Security

Agenda

Overview

Why security?

An example

Applied cryptography overview

Some useful tools

Oscilloscope, Signal analyzer ….

Exercises

Overview

Why security?

Authentication

Who is it (credentials)?

Confidentiality

Intended recipients only

Integrity

Data was not manipulated in transit

Authorization

Intended actors only

Anonymity, non-repudiation …

Authorizing actions without revealing subject identity …

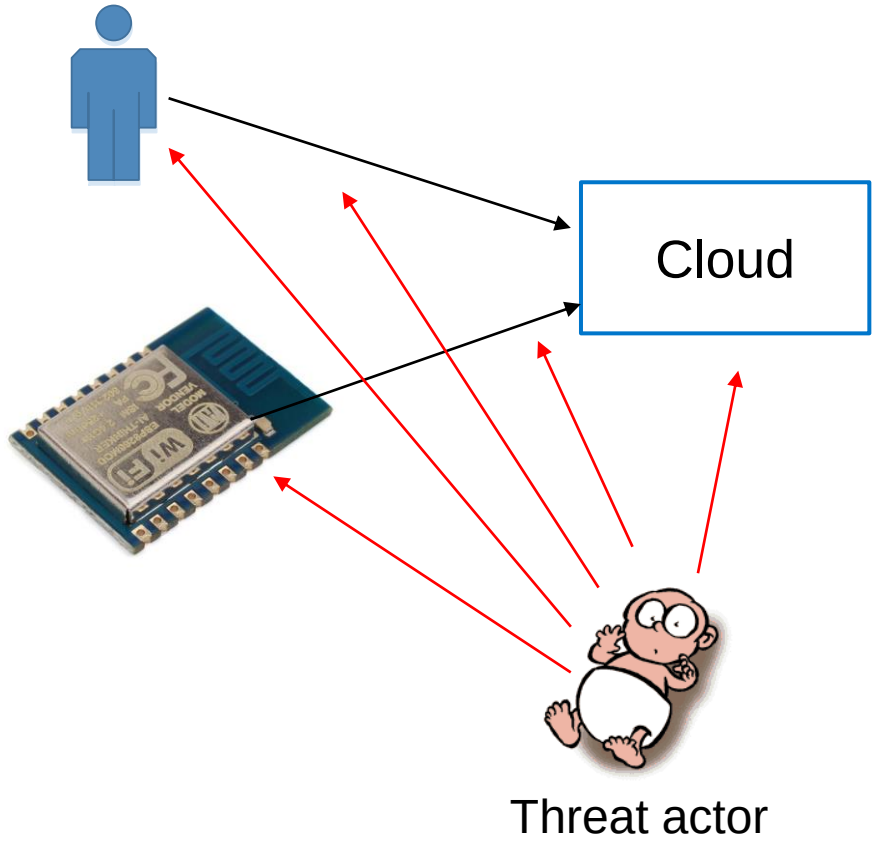


Image: http://www.netanimations.net/animated-baby-looks-then-cries.gif

Security is a complex topic

Availability, access control, ACL, audit, DoS, DDoS, Backdoor, BASIC, Block Cipher, Stream Cipher, Botnet, Brute force, Buffer overflow, Cleartext / Ciphertext, Compression bomb, Disaster recovery (MTTR, RPO), DES, AES, RSA, Diffie-Hellman, Dictionary attack, PKI, x509, Eavesdropping, Escrow passwords, Fingerprinting, Hash, Hijacking (click, session, domain …), Honeypot, Inference attack, Intrusion detection, Flooding, Least privilege, LDAP, Logic bomb, MITM,NAT, NIST (NVD), Network taps, Non-repudiation, Penetration testing, Phishing, Ping of death, Privilege escalation, Promiscuous Mode, Resource exhaustion, Reverse engineering, RBAC/RSBAC, SSH, SSL, SHA, SIGINT, HUMINT, TECHINT, OSINT, Signature, Smurf attack, Sniffing (passive wiretapping), Social engineering, Stealthing, SYN Flood, Tamper, Trojan horse, Trust, Threat vector, Web of trust, Zero Day, Zombie, WPA2-PSK, PBKDF2, SCRAM ….

Example: St. Jude Medical cardiac devices

April 2016

St. Jude Medical to be acquired by Abbot for $25B

August 2016

Muddy Waters Capital & MedSec announces vulns

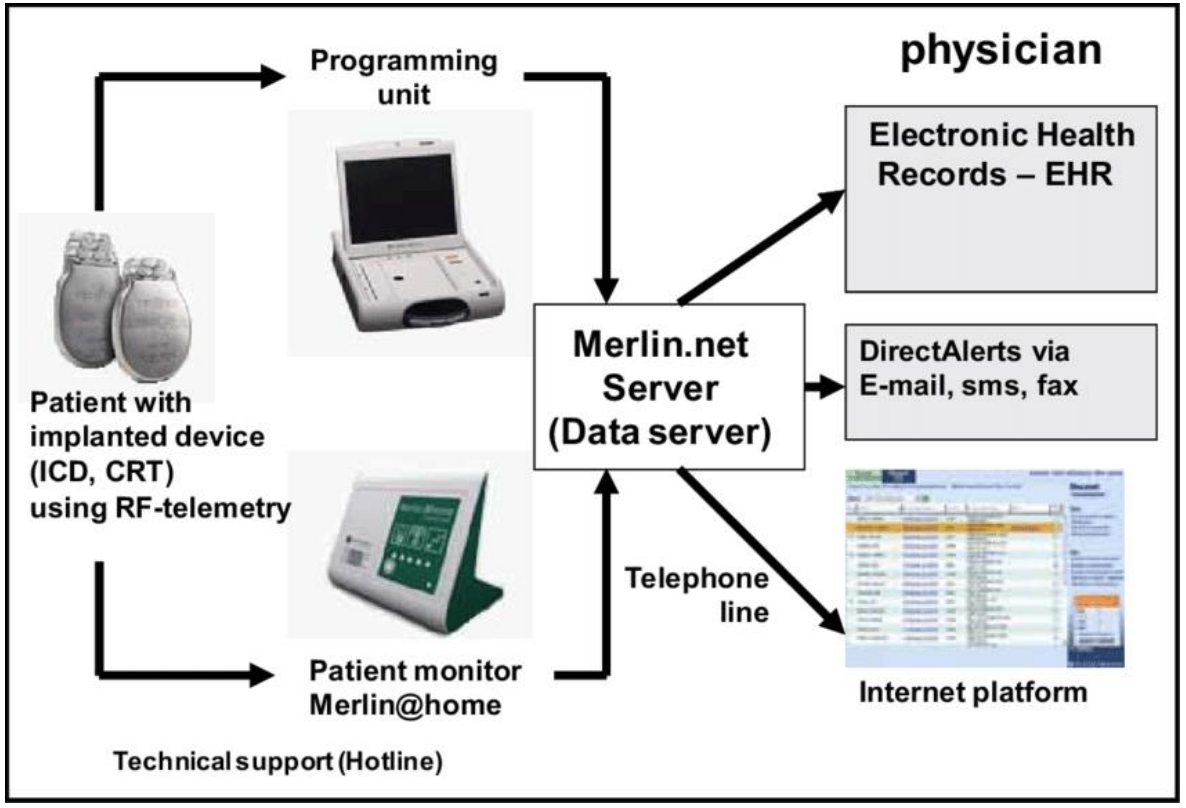
- Remote, RF control that can send shock to patient
- Quickly drain battery

Incentive: shorting stocks

St. Jude denies and sues for defamation

January 2017

FDA and dept. of Homeland Security confirm



Source: http://www.profitsoverpatients.com/

https://blog.erratasec.com/2016/08/notes-on-that-stjudemuddywattersmedsec.html

https://www.researchgate.net/figure/Complex-remote-monitoring-with-St-Jude-Medical-Merlinnet-Integration-of-telemedical_fig4_221910869

Cryptography

Applied crypto: Hash & Encryption

Hash

Data -> fingerprint

Examples: MD5, SHA, SHA3

Symmetric encryption (see AEAD)

Data + key <-> Cyphertext

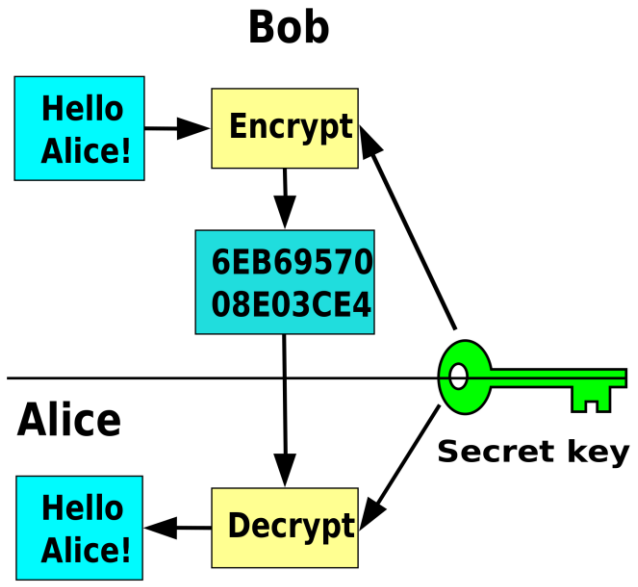
Examples: AES, 3DES, Blowfish

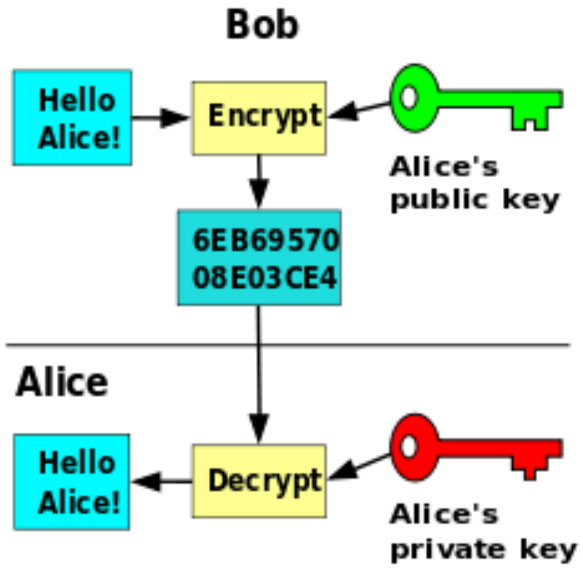
Asymmetric (public key) encryption

Data + public key -> Cyphertext

Cyphertext + private key -> Data

Examples: RSA, Diffie-Hellman, DSA





Applied crypto: X509 certificates & PKI

Signing process

Data (hash of data) + Private key -> Signature

Signature + Public key -> Data(hash of data)

X509

A format for public key certificate

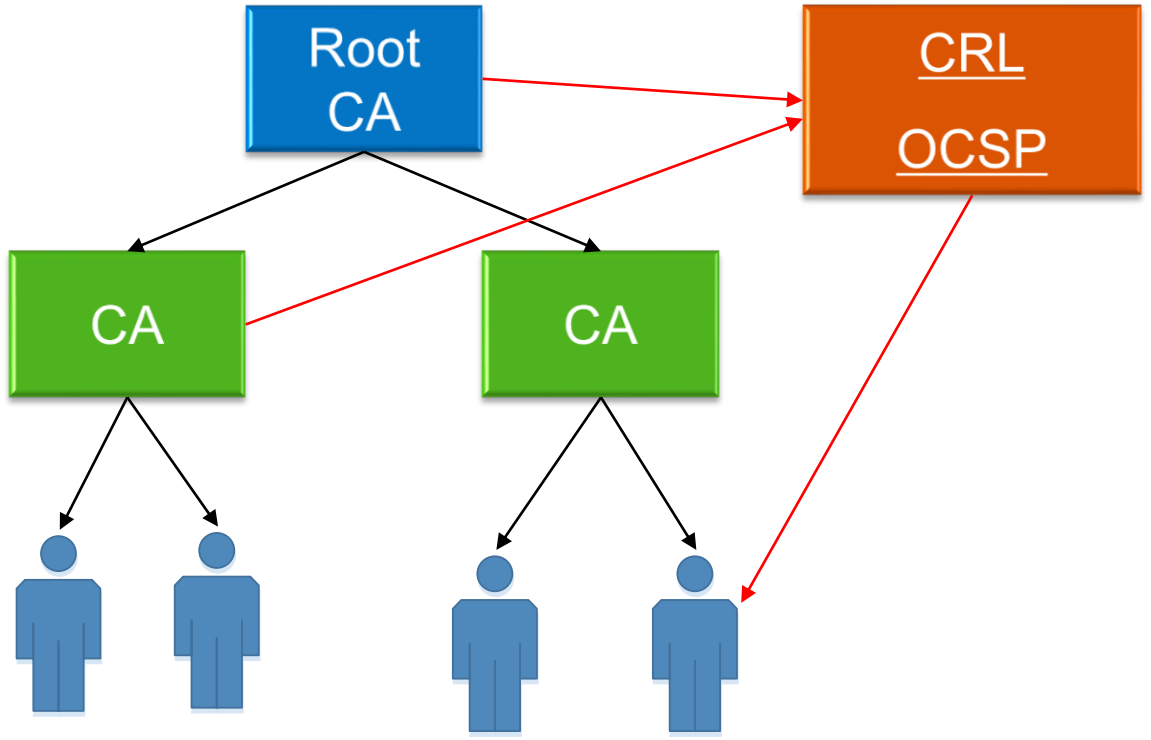
Contains public key and identity

Signed (either by CA or self signed)

Revocation lists

PKI

Certificate authorities, Web of trust, Blockchain based …



How does this apply to IoT?

Encryption

HTTPS & MQTTS

- SSL/TLS is used to encrypt the communication

Popular libraries: NaCl, libsodium, libhydrogen, liblithium, monocypher

Authentication & Authorization

Passwd files & ACLs

OAuth 2.0 / OIDC

- Client credentials flow

ESP32 security features

ESP32 security features

Remote communication

Use TLS (mbedTLS)

Specify CA certificate (or host is trusted implicitly!!!)

Secure boot **(esp-idf)**

Signed firmware & secure bootloader

Keys in eFUSE and SW bootloader

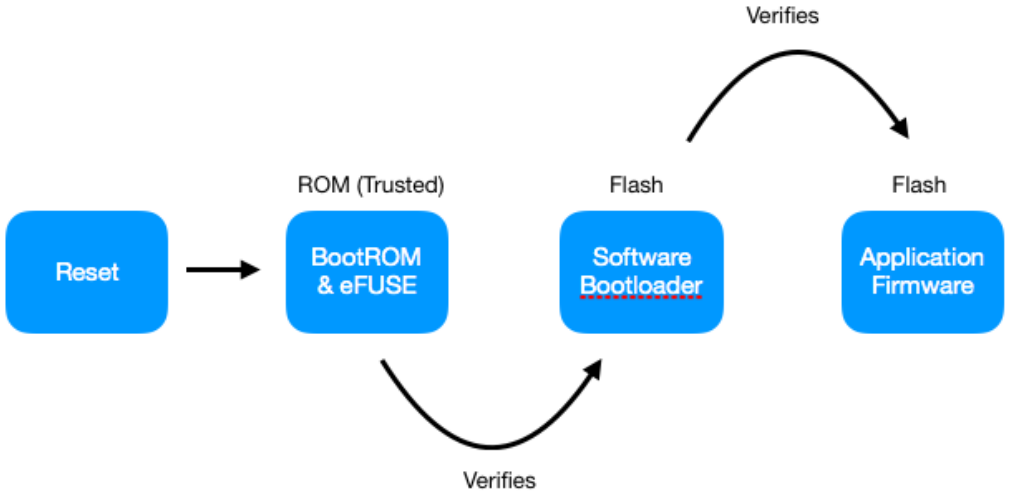
Encrypted Flash **(esp-idf)**

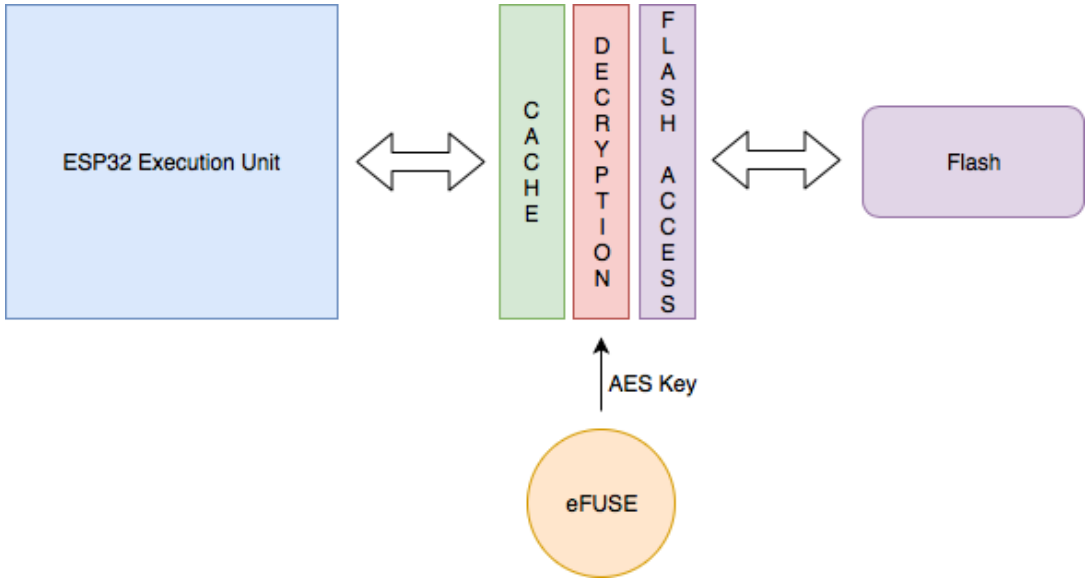
AES key in eFUSE

Encrypted NVS **(esp-idf)**

Keep crypto keys in encrypted flash

XTS-AES based (disc encryption)





https://docs.espressif.com/projects/esp-jumpstart/en/latest/security.html

https://blog.espressif.com/understanding-esp32s-security-features-14483e465724

Some ESP32 security flaws

Known exploits (CVE-2021-28139, CVE-2021-28136, CVE-2021-28135, CVE-2021-34173, CVE-2023-35818, CVE-2023-6249)

Remote code execution, memory corruption, DoS

Forever-Hack (CVE-2019-17391)

Inject power supply glitch -> read read-protected eFuses (flash encryption, secure boot)

Zero PMK (CVE-2019-12587)

Device hijacking when connected through EAP (user & pass - Raidus)

Client crash (CVE-2019-12586)

Crash a device connected through EAP

Beacon Frame Crash (CVE-2019-12588)

DoS in radio range by crafted message

https://www.espressif.com/en/news/ESP32_FIA_Analysis
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=esp32
https://www.infoq.com/news/2019/12/esp32-fatal-fury/

Some useful tools

To verify your own security

Security tools (hardware)

Logic analyzer

Acquire digital signals from wires

Decode common protocols (SPI, I2C, 1-wire …)

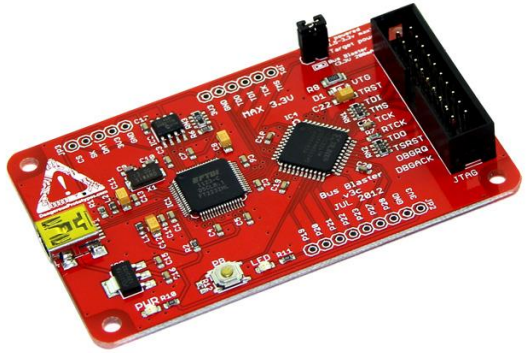
SDR

Acquire, analyze/synthesize radio signals

JTAG (e.g. Bus Blaster)

Debug on-board processors and chips

Reprogram



Oscilloscope

Visually inspect signals

Record and capture waveforms

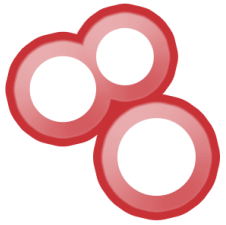
Security tools (software)

Network scanners

Analyze the network (Live hosts, open ports …)

Fingerprint (OS, software, version …)

Examples: nmap, masscan, Shodan.io …



SHODAN

Metasploit

Penetration testing

Database of existing exploits

WiFi & routers security

Analyze and attack WiFi: Kismet, Aircrack-NG

Routersploit: known router exploits

Exercises