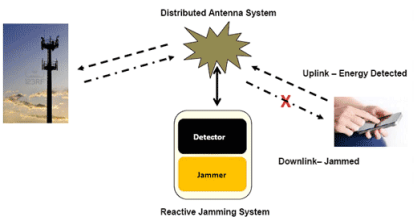
Datasikkerhed

For så vidt sikkerhed omkring data, bør man foretagen en grundig datasikkerhedsanalyse. Der er typisk tre sikkerhedsmæssige forhold man bør overveje og evt. dæmme op mod:

- Jamming – er det muligt og et problem, hvis ens data i perioder ødelægges af andre systemer og ikke når frem?
- Aflytning – er det muligt og et problem, hvis andre lytter med på de data der sendes/modtages?
- Identitet – er det muligt og et problem, hvis en fremmed enhed kan give sig ud for ens eget udstyr og kommunikere med?




Hvis man ønsker ar gardere sig mod ovenstående er svarene typisk:

- Jamming: Benyt sikre og/eller lukkede netværk/forbindelser, f.eks. GSM og LAN. Hvis dette ikke er muligt, er man nødt til at designe løsningen så den "lider" mindst muligt under et sådan angreb…
- Aflytning: Benyt mere eller mindre kompleks kodning (kryptering). TLS (Transport Layer Security) er en af de gode løsninger.
- Identitet: Benyt f.eks. autorisation (authentication) elle ring tilbage (dial back). TLS kombineret med server certificat og individuelle client certifikater er her en god løsning her.

Ud over produkter som er pivåbne, ser man også systemer som er overbeskyttede, måske beroende på en manglende datasikkerhedsanalyse.

Systemsikkerhed

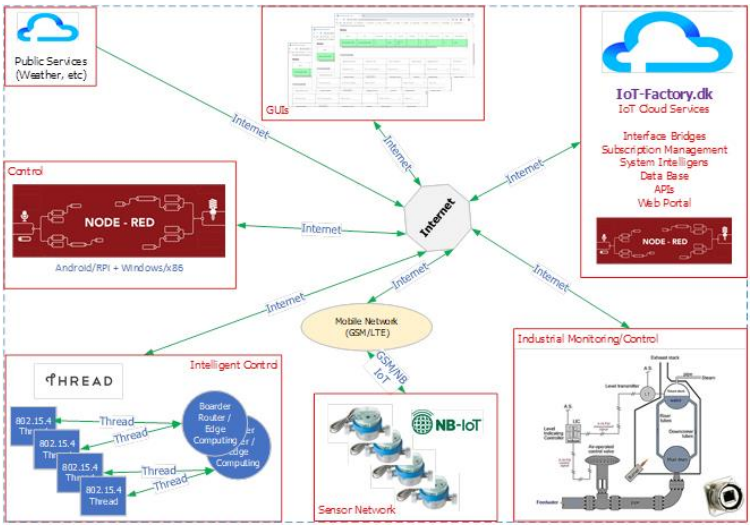
Problemet her er om det er muligt og et problem hvis fjendtligsindede opdaterer enhederne med fjendtlig software/firmware, som efterfølgende tilsyneladende agerer rigtigt.

Hvis dette er tilfældet, er det specifikt processen omkring softwareopdatering (DFU, Device Firmware Update) som ofte foregår ud over IoT netværket (OTA, Over The Air), der skal analyseres og sættes ind overfor. OTA kanalen kan f.eks. beskyttes med TLS.

Det kan være Særlige sikkerheds IC som sammen med certifikater fra en troværdig (trusted) server skal benyttes. Ikke en simpel proces, men desværre nødvendig når dette er et problem man vil modvirke. Moderne PC'er ol. benytter denne teknologi, men for mindre/små embeddede løsninger er dette måske en noget kompleks tilføjelse!?

Nogle vælger at udelader OTA DFU, og i stedet giver mulighed for DFU lokalt på enhederne af servicemedarbejder og/eller kunder. Med mindre værktøjer er sikrede kan det imidlertid ikke generelt anbefales, da en hacker kan antages at have adgang til avancerede analyse- og programmeringsværktøjer.

IoT-Factory.dk og sikkerhed…



Hensigten med IoT-Factory (ITF) er et simpelt heterogen demonstrator-system, som illustrerer principperne i ægte IoT (publish/subscribe connectivity).

Systemet er designet til fleksibelt at kunne teste forskellige funktionelle løsninger uden det overhead og den kompleksistet der følger med brug og konfiguration af sikkerhedsprotokoller.

MQTT-kanalen mellem tingesterne og brokeren er således ikke sikret på nogen særlig måde ud over hvad en normale TCP/IP socket eller mobilnetværkenes forbindelser tilbyder. Når sikkerhed kræves, kan MQTT kanalen imidlertid ret let opgraderes med TLS på Brokeren, men for ”tynde” Tingester kan det være noget mere komplekst – men ikke umuligt!

Den web-baserede ITF-data portal samt selve ITF-hjemmesiden benytter sikker https, ikke mindst fordi mange selskaber ikke tillader tilgang til almindelige usikre http sider. Password til dataportalen gemmes krypterede dog efter best practise med brug af bcrypt/salt.