IoT [lackof] Security

Besides the coding/dev side of things.. also, lets get particular to some hardware-software combination so that the discussion remains practical.

So, we say

- hardware: Raspberry Pi 3 Model B+ (Broadcom BCM2835 based SoC with quad core ARM Cortex-A53); commonly used in several DIY IoT projects
- software: Raspbian OS (Debian-based), Linux kernel 4.x

Ref:

How to secure your Raspberry Pi
Find out what sensible steps you can take to protect your Raspberry Pi and other IoT devices. Ian Kluft.

Attack surface reduction

- Physical security (what if someone steals the microSD / device itself!)
  - USB ports, ethernet – disable?
- Risk matrix – categorize components 'risk' (critical, high, medium, low)
- change the default password! (to a secure one)
- use addition security at the OS- Linux LSMs like SELinux in enforcing mode
- use encryption (SSL/TLS, SSH, etc) – all via software packages
- keep the system updated
  - products Must have a secure & tested OTA or other update framework in place
- check security updates /status - CVEs / NIST / etc

Web: OWASP Top Ten Cheat Sheet

Securing a Raspberry Pi embedded in your IoT device, Ori Pomerantz, May 17, 2017, IBM Developer
Biased towards network traffic monitoring, firewall (iptables) setup.. code-based (Node.js).

IOT SECURITY: HARD PROBLEM, NO EASY ANSWERS Fahmida Y. Rashid

IoT Security Wiki : One Stop for IoT Security Resources
Huge number of resources (whitepapers, slides, videos, etc) on IoT security

Hacks-

- US-CERT Alert (TA16-288A) - Heightened DDoS Threat Posed by Mirai and Other Botnets
"On September 20, 2016, Brian Krebs' security blog (krebsonsecurity.com) was targeted by a massive DDoS attack, one of the largest on record, exceeding 620 gigabits per second (Gbps).[1] An IoT botnet powered by Mirai malware created the DDoS attack. The Mirai malware continuously scans the Internet for vulnerable IoT devices, which are then infected and used in botnet attacks. The Mirai bot uses a short list of 62 common default usernames and passwords to scan for vulnerable devices. Because many IoT devices are unsecured or weakly secured, this short dictionary allows the bot to access hundreds of thousands of devices.[2] The purported Mirai author claimed that over 380,000 IoT devices were enslaved by the Mirai malware in the attack on Krebs' website.[3]
In late September, a separate Mirai attack on French webhost OVH broke the record for largest recorded DDoS attack. That DDoS was at least 1.1 terabits per second (Tbps), and may have been as large as 1.5 Tbps.[4] ..."

- *Reg insecure / weak passwords, see this tweet*

https://github.com/lcashdol/IoT/blob/master/passwords/list-2019-01-29.txt

- *Hacking DefCon 23's IoT Village Samsung fridge, Aug 2015 (DefCon 23)*

- *HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities*
"... these devices are marketed and treated as if they are single purpose devices, rather than the general purpose computers they actually are. ...
...
IoT devices are actually general purpose, networked computers in disguise, running reasonably complex network-capable software. In the field of software engineering, it is generally believed that such complex software is going to ship with exploitable bugs and implementation-based exposures. Add in external components and dependencies, such as cloud-based controllers and programming interfaces, the surrounding network, and other externalities, and it is clear that vulnerabilities and exposures are all but guaranteed."

<< See pg 6, 'Ch 5: COMMON VULNERABILITIES AND EXPOSURES FOR IoT DEVICES' ; old and new vulnerabilities mentioned;

Pg 9: 'Disclosures' - the vulns uncovered in actual products >>

Just too much. Bottom line: critical to perform adequate pentesting – either outsource or DIY

Miscellaneous

"Unsafe at any clock speed: Linux kernel security needs a rethink"
Ars reports from the Linux Security Summit—and finds much work that needs to be done.
J.M. PORUP - Sept 2016.

IoT App Development Protocols

• Advanced Message Queuing Protocol

• OASIS Message Queuing Telemetry Transport

- Very Simple Control Protocol
- Constrained Application Protocol
- Extensible Messaging and Presence Protocol

Misc

MQTT Protocol – How it Works *(Message Queuing Telemetry Transport)*

Why is My Perfectly Good Shellcode Not Working?: Cache Coherency on MIPS and ARM
short ans: cache coherency issues.
