Sakernas internet: Integritet och säkerhet ­– en modell för riskbedömningen

Tommy Löwendahl

Kandidatavhandling i datavetenskap

Handledare: Marina Waldén

Fakulteten för naturvetenskap och teknik

Åbo Akademi

Våren 2018

Referat – Sakernas internet (IoT) har väckt mycket intresse på senaste tider. IoT är delen av framtidens internet som byggs upp av miljarder driftskompatibla IoT-enheter. Säkerhet inom ett IoT-system är fortfarande ett problem som berör både tillverkaren och utvecklaren av IoT-lösningar. Avhandlingen fokuserar på att identifiera vilka säkerhetsfrågor inom IoT-topologin som är de mest kritiskaoch vilka sätt det finns för att skydda data. De flesta brister på säkerhet gäller osäker autentisering, oskyddat användargränssnitt och brist på kryptering. Huvudbudskapet i avhandlingen är en tredelad modell för identifieringen av säkerhetsnivån i ett IoT-system med avseende på varierande hot och integritet.

Nyckelord – Sakernas internet (IoT), säkerhet, hotbild, IoT-topologi, riskbedömning, säkerhetskrav

Innehållet

[1 Inledning 1](#_Toc509938234)

[1.1 Syftet i avhandlingen 3](#_Toc509938235)

[2 Sakernas internet 4](#_Toc509938236)

[2.1 Teknologier för sakernas internet 5](#_Toc509938237)

[2.2 En IoT-topologi 5](#_Toc509938238)

[3 Attacktyper och hot mot funktionalitet i ett IoT-system 8](#_Toc509938239)

[3.1 Hot i gränssnittslagret 9](#_Toc509938240)

[3.2 Hot i servicelagret 9](#_Toc509938241)

[3.3 Hot i nätverkslagret 10](#_Toc509938242)

[3.4 Hot i sensorlagret 11](#_Toc509938243)

[4 Att bevara integritet i ett IoT-system 13](#_Toc509938244)

[4.1 Integritet i gränssnittslagret 15](#_Toc509938245)

[4.2 Integritet i servicelagret 16](#_Toc509938246)

[4.3 Integritet i nätverkslagret 17](#_Toc509938247)

[4.4 Integritet i sensorlagret 18](#_Toc509938248)

[5 En modell för att kartlägga säkerhetsnivån för ett IoT-system 19](#_Toc509938249)

[6 Slutsatser 21](#_Toc509938250)

[7 Referenser 22](#_Toc509938251)

Termer på svenska och engelska

* 6LoWPAN, IETF low-power wireless personal area networks
* ASIC, application specific integrated circuit
* BLE, bluetooth low energy
* CoAP, constrained application protocol
* DoS, denial of service, överbelastningsattack
* ECDSA, elliptic curve digital signature algorithm
* ENISA, European union agency for network and information security
* FPGA, field-programmable gate array
* IEC, international electrotechnical commission
* IEEE, institute of electrical and electronics engineers
* IERC, european research cluster on the internet of things
* IETF, internet engineering task force
* Igenkänningstecken, eng. security token
* ISA, international society of automation
* ISO, international organization of standardization
* ITU, international telecommunication union
* M2M, machine-to-machine, kommunikation mellan maskiner
* MQTT, message queuing telemetry transport
* OAuth 2.0, auktoriseringsprotokoll av IETF
* OpenID, identitetservice
* RFID, radio frequency identification
* Sniffer, ett program som analyserar trafik i datornät
* W3C, world wide web consortium
* WiFi, IEEE 802.11, trådlös dataöverföring
* Z-wave, en trådlös dataöverföring för hemautomation
* Zigbee, IEEE 802.15.4, strömsnål trådlös dataöverföring

# Inledning

Sakernas internet (IoT) har växt snabbt till ett stort ekosystem inom WWW-domänen. Enligt de senaste estimeringarna kommer det att finnas 20–30 miljarder aktiva IoT-enheter globalt innan år 2020 [1] [2]. Det kan tänkas att stor tillväxt leder till utmaningar speciellt inom säkerhet och integritet för IoT-produkter, om standardiserade protokoll och tydlig uppfattning av IoT-ekosystem inte hinner med utvecklingen. Det är möjligt att brist på helhetssyn försvagar designen av IoT-system och därför strävar avhandlingen efter att undersöka förslag för god praxis inom IoT-system i fråga om säkerhet och datas integritet.

IoT-domänen är mer och mer fokuserad på att skapa, samla och utnyttja information om omgivningen med hjälp av olika sensorer. I industriell omgivning cirkulerar data mellan intelligenta sensorer, inbyggda logiska kontroller och robotstyrda system [3]. IoT-enheternas integritet är kritisk för att behålla dels data och dels kontroll över systemet.

Data som har skapats av IoT-system kan vara en stor tillgång. Frost och Sullivan estimerar enligt [4] att senast 2020 samlas 40 % av alla tillgängliga data in av IoT-enheter. Insamlade data kan vara mycket värda för ägaren om de kan säljas vidare eller utnyttjas mot konkurrenter i samma bransch. Samtidigt kan data vara av stort intresse för olagliga kretsar. Det finns alltså stort intresse för att använda data som tillgång och således är det naturligt att bra säkerhet behövs för att skydda denna nya prisvärda tillgång.

Det är inte bara mängder av data som drar in attacker. Behovet av bra kontroll över IoT-system dyker upp hela tiden i dagspressen och forskningen. År 2016 uppstod ett bra exempel på brist på säkerhet för IoT-enheter då det så kallade Mirai botnätet, som kapade IoT-enheter, kunde växa så stort att en distribuerad överbelastningsattack nådde 1 terabyte per sekund och förstörde flera stora webbsajter som Netflix, Twitter och Paypal [5]. En studie från Kommunikationsverket visar att år 2017 fanns närmare 10 000 öppna och oskyddade enheter för byggnadsautomatisering, industriella hanteringssystem och individuella hemmaliggande anordningar i Finland [6]. Globala data visar att till exempel så kallade honungsfällor för att testa IoT-enheternas dataintrångstrafik är utsatta för mer än 8 attacker i timmen [5]. Dessa exempelsiffror om oskyddade IoT-enheter och attackhastigheten visar en alarmerande trend, och problemet är tvåfaldigt. Det som syns här är att om det finns en IoT-enhet kopplad till internet så blir den med stor sannolikhet utsatt för ett attackförsök. Problemet är också att å ena sidan prioriterar tillverkaren av IoT-anordningar inte nödvändigtvis säkerhet och å andra sidan är användarna inte heller aktiva i att säkra de anskaffade IoT-anordningar. Exempelvis i Symantecs hotrapport om internetsäkerhet [5] lyfts det fram många fall där förvalda lösenord är antingen omöjliga eller svåra att ändra för en IoT-anordning. Enligt samma rapport var ”admin” fortfarande det vanligaste förvalda lösenordet vilket för sin del också visar hur svag säkerheten kan vara. Ur användarens perspektiv hänvisar F-secure till en tysk undersökning av Gemalto som beskriver att bara 14 % av de som äger en IoT-anordning vet hur enheten kan skyddas [7]. Man kan dra slutsatsen att både tillverkarna av IoT-system och användarna behöver mer information samt utbildning om sakernas internet för att ändra attityder. Denna kan slutligen förvandlas till ett positivt resultat, som ENISA:s (European Union Agency for Network and Information Security) verksamhetsledare Helmbrecht [1] uttrycker i sitt tal för Europaparlamentet, ska den här aktuella hotbilden utmana oss att skapa ett nytt led av ett säkert sakernas internet.

Det är viktigt att identifiera olika hot mot IoT-system men ännu viktigare är att IoT-system per definition är *”secure by design”* [8] vilket betyder att säkerheten ska vara designad inne i systemet från början. Som Li och Xu [3] betonar blir IoT-system skyddade, kompatibla, pålitliga och effektiva då alla nivåer inom IoT-topologin har standardiserade skyddsmekanismer. Fast denna princip med *secure by design* är en bra start för att skydda sakernas internet, är principen ändå en utmaning att utföra på grund av de många olika standarder som finns. Speciella utmaningar berör protokoll för accesskontrollen och nätverkssäkerheten som inte ska vara för resurskrävande i ett begränsat IoT-system [9].

## Syftet i avhandlingen

Syftet vid denna avhandling är att etablera två synvinklar på IoT-system. För det första attacktyper mot ett IoT-system över hela topologin och för det andra hur ett IoT-system kan skyddas i förhållande till de senaste förslag. Ett IoT-system är här begränsade till en IoT-anordning och den omgivningen där anordningen har interaktion med. Fokus med avhandlingen ligger på att identifiera vilka säkerhetsfrågor inom IoT-topologin som är de mest kritiskaoch vilka sätt det finns för att skydda data. Avgränsningen hålls till hottyper och säkerhetskrav på ett IoT-system. Som studiefrågan ska avhandlingen undersöka hur kända hottyper och skyddsmekanismer kan relateras till deras miljö och topologi. Avslutningen i avhandlingen ska presentera en modell för att kartlägga en säkerhetsnivå för att skydda ett IoT-system.

Dispositionen i avhandlingen är strukturerad så att avsnittet 2 introducerar ett kort historia för sakernas internet samt presenterar uppdelningen av IoT-topologin. Avsnitt 3 och 4 klargör attackmekanismer mot ett IoT-system samt mekanismer för att skydda ett IoT-system. Den funktionella delen i avsnittet 5 presenterar en modell för riskbedömningen som kan hjälpa i att identifiera en generell skyddsnivå för ett IoT-system. Avhandlingens avslutande del drar slutsatser och diskuterar framtidens möjligheter för ett säkert sakernas internet.

# Sakernas internet

År 1932 skrev Jay B. Nash en fiktiv beskrivning av mekaniska slavar som arbetar dygnet runt för att göra livet lättare för människorna: *”Another slave sits twenty-four hours a day at our thermostat, regulating the heat of our home. Another sits night and day at our automatic refrigerator.”* [10]. Inte mycket mer rätt kunde han ha haft. Utvecklingen har varit snabb och nu finns de mekaniska slavar av Nash överallt.

Under utvecklingsperioden på sakernas internet som började på 1980-talet, var sakernas internet beskriven som *”ambient intelligence”*, *”calm computing”* eller *”pervasive computing”* [11]. Idag är sakernas internet (IoT) definierat enligt IERC (European Research Cluster on the Internet of Things) som en global infrastruktur bestående av driftskompatibla enheter; en enhet har en unik identitet, fysiska och virtuella egenskaper, ett gränssnitt och är dynamiskt integrerat med nätverket [12]. Figur 1 visar ett exempel på ett IoT-system. Gemensamt för alla de här definitionerna är idén om ett dynamiskt ihopkopplat nätverk och allmänt förekommande enheter. Det som gör sakernas internet speciell är egenskapen som självständighet och autonomisk funktion. IoT-enheter kan samarbeta, samla samt dela information och behandla data utan att en person styr detta. Naturligtvis är all funktion fastställt på förhand. Den autonoma aktiviteten kommer med priset och utmaningen är med övervakningen av IoT-enheter som kan bestå av flera olika funktionsnivåer.



Figur 1. Exempel för ett IoT-system enligt [3].

## Teknologier för sakernas internet

Sakernas internet behöver teknologier för identifiering, kommunikation och säkerhet som är anpassade för begränsade funktion vid ett IoT-system [3]. Aspekter som energiförbrukning, processorkraft, kapacitet för dataöverföring och minneskapacitet kan betydligt begränsa funktionalitet för ett IoT-system om de inte är optimerade [13]. Således ska sakernas internet ha egna protokoll istället för de teknologier som finns för den vanliga internet. Härnäst ges en överblick till de teknologier som har möjliggjort utvecklingen av sakernas internet.

Identifiering och spårningsteknologier som rf-etikett (RFID) och streckkoder har haft en stor nytta till att befrämja sakernas internet. Flera spårningssystem inom industrin och logistiken kunde inte ha utvecklat så snabbt utan de här lätta lösningar för realtidsspårningen. Kommunikationen – den andra viktiga områden för IoT-specifika lösningar – är ofta mycket heterogent och utmanar utvecklingen av lätta kommunikationssystem. De huvudsakliga kommunikationsprotokollen anpassade för sakernas internet är RFID, NFC, BLE, WiFi, 6LoWPAN, M2M och IP-teknologier. Flera kommunikationsteknologier mellan flera IoT-enheter kan hanteras av en gateway vilken fungerar som en styrningscentral för alla olika protokoll. [13, 14, 3].

## En IoT-topologi

Olika beteenden, funktioner och implementeringar behöver ett system för att inkapslas [14]. Inkapslingen gömmer variationen i systemet och det blir lättare att sammanlänka olika implementeringar i ett IoT-system [13]. Kraven för sammanlänkade funktioner mellan olika inkapslade delar av systemet frambringar kraven för en arkitektur. Ett IoT-system kan tänkas som en vertikal uppsättning bestående av flera funktionsnivåer. Dessa subsystem möjliggör skalbarhet och modulära egenskaper men samtidigt delar IoT-systemet in i flera komponenter. Det finns uppdelningar mellan fem och tre nivåer för en IoT-arkitektur beroende på hurdant perspektiv på systemet finns [14]. I denna avhandling används en uppsättning för ett IoT-system bestående av fyra nivåer som bygger en serviceinriktad arkitektur; gränssnittlagret, servicelagret, nätverkslagret och sensorlagret enligt [3, 14, 13]. Figur 2 visar uppsättningen för en serviceinriktad IoT-arkitektur. Fördelen med den serviceinriktade arkitekturen är, att den ger systemet en händelsedriven uppsättning, vilket är ett bra sätt att skapa ett driftskompatibelt system [14].



Figur 2. Serviceinriktad arkitektur från [14].

Sensorlagret använder identifierbara IoT-enheter. Deras sensorer eller funktioner skickar information vidare till nätverket. Nätverkslagret sammankopplar flera IoT-enheter och möjliggör kommunikation mellan dem och resten av nätverket. Mappningen och hanteringen samt synkroniseringen av data mellan IoT-enheter är nätverkslagrets huvudarbete. Servicelagret består mest av olika mellanprogram som stöder applikationskrav och affärslogik i systemet. Det sista lagret och närmaste till användaren är gränssnittlagret som simplifierar hanteringen av IoT-systemet. Tabell 1 sammanfattar egenskaper för topologin i ett IoT-system enligt [14].

Tabell 1. En serviceinriktad arkitektur för ett IoT-system enligt [14] (fritt översatt).

|  |  |
| --- | --- |
| **Lagret** | **Beskrivning** |
| Gränssnittslager (*eng.* *interface layer)* | Möjliggör interaktion mellan användare, applikationer och IoT-enheter. |
| Servicelager (*eng. service layer*) | Skapar och hanterar affärslogiken (API, datacenter, servrar). |
| Nätverkslager (*eng. network layer*) | Skapar en infrastruktur för nätverket och möjliggör kommunikationen mellan IoT-enheter. |
| Sensorlager (*eng. sensing layer*) | Består av hårdvaran (RFID, sensorer m.fl.) som automatiserar informationsinsamlingen från IoT-enheter. |

# Attacktyper och hot mot funktionalitet i ett IoT-system

I följande avsnitten presenteras först generellt kända attacktyper mot sakernas internet och det följs av hurdana hot det finns på olika nivåer av IoT-system. Nivåerna följer uppdelningen för en serviceinriktad arkitektur i ett gränssnitts-, service-, nätverks- och sensorlager [3, 14, 13]. Författarna Xu och Li [3] har presenterat en täckande uppdelning av hot mot säkerheten på dessa olika nivåer av ett IoT-system, och dessa används som basis i följande beskrivningar av hotbilden mot en IoT-topologi.

Attacker mot ett IoT-system utnyttjar dels de stora mängder av IoT-enheter som finns tillgängliga i nätverket och dels de många slags inträdespunkter ett IoT-system omfattar [4]. Med så många IoT-enheter anslutna till internet är det med stor sannolikhet möjligt att IoT-enheten har kvar en förinställd installation med ett enkelt eller inget lösenord samt öppna nätverksportar. Som F-secure [7] lyfter fram, vet bara 14 % av användarna för IoT-enheter hur de kan skyddas. Lika problematiskt är det med stora mängder av tillgängliga IoT-enheter, då ägaren ofta glömmer bort IoT-enheten och nödvändiga säkerhetsuppdateringar saknas, som Symantec [5] rapporterar. Detta kan leda till att IoT-enheten komprometteras utan att någon ens vet om det. Att det finns många inträdespunkter utgör en annan svaghet för ett IoT-system, om dessa inte gjorts säkra. Attacker på olika nivåer kan bestå av till exempel störning, trafiklyssnande eller kapning [4].

Typiska attacker mot ett IoT-system kan enligt Miloslavskaya och Tolstoy [4] kategoriseras som passiva eller aktiva. Passiva attacktyper är svåra att upptäcka därför att de bara observerar systemet utan att lämna spår av aktiviteten. Trafiklyssnande och monitorering är det vanligaste sättet att göra en passiv attack och speciellt okrypterad trafik har inget skydd mot trafiklyssnande [15]. Aktiva attacktyper påverkar däremot IoT-systemet på något sätt. Vanliga aktiva attacker antingen hindrar funktionalitet som en överbelastningsattack eller manipulerar kommunikationen mellan två IoT-enheter som en man-i-mitten-attack [4]. Enligt Li [3] är de svagaste nivåer i ett IoT-system nätverks-, service- och gränssnittslagren; och i flesta fall blir integriteten komprometteras på grund av dålig autentisering, osäkert gränssnitt och osäker kryptering.

## Hot i gränssnittslagret

Gränssnittslagret har inte stora externa eller aktiva hot som kommer utifrån. De flesta problem uppstår från ett fel i funktion eller autentisering vid gränssnittet. Följande Tabell 2 sammanfattar typiska hot mot gränssnittslagret i ett IoT-system enligt [3].

Tabell 2. Hot mot gränssnittslagret i ett IoT-system enligt [3] (fritt översatt).

|  |  |
| --- | --- |
| **Typen av hot** | **Beskrivning** |
| Konfigurering på distans | Konfigurering misslyckas vid gränssnittet. |
| Felkonfigurering | En IoT-enhet eller en gateway har en felkonfigurering. |
| Säkerhetshantering | Loggfilerna eller säkerhetsnycklarna blir avslöjade. |
| Hanteringssystem | Hanteringssystem blir felaktig |

Gränssnittslagret är den huvudsakliga ingången till ett IoT-system. Gränssnittet sammankopplar applikationer och IoT-systemet, och således kan de flesta problem förekomma med blockerad eller otillåten tillgång på grund av fel i autentisering eller konfigurering i systemet. Ett komprometterat gränssnittslager kan leda till problem med otillåten åtkomst och orsaka skador samt leda till förlust av data eller kontroll av ett IoT-system. En konfigurering av ett IoT-system som inte är säker kan till exempel nås av en otillåten instans eller felen vid IoT-enhetens hanteringssystem orsakar tappad kontroll av IoT-systemet. Otillåten åtkomst kan också leda till avslöjad säkerhetsinformation som säkerhetsnycklarna eller loggfilerna; och i värsta fall ges angriparen tillgång till alla lager i ett IoT-system vid dålig säkerhetshantering.

## Hot i servicelagret

Servicelagret är ofta komplicerad på grund av flera olika fragment som skapar affärslogiken för servicen. Detta innebär analysmetoder, integrering, programmeringsgränssnitt och serviceprotokoll m.fl. De huvudsakliga hoten mot servicelagret är otillåten användning av data och komprometterad integritet. Tabell 3 sammanfattar typiska hot mot servicelagret i ett IoT-system enligt [3].

Tabell 3. Hot mot servicelagret i ett IoT-system enligt [3] (fritt översatt).

|  |  |
| --- | --- |
| **Typen av hot** | **Beskrivning** |
| Hot mot integritet  | Integriteten blir riskerad. |
| Missbruk av service  | Otillåtna användare har tillgång till servicen. |
| Maskering av identitet  | Angriparen gömmer en IoT-enhet eller en gateway. |
| Manipulering av serviceinformation | Informationen av servicen blir manipulerad av angriparen. |
| Förnekbarhet  | Kommunikationen eller servicen blir nekad. |
| Överbelastningsattack (*eng. DoS*) | Ett försök att göra IoT-enheten otillgänglig. |
| Replay-attack | Angriparen skickar kapad information på nytt för att lura fram information från mottagaren. |
| Dirigeringsattack  | En attack mot ruttdirigering i ett IoT-system. |

Aktiviteter som informationsutbyte, dataprocesser, datalagring och servicekommunikation kan till exempel attackeras genom otillåtna åtkomster, överbelastningsattacker, sniffers och replay-attacker. Dessa typer av attacker skadar systemets integritet. De andra hoten som gäller otillåten användning, är missbruket och manipulering av serviceprogram samt replay-attacker. I värsta fall blir säkerhetskritiska eller personliga data komprometterad, men attacker kan också leda till förlust av data eller till att service blir otillgänglig. Hot mot tillgänglighet händer ofta på grund av förnekbarhet, ruttdirigerings- och överbelastningsattacker.

## Hot i nätverkslagret

Nätverkslagret sammankopplar kommunikationen mellan flera IoT-enheter. Utmaningar för att skydda nätverkslagret beror på flera olika kommunikations-, nätverk- och säkerhetssystem. Typiska hot i nätverkslagret är komprometterad kryptering, manipulationer i överföringen eller ruttdirigering av data samt överbelastningsattacker. Tabell 4 sammanfattar typiska hot mot nätverkslagret i ett IoT-system enligt [3].

Tabell 4. Hot mot nätverkslagret i ett IoT-system enligt [3] (fritt översatt).

|  |  |
| --- | --- |
| **Typen av hot** | **Beskrivning** |
| Informationsläckage  | Skyddad information släps ut till en främmande omgivning. |
| Överbelastningsattack (*eng. DoS*) | Ett försök att göra IoT-enheten otillgänglig. |
| Publika och privata nycklar  | Säkerhetsnycklar blir riskerade. |
| Fientlig kod  | Ett virus, en trojansk häst eller ett skräpmeddelande som orsakar fel i mjukvaran |
| Överföringshot  | Hot mot överföring som avbrytning, blockering, datamanipulering, förfalskning m.fl. |
| Dirigeringsattack | En attack mot ruttdirigering i ett IoT-system. |

Ett osäkert nätverkslager blir snabbt utsatt för fientlig kod eller informationsläckaget om krypteringen saknas. Därtill kan säkerhetsnycklar bli komprometterade vid en bristfällig kryptering. Exempelvis kan en man-i-mitten-attack ta över en osäker kommunikation mellan två lager i ett IoT-system och orsaka falsifierad dataöverföring som i värsta fall kan leda till en tappad kontroll av till exempel ett säkerhetskritiskt system. Attacker som överbelastar nätverket kan likaväl blockera den normala funktionen av ett IoT-system då IoT-enheten blir onåbar.

## Hot i sensorlagret

Sensorlagret består av fysiska sensorer och IoT-enhetens hårdvara. De flesta hot gäller fysiska manipuleringar i ett IoT-enhet eller falska autentiseringar som ger otillåtet tillträde till IoT-enheten. Tabell 5 sammanfattar typiska hot mot ett IoT-system i sensorlagret enligt [3].

En fysisk kapning av IoT-enheten kan leda till förlust av integriteten eller även tillgängligheten i ett IoT-system. Lika mycket kan falska IoT-enheter med falska autentiseringar skicka falsifierade data och i värsta fall orsaka skador i till exempel i ett industriellt IoT-system. Hoten som överbelastningsattacker leder till själviska hoten som blockerar tillgången till IoT-enheten på grund av resursbristen. Andra hot som skadeprogram och datamanipuleringar är vanliga på grund av dålig säkerhet vid mjukvaran. Speciellt förinställda installationer och lösenord underlättar angriparens tillgång till IoT-enheten; men också okrypterad trafik från IoT-enheten kan leda till avlysningen och förlusten av integriteten vid överföringen av data (se även Figur 3).

Tabell 5. Hot mot sensorlagret i ett IoT-system enligt [3 (fritt översatt).

|  |  |
| --- | --- |
| **Typen av hot** | **Beskrivning** |
| Dataintrång  | En fysisk kapning eller attack mot systemets logik som ger angriparen sensitiv information från IoT-enheten. |
| Tillgänglighet | IoT-enheten slutar fungera på grund av kapning eller attack mot systemets logik. |
| Identitetsbluff (*eng. spoofing*) | Ett skadeprogram maskerar sig som en IoT-enhet eller en gateway genom att falsifiera data. |
| Självisk hot  | IoT-enheten slutar fungera för att spara resurser eller bandbredd. |
| Fientlig kod  | Ett virus, en trojansk häst eller en skräpmeddelande som orsakar fel i mjukvaran. |
| Överbelastningsattack (*eng. DoS*) | Ett försök att göra IoT-enheten otillgänglig. |
| Överföringshot  | Hot mot överföring som avbrytning, blockering, datamanipulering, förfalskning m.fl. |
| Dirigeringsattack  | En attack mot ruttdirigering i ett IoT-system. |

I Figur 3 utnyttjar falska servrar eller IoT-enheter identitetsbluffen för att skicka falska data som utsätter IoT-systemet för ett otillåtet dataintrång. Detta kan även ge angriparen en total kontroll över IoT-enheten och också möjligheten för att gömma synligheten för en fysisk kapning av den äkta IoT-enheten.



Figur 3. Exempel för sårbarhet i ett osäker IoT-enhet enligt [3].

# Att bevara integritet i ett IoT-system

Varje lager i en IoT-topologi ger ett möjligt inträde till ett IoT-system. Flera nivåer i systemet gör det svårare att behålla integriteten av till exempel personliga data, affärsdata eller hantering av systemet. För att skydda ett IoT-system behövs en systematisk överblick över alla nivåer i ett IoT-system. Följande avsnitt beskriver flera ändamål som kan göra ett IoT-system mer säkert. Först presenteras en generell bild av olika säkerhetskrav och därefter följer indelningen i avsnittet en serviceinriktad arkitektur och varje nivå diskuteras separat i fråga om säkerhet.

Integriteten i ett IoT-system är ett stort pussel. Det finns flera sätt att kategorisera säkerhetskrav på sakernas internet och varje sätt har sina fördelar. Miloslavskaya och Tolstoy [4] delar skyddet av säkerheten i ett IoT-system i fyra delar: (1) skydd för anslutbarhet och kommunikation, (2) skydd för den fysiska IoT-enheten, (3) kontroll över inkommande trafik och (4) policyer. Betoningen i denna uppdelningen ligger i krypteringen och i kontroll över inkommande trafik med filtreringen och loggningen enligt [4]. Företrädesvis borde det alltid finnas ett system som loggar trafik i IoT-systemet för den inkommande trafiken. Som Kommunikationsverkets rapport [6] påminner om, blir det nästan omöjligt att undersöka ett säkerhetsbrott om ett loggningssystem saknas. Policyer för sin del förebygger mänskliga orsaker till säkerhetsslarv. I policyer ingår reglering och begränsningar av till exempel användning, trådlös tillgång, lösenord, serversäkerhet och kryptering. Li [3] ser säkerheten i ett IoT-system som ett samspel mellan sex aspekter där *tillgång*, *integritet* och *konfidentialitet* reflekteras på *autenticitet*, *oförnekbarhet* och *sekretess*. Figur 4 visar Lis säkerhetssyn som en triangel. Speciellt konfidentialitet, integritet och tillit betonas i Lis säkerhetssyn, vilka säkerställer till exempel autentisering, skydd av data och servicekontinuitet i ett Iot-system. Andra delar i figuren, som sekretess och oförnekbarhet, tryggas med initialt säker design av IoT-systemet samt med användningen av säkra (oförnekbara) registeringskedjor eller loggningssystem. Med hjälp av Lis riktlinjer kommer säkerhetskraven att mötas för ett IoT-system som helhet.



Figur 4. Säkerhetskrav på ett IoT-system enligt [3].

Det som oftast framhävs då säkerheten adresseras, är enligt Li och Xu [3] en accesskontroll. Med en accesskontroll kan alla nivåer av ett IoT-system begränsas med rättigheter. Det minimerar skador eftersom tillgången till andra delar i IoT-systemet har avgränsats, ifall av otillåten åtkomst. Accesskontrollen kan finnas i IoT-enheter, gateway-anslutningar, nätverks-, service- och gränssnittslagret, dvs. överallt, och den är en av de viktiga byggklossarna för ett säkert IoT-system. Därtill kan en väldesignad accesskontroll förebygga flaskhalsar i ett IoT-system. Om till exempel IoT-enheten har begränsade resurser, kan en åtkomstlista vara för resurskrävande för IoT-enheten. Med en accesskontroll baserad på förmågan (eng. capability based access control) garanteras användaren igenkänningstecken för att utföra en begränsad aktion i ett IoT-system. Samtidigt blir resurskraven minimala då bara information om igenkänningstecken behöver sparas. [3, 16].

Det är viktigt att ha en bra helhetssyn på IoT-topologin och på olika perspektiv som gäller säkerhet. Detta bidrar till att säkerhet blir designad inne i systemet (*secure by design*). Därtill kommer det till ett stort område där säkerheten skapas för IoT-system. Standardisering bidrar mycket till säkerheten och leder till gemensamma regler för hela IoT-industrin och utvecklingen av IoT-system. Detaljerade specifikationer för standarder är utanför avhandlingens fokus och kommer att lämnas bort, men en översikt presenteras här. Det finns flera aktörer för standarder och de största internationella påverkarna är IEEE (Institute of Electrical and Electronics Engineers), IEC (International Electrotechnical Commission), ISO (International Organization of Standardization), ISA (International Society of Automation), ITU (International Telecommunication Union), IETF (Internet Engineering Task Force) och W3C (World Wide Web Consortium) [17]. De har påverkat att protokoll för säkerhet, trådlös kommunikation och IP-standarder finns tillämpade på sakernas internet. Kända protokoll är till exempel OAuth 2.0 och OpenID för autentisering; ECDSA, MQTT och CoAP för krypterad kommunikation; ASIC och FPBA för krypteringen av hårdvaran [3, 4]. Dessa protokoll kommer att behandlas senare i texten.

Generella riktlinjer för IoT-domänen enligt ENISA:s (European Union Agency for Network and Information Security) verksamhetsledaren Helmbrecht [1] är målen för säkerhetsbasnivån, certifieringen och etiken inom designen. Därtill behövs beaktande för driftkompatibla och skalbara system samt referensmallar [17]. Bakom alla rekommendationer och standarder är tanken att säkerhet införlivas med designen i sakernas internet. Integriteten av ett IoT-system är lika bra som dess inbyggda mekanismer för accesskontroll, autentisering, loggning och kryptering både internt och externt [3].

Följande serviceinriktad IoT-arkitektur i resten av kapitlet kommer att presentera generella råd för att bevara integritet i ett IoT-system som har sammanfattats av Li och Xu [3].

## Integritet i gränssnittslagret

Gränssnittslagret består av flera olika applikationer som ger ett gränssnitt för kommunikationen i ett IoT-system. Säkerhetskraven på denna nivå gäller mest på mjukvaran i applikationer. Målet för säkerhetskraven är att interaktion med ett IoT-system är auktoriserad och pålitlig och därför fokuseras här mest på autentisering och accesskontroll.

Autentisering sker ofta med ett lösenord och SSL-protokoll men ett IoT-system är dåligt skalbar för SSL på grund av flera olika IoT-enheter med olika kommunikationsprotokoll. Därtill är autentisering inte enbart för personer som använder systemet utan också mellan IoT-enheter och för självidentifiering. Li och Xu föreställer säkra igenkänningstecken (eng. security tokens) vilka är skalbara och möjliggör även delegerad autentisering. Speciellt OpenID eller dess företrädare OAuth 2.0, som är öppen autentiseringsstandard från IETF, rekommenderas för IoT-system där flera klienter eller IoT-enheter behöver tillgången genom gränssnittet.



Figur 5. Introduktion till API Gateway OAuth 2.0 [18]

I figur 5 beskrivs OAuth 2.0 som ett flödesschema: Resursägaren ger en delegerad accessrättighet för att komma åt en skyddad resurs som finns i en säker server. Servern skickar accessrättigheten till en IoT-enhet. IoT-enheten kan använda den delegerade accessrättigheten för att kontakta servern tillbaka och komma åt skyddad information i servern.

Säkerheten vid gränssnittslagret begränsar otillåten tillgång till konfigurering, säkerhetshantering, hanteringssystem och data i ett IoT-system, vilket till stor del är hanterat av en pålitlig autentisering; därför är autentiseringen ett av de viktigaste säkerhetskraven i gränssnittslagret.

## Integritet i servicelagret

Servicelagret stöder aktiviteter som informationsbyte, databehandling, databasaccess och kommunikation mellan flera serviceprogram. Det är viktigt att designa servicelagret så att autentisering förebygger integritet och skapar en säker kommunikationskanal mellan serviceprogram. Samtidigt ger en passlig autentisering gränser för användningen så att bara nödvändiga accessrättigheter är aktiva vid en session i IoT-systemet (en rollbaserad accesskontroll).

Säkerhetsstrategin vid servicelagret behöver en speciell hänsyn till säkerheten i dataöverföring och accesskontroll. Skyddet mot attacker som överbelastningsattacker, replay-attacker eller missbruket av services kan adresseras i servicelagrets mellanprogram med accesskontroll, loggning och med bruket av igenkänningstecken för autentisering.

Listan nedan sammanfattar centrala säkerhetskraven som gäller servicelagret:

* Pålitlig autentisering och auktorisering, säkra nycklar eller igenkänningstecken (till exempel OAuth 2.0 och OpenID).
* En accesskontroll som förebygger otillåten och begränsad tillgång till serviceprogram.
* Säker identifikation för IoT-enheten.
* Hantering av överbelastningsattacker.
* Skyddet mot replay-attacker (igenkänningstecken).
* Oförnekbarhet med en registeringskedja eller loggning.

## Integritet i nätverkslagret

Nätverkslagret sammankopplar IoT-infrastrukturen till enskilda enheter och mellanprogram i IoT-topologin. Möjliga överföringsteknologier som BLE, WiFi, Z-wave, Zigbee och RFID används för att överföra data och kommunikation. Utmaningar för att bevara integritet i nätverkslagret beror till stora del på dessa olika implementeringar, vilka i värsta fall ska vara aktiva samtidigt i ett IoT-system bestående av flera olika IoT-enheter. Säkerhetskrav på nätverkslagret ska ta speciella hänsyn till dess huvudfunktion som är en överföring av information. Med säker överföring av information kan IoT-systemet skyddas mot komprometterad integritet och kommunikation.

Listan nedan sammanfattar de centrala säkerhetskraven som gäller nätverkslagret:

* En pålitlig autentisering och tillgång som är anpassat för sakernas internet (till exempel OAuth 2.0 och OpenID).
* Ett pålitligt säkerhetsprotokoll för överföringen av krypterad information som är anpassad för sakernas internet (ECDSA, MQTT och CoAP).
* Skydd mot överbelastning, man-i-mitten-attacker och replay-attacker i nätverket.
* Skydd mot komprometterad integritet och kommunikation (autentisering och kryptering).
* Identifiering av falska nätverksmeddelanden.

Speciellt attacker mot överföringen av information som man-i-mitten och replay-attacker, kan förebyggas med pålitliga krypteringsprotokoll och med ett bra autentiseringssystem. De viktigaste målsättningar med kryptering och autentisering är att hindra falska och otillåtna meddelanden från att påverka ett IoT-system samt att hålla integritet i kommunikationen.

## Integritet i sensorlagret

Sensorlagret innehåller den fysiska IoT-enheten som varierar på storlek, pris, energiförbrukning, hårdvara, mjukvara och tillgängliga sensorer. Dessa element ska hitta en balans för att satisfiera kraven för användningsändamålen och säkerheten. Säkerheten ska vara inbyggt i systemet så att alla säkerhetskrav blir satisfierade; både för mjukvaran och hårdvaran.

Om sensorlagret delas i två kategorier så finns det själva IoT-enheten som en fysisk apparat samt även sensorer som samlar information från omgivningen. Säkerhetskrav på en IoT-enhet ska fokuseras till skydd mot fysisk manipulering, accesskontroll, identifiering av betrodda enheter och rapportering/loggning för otillåtet bruk; även IoT-anpassad krypteringsmaskinvara som ASICs eller FPGA är rekommenderade. Eftersom IoT-enheter har ofta begränsade resurser, är också ett av de säkerhetskrav att förebygga själviska hot eller överbelastningsattacker som kan blockera tillgången till IoT-enheten. Säkerhetskrav på sensorer ska fokusera på autenticitet av insamlade data.

# En modell för att kartlägga säkerhetsnivån för ett IoT-system

I detta avsnitt föreslås en modell för att kartlägga säkerhetsnivån för ett IoT-system. Modellen bygger på de hittills etablerade observationer från tidigare presenterade litteraturen. Med hjälp av denna modellen för riskbedömningen, ska det vara möjligt att kartlägga den generella skyddsnivån för ett IoT-system, och reagera på säkerhetsproblem, som uppkommer från analysen av modellen.

Hot samt attacktyper mot ett IoT-system ska reflekteras på den identifierade topologin för IoT-systemet enligt modellen i Figur 6. Hot och integritet bygger en bas för denna modell. Detta ska tolkas så att balansen mellan hotet och integriteten leder tillsammans för en identifierbar säkerhetsnivå. För varje nivå i den kända IoT-topologin ska det finnas mekanismer för att skydda den; dvs. sensor, nätverks-, service- och gränssnittslager i den serviceinriktade arkitekturen kan värderas skilt med denna samma modell.

Figur 6. Modell för etablering IoT-systemets säkerhetsnivå.

Kartläggningen av säkerhetsnivån i ett IoT-system ska börja med en systematisk undersökning för att identifiera IoT-systemets topologi och de gränser som konstruerar övergången mellan olika nivåer i systemet. Detta betyder att i sensorlagret identifieras hårdvaran och sensorer för IoT-enheten samt de mekanismer vilka möjliggör kommunikationen till resten av IoT-systemet. Vid nätverkslagret ska de använda kommunikationsprotokollen listas ut och kartläggningen av nätverket ska ge en bra bild av ankopplade enheter. Undersökningen av servicelagret är viktigt för att identifiera de tjänster som står till förfogande i IoT-systemet. Vid gränssnittslagret är det viktigt att förstå hur IoT-systemet kontrolleras och styrs genom gränssnittet; dvs. vart finns access, vilka rättigheter finns utdelade och hurdana programmeringsgränssnitt har använts i IoT-systemet. En bra kartläggning av IoT-systemet ger större möjligheter för att bedöma säkerhetskrav i detta system.

Nästa steg är att identifiera de risker som uppstår om IoT-systemet blir komprometterat. Varje nivå i IoT-systemet ska undersökas skilt och åtminstone följande scenarier ska bedömas för konsekvenser: (1) Privat data blir oskyddad, (2) Tillgången eller kontrollen för systemet eller IoT-enheten tappas, (3) Kontrollen av systemet eller IoT-enheten är kapat, (4) Kommunikationen och nätverkstrafiken blir utsatt för avlyssning, sniffing eller överbelastning. Konsekvenser ska bedömas enligt skador som är möjliga i de eventuella scenarierna.

Det tredje steget är att identifiera nuvarande IoT-systemets säkerhetsmekanismer samt undersöka deras ändamålsenlighet. Den största fokusen ska ligga på mekanismer för accesskontrollen, autentiseringen, loggningen och krypteringen; se Figur 7. Om balansen mellan de identifierade riskerna och de nuvarande säkerhetsmekanismerna i IoT-systemet visar sig vara ogynnsam, möjliggör de tre ovannämnda stegen – kartläggningen av topologi, risker, samt nuvarande säkerhetsmekanismer – att man kan reagera förebyggande för att skapa ett säkert IoT-system.

Figur 7. Ett IoT-topologi och deras viktigaste säkerhetskrav

# Slutsatser

IoT-domänen är fortfarande i en process i synnerhet vad beträffar säkerhetskraven och säkerhetshoten. Nya IoT-implementeringar dyker upp i snabb takt och med dem kommer nya hot och krav på säkerhetsfrågor. Olika IoT-domäner, som finns till exempel för industrin, hälsovården, logistiken och för personlig användning [14], lyfter fram frågor gällande både integritet och etik. Till exempel ansvaret för designen och användningen av ett IoT-system eller ansvaret för datasekretessen är sådana frågor.

Utmaningen med många olika IoT-system är naturligtvis i de mångfaldiga protokoll och kommunikationssystem som finns. Med variationen i IoT-system kommer dessutom variation i hottyper. Avhandlingen har undersökt hot och säkerhetsmekanismer i ett serviceinriktade IoT-system, men detaljerade implementeringar har utelämnats. Det som presenterades i avhandlingen för uppdelningen av IoT-topologin ger en bas för att kartlägga både nya och gamla IoT-system i synnerhet med avseende på varierande hot och integritet. Budskapet i avhandlingen är den tredelade modellen för identifieringen av säkerhetsnivån. Därtill har de viktigaste säkerhetskraven identifierats. Balansen mellan hot och integritet i ett IoT-system ska alltid vara känd och den presenterade modellen för säkerhetsnivån i ett IoT-system är en bra startpunkt för att identifiera säkerhetsfrågor.

Fast avhandlingen inte går djupt på detaljnivå så erbjuder den förevisade litteraturen och modellen stöd i situationer där ett IoT-system ska säkerhetsgranskas. Det som kan lyftas fram från den förevisade litteraturen är att de största säkerhetshoten vid ett IoT-system gäller dålig autentisering, oskyddat användargränssnitt och osäker kryptering. Genom att kartlägga topologi, risker och nuvarande säkerhetsmekanismer i ett IoT-system, kan en säkerhetsnivå bestämmas. Det som kan konstateras vara viktigt för att skydda ett IoT-system, är att säkerhetskrav på accesskontroll, autentisering, loggning och kryptering ska vara beaktade. Efter att säkerhetsnivån har identifierats är det lättare att börja reagera på säkerheten i detalj.

# Referenser

|  |  |
| --- | --- |
| [1]  | U. Helmbrecht, ”Security Challenges and best practices in the IoT Environment,” European Parliament, 2017. |
| [2]  | Statista, ”Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025,” 2018. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. |
| [3]  | S. Li och L. D. Xu, Securing the Internet of Things, Elsevier, 2017.  |
| [4]  | N. Miloslavskaya och A. Tolstoy, ”Ensuring Information Security for Internet of Things,” i *2017 IEEE 5th International Conference on Future Internet of Things and Cloud*, 2017.  |
| [5]  | Symantec, ”Internet Security Threat Report 2017,” Symantec, 2017. |
| [6]  | Viestintävirasto, ”Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2017,” Viestintävirasto, 2017. |
| [7]  | F-secure, ”Cyber Security Research Institute report into the Internet of Things,” F-secure, 2017. |
| [8]  | M. Rouse, ”Security by design,” Tech Target, 2017. [Online]. Available: http://whatis.techtarget.com/definition/security-by-design. |
| [9]  | S. L. Keoh, S. S. Kumar och H. Tschofenig, ”Securing the Internet of Things: A Standardization Perspective,” *IEEE Internet of Things Journal,* vol. 3, nr 1, pp. 265 - 275, 2014.  |
| [10]  | J. B. Nash, Spectatoritis, A.S. Barnes and Compant, 1937, p. 265. |
| [11]  | E. Anzelmo, A. Bassi, D. Caprio, S. Dodson, R. van Kranenburg och M. Ratto, ”Discussion Paper on the Internet of Things commissioned by the Institute for Internet and Society, Berlin,” Institute for Internet and Society, 2011. |
| [12]  | IERC, "Internet of Things," European Research Cluster on the Internet of Things, 2016. [Online]. Available: http://www.internet-of-things-research.eu/about\_iot.htm. |
| [13]  | S. Li, L. D. Xu och S. Zhao, ”The internet of things: a survey,” *Information Systems Frontiers,* vol. 2, nr 17, p. 243–259, 2015.  |
| [14]  | L. D. Xu, W. He och L. Shancang, ”Internet of Things in Industries: A Survey,” *IEEE Transactions on Industrial Informatics,* vol. 4, nr 10, pp. 2233 - 2243, 2014.  |
| [15]  | V. P. Mohan och J. Anuradha, ”Network Security and Types of Attacks in Network,” i *International Conference on Intelligent Computing, Communication & Convergence*, 2015.  |
| [16]  | N. Fotiou, T. Kotsonis, G. F. Marias och G. C. Polyzos, ”Access Control for the Internet of Things,” i *2016 International Workshop on Secure Internet of Things (SIoT)*, 2016.  |
| [17]  | IEEE, ”IEEE-SA Internet of Things (IoT) Ecosystem Study,” The Institute of Electrical and Electronics Engineers, 2015. |
| [18]  | Oracle, ”Introduction to API Gateway OAuth 2.0,” Oracle, 2017. [Online]. Available: https://docs.oracle.com/cd/E50612\_01/doc.11122/oauth\_guide/content/oauth\_intro.html. |
| [19]  | Y. J. Jia, Q. A. Chen, S. Wang, A. Rahmati, E. Fernandes, Z. M. Mao och A. Prakash, ”ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms,” i *21st Network and Distributed System Security Symposium* , 2017.  |