Security

April, 2019

Agenda

Overview

Why security?

Funny 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 …

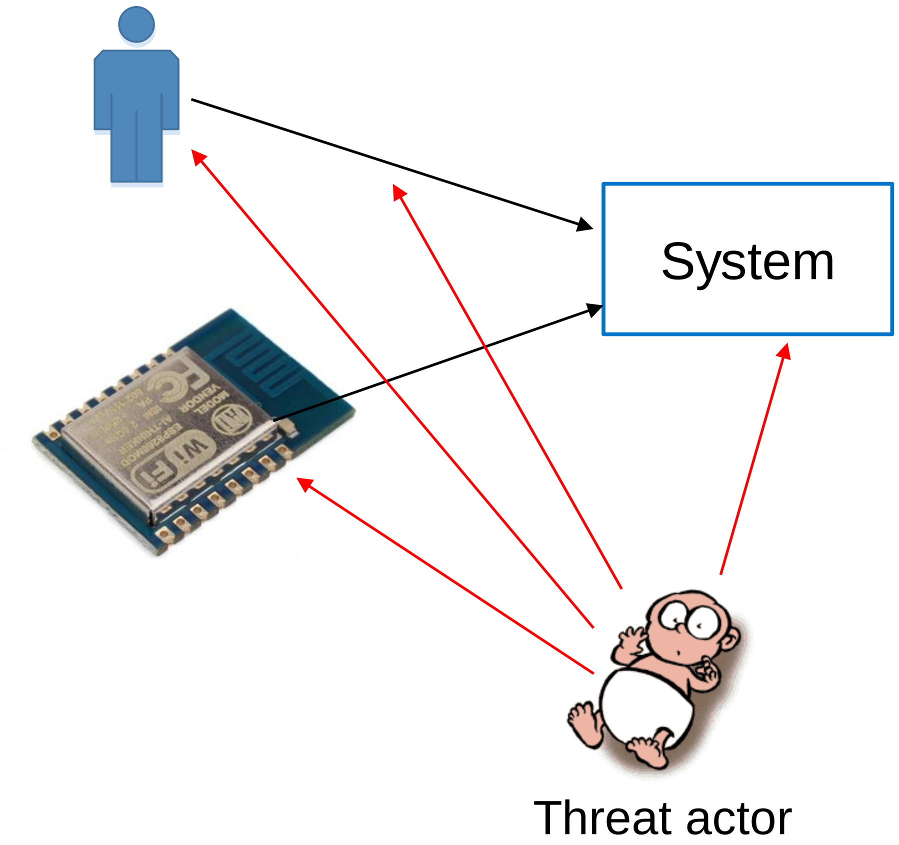


Image: http://www.netanimations.net/animated-baby-looks-then-cries.gif

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 ….

Funny example: K-129 submarine case study

K-129

Was a soviet ballistic missile submarine -> sunk on 8th of March 1968

Russia could not find the wrecks (wanted back its nuclear missiles & code books)

US found it on 20 August 1968. -> one of the most expensive Cold War secrets

SOSUS (Sound surveillance system)

Listens for submarine sounds at multiple locations

Estimates their location by triangulation

It was used to locate the wreck time & site (e.g. looking for explosion signatures)

Funny contemporary analogue

Mobile phones and WiFi probing

Source: https://en.wikipedia.org/wiki/Soviet_submarine_K-129_(1960)

Cryptography

Applied crypto: Hash & Encryption

Hash

Data -> fingerprint

Examples: MD5, SHA, SHA3

Symmetric encryption

Data + key -> Cyphertext

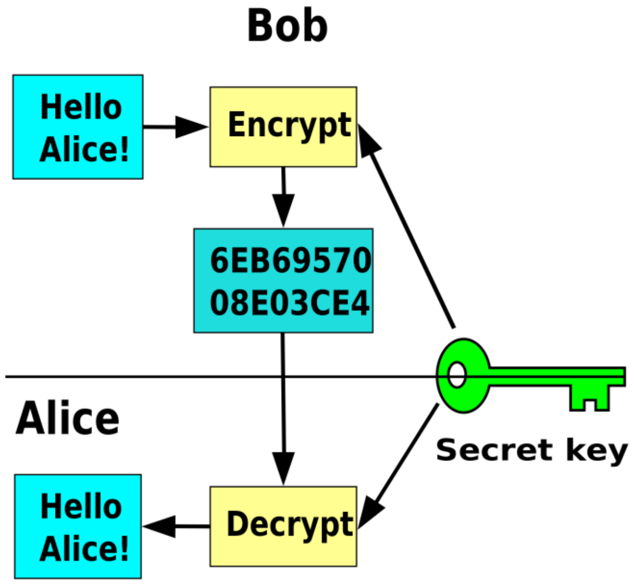
Examples: AES, 3DES, Blowfish

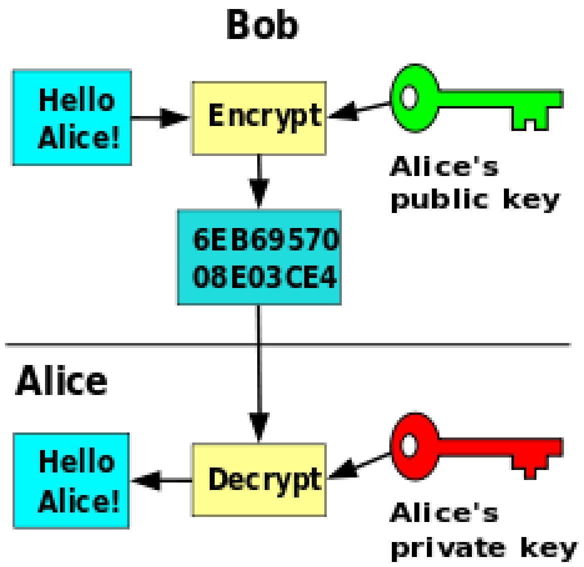
Asymmetric (public key) encryption

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

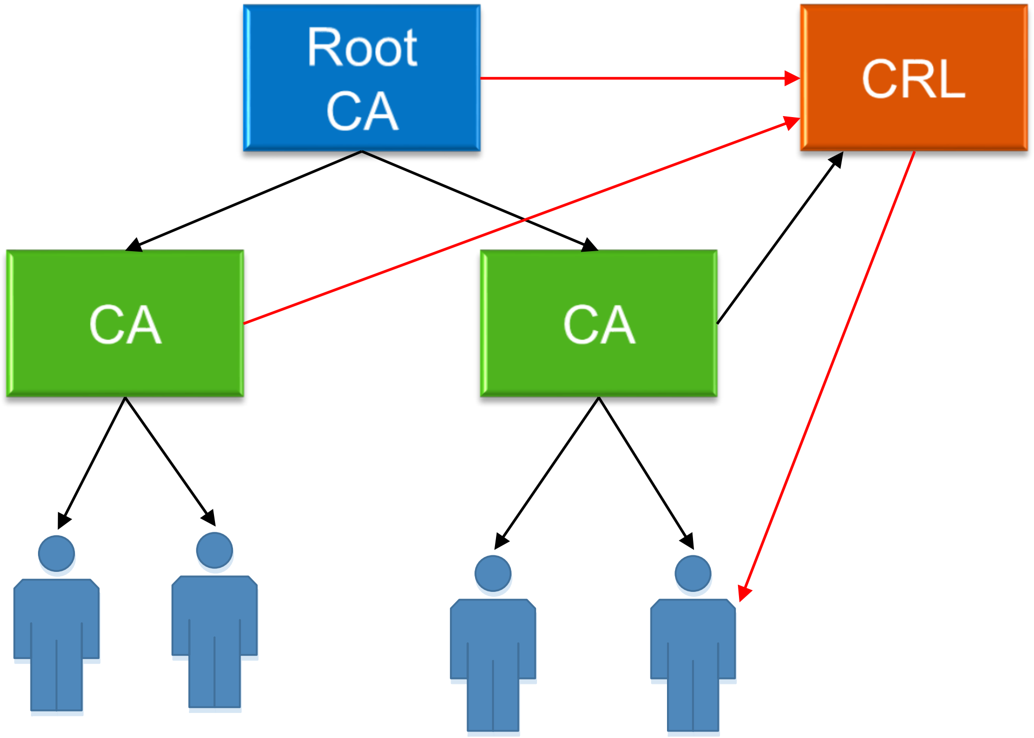
Contains public key and identity

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

Authentication & Authorization

Passwd files & ACLs

OAuth 2.0

ESP32 security features

ESP32 security features

Remote communication

Use TLS (mbedtls)

Specify CA certificate (or host is trused implicitly)

Secure boot

Signed firmware & bootloader

eFUSE for key storage

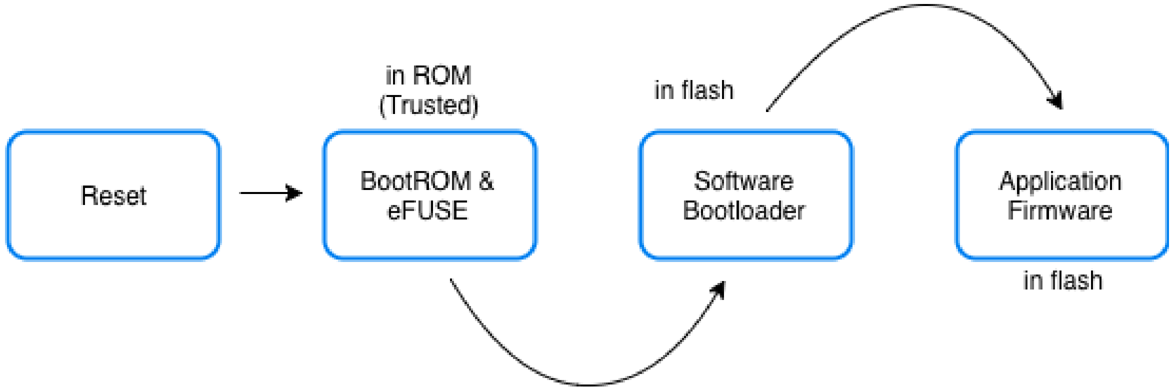
Encrypted Flash

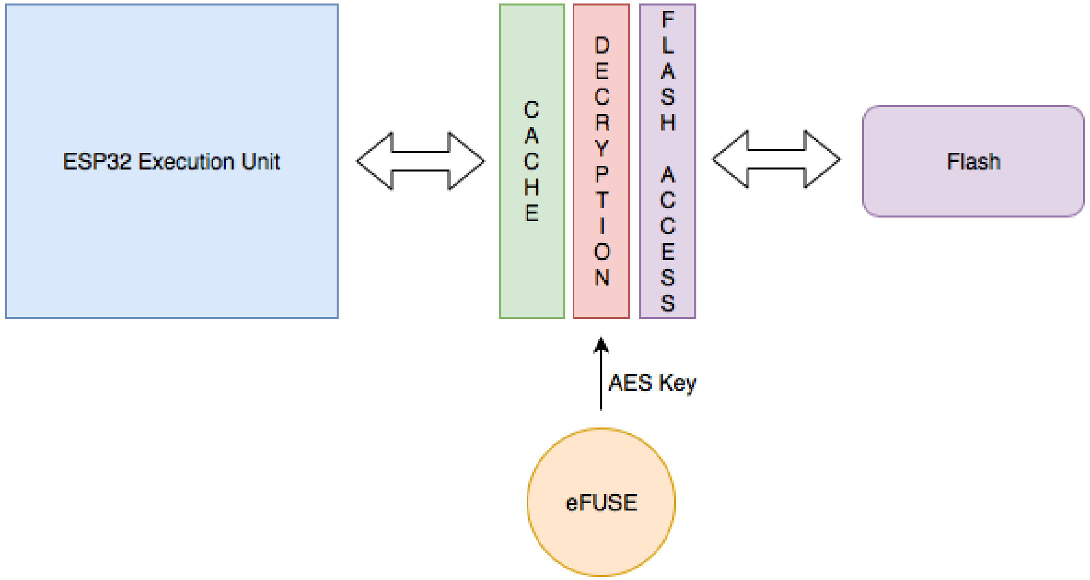
AES key in eFUSE

Encrypted NVS (non-volatile storage)

Keep crypto keys in encrypted flash

XTS-AES based (disc encryption)





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

ESP32 security flaws

Forever-Hack (CVE-2019-17391)

Use TLS (mbedtls)

Specify CA certificate (or host is trused implicitly)

Zero PMK (CVE-2019-12587)

Device hijacking when connected through EAP (user & pass)

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://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)

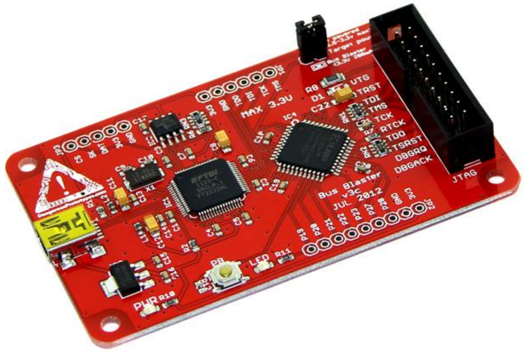
Debug on-board processors and chips

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 …

Metasploit

Penetration testing

Database of existing exploits

WiFi & routers security

Analyze and attack WiFi: Kismet, Aircrack-NG

Routersploit: known router exploits

Exercises