Security

April, 2018

Agenda

Security refresher

Why security?

Vocabulary building & discussion

Some tools of the trade

Oscilloscope, Signal analyzer ….

Exercises

Security refresher

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 …

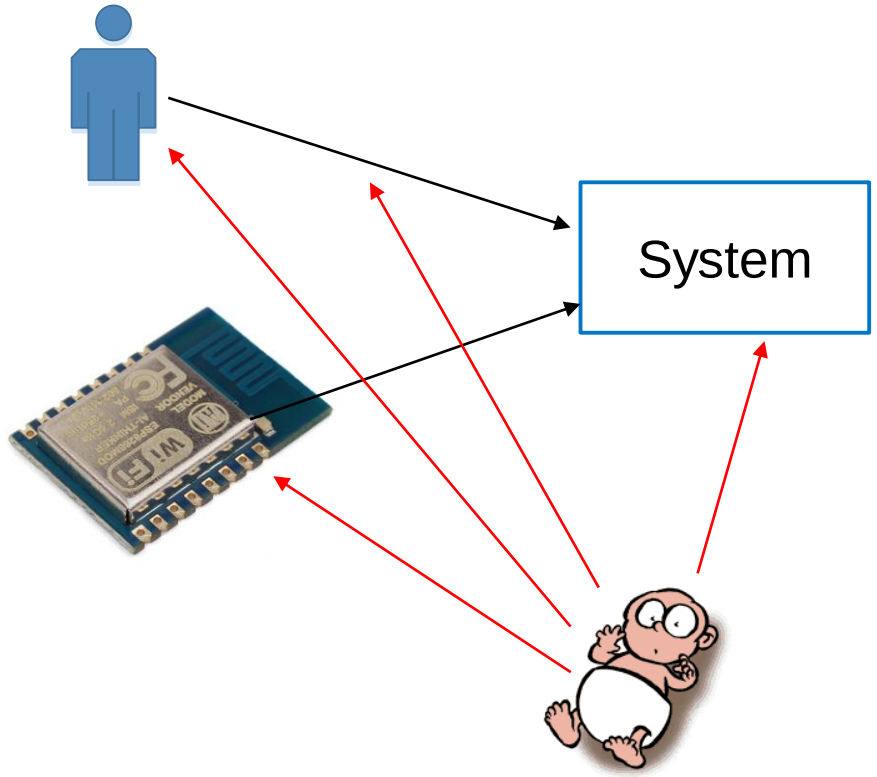


Image: http://www.netanimations.net/animated-baby-looks-then-cries.gif

Vocabulary building

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 (COMINT, ELINT), HUMINT, IMINT, MASINT (signature), TECHINT (tech capabilities K-129/ SOSUS), 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, CRAM ….

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)

Contemporary analogue

Mobile phones and WiFi probing

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

Glossary: Crypto

Hash

Data -> fingerprint

Examples: MD5, SHA, SHA3

Symmetric encryption

Data + key -> Cyphertext

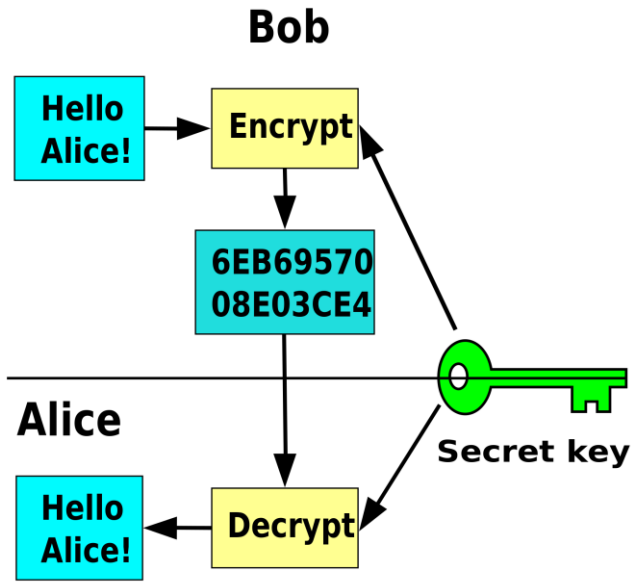
Examples: AES, 3DES, Blowfish

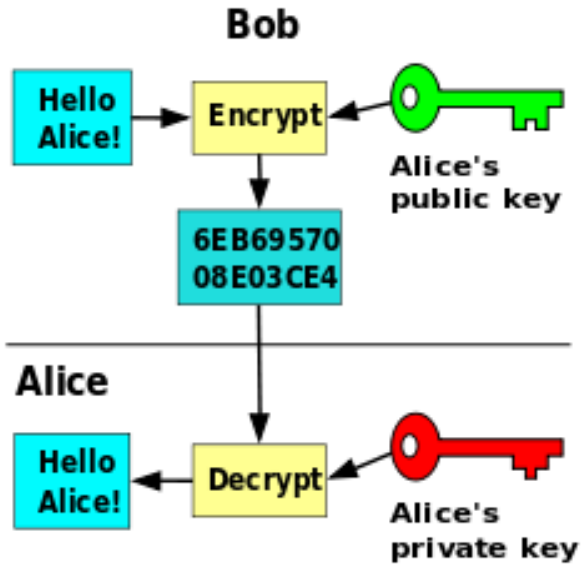
Asymmetric (public key) encryption

Data + public key -> Cyphertext

Cyphertext + private key -> Data

Examples: RSA, Diffie-Hellman, DSA





Glossary: 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

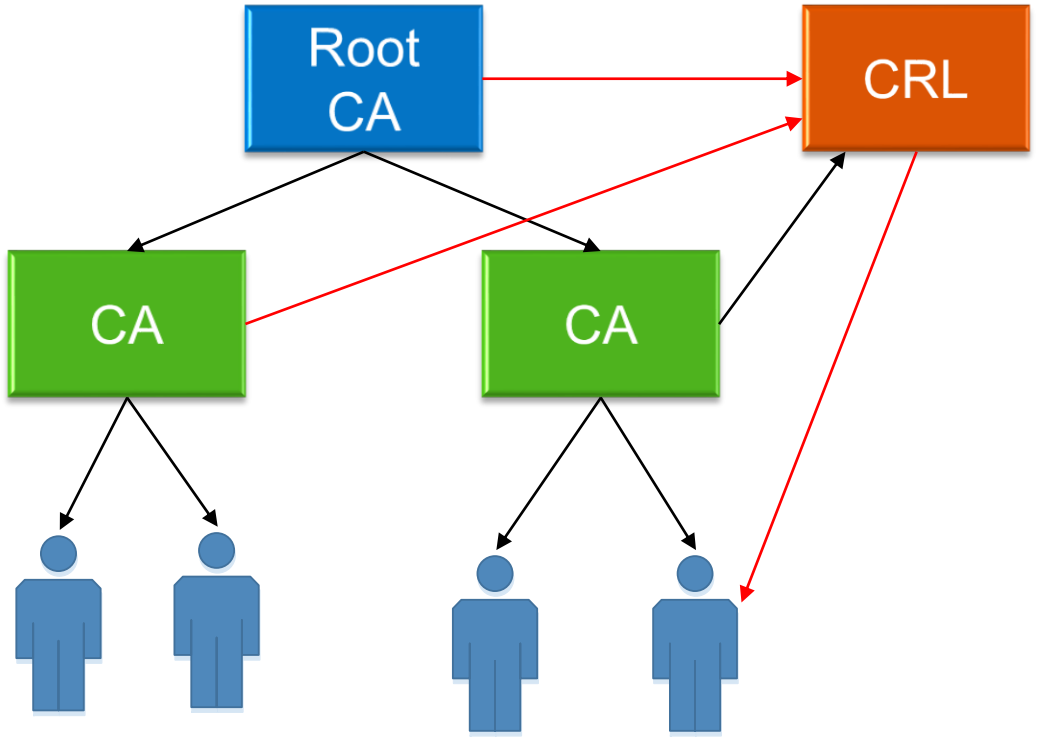
Contains public key and identity

Signed (either by CA or self signed)

Revocation lists

PKI

Certificate authorities, Web of trust, Blockchain based …



Some tools of the trade

Some tools of the trade (hardware)

Logic analyzer

Acquire data

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

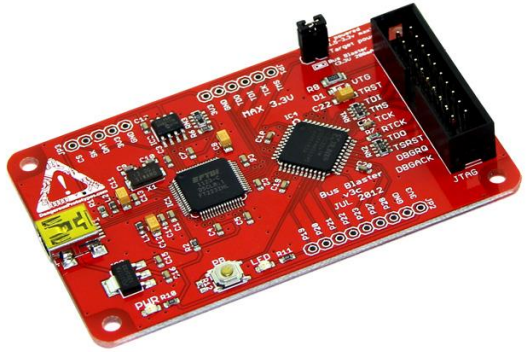
SDR

Acquire, analyze and synthesize radio signals

JTAG (e.g. Bul Blaster)

Debug on-board processors and chips

Reprogram



Oscilloscope

Visually inspect signals

Record and capture waveforms

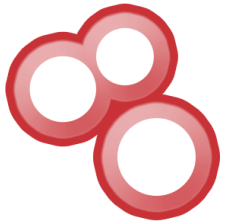
Some tools of the trade (software)

Network scanners

Analyze the network (Live hosts, open ports …)

Fingerprint (OS, software, version …)

Examples: nmap, masscan, Shodan.io …



SHODAN

Metasploit

Penetration testing

Database of exploits

WiFi & routers security

Analyze and attack WiFi: Kismet, Aircrack-NG

Routersploit: known router exploits

Exercises