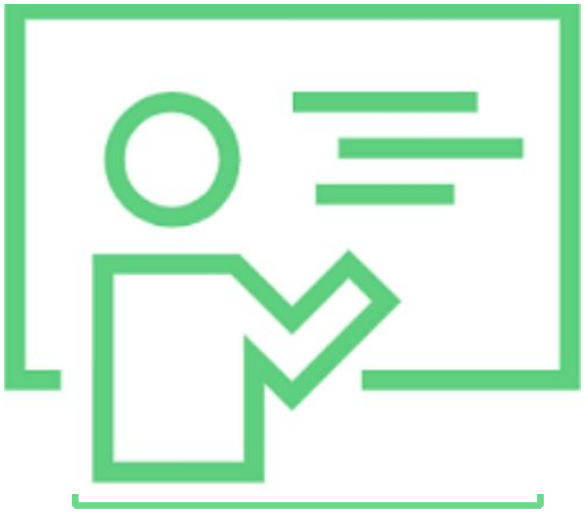

Säker nätverkskommunikation

Joakim Englund, Systementor AB

Repetition från dag 6

- Segmentering begränsar nätverksvägar
- Brandväggen avgör vilka anslutningar som tillåts
- Tjänsten behöver fortfarande kontrollera motparten

Dagens mål

- Förklara kryptering och identitetskontroll
- Verifiera en MQTT-broker med certifikat
- Testa godkänd och nekad åtkomst
- Hantera certifikat och hemligheter med rätt skydd

Tillgång, hot och kontroll

Tillgång	***Hot***	***Kontroll***
Telemetri	Avlyssning	TLS
Brokeridentitet	Falsk broker/MITM	Certifikatkontroll
Topic	Obehörig publicering	Klientbehörighet

Konfidentialitet, integritet och tillgänglighet

- Konfidentialitet (C): Rätt mottagare kan läsa
- Integritet (I): Förändringar upptäcks eller stoppas
- Tillgänglighet (A): Tjänsten fungerar och kan återhämta sig

MQTTS

1. TCP-anslutning
2. TLS-handshake och certifikatkontroll
3. Skyddad MQTT-session
4. Publish och subscribe

För djupare förklaring av TLS-handshakeprocessen, kolla länken:
https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/

Certifikatkedjan

- Brokern visar sitt servercertifikat
- Klienten kontrollerar namn och giltighetstid
- Klienten följer kedjan till en betrodd CA (Certificate Authority)

Autentisering och auktorisation

Autentisering: Vilken identitet eller uppgift visas?

Auktorisation: Vilka operationer (t.ex. topics) tillåts?

Minsta behörighet

Roll	***Tillåten operation***
Sensor	Publicera eget telemetritopic
Konsument	Prenumerera på avsedda topics
Drift	Läsa status och hantera konfiguration

Vad lagras på ESP32/sensorenhet?

- CA-certifikat: Offentligt tillitsankare
- Klientcertifikat: Offentlig enhetsidentitet
- Privat klientnyckel: Hemlighet
- Brokerens privata nyckel? *Nej*. Den ska förstås stanna på brokern.

Skydd av privata nycklar

- Unik nyckel per enhet
- Skyddad provisionering
- Krypterad lagring där hotbilden kräver det
- Plan för återkallelse och rotation

Certifikatets livscykel

1. Provisionera tillit
2. Verifiera anslutning
3. Överlappa gammal och ny CA vid byte
4. Kontrollera MQTTS och OTA
5. Ta bort gammalt förtroende

Att tänka på vid loggning

Logga saker som:

- Tid och klientidentitet
- Operation och topic
- Godkänt eller nekat utfall

Logga aldrig privata nycklar, tokens eller lösenord.

Dagens MQTTS-demo

- Fel CA stoppar anslutningen före MQTT
- Rätt CA verifierar brokern
- Publisher skickar JSON
- Subscriber tar emot samma payload

Eftermiddagens laboration

- Kör och tolka MQTTS-testet
- Inspektera servercertifikatet
- Koppla kontrollen till ett hot
- Dokumentera MCU-lagring och begränsningar

IoT-caset inför dag 8

- Välj en kommunikationsväg
- Skydda transport och identitet
- Testa nekad åtkomst
- Behåll skyddet efter återanslutning