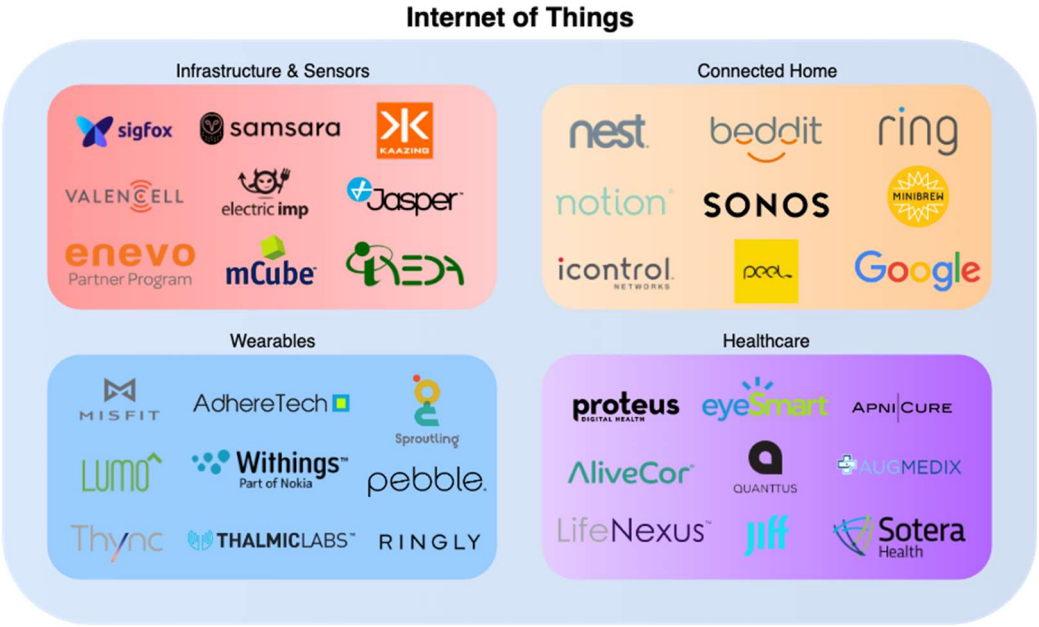
IoT Security – en översikt

Innehåll

Introduktion

IoT genomgår – tillsammans med begrepp som AI, Cloud, en explosionsartad utveckling. IoT är, till skillnad från de andra, främst en accessteknik, dvs metoder att inhämta data från omgivningen och dess föremål, samt att styra, kontrollera, reglera och övervaka dessa föremål. Eftersom dessa devices oftast befinner sig ute i den riktiga världen, har de en hel del säkerhetsproblem behäftade med sig.



Inledning och begrepp

Security och Safety

På engelska skiljer man på ”**security**” och ”**safety**”. På svenska kallar vi dem lite olyckligt bägge för ”**säkerhet**”, den sistnämnda borde kanske egentligen benämnas ”**trygghet**” istället. ”Security” betyder åtgärder för att förebygga illvilliga händelser, t ex skalskydd, perimeterförsvar, kryptering, Intrusion detection, medan ”Safety” snarare betyder frånvaro av olyckor, såsom datakrascher, raderade data osv.

IoT- Internet of things – ”Sakernas Internet”

Wikipedia talar om att det främst avser ”Vardagsföremål som är uppkopplade mot internet” vilket gör att de kan styras och utbyta data därigenom. Just termen ”vardagsföremål” är nyckeln här – för vanliga datorsystem har ofta möjlighet att ha adekvat säkerhet inbyggt i sig, vilket inte nödvändigtvis är möjligt för t ex en brödrost. Enligt Wikipedia har det redan förekommit att hissar, jordvärmepumpar, A/C-apparater eller övervakningskameror har hackats och sedan deltagit i DDOS-attacker genom att ingå i ett botnet (t ex Mirai-attacken 2016[1]). Även det avancerade hacket STUXNET[2] kan sägas ligga i IoT-sektorn, eftersom målet var att manipulera datoriserade styr/reglersystem.

[1] https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html
[2] https://www.bbc.com/timelines/zc6fbk7

Mobilt och stationärt

En viktig distinktion inom IoT är den mellan rörliga enheter (främst uppkopplade bilar och liknande s k kinetiska system) och fasta installationer (som då mest liknar klassiska el-, styr-, och reglersystem, fast datoriserade och internetanslutna). Stationära enheter kännetecknas ofta av stora nät, många enheter, enkelhet, kostnadskänslighet.

Kritiska system

Kritiska system innebär att allvarliga olyckor kan inträffa om de fallerar eller manipuleras. Här är några exempel ur verkliga livet:

- Hackade uppkopplade bilar där t ex bromsverkan, värmereglering, vindrutetorkare slutat fungera.
- Reningsverk där klorhaltregleringen saboterats till giftiga nivåer
- Fjärrmanövrerade öppningsbara broar som tagits över av illasinnade
- Elleverantörer som hackats så svårt att alla kraftverk tvingades starta om manuellt
- Kylsystem som manipulerats att tro att temperaturen är en annan än den faktiska
- Varmvattenberedning som satts ur funktion efter dataintrång
- Avlyssning via hemapparater såsom modem/routrar, röststyrda funktioner (bl a babymonitorer, scanners, kaffekokare, lampor, TV-spelare, kylskåp osv)[3]

Det är uppenbart att IoT-sektorn är väldigt känslig och beroende av säkerhetslösningar samt har sina egna utmaningar, främst genom sin utbredning men även genom sin exponering – IT-funktioner i sammanhang som tidigare inte varit IT-relaterade.

Ett sätt att kategorisera olika fall av IoT är enligt[4] :

1) Massivt IoT -stora mängder samtidigt inkopplade enheter, begränsat antal accesspunkter, låg strömförbrukning, låg dataöverföring, t ex anslutna via 5G (hit hör oftast de system som ibland också kallas ”Connected SIMs”).
2) Bredbands-IoT – liknar föregående, men med krav på datahastigheter och bandbredd. Exempel är hela bil-sektorn, avancerade drönare, AR/VR-lösningar, bärbara enheter, smart tillverkning. Här behövs funktioner för t ex grupphantering, network slicing, optimering av datagenomströmning. (Hit hör de lösningar som ibland kallas ”Kinetic IoT”).
3) Industriell automatisering- (kallas även IIOT – industrial IoT) kräver bl a nätverksfunktioner för högt ställda konnektivitets- och tillgänglighetskrav, noggrannhet i positioneringstjänster (även inomhus). Även högt ställda krav på att hantera utsatta miljöer och högt ställda säkerhetskrav.
4) Kritisk IoT: kräver omedelbar kommunikation och nästintill perfekt pålitlighet, för t ex smart tillverkning, hälso/sjukvård, m m.

[3] https://www.svt.se/nyheter/lokalt/jonkoping/riskerna-med-uppkopplade-hem-sakerhetsexperten-forklarar
[4] https://www.businessinsider.com/ericsson-announces-new-cellular-iot-approach-2019-2?r=US&IR=T&IR=T

CIA-triaden (Confidentiality, Integrity, Availability)

Gäller för alla IT-system och såklart även för IoT. Ämnet behandlas utförligt i en Windriver-presentation[5]. Windriver skiljer bl a på hantering av ”data in motion” och ”data in rest”.

1) Konfidentialitet: Detta innefattar data som samlas in och skickas ut via IoT-systemet samt data som lagras I IoT-systemet (diskar och icke-flyktiga minnen). Konfidentialiteten delas in i tre underkategorier:
    a. Privacy (via kryptografiska funktioner – olika algoritmer för olika delar i datapath och för olika sorters datalagring)
    b. Separation: partitioneringen inom systemet; informationsflödet mellan dessa delar, enheterna som olika partitioner kan accessa, de APIer som tillåts anropas.
    c. Nyckelhantering: de listade kryptonycklarna och deras giltighet. Hur varje nyckel skyddas och hur de förstörs efter användning.
2) Integritet: funktioner som säkerställer att IoT-systemets data inte har raderats eller förvrängts. Även här kan man prata om “data i vila”, “data i rörelse”, “data i processning”. IoT-fokus på:
    a. Dataintegritet - vilka integritetsmekanismer används, på vilka data, T ex HMAC.
    b. Bootprocessen – vad behöver verifieras vid start, vad händer om verifieringar fallerar vid boot?
    c. Trippel-A – Vilken kommunikation måste vara autentiserad, vad skall tillåtas ge access till en enhet, hur hanterar vi säkerhets-events ur loggnings- och fjärrstyrningshänseende och snarlika frågor.
3) Availability (tillgänglighet) för IoT fokuserar på att hela IoT-plattformen faktiskt utför sin avsedda funktion. Enklast möjliga approach till detta är att aldrig tillåta att IoT-enheten får modifieras, vilket förstås är kraftigt begränsande. Dikotomin står dock mellan tillgänglighet och modifieringsmöjligheter, och en väl vald balans mellan dessa måste hittas.
    a. Whitelistning – vilka accesskontrollmetoder används, listor på de resurser på en enhet som kräver kontrollerad access, ACLer osv
    b. IDS/IDP - tillåtna APIer att applikationerna exekverar, filsystemsintegritet, osv.
    c. Managering - hantera serverinformation, kommunikationsflödesdefinitioner, hantera falska och upprepade kommandon osv.
    d. Motmedel – respons till intrångsevent, attesteringsfel, etc.

[5] http://events.windriver.com/wrcd01/wrcm/2017/09/A-Survey-of-Information-Security-Implementations-for-the-Internet-of-Things-WP-1.pdf

Säkerhetsrelaterade IoT-problem

- IoT-tekniken är fortfarande i ”pionjärstadiet” – strukturer för t ex ansvar är således oklart. Är det tillverkaren av en IoT-ansluten apparat som skall sörja för tillräcklig säkerhet? Eller ISP:n (net provider). Aktuella fall har visat att detta orsakar mycket problem, ingen anser sig vara ansvarig för helheten.
- Fysisk tillgång till apparaten gör intrång lätt.
- Standardsinloggning/lösenord byts ej ut vid skarp idrifttagning.
- För stationära enheter i mass-deployment (t ex omfattande nät av enkla temperaturgivare) är kostnad och enkelhet viktiga. Att då dra in en hel CPU med kärna, OS och IP-stack för att kunna säkerställa en rimlig nivå av IT-säkerhet, är då helt enkelt inte kostnadsmässigt vettigt.

Den ledande tillverkaren Ericsson listar dessa aspekter som mest kritiska (Advanced and Persistent Threats, APT) för IoT-säkerheten[6]:

1) Identitets- och dataaccessmanagement (IAM)
2) Dataintegritet måste säkras
3) Inga IoT-system kommer någonsin vara 100% säkra – hantera detta faktum
4) Automation och management-verktyg för IoT-säkerhet måste finnas

Myndigheten för Samhällsskydd och Beredskap, MSB, listar följande IoT-relaterade hotkategorier[7]:

1) Konfidentialitet: IoT enheter kan användas som språngbräda in i traditionella IT system för att stjäla information. De möjliggör även direkt genom sin användning inhämtning av individinformation och spionage.
2) Riktighet där IoT är måltavlan: möjligheten att manipulera enheter medför risk både på individ- och samhällsnivå. Exempelvis om en enskild medicinpump manipuleras eller storskalig manipulation av smarta elnät.
3) Riktighet där IoT är verktyget: möjligheten att ta över IoT enheter för att skapa exempelvis botnet för DDOS-attacker.
4) Tillgänglighet: IoT-enheter kan göras obrukbara, exempelvis i utpressningssyfte, eller som en sidoeffekt av att de tas över för andra ändamål, exempelvis som en del i ett botnet.

[6] https://www.disruptive-technologies.com/sensing-solution/iot-sensor-security/

[7] https://kryptera.se/assets/uploads/2018/06/iot_begrepp-och-kategorisering_180614_kb.pdf

Aspekter rörande IoT-säkerhet i synnerhet

Aspekter som rör IT-system generellt gäller såklart även här, men det tas inte upp i ett IoT-inriktat dokument.

1) Systemens storlek och komplexitet:
    a. Antalet IoT enheter ökar mycket snabbt (”en explosion av sensorer!”[8])
    b. Antalet kommunikationsvägar mellan enheterna ökar exponentiellt mot antalet
    c. Antalet tillverkare och antalet varianter av hårdvara och mjukvara och protokoll att växa vilket medför problem, inom interoperabilitet, säkerhet, OPEX/CAPEX, systemöverblickbarhet och systemförståelse.
2) Designförutsättningar: IoT-enheter har generellt mycket begränsade resurser vad gäller energi- och beräkningskapacitet vilket slår mot säkerhetsmekanismer generellt. Detta gäller även t ex de protokoll som används, en känd incident är t ex säkerhetshålen i ett felkonfigurerat MQTT-protokoll[9][10].
3) Exponering: Detta rör hur enheter används. IoT-enheter är sårbara för fysisk åtkomst vilket förenklar manipulation. Deras antal skapar möjlighet att otillåtet aggregera information. Det kan antas att lösenordsskydd från både tillverkare och användare kommer hålla en låg nivå vilket ökar risken för otillbörligt användande och skadlig kod.
4) Attackvektorer mot IoT: Dessa är i många fall gemensamma med dem för klassisk IT. Dock kan de grupperas enligt vilken del av IoT de riktas mot. Exempelvis kan störsändning användas mot de första två.
    a. perceptionslagret
    b. överföringslagret
    c. applikationslagret

Det finns såklart redan en uppsjö av tillverkare som erbjuder IoT-säkerhetsfunktioner. Problemet är bara att i brist på standardiseringar, har varje tillverkare skapat egna ekosystem av lösningar, som inte alltid är kompatibla eller ens kan samarbeta. Å andra sidan har flera tillverkare ganska kompletta kataloger med IoT-funktioner, t ex Cisco[11].

[8] https://arstechnica.com/information-technology/2019/06/more-sensors-more-problems-industrial-iot-platforms-need-safeguarding/
[9] https://www.darkreading.com/iot/researcher-finds-mqtt-hole-in-iot-defenses/d/d-id/1332573
[10] https://www.cert.se/2016/09/mqtt-i-sverige
[11] https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1964024

Metoder för ökad IoT-säkerhet[12] [13]

Några metoder för ökad säkerhet i området internet-of-things är:

- Koppla in enkla apparater utan egen säkerhet till ett (virtuellt) Intranät
- Använd protokoll som förenklats till att hantera de enklare sensorer som lösningen nyttjar, t ex NetFlow[14], TrustSec[15].
- Hårdvaran skall ha inbyggda säkerhetsattribut som stödjer t ex kryptering och anonymitet.
- Mjukvaran som används underhålls kontinuerligt och att kända säkerhetsbrister har åtgärdats.
- Mjukvaran i en enhet kan säkerhetsuppdateras på ett säkert och kontrollerat sätt.
- Enheten är designad med viss tolerans mot avbrott eller fel hos andra enheter.
- Enheterna har ett bra lösenordsskydd, exempelvis genom att produkterna levereras med ett unikt lösenord som kan ändras.
- Säkerhet beaktas i utveckling- och implementationsprocessens alla steg, inklusive val av plattformar, programspråk och verktyg. Som systemägare och nyttjare handlar det därtill om att vidta ett antal åtgärder, som till exempel att:
    - Installera utrustning på ett säkert sätt. Det kan handla om att minimera risken för fysisk manipulation om den är placerad på en offentligt tillgänglig plats eller att segmentera IoT-enheterna på ett separat nät (VPN eller liknande) för att kunna kontrollera trafiken och tillse att endast godkänd trafik släpps igenom.
    - Tillämpa medveten uppkoppling med kunskap om de risker som uppkopplingen medför. Detta innebär exempelvis att:
        - Direkt internetuppkoppling ska inte vara nödvändigt eller tillåtet för kritiska funktioner i ett IoT-system, särskilt inte i industriella sammanhang.
        - Avsikten med olika nätverksanslutningar ska klargöras och kommuniceras med berörda parter samt dokumenteras väl.
    - Om möjligt - installera program som skyddar mot virus och annan skadlig kod.
    - Genomföra säkerhetsuppdateringar, övervakning och underhåll på ett organiserat och kontrollerat sätt, gärna genom automatisering.
    - Logga och analysera händelser i systemet för att upptäcka intrång och manipulation.
    - Skydda autentiseringsuppgifter och använda starka lösenord.
    - Tillämpa ett djupt försvarstänkande, det vill säga att säkerhet implementeras i olika abstraktionslager, ytterst med verktyg på användarnivå för att skydda mot angrepp från exempelvis insiders (”Defense-in-depth”, ”lökprincipen”).
    - Uppmärksamma systemanvändare på riskerna med nätfiske (phishing) och social manipulation (social engineering).
    - Var aktiv i olika communities för informationsdelning.

Ett intressant initiativ är NERC/CIP[16], som ämnar till att säkra kritisk elförsörjning i Nordamerika. Detta innefattas av ett 40-tal regler[17] och över 100 krav som alla är rekommenderad läsning.

---

[12] https://kryptera.se/assets/uploads/2018/06/iot_rekommendationer-till-myndigheter_180614_kb.pdf
[13] https://kryptera.se/assets/uploads/2018/06/28547.pdf
[14] https://en.wikipedia.org/wiki/NetFlow
[15] https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html#~stickynav=1
[16] https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/what-you-need-to-know-about-nerc-cip-cybersecurity-standards/
[17] https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx