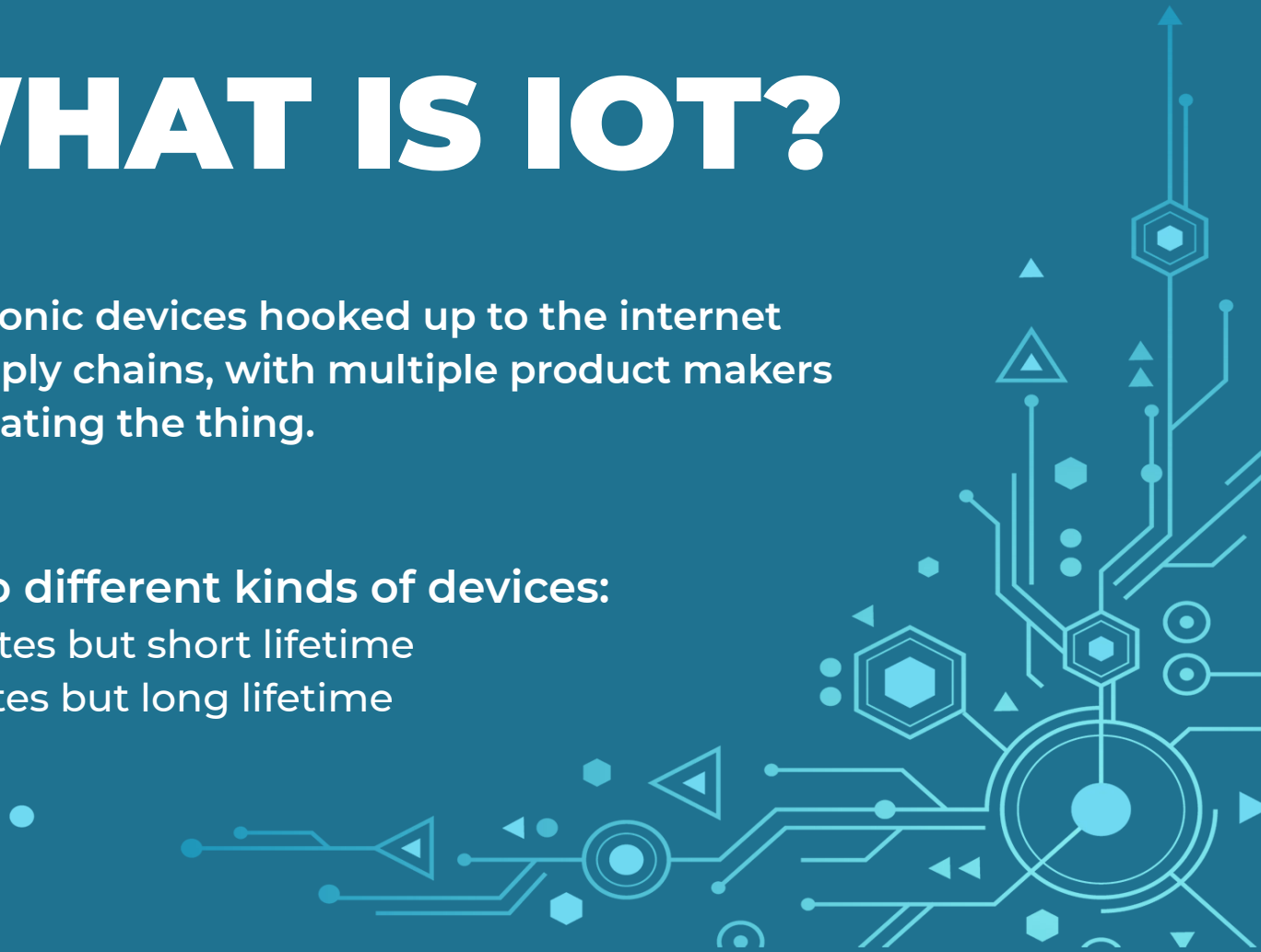








WHAT IS IOT?

- They are electronic devices hooked up to the internet
- Have huge supply chains, with multiple product makers and people creating the thing.

There are two different kinds of devices:

- Frequent updates but short lifetime
- Very rare updates but long lifetime



		IoT Characteristics	Potential Security Weaknesses & Targets
Web & Mobile Applications		<ul style="list-style-type: none"> > Closed/open platforms > Variable policies > High data volume handling 	<ul style="list-style-type: none"> > Code > Lack of penetration testing > Weak User/Third Party Authentication
Cloud		<ul style="list-style-type: none"> > Public/private/hybrid cloud deployment 	<ul style="list-style-type: none"> > Code > Policy management
Communications		<ul style="list-style-type: none"> > 2G, 3G, LTE, 5G > DSL, Fibre, LPWAN > Wi-Fi, Bluetooth > MQTT, IP, ZigBee, Mesh RF, Wi-Fi etc 	<ul style="list-style-type: none"> > Insecure communications
Gateways / Smart Edge Devices		<ul style="list-style-type: none"> > Variable communications protocols > Time-sensitive data analysis 	<ul style="list-style-type: none"> > Policy management > Denial-of-service > No / insecure updates > Poor hardware design
IoT Sensors / Actuators		<ul style="list-style-type: none"> > Limited power > Low bandwidth > Constrained capabilities 	<ul style="list-style-type: none"> > Design faults > Software / firmware implementation faults > Inability to update
Data Types		<ul style="list-style-type: none"> > Sensitive data: video, audio, location, personal information > Technical data: environmental measurement, uptime reports 	<ul style="list-style-type: none"> > Users > Policy management > Data storage

Source: Juniper Research

WHAT MAKES IOT DEVICES MORE VULNERABLE?

IOT devices are:

- Pre packaged with barely any security
- PCs come with firewalls, and anti-virus and random hardware memory allocations that improve the security

The primary reason behind manufacturers not taking these precautions is for them to be able to push out products at a faster and cheaper to beat their competitors.



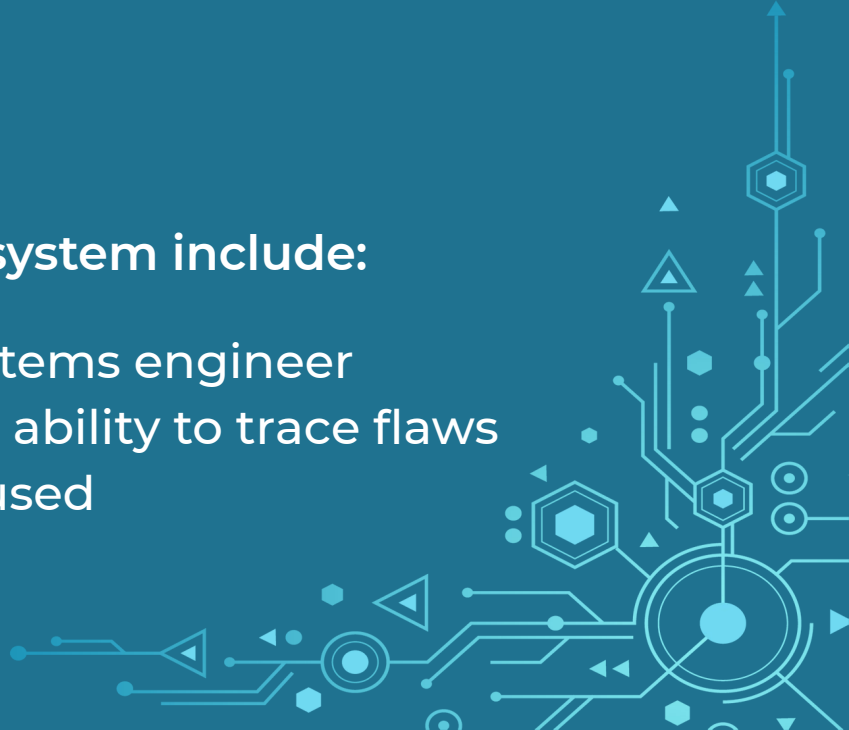
TYPES OF IOT ATTACKS

IOT attacks are primarily of two types:

- Software
- Hardware

The requirements to develop or hack a system include:

- The knowledge of an Embedded Systems engineer
- Understanding of cyber security and ability to trace flaws
- Understanding of the kernel that is used



TYPES OF IOT ATTACKS

IOT attacks are further divided as follows:

Software Attacks

- Bug Finder
- Web Server
- Shell injections

Hardware Attacks

- Non invasive
- Side channel
- Fully invasive



DIFFERENTIATION BETWEEN TYPES

Hardware attacks are less rare but are guaranteed attacks

Software attacks are rare but when started can flow for a long time and are hard to stop

However most of them are only theoretical, the real world attacks usually are:

- UART
- EMMCS
- Injections



UART ATTACKS

- They have 4 or 5 pins being Tx, Rx, VCC, GND
- They may or may not be populated
- Populated ones are easier for the hacker

Things to look for while hacking:

- Well formatted data coming out like a menu driven option
- U-boot being accessible to prevent bootloaders being changed
- Shell injections like `init=/bin/sh`
- Shorting NAND pins 29 and 30
- Bruteforcing and other shell injections



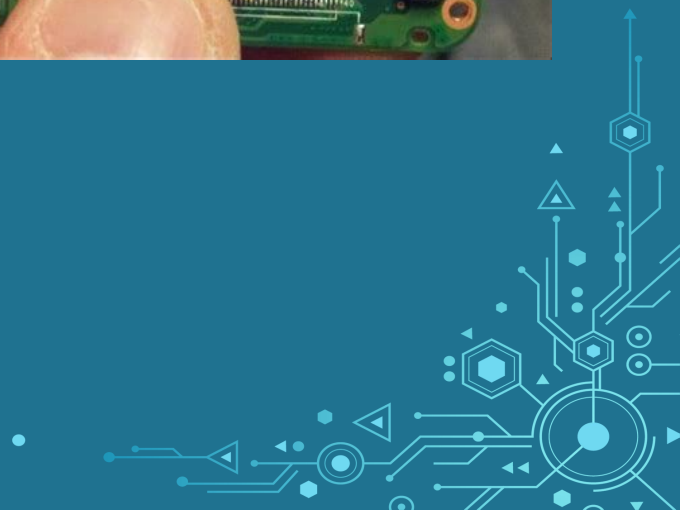
EMMC ATTACKS

- On board soldered chips that contain data
- Do not contain bit and parity checks
- Can be read with a EMMC reader
- Direct contact with storage



Things to look for while hacking:

- Modifying the storage files and the OS permissions
- Installing stuff like SuperSu
- Replacing the sys.fs file



SOFTWARE ATTACKS



- Man in the middle
- Poorly designed software
- Side channel hits

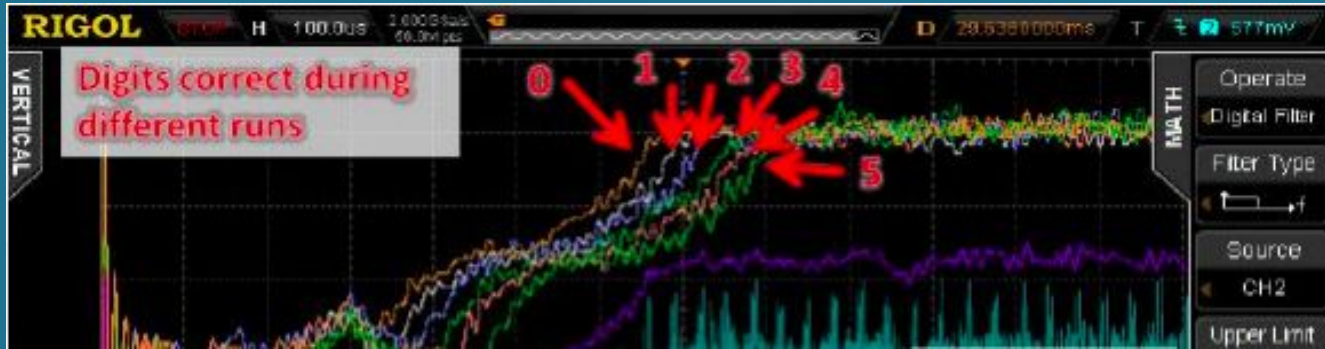
SHELL INJECTIONS

- Developers use code like `system("ls %s")` and then pass in 's' as a variable
- This enables the hackers to execute code in these by using the semicolon ';'
- An example would be `;reboot;` and now the linux system would execute a reboot

Things to look out for while hacking:

- Supported web pages on the IOT where you can SQL and Shell inject
- Old protocols like FTP and telnet
- Unpatched or un reduced kernel files
- Bruteforce on a dictionary

REAL-LIFE EXAMPLES OF BAD SOFTWARE DESIGN



- Saving data on EEPROM
- Encoding instead of Encrypting
- Not disabling telnet, ftp, other old protocols
- Not using hop frequency keys on bluetooth

REAL WORLD ISSUES

- **Mirai** - based on the fact that people didn't change the default credentials. DDOS on Twitter, Facebook, MakeMyTrip, and many more
- **PewDiePie vs T-Series** - printers and home security cameras were hacked
- **Ransomware** - ransomware attacks on cars is a future possibility
- **Cayla** - a baby monitoring doll that can be connected to by anyone, banned in several European countries



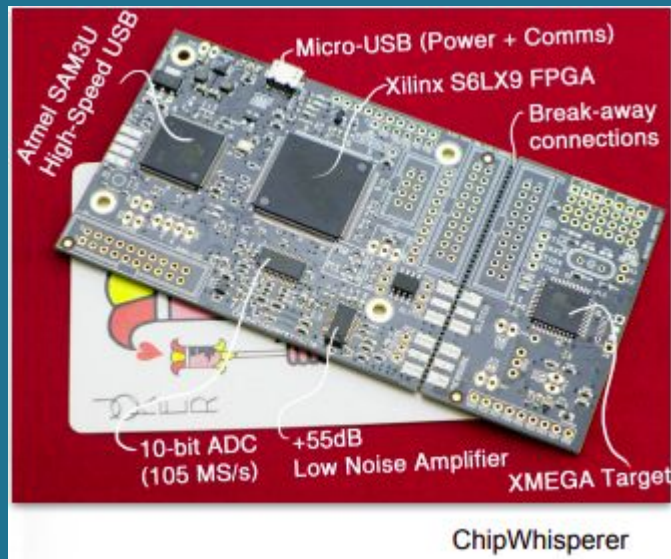
TOOLS THAT CAN BE USED

Hardware:

- JTAG
- USB
- SDR

Software:

- Binary Reversing
- Bug Finder
- Firmware Analysis



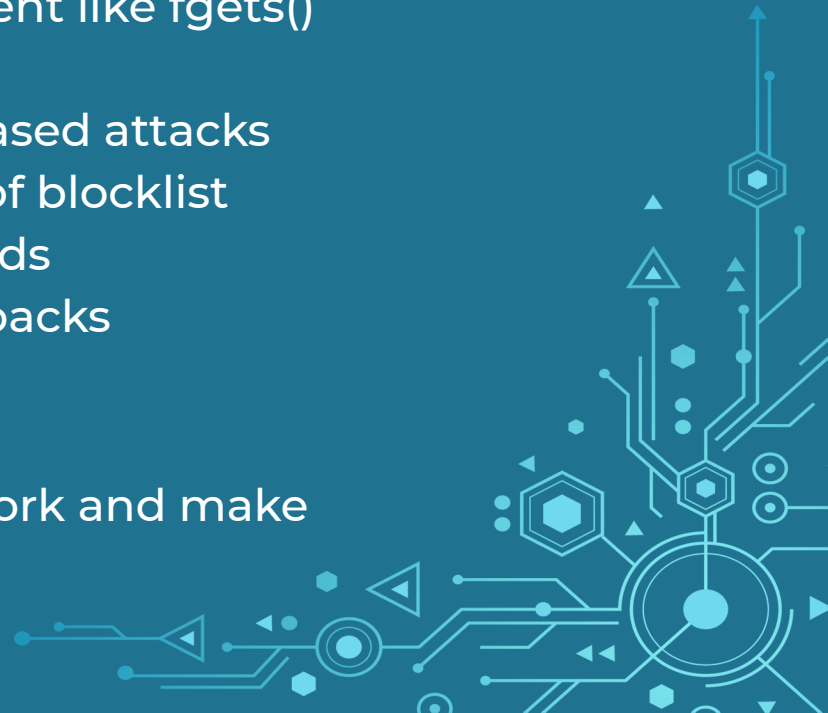
PSA SECURITY STANDARD

- Unique Identification
- Security Lifecycle
- Attestation
- Secure boot
- Security Update
- Anti-rollback
- Isolation
- Interaction
- Secure Storage
- Cryptography/trusted service



SOFTWARE IMPLEMENTATION

- Closing backdoors
- Encryption
- Use safer functions for buffer management like fgets() over gets()
- Run in constant time to prevent timer based attacks
- Add commands to the allowlist instead of blocklist
- Don't let user execute system() commands
- Don't hardcode secrets and prevent rollbacks
- Test SQL injections, XSS, Shell injections
- Remove/Disable unused features
- Connect IOT devices on a seperate network and make each device have a different password



SOURCES

- ARM
- TEDxTalks
- PSACertified
- gtvhackers
- Android authority
- Computerphile

