Tiedonsiirto

Emil

Osiot

Teknologioita

Protokollista

Salaus, luotettavuus ja varmistettavuus

Langaton tiedonsiirto

Langaton == johdoton

Ääni, valo, värähtely, magneetit, jne

Radio

Yksisuuntaisuus, kaksisuuntaisuus, luotettavuus, tarvittava infra, virrankäyttö, kantama, …

Luotettava tiedonsiirto = siirto + integriteetti ja varmistettavuus, salaus

Pakettipohjaisuus fokuksessa

Omat radiot ja “teknologiat”

Ei voi hyödyntää olemassaolevia teknologioita ja integrointia

Kompleksisuusvastuu itsellä

Saa juuri sen mitä tekee eikä enempää

Tiukkoja

Tehokkaita? Ehkä?

Latenssi

Kannattaa pitäytyä olemassaolevassa raudassa siltikin

Bluetooth

Luotettava

Vähävirtainen

Yksisuuntainen ja kaksisuuntainen

Lähellä, vähän pidemmälle, 0-25m, 0-100m

Joustavahko, voi yhdistää esim suoraan puhelimeen, tietokoneeseen, selaimeen

Paikallinen infra

Wlan/Wifi

Luotettava

Käyttää paljon enemmän virtaa

Lähinnä kaksisuuntainen, kikkailemalla yksisuuntainen

Lähellä, 0-10m, 0-50m

Hyvä tiedonsiirtokyky

Paikallinen infra, voi yhdistää suoraan puhelimeen, tietokoneeseen

Zigbee

Teollisuus

LoRa

“Long Range”, 0-100, 0-3km

Jonkun muun infra

Pieni tiedonsiirtokyky

Mobiiliverkot

GSM, 3G/4G, 5G, LTE-M, NB-IOT

Pitkän matkan, 2+km, 5km, 10km

Paljon enemmän energiaa

Joustavia

Jonkun muun infra

Hyvä tiedonsiirtokyky

Tutut ja helposti ymmärrettävät käyttöliittymät (SMS)

Protokollat

Speksit, rajoitteet, data, taso

OSI

Joustavuus, laajennettavuus

Tehokkuus

Serialisointi ja parsiminen

Muotoilu, kehystys, strukturoitu data

Synkronisointi

Kompressointi

Olemassaoleva infra, tuki, jne


Verkkoon lähettäminen
Verkosta vastaanottaminen
Ylemmät kerrokset
Alemmat kerrokset
7. Sovelluskerros
6. Esitystapakerros
5. Istuntokerros
4. Kuljetuskerros
3. Verkkokerros
2. Siirtokerros
1. Fyysinen kerros
HTTP, FTP, SMTP
TCP, UDP, SPX
IP, ICMP, IPX
reititin
ATM, Ethernet
silta, kytkin
Ethernet, Token ring
hub, toistin

(JSON)
HTTP + WEBSOCKETS
TCP
IP
WLAN/WiFi

Oma
Bluetooth

Verkko

IP-pohjainen

UDP

TCP/IP

Näiden päälle yleensä muita

Verkossa myös useita muita pakollisia sivuprotokollia, kuten DNS

UDP

Latenssi

Ei “luotettava”

Vähäresurssinen

Kompleksisuusvastuu itsellä kun lisäkehittää

Striimaus, vain nykyinen data merkitsee

TCP/IP

Standardi

Kaikkialla

Kaikki tukee

“Luotettava”

Voi mennä jumiin

“Epätehokas”, voi joutua bufferoimaan paljon dataa

Systeemi tarjoaa ja tekee

HTTP

Standardi

Kaikkialla

Parsiminen itse tuskaa

WebSockets

Webbiteknologia

Yksinkertainen kehystys

Yksinkertaistaa protokollastäkkiä, jos kaikki laitteet puhuvat samaa

JSON

Jos mikrokontrollerilla, älkää pls siirtäkö JSON vaan jollain muulla

Jos tietokoneella, ihan OK, standardimeno

MQTT

IOT-protokolla

Tehokas

PUBSUB

Infra

Salaus, luotettavuus ja varmistettavuus, sekä saatavuus

Hyökkäykset, kuten raaka voima, uudelleenlähetys

Tallennettava “tilaa”, oltava jaettu tila tai salaisuus

CIA-kolmikanta

Tehokkuus

The CIA Triad

What Is the CIA?		
Confidentiality	**Integrity**	**Availability**
The information is safe from accidental or intentional disclosure.	The information is safe from accidental or intentional modification or alteration.	The information is available to authorized users when needed.
Example		
I send you a message, and no one else knows what that message is.	I send you a message, and you receive exactly what I sent you (without any modification)	I send you a message, and you are able to receive it.
What's The Purpose of the CIA?		
Data is not disclosed	Data is not tampered	Data is available
How Can You Achieve the CIA?		
e.g., Encryption	e.g., Hashing, Digital signatures	e.g., Backups, redundant systems
Opposite of CIA		
Disclosure	Alteration	Destruction

Miten salaus

Symmetrinen

Data, joka halutaan lähettää, D

Salataan se avaimella K, E(D, K)=C

Otetaan jaetusta ja avoimesta tilasta ja C:stä MAC, M(S+C)=A, “tägi”

Viesti=S+C+A

Asymmetrisessä sovitaan/johdetaan avain K yhdessä, koska tehokkuus

Jaettu ja julkinen tila

Satunnaisdata

Laskuri

Ajastin

Avain

Viestin pituus

SCA

S:n uniikkius ja A:n pituus oleellisia

S:n pituus riippuu viestien määrästä

A:n pituus riippuu viestien määrästä, siirrosta ja S:n pituudesta jne.

A mieluusti 256 bittiä = 32 tavua

S mahdollisimman suuri, esim 8 tavua satunnaisdataa, 8 tavua ajastin, 8 tavua laskuri

Esimerkki Bluetooth

Bluetooth 4 LE beaconiin/mainokseen voi paketoida 29 tavua kikkailemalla (27 helposti, 33/35 ninjailemalla)

Joka sekunti yksi viesti 20v ajan => 60*60*24*365*20=630720000, ~15% 2^32:sta

Ajastin suojaamaan uudelleenhyökkäykseltä, 4 tavua

Laitteet erotettava toisistaan jollain tavalla, ID-kenttä, 4 tavua (vai käytetäänkö laite-maccia)

MAC 16 tavua

4+4+4+x+16 => x=1

Sisäisesti myös kehystys?

Oikeasti pienemmät turvatasot riittävät, lähinnä halutaan estää datan valehtelu

Voidaan tinkiä monesta eri asiasta, esim mac -> 12 tavua -> x=5 => 1 tavu kehystykseen, 4 dataan?

Maksetaankin MACista -> 4+4+x+16 => 1 kehystykseen, 8 dataan? Kehystys=>12, 12 dataan?

Miten salaus

Käyttäkää valmiita kirjastoja

Käyttäkää valmiita apeja, rautakiihdytystä

Käyttäkää moderneja standardeja

Esim openssl

Palvelimet

Meillä on teille palvelimet

Käyttäkää niitä eikä muita palvelimia

Pyytäkään kun tarvitsette