

Uppsala Universitet
Inst. för Informatik och Media



Säker Internet of Things-kommunikation

XMPP och distribuerade sociala nätverk analyserat enligt OWASP top 10 Internet of Things Vulnerabilities

Anton Ydrefors & Mikael Örn

Kurs: Examensarbete

Nivå: C

Termin: VT-16

Datum: 2016-05-26

Sammanfattning

Nästa stora teknologiska revolution går under samlingsnamnet Internet of Things och syftar till att ansluta fysiska objekt, allt från hemmet och industriella maskiner, till Internet. Detta kan leda till stora vinster för alla delar av samhället, både ekonomiskt och miljömässigt. Men det medför också risker om inte säkerheten tillåts ligga i fokus. Detta arbete undersöker en föreslagen teknologi som kan utgöra grunden för kommunikation mellan objekt ur ett informationssäkerhetsperspektiv. Ett kommunikationsprotokoll, XMPP, i kombination med Distribuerade sociala nätverk. Information inhämtas från forskning och annan litteratur samt intervjuer med experter på XMPP. Denna lösning utvärderas utefter en global ideell organisations, OWASP, lista över de största säkerhetsriskerna som IoT står inför. Studien visar att XMPP i grunden är ett säkert protokoll som väl uppfyller många av dessa krav. Dock finns det fortfarande saker att förbättra.

Nyckelord

Internet of things, XMPP, säkerhet, OWASP, Distribuerade Sociala Nätverk, Kommunikationsprotokoll

Abstract

The next big technological revolution is collectively known as the Internet of Things and aims to connect physical objects, everything from your home to industrial equipment, to the Internet. This can lead to great profits for all parts of society, both economically and environmentally. But it also comes with great risks if security is not given enough focus. This work examines one proposed technology that can provide the foundation for communication between objects from an information security point of view. Data has been gathered from other research and literature as well as interviews with experts in XMPP. A communications protocol, XMPP, combined with Distributed Social Networks is evaluated using a nonprofit organizations, OWASP, list of the greatest security risks that IoT is facing. XMPP is a fundamentally secure protocol that covers many of these requirements well.

Keywords

Internet of things, XMPP, security, OWASP, Distributed Social Networks, Communication protocol

Begreppsförklaring

Nedan presenteras ett antal centrala begrepp i syfte att underlätta läsning. Dessa presenteras närmare längre fram i uppsatsen.

API: Application Programming Interface. Gränssnitt mot till exempel en tjänst så som Facebook vilket möjliggör informationsutbyte med andra tjänster.

Distribuerade Sociala Nätverk: System för kommunikation där inget enskilt företag eller plats agerar knutpunkt. Det är istället uppbyggt som ett nätverk i likhet med epost.

Informations- och IT-säkerhet: Arbetet med att skydda information och system från åtkomst av obehöriga.

Internet of Things: Samlingsnamn för uppkopplade fysiska objekt som getts möjligheten att skicka och ta emot data om sig själv eller sin omgivning.

IT/ICT: samlingsnamn för Information Technology och Information Communication Technology.

Kommunikationsprotokoll: Överenskommelse mellan parter för hur digital kommunikation ska utformas.

M2M: Machine to Machine-kommunikation: Direkt kommunikation mellan maskiner/objekt utan mänsklig inblandning.

OWASP: Open Web Application Security Project. Oberoende organisation som verkar för att sprida kunskap om säker mjukvaruutveckling

XMPP: Kommunikationsprotokoll från början använt för instant messaging. Föreslås kunna utgöra standard för kommunikation i Internet of Things.

Innehållsförteckning

1. Inledning.....	1
1.1 Bakgrund	1
1.2 Problemformulering.....	2
1.3 Syfte och forskningsfrågor.....	3
1.4 Tidigare forskning.....	4
1.4.1 Tidigare forskning inom XMPP	4
1.4.2 Tidigare tillämpningar av OWASP i forskning.....	5
1.4.3 Forskningslucka	5
1.5 Avgränsningar.....	6
1.6 Kunskapsintressenter	7
2 Teori	8
2.1 Internet of Things.....	8
2.2 Distribuerade sociala nätverk.....	9
2.3 XMPP	11
2.4 Informations- och IT-säkerhet.....	12
2.5 OWASP	13
3. Metod och Genomförande.....	15
3.1 Forskningsstrategi	15
3.2 Forskningsparadigm	15
3.3 Datainsamlingsmetodik.....	16
3.3.1 Informationssökningsstrategi.....	16
3.3.2 Insamling av dokumentation och forskning	17
3.3.3 Intervjuer.....	18
3.3.4 Metodik för dataanalys	19
4. Resultat	20
4.1 Presentation av informanter	20
4.2 Insufficient authorization/authentication	20
4.2.1 Insufficient authorization/authentication i intervjuerna.	20
4.2.2 Insufficient authorization/authentication i dokumentationen	21
4.3 Insecure network services.....	22
4.3.1 Insecure network services i intervjuerna	22
4.3.2 Insecure network services i dokumentationen	23
4.4 Lack of transport encryption	24
4.4.1 Lack of transport encryption i intervjuerna.....	24
4.4.2 Lack of transport encryption i dokumentationen	25

4.5 Privacy concerns.....	26
4.5.1 Privacy concerns i Intervjuerna	26
4.5.2 Privacy concerns i Dokumentationen.....	26
4.6 Insufficient security configurability	27
4.6.1 Insufficient security configurability i Intervjuerna	27
4.6.2 Insufficient security configurability i dokumentation	27
4.7 Insecure Software/Firmware.....	28
4.7.1 Insecure software/firmware i intervjuerna	28
4.7.2 Insecure Software/Firmware i dokumentation	28
5. Analys	29
5.1 Insufficient authorization/authentication	29
5.2 Insecure network services	30
5.3 Lack of transport encryption	31
5.4 Privacy concerns.....	31
5.5 Insufficient security configurability	32
5.6 Insecure software/firmware	33
6. Slutsats och diskussion	34
6.1 Slutsats	34
6.2 Reflektioner	36
6.3 Förslag på ytterligare forskning.....	37
7. Källförteckning	38
7.1 Muntliga Källor	38
7.2 Skriftliga Källor	38
7.3 Figurer	42
Bilagor	43
Bilaga 1 - Intervjumall.....	43
Bilaga 2 - OWASP top 10	44

1. Inledning

1.1 Bakgrund

Världen har flera gånger i historien genomgått stora förändringar, revolutioner om man så vill, till följd av ny teknik och nya uppfinningar. Ångmaskinen satte fart på den industriella revolutionen under sent 1700-tal och gjorde det möjligt att på riktigt börja massproducera varor och människor bytte i stor utsträckning landsbygden till förmån för städer. I mitten av 1900-talet började datorn sitt intåg i samhället. Jättelika hallar fylldes av datorer med en beräkningskraft som knappt står i paritet med dagens enklare miniräknare. Sedan dess har utvecklingen gått framåt och datorn är numera en hörnsten i vår civilisation och globala världsledande företag ner till den enskilde individen är beroende av dess existens. Under slutet av 80- och början av 90-talet lades grunden för den senaste av tekniska revolutioner: Internet. Internet etablerade sig i samhället och revolutionerade sättet människan kommunicerade på. Det var nu inte längre någon konst att prata med en person på andra sidan jordklotet, handla kläder hemifrån eller att på både laglig och olaglig väg åtnjuta den senaste musiken. Sedan dess intåg har Internet underlättat revolutioner i mellanöstern, skapat en börskrasch och genererat en helt ny marknad.

Det första steget i Internets utveckling kallades för Web 1.0 och innebar få aktörer som skapade majoriteten av innehåll på Internet och de allra flesta användare enbart agerade konsument av detta innehåll (Viswanathan, 2009). I nuläget befinner vi oss i Web 2.0, en fas där användaren är mycket mer engagerad i skapandet av material men också där interoperabilitet och samverkan mellan användare är centralt (Viswanathan, 2009). Detta blir tydligt med tjänster så som Youtube, Facebook och Instagram. Framtidens Internet kommer dock att skilja sig från dagens på många sätt. Web 2.0 kommer att övergå i Web 3.0, eller som det också kallas "den semantiska webben". Web 3.0 kommer möjliggöra skapandet av så kallade "smarta städer". Web 3.0 innebär en global standard för data och överföring av data vilket möjliggör utbyte och återanvändning av denna data av allt ifrån globala aktörer till enskilda användare samt möjligheten för datorer att själva tolka innehållet på Internet och agera därefter (Shadbolt, Hall, & Berners-Lee, 2006). En globaliserad standard skulle möjliggöra autonom kommunikation mellan maskiner. Det är mer specifikt detta som kommer leda till att man kan skapa "smart cities" eller den smarta staden. I denna stad styrs allt ifrån sophantering, trafikflöden och polisverksamhet till stor del av maskiner som kommunicerar med andra maskiner och utbyter data med varandra (Waher, 2016-04-16).

Grunden till Web 3.0 skapas genom en av de senaste trenderna inom IT/ICT, en trend som innebär att man kopplar upp saker mot Internet som tidigare inte haft möjligheten att kommunicera med sin omgivning (Bowerman, Braverman, Taylor, Todosow & Von Wimmersperg, 2000). Denna nya teknik går under samlingsnamnet Internet of Things, som i detta arbete kommer benämnas som "IoT". Tänk dig ett hem där alltifrån kaffekokaren, värmepumpen, hemlarmet till termostaten kommunicerar med varandra och andra enheter runt om i samhället så har du en bild över hur framtiden kan se ut.

För konsumenten kan IoT innebära vardagstjänster så som att starta ugnen med mobilen eller övervaka sin egen hälsa. Företag kan låta sina maskiner och tillverkningsprocesser reglera sig själva och varna om något går fel. Städer kan effektivisera allt från sophantering till trafikflöden med tillgång till realtidsdata över konsumtion och fordonsrörelser. Men innan denna framtidssyn kan bli verklighet måste ett antal utmaningar överkommas.

Enligt vissa estimat kommer antalet uppkopplade enheter år 2020 ha nått över 20 miljardersgränsen (gartner.com, 25/4 -16). Stora aktörer som IBM och AT&T budgeterar kommande åren miljardtals dollar till sina IoT-avdelningar och exempelvis Samsung har som mål att innan 2020 ska alla sålda produkter vara uppkopplade (Mohammed, 2015).

Dagens web 2.0, består i stor utsträckning av människor som skapar data menad för andra människor att läsa. IoT består i stället av objekt som talar med objekt, så kallad machine to machine communication eller M2M. För att detta ska vara möjligt mellan miljarder olika objekt av olika typ på olika platser i världen krävs enligt forskare en global standard för kommunikation likt TCP/IP för dagens Internet (Tan & Wang, 2010). Flexibiliteten som detta medförde möjliggjorde Internets tillväxt och liknande metoder skulle kunna hjälpa IoT att växa fram på samma sätt. Internets framgång beror enligt forskare och kritiker på att det lyckades lösa nyckelproblemen för att undvika avstanning i tillväxten. Att det tidigt lockade många användare med enkel funktionalitet, byggde på öppna standarder framtagna i samarbete mellan många aktörer och tillät heterogena system att samverka via teknologier så som packets är några av dessa (Hanseth & Lyytinen, 2010). De standarder som bygger upp dagens internet var dock enligt vissa långt ifrån optimala säkerhetsmässigt redan när de infördes och kan inte användas på ett bra sätt för framtidens Web 3.0 där saker ingår. Skaparna av TCP/IP fokuserade på de tekniska problemen för stunden och kunde svårligen ha föreställt sig framtidens behov eller att Internet kunde användas för så mycket brottslig verksamhet (Kolias, Stavrou, & Voas., 2015). Kommunikationsstandarder som slåss om utrymmet finns det gott om och de innefattar bland annat PROBE-IT, ICore, OpenIoT och LinkSmart men de är kvar i förslagsstadiet och ingen har fått momentum (Al-Fuqaha, Guizani, Mohammadi, Aledhari, & Ayyash, 2015).

Det finns en metod, som just nu är i utvecklingsstadiet, som ämnar vara en möjliggörare för IoT. Lösningen använder sig av kommunikationsprotokollet Extensible Messaging and Presence Protocol (XMPP) tillsammans med distribuerade sociala nätverk och globalt autentiserade identiteter för att skapa ett Internet of Things där interoperabilitet och säkerhet tar lika stor plats (Waher, 2016-04-16). XMPP är ett protokoll för kommunikation som idag främst används för olika typer av chatt. Bland annat den kända instant messaging appen Whatsapp använder sig av en något modifierad variant av XMPP (Sahu, 2014). Tanken med en vida spridd tillämpning av XMPP är alltså att lösa nämnd problematik.

1.2 Problemformulering

En av de viktigaste aspekterna som måste tas i beaktning är säkerheten. Säkerheten för IoT är mycket viktig då konsekvenserna av en incident i värsta fall kan bli långt allvarligare än vid en incident där exempelvis din bärbara dator utsatts för ett intrång. Läget för säkerhet i de IoT-produkter som existerar idag har dock visat sig bristfällig i stor utsträckning. Det finns

fall där bilar hackats på motorvägen och bromsarna satts ur funktion, där angripare chockar en patients hjärta genom wi-fi access till dennes pacemaker eller där insulin- och morfinpumpar förmås dela ut livshotande doser till sina bärare (Greenberg, 2015). Vad händer om en icke-auktoriserad person kan läsa av alla el- och värmemätare i ett kvarter för att se vilka som är hemma? Det skulle kunna underlätta inbrott i stor skala. Siffror framtagna i en undersökning gjord av ett av världens största It-företag som säljer lösningar inom hårdvara, mjukvara, finanser och tjänster relaterade till IT, Hewlett-Packard Enterprise (HP) där populära produkter som faller under IoT-kategorin analyserats visar på bristerna i dagens säkerhet. 70 % av de undersökta enheterna var öppna för cyberattacker, 90 % av dessa enheter lagrade samtidigt någon form av personuppgifter om användaren och 70 % av enheterna kommunicerade informationen med hjälp av okrypterade nätverkstjänster (HP.com, 2014). Sammantaget målar ovanstående information upp en besvärande bild. Kunskapen om hur viktig säkerheten i framtidens Internet of Things är finns tillgänglig samtidigt som långt mer än hälften av de enheter som i nuläget produceras är öppna för attacker och exploatering. Enligt Joachim Lindborg, CTO på Sustainable Innovations AB, skulle detta kunna bero på det faktum att säkerheten varken syns eller efterfrågas i hög grad av konsumenten och därför ofta ses enbart som en kostnad av tillverkare. Företag väljer då ofta att lägga större fokus på andra aspekter som har större kraft som säljargument hos konsumenter.

Det finns alltså ett behov av ett säkert kommunikationsprotokoll för IoT. Än så länge finns ingen standard och inget protokoll har heller erövrat hela marknaden. XMPP lyfts av sina utvecklare och förespråkare fram som en helhetslösning där säkerhet är en grundbult och lösningar finns på de flesta krav IoT-kommunikation har. Med tanke på de risker osäker kommunikation inom IoT innebär finns det god anledning att någon utomstående granskar dessa påståenden för att det inte enbart skall kunna ses som marknadsföring.

Säkerheten i XMPP behöver säkerhetsställas genom validerade och vedertagna metoder för att på bästa möjliga sätt kunna garantera användarens säkerhet.

1.3 Syfte och forskningsfrågor

Arbetet syftar till att granska om XMPP i kombination med distribuerade sociala nätverk kan åstadkomma tillräcklig säkerhet för att utgöra grunden i framtidens IoT-samhälle. Detta anses vara av vikt då framtiden för IoT nu är på väg att fastslås. En lösning som baseras på teknik med otillräcklig säkerhet skulle potentiellt kunna hindra utvecklingen. Som resultat kommer att produceras en bedömning av hur lämpligt XMPP över Distribuerade Sociala Nätverk är som grund för IoT.

Frågeställningen som arbetet ämnar svara på är således:

1. Hur väl kan XMPP över Distribuerade Sociala Nätverk som IoT-standard hantera de, enligt "OWASP top 10", största hoten emot Internet of Things?

1.4 Tidigare forskning

Här presenteras tidigare forskning runt XMPP. Efter detta motiveras användandet av OWASP genom att lista vetenskapliga artiklar där det använts på ett liknande sätt som detta arbete. Sist motiveras arbetet genom att visa på den forskningslucka som existerar i denna tidigare forskning.

1.4.1 Tidigare forskning inom XMPP

XMPP i kontexten Internet of Things har undersökts i en rad vetenskapliga artiklar som exempelvis Bendel (Bendel m.fl., 2013) och Al-Fuqaha (Al-Fuqaha m.fl., 2015) med flera. Dessa artiklar utvärderar dock inte XMPP utifrån vilken säkerhet man kan uppnå genom att använda sig av protokollet. I Bendel m.fl. behandlas endast XMPP medan studien av Al-Fuqaha är mycket övergripande över möjliggörande teknologier som kan bana väg för IoT-utvecklingen. Här behandlas ett stort antal protokoll så som MQTT och XMPP ytligt i syfte att ge en snabb inblick i möjliggörande teknologier utan att behöva läsa tusentals sidor dokumentation. De fokuserar på interoperabilitet och användbarhet först och främst. Al-Fuqaha anmärker dock kort på protokollens säkerhet och säger om XMPP att det är säkert tack vare just sin decentraliserade uppbyggnad (beskrivs närmare i del 2, teoretiskt ramverk). Denna utvärdering av säkerheten är dock långt ifrån uttömmande då studien även behandlar så många andra aspekter.

Bendel m.fl. använder två fallstudier för att argumentera för XMPP som en lösning för att uppnå realtidskommunikation mellan objekt. De beskriver resultatet som effektivt och mycket skalbart. Ingen fokus läggs dock på säkerheten då artikeln mer fungerar som ett bevis på XMPPs förmåga att agera som det underliggande kommunikationsprotokollet för IoT (Bendel m.fl., 2013).

Forskning har också genomförts på säkerheten i IoT. Sicari m.fl. (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015) tar upp XMPP som lösning på många säkerhetsproblem idag och i framtiden. XMPP nämns i korthet som en del av en lösning och beskrivs i positiva ordalag som säkert tack vare SASL och TLS (krypteringsmetoder som beskrivs i del 4, Resultat) Sicari m.fl. undersöker relativt många olika aspekter men inte efter det ramverk denna artikel använder. Främst utvärderar de olika Europeiska samarbetsprojekt för IoT-teknologier och hur de behandlar säkerhetsaspekter som till viss del överensstämmer med de som OWASPs IoT topp 10 ställer upp. Fokus ligger alltså inte på de olika kommunikationsprotokollen.

Conzon (Conzon m.fl., 2012) är ett annat exempel där en arkitektur baserad på XMPP används för att säkra ett IoT-nätverk. För att beskriva säkerheten behandlas XMPPs förmåga till kryptering med SASL och TLS som i Sicario m.fl. Artikeln är inte heller så uttömmande vad gäller säkerhet som detta arbete.

1.4.2 Tidigare tillämpningar av OWASP i forskning

För att visa på trovärdigheten hos ramverket som används i detta arbete samt OWASP som organisation listas här nedanför ett antal vetenskapliga artiklar som på någon sätt använt material i form av listor, best practices och riktlinjer hämtade från OWASP.

Acharya m.fl. (Acharya, S., Ehrenreich, B. & Marciniak, J., 2015) använder sig av OWASPs Top 10 Web Application Vulnerabilities som ett ramverk för att skapa en checklista av säkerhetskrav som utvecklare av mobila applikationer riktade mot sjukvården ska kunna implementera. Författarna av artikeln har, på liknande sätt som återfinns i detta arbete, använt sig av OWASPs lista i tabellform för att på ett övergripande och enkelt sätt presentera de risker som finns för läsaren.

Guamán m.fl. (Guamán, D., Guamán, F., Jaramillo, D., & Correa, R., 2016) beskriver i denna artikel hur de tillämpat ett antal metoder som OWASP listar för att skydda sig mot XSS(Cross Site Scripting) och SQL-injektioner. Metoderna har implementerats vid utvecklingen av en prototyp till en RESTful applikation. Slutsatsen i artikeln är att OWASPs förhållandevis enkla åtgärder och riktlinjer ger en betydligt ökad säkerhet.

Bann m.fl. (Bann, L. L., Singh, M. M., & Samsudin, A., 2015) presenterar i en artikel från 2015 ett problem som uppstår hos företag som följer metoden BYOD (Bring Your Own Device). BYOD ökar i popularitet och innebär att anställda tar med och använder sina egna mobiltelefoner och datorer på arbetsplatsen. Enligt författarna finns en ökad risk för spear phishing attacker i denna miljö. Spear phishing är attacker som riktar sig specifikt mot en organisation i syfte att komma över konfidentiell data. Den genomförs ofta via epost och fungerar genom att epost med skadlig kod skickas till anställdas e-postadress. Genom att använda sig av OWASPs Risk Rating Methodology skapas och presenteras ett ramverk för införandet av säkra policies.

Adedayo m.fl. (Adedayo, L., Butakov, S., Ruhl, R., & Lindskog, D., 2013) presenterar ett säkert ramverk som ämnar skydda personuppgifter i e-government miljöer i utvecklingsländer. Artikeln är en fallstudie där personuppgiftshanteringen på ett antal ambassader i Nigeria har undersökts. Ramverket som presenteras baseras på OWASPs Application Security Verification Standard. Där ingår verktyg för att kontrollera webapplikationers tekniska säkerhet men också riktlinjer för säker utveckling. Artikeln använde sig också av OWASPs Top 10 Web Application Vulnerabilities för att visa på de risker som finns inom e-governance.

1.4.3 Forskningslucka

Som man kan se i tidigare forskning har XMPP undersökts på en mängd olika sätt. Dock har säkerheten sällan något stort fokus och OWASP har inte påträffats i kombination med XMPP någon gång. Detta gör att det existerar en forskningslucka som detta arbete ämnar fylla.

En sökning via Uppsala universitetsbiblioteks sökmotor på nyckelorden XMPP samt OWASP ger endast 15 träffar där ingen av dem är relevant. Även Google Scholar returnerar mycket få artiklar vid samma sökning. Detta tyder på att denna typ av undersökning ej tidigare genomförts på det sätt detta arbete är utformat. En undersökning av ett specifikt kommunikationsprotokoll för IoT utifrån OWASPs rekommendationer verkar ej tidigare ha publicerats. Hela ämnet Internet of Things är relativt nytt jämfört med många andra teknologier vilket kan förklara bristen på liknande studier.

1.5 Avgränsningar

I detta arbete kommer endast den säkerhetsmässiga lämpligheten för XMPP över Distribuerade Sociala Nätverk att undersökas. Det kan finnas andra orsaker till varför denna lösning är lämplig eller olämplig men det kommer inte att behandlas.

Säkerhet avser i detta arbete de aspekter som tas upp i OWASPs top 10 Internet of Things Vulnerabilities som förklaras närmare under rubrik 2.2 (OWASP.org, 2016a). Ett antal av de aspekter som finns med i listan bedöms dock inte vara relevanta i sammanhanget då arbetet endast ämnar undersöka säkerheten hos ett kommunikationsprotokoll med tillhörande koncept som aldrig har för avsikt att åtgärda vissa av de problem som ställs upp av OWASP.

De delar ur OWASP Top 10 IoT Vulnerabilities som därför inte kommer att behandlas är som följer:

1. Insecure web interfaces
2. Insecure mobile interfaces
3. Insecure cloud interfaces
4. Poor physical security

Punkterna 1-3 har utelämnats av samma anledning. De behandlar alla någon form av säkerhetsluckor i olika användargränssnitt och är därför oberoende av det underliggande kommunikationsprotokollet. XMPP-nätverk ämnar inte lösa problem så som cross site scripting, SQL-injektioner, implementering av lösenordsstandards eller att användaren låses ute från enheten efter 3 felaktiga inloggningsförsök. Även om XMPP vore 100% säkert i sig självt skulle luckor i användargränssnittet, till följd av fel eller misstag begångna av tillverkare och utvecklare, underminera säkerheten.

Dålig fysisk säkerhet innebär bland annat att man kan komma åt känslig information, ta över en enhet eller ta sig in i ett nätverk via fysisk kontakt med aktiva portar och kontakter. Detta är ingenting som XMPP eller något annat kommunikationsprotokoll för den delen ämnar åtgärda och därför anses denna punkt vara irrelevant för arbetet.

Det finns en mängd olika protokoll som kan tillämpas för kommunikation inom IoT. I detta arbete kommer enbart Extensible Messaging and Presence Protocol (XMPP) behandlas. Den

största anledningen till detta är att det funnits god tillgång till och kontakt med specialister på just XMPP samt att det finns relativt god tillgång till facklitteratur.

1.6 Kunskapsintressenter

Gruppen intressenter till denna studie är relativt bred då den innefattar allt från utvecklare och tillverkare av IoT produkter, standardiseringsorgan för IoT, utvecklare av XMPP och andra IoT relaterade protokoll samt användare av IoT som är mer intresserade av området än enbart som konsumenter. Resultatet kommer visa de fördelar som finns men även peka på de eventuella brister som existerar hos XMPP-baserade nätverk utifrån aspekter satta av en icke vinstdrivande organisation med gott rykte. Därför finns det ett värde i arbetet då det förhåller sig neutralt till olika lösningar och endast genomför en saklig analys.

2 Teori

I denna del presenteras arbetets mer centrala begrepp närmare för läsaren.

2.1 Internet of Things

Ingen exakt fastslagen definition existerar som beskriver vad IoT är då ingående tekniker och koncept kan varieras mycket. I detta arbete kommer därför International Telecommunications Unions (ITU, 2012) definition att gälla. ITU är FN:s organ för ICT-frågor. Dess definition beskriver IoT som:

“A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.”

Internet of Things är ett brett begrepp som syftar på det nya Internet där även fysiska saker ingår. Detta genom att sakerna förses med till exempel processorer, sensorer och sändare i syfte att ge möjligheten att sända och ta emot data. Slutmålet är att i princip allt ifrån små personliga saker till industriella objekt så som verkstadsmaskiner, flygplansmotorer eller hela fartyg skall ingå i ett nätverk och också vara en del av Internet. Syftet är att effektivisera olika processer för att gynna ekonomi, miljö och andra områden i det växande samhället (iotsverige.se).

Vikten av detta nya steg i utvecklingen av informationssamhället blir tydligt när prognoser visar att antalet uppkopplade enheter i världen beräknas uppgå till 20 miljarder år 2020. Det kommer att skapa stora ekonomiska möjligheter för bland annat energi-, fastighets-, och sjukvårdsbranscherna i Sverige. Det faktiska framtida monetära värdet är svårt att beräkna men förväntas uppgå till mångmiljardbelopp (kungl. ingenjörsvetenskapsakademien, 2013).

Vägen fram till dagens och framtidens Internet of Things kan beskrivas som framtagandet av en rad separata teknologier som tillsammans möjliggör uppkopplingen av fysiska objekt. Från radion på 1800-talet, datorn och streckkoden via RFID-taggen (Radio frequency identifier) till dagens teknologiska miljö. Just RFID är en mycket viktig möjliggörare som inte behöver fri sikt för att läsas av till skillnad från en streckkod. Det finns också varianter som inte behöver en kraftkälla utan får energi i avläsningstillfället av de elektromagnetiska vågor avläsaren transmitterar (Want, 2006). Dessa teknologier har först nyligen sjunkit så mycket i tillverkningskostnad att storskalig implementation möjliggjorts. Ett tidigt exempel på en uppkopplad sak är när en läskautomat på Carnegie Mellon School of computer science i USA försågs med sensorer så att personalen kunde se på sina datorer när den behövde fyllas på. Om man jämför denna enkla tillämpning med till exempel ett elkraftsbolag som har sensorer som mäter alla dess kunders elförbrukning i realtid eller städer som exakt vet hur trafiksituationen ser ut tydliggörs hur stor tillämpning IoT kan ha. Begreppet Internet of things fick fäste runt sekelskiftet men har tagit fart de senaste åren (Press, 2014).

2.2 Distribuerade sociala nätverk

Distribuerade sociala nätverk skiljer sig från traditionella centraliserade varianter som till exempel Facebook eller Instagram där tjänsteleverantören kontrollerar all information och dess flöde. Istället fungerar den distribuerade arkitekturen mer som eposttjänster där vem som helst kan ha en e-postserver hos sig och informationen sparas där (Tramp, Frischmuth, Ermilov, Shekarpour & Auer 2014). Motsatsen till distribuerade nätverk är centraliserade nätverk. Dessa existerar som silos, där data samlas och kontrolleras och möjligheten att kommunicera mellan olika silos begränsas. Även om det exempelvis går att lägga upp en bild både på Facebook och Instagram samtidigt med ett knapptryck eller logga in med hjälp av Facebook på olika sidor är detta inte exempel på att de båda använder kommunikationsmetoder som fritt kan tolkas mellan dem. APIer för Facebook finns för exempelvis inloggning, delande från andra sidor till Facebook-flödet med mera. Dessa båda aktörer erbjuder alltså ingen universell möjlighet att kommunicera över plattformsgränser utan isolerar sin användarbas samt skyddar data de genererar. Tekniskt sett skulle det inte vara komplicerat att erbjuda en plattformsoverskridande kommunikation, men det finns inget intresse hos de stora aktörerna att göra så då de i nuläget kontrollerar enorma användarbasen. Sann interoperabel kommunikation innebär i stället det som XMPP ämnar införa.

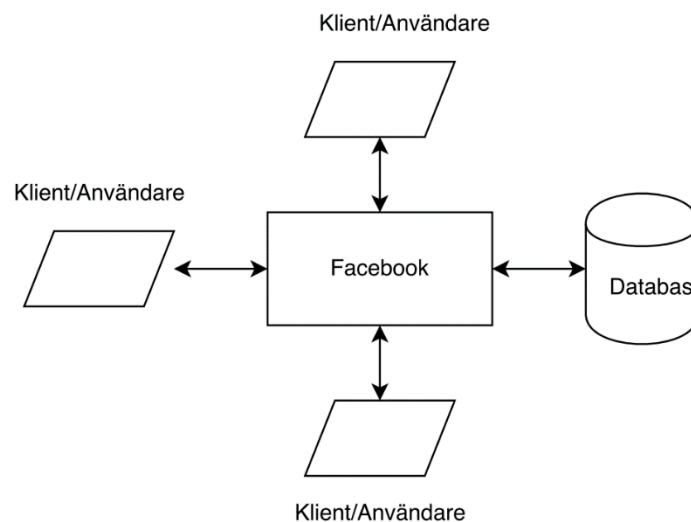


Fig 1. Den traditionella bilden av internetbaserade sociala nätverk. All kommunikation går via leverantören och denne sparar kommunikation i en databas som användare ej har tillgång till.

Genom att i stället basera det sociala nätverket på kommunikationsprotokoll likt eposttjänster som sedan kan tolkas mellan olika leverantörer via API:n och tjänster får man en decentraliserad struktur som möjliggör ett samarbete mellan aktörer i det sociala nätverkslandskapet. Den typ av socialt nätverk som behandlas i detta arbete är dock inte av samma karaktär som Facebook eller Instagram. Det har inget grafiskt interface för att utbyta privat information utan är till för att olika typer av IoT-objekt ska kunna kommunicera med varandra. Den sociala aspekten finns där tack vare att alla entiteter som kommunicerar har registrerade relationer som möjliggör utbyte av data. En enhets relationslista kan liknas vid en vänlista på till exempel Facebook. De XMPP-servrar som i dagsläget används för messaging har dock gränssnitt för att registrera nya användare (Waher, 2016-04-16).

Vinsten av att ha dem distribuerade är att man underlättar samarbetet, eller federeringen, av många olika aktörer så att IoT kan bli en globalt interoperabel kommunikationsplattform. En stor användarbas är nödvändigt för att en teknologi ska kunna evolvera (Hanseth & Lytinen, 2004). Med detta hoppas personer som Peter Waher att IoT kan göra samma framgångsresa som Internet.

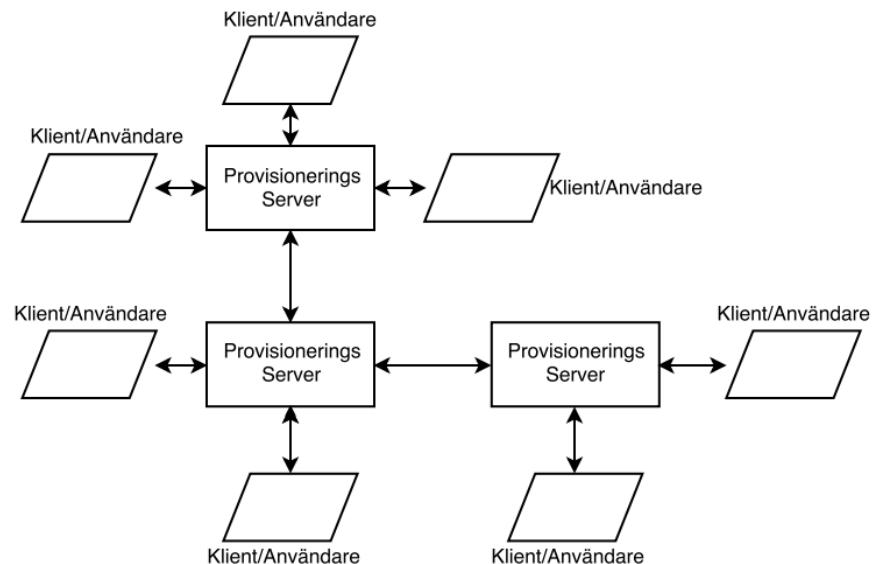


fig 2. I ett XMPP-nätverk finns istället ingen central kontrollerande entitet. Det är ett nätverksbaserat system där en användare själv kan välja vilken leverantör av provisioneringsserver som är lämpligast för ens behov. Det är också möjligt att själv driva en server och på så sätt få full kontroll över alla aspekter av kommunikationen.

Klienter i bilden ovan är alltså smarta objekt i ditt hem medan användare är du själv. Kommunikationen i IoT-implementationen av detta system består av olika data som skickas mellan smarta objekt och inte IM-meddelanden som i de traditionella centraliserade nätverken.

Federering i detta sammanhang syftar på den samarbetande och distribuerade struktur som föreslås ligga till grund för IoT-infrastrukturen. Den består av många heterogena tjänster som ingår en federation för att möjliggöra interoperabilitet över större nätverk. Tjänster och tjänsteleverantörer kan vara konkurrenter men ändå möjliggöra kommunikation mellan sig då de livnär sig på själva kommunikationslösningen snarare än samlandet av data och användare i silos enligt ovan (Schuster m.fl., 2014). För att illustrera konceptet kan Schuster m.fl. modell för att samla objekt i så kallade Multi User Chatrooms (MUC) användas. Där kan enheterna sedan skicka och ta emot data till rätt enheter. Enheter och användare får unika identifierare liknande en e-postadress. I figur 3 illustreras detta. Smarta objekt samlas i MUCer på servrar som sedan kommunicerar med andra servrar inom sin egen tjänsteleverantör eller andras. XMPP möjliggör detta med sin extension för discoveryfunktionalitet. Tack vare detta tillägg finns verktyg för att upptäcka information om andra enheter som exempelvis vilka metoder de erbjuder (Hildebrand, Millard, Eatmon & Saint-Andre, 2008) Dessa MUCs skulle i framtiden existera som relationer mellan objekt på de provisioneringsservrar som hanterar IoT-nätverket.

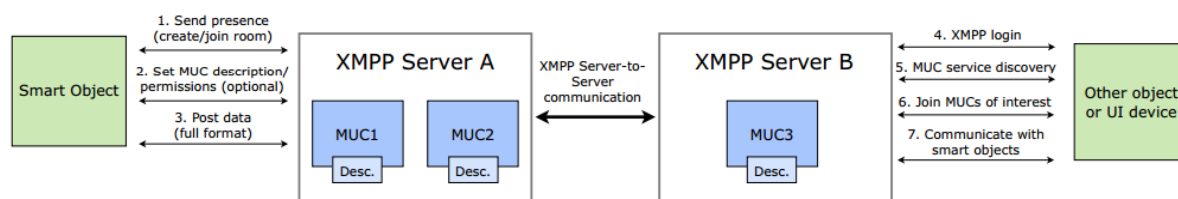


fig 3. Konceptuell modell över XMPP-kommunikation i MUC via federerade tjänsteleverantörers servrar. (Schuster m.fl., 2014)

Provisionering är den tjänst som håller reda på vilka enheter som får kommunicera med varandra genom att lagra listor på ett objekts godkända och/eller icke godkända kontakter med andra objekt (Waher, 2016). Denna tjänst kommer i framtiden att hanteras på servrar så som XMPP-servrar i dagsläget hanterar relationer mellan användare för instant messaging.

2.3 XMPP

XMPP står för Extensible Messaging and Presence Protocol och är ett XML-baserat kommunikationsprotokoll som från början använts för instant messaging, multi-party chatt, röst- och videosamtal, som lättvikts middleware (hantering av identifiering, autentisering och säkerhet mellan två mjukvaror), närvarohantering (underlättar för upptäckbarhet samt tillgänglighet av olika services och andra enheter lokalt eller över nätverk) samt transport av XML-data (xmpp.org, 2016a).

Inom informationsteknologi beskrivs ett kommunikationsprotokoll som en uppsättning regler och procedurer som behandlar hur data skickas mellan enheter som till exempel datorer och mobiltelefoner och ställer krav på vilket format som den kommunicerade datan ska ha. Detta är avgörande för digital kommunikation då en dator som tar emot felaktigt formaterad data inte kan använda denna. Dessa protokoll konstrueras ofta av internationella intresseorganisationer (Encyclopaedia Britannica, 2015).

1999 lades grunden för meddelande- och närvarotjänsten “Jabber” som tillsammans med tillhörande kod-bibliotek, open source klienter och protokoll för streaming av XML-data senare övergick till att bli XMPP. Idag utvecklas kärnan av protokollet av organet Internet Engineering Task Force (IETF) medan XMPP Standards Foundation står för kontroll av XEPs (Extension Protocols) samt förslag på nya XEPs. Protokollet är decentraliserat och fungerar som e-post vilket innebär att vilken användare som helst kan sätta upp en XMPP-klient. Dokumentationen för dess kärna kallas XMPP core (XMPP.org, 2016c).

XEPs är extensions(förlängningar/utökningar) till XMPP protokollet och innebär att man adderar funktionalitet till det existerande protokollet. Vem som helst kan skicka in förslag på nya extensions. XMPP Standards Foundation utvärderar dessa förslag och kan sedan välja att publicera dem på XMPP.org. Publicerade XEPs får olika typer av status vilken visar på hur accepterad och utvecklad en XEP är. Redan godkända XEPs kan också tas bort eller

modifieras beroende på nya råd och rön. Under arbetet med studien fanns 372 XEPs i olika stadier. Vissa är tagna i drift medan andra är i utvecklingsstadiet och några väntar på att bli godkända. En XEP kan behandla allt från best practices i hur man hanterar DDOS-attacker (XEP-0205) till Peer-to-Peer mediaöverföring (XEP-0166) och hantering av användarnamn (XEP-0172). XEP-0323 till och med XEP-0326 och XEP-0347 hanterar Internet of Things vilket gör dem intressant i arbetet.

För att kunna identifiera och kommunicera med aktörer på XMPP-nätet skapar aktörerna så kallade JIDs (Jabber Identifications) (XMPP.org, 2016b). En aktör kan vara allt från en enhet i hemmet till en person eller ett företag. En JID ser ut som en helt vanlig email-adress på formen namn@domän.toppdomän/Resurs. Exempelvis skulle ett larmsystem hemma hos Kalle kunna använda adressen larm@telia.se/inbrottslarm där Kalle använder sig av en XMPP-server som ägs av Telia. "Resurs" exponerar en specifik resurs som finns kopplad till en adress. Alltså skulle Kalles larm också kunna exponera sitt brandlarm på liknande sätt med ../Brandlarm. Hur man väljer att exponera resurser är helt upp till användaren själv. En JID kodas i UTF-8 och de tre delarna "namn", "domän" och "resurs" får innehålla 1024 bytes. Det gör att en JID kan innehålla drygt 3000 bytes vilket gör att systemet med JIDs täcker det nuvarande systemet med IPv6-adresser flera hundra miljarder gånger om (Lindborg, 2016-04-12). Detta kommer i framtiden vara en viktig styrka då, som tidigare förklarats, antalet enheter i behov av adresser beräknas bli enormt.

2.4 Informations- och IT-säkerhet

Informationssäkerhet är arbetet med att skydda information från åtkomst av obehöriga (dess konfidentialitet), påverkan (dess riktighet) samt förhindrande av tillträde (dess tillgänglighet) (Andersson, 2015). Detta är de tre grundkraven som måste uppnås för att information ska anses vara säker. För att åstadkomma detta krävs arbete på alla nivåer av till exempel ett företag eller en myndighet. Dessa olika arbetsområden är exempelvis organisatorisk säkerhet som syftar till organisationens arbetsrutiner som att utbilda personal och liknande. Ett annat exempel är detta arbetes huvudfokus, teknisk säkerhet. Detta berör de delar av systemet som är till för att skydda informationen. Här ryms både mjukvara så som krypteringstekniker men också fysisk säkerhet. Ytterligare ett steg ner hittas IT-säkerhet som utgörs av datasäkerhet, alltså att skydda data på olika sätt, samt kommunikationssäkerhet som ämnar skydda kommunikation inom och utanför organisationen.

En jämförelse med OWASP topp 10 visar att det är just IT-säkerhet som ligger i fokus för denna lista och arbetet i stort. Detta har valts då lösningen XMPP och distribuerade sociala nätverk adresserar dessa i första hand snarare än organisatoriska aspekter av säkerhet.

2.5 OWASP

Open Web Application Security Project (OWASP) är en ideell icke vinstdrivande organisation med målet att vara drivande för transparens och säkerhet i mjukvara. Organisationen bildades i USA 2001. All dess programvara är open source (owasp.org, 2016b). Produkter som OWASP levererar sträcker sig från böcker och standarder till olika verktyg för test av applikationer. Allt för att främja säker utveckling av mjukvara.

OWASPs topp 10 lista är en sammanfattning av de punkter som anses utgöra de största sårbarheterna hos IoT. Dessa inbegriper allt från fysisk säkerhet till kryptering av data. Listan är en del av ett större skalprojekt inom IoT som drivs för att aggregera kunskap och riktlinjer för säker utveckling av IoT.

Detta ramverk valdes då det täcker in de viktigaste aspekterna av säkerhetshot mot IoT och som visats under punkten tidigare forskning är det en vedertagen metod som tidigare använts för att utvärdera säkerheten inom både IoT och andra IT-relaterade miljöer. På grund av omfattningen är dock allt inte relevant vilket nämndes i 1.5, Avgränsningar. Enbart de i denna studie ingående delarna beskrivs här. För den fullständiga listan hänvisas till OWASP.org samt bilaga 2.

Inga reella alternativ kunde hittas för att lista säkerhetsproblem just inom IoT. Andra rekommendationer existerar som till exempel ISO 27000-serien av standarder rörande informationssäkerhet men bedömdes för breda då de behandlar inte bara tekniska aspekter utan allt annat så som organisation och ledning.

I nedanstående tabell presenteras de punkter hämtade ur OWASPs lista som kommer användas i detta arbete (De förklaras närmare i del 4, Resultat):

Huvudproblem	Förklaring
Insufficient authorization/authentication (Otillräcklig autentisering/auktorisering)	Autentisering är kontrollen att någon är den som den påstår sig vara (Microsoft, 2016a) medan auktorisering är bestämmelser kring vad den autentiserade enheten har för rättigheter i systemet (Microsoft, 2016b). Detta måste göras på ett säkert sätt för att förhindra tillträde för obehöriga.
Insecure Network Services (Osäkra nätverkstjänster)	Nätverkstjänster är applikationer, t.ex. Domain name System, i nätverkslagret och sköter allt ifrån lagring till facilitering av kommunikation. Angripare kan använda inbyggda fel eller felkonfigurationer i dessa tjänster för att manipulera eller stjäla data samt störa ut eller ta över system, hela nätverk eller enskilda enheter. Penetrerade enheter kan dessutom användas för att attackera ytterligare nätverk och system.
Lack of transport encryption	Transport av meddelanden mellan servrar samt till och från klienter skall krypteras för att undvika

<p>(Brist på kryptering vid transport)</p>	<p>möjligheten till avlyssning. Görs inte detta riskerar man brister i konfidentialitet om någon lyckas läsa meddelanden under transport. Förflyttningen kan vara mellan servrar eller mellan server och klient. Detta kan utgöra ett mycket allvarligt hot mot exempelvis den personliga integriteten om persondata skickas okrypterat. Att avläsa meddelanden på detta sätt kallas för en “man in the middle”-attack då angriparen placerar sig själv mellan två kommunicerande entiteter. Man kan då få tillgång till större delar av systemet genom att avläsa autentiseringsdata.</p>
<p>Privacy concerns (Integritetsproblem)</p>	<p>Personlig integritet i sammanhanget definierar OWASP som sårbarheter i vilken data som system samlar in, hur denna data skyddas efter insamlande och vid transport samt vem som har tillgång till datan.</p>
<p>Insufficient security configurability (Otilräcklig säkerhetskongfigurabilitet)</p>	<p>Möjligheterna att konfigurera säkerhetsinställningar för att uppnå god säkerhet beroende på implementation. Vissa system kräver större säkerhet än andra. Detta regleras främst genom administratörers gränssnitt och vilka möjligheter som där finns för konfiguration. Exempel på inställningar kan vara tvång av starka lösenord, krypteringsinställningar samt administratörsfunktioner och superanvändarstatus.</p>
<p>Insecure software/firmware (Osäker mjukvara/mjukvara inprogrammerad i enheter)</p>	<p>Applikationer är inte säkra över tid och måste uppdateras för att täppa till säkerhetshål. Detta måste utföras säkert för att undvika avlyssning bland annat. Firmware är den mjukvara som styr hårdvara i form av exempelvis enheter i IoT. Uppdateringar måste ske både för servrar och enheter.</p>

fig 4. Sammanfattning av definitioner för OWASPs lista över sårbarheter (owasp.org, 2016a).

3. Metod och Genomförande

Här redogörs för de vetenskapliga metoder som använts och argument för dess användande framförs. Först presenteras forskningsstrategin i allmänhet samt den paradigm arbetet förhåller sig till. Därefter behandlas datainsamling och sist tas de analysmetoder upp som applicerats på insamlad data.

3.1 Forskningsstrategi

Målet för arbetet är att utvärdera XMPP över distribuerade sociala nätverk ur ett säkerhetsperspektiv och bedöma dess säkerhetsmässiga lämplighet som grund för IoT. Som ramverk används OWASPs lista över sårbarheter. Den information som inhämtas via intervjuer kontrolleras med hjälp av information främst i den tekniska dokumentation som utgör XMPP. Arbetet definieras som en kvalitativ intervjustudie som kompletterats med forskning och teknisk dokumentation om protokollet som undersöks. Detta arbetsätt bedöms ge den djupkunskap som krävs för att kunna göra bedömningar av lämpligheten i lösningen.

Intervjuinformation tillsammans med bekräftande eller dementerande uppgifter från andra källor utgjorde sedan grunden för att bedöma lämpligheten för varje punkt i OWASPs lista. I de fall där intervjuernas uppgifter inte kunde styrkas med andra källor påpekas detta och anses vara en brist. Intervjuer valdes då dessa gav djup förståelse för de tekniska aspekterna av ämnet. De personer som intervjuades arbetar själva med XMPP och är experter på området. På grund av den begränsade tiden som stod till förfogande var det nödvändigt att inhämta denna typ av hjälp för att förstå ämnet. Efter detta kunde XMPPs dokumentation analyseras vidare. Andra litterära källor används i begreppsförklarande syfte när så är nödvändigt.

3.2 Forskningsparadigm

I och med arbetets utformning som en övergripande studie baserad på intervjuer, insamling av teknisk dokumentation och tidigare forskning kommer den vetenskapliga grundparadigm som styr vara interpretivism. Den stämmer mycket bra in på denna typ av forskning då den grundar sig på problemet att förstå och tolka sociala kontexter och sammanhang. Människan kommer att vara i fokus i synnerhet i intervjuarbetet men även i andra källor då denna kommer att behandla data producerad av människor för människor och således är föremål för samma sociala processer, sammanhang och åsikter som intervjuer. Resultatet kan förväntas präglas av de karaktärsdrag för interpretivism som kursboken beskriver som till exempel multipla subjektiva åsikter, forskarreflexivitet, kvalitativdataanalys och multipla tolkningar. Enligt samma författare är det dessutom viktigt att vid interpretivistiska studier fokusera på bland annat trovärdighet, verifierbarhet och kredibilitet (Oates, 2006, s.261-272).

3.3 Datainsamlingsmetodik

Som tidigare nämnts har två datainsamlingsmetoder använts: intervjuer och insamling av teknisk dokumentation samt forskning. Detta kallas för “metodtriangulering”. Enligt Oates rekommendationer räcker dessa två metoder för att uppnå detta (Oates, 2006, s. 49). Genom att använda mer än en metod minskar sannolikheten att felaktig data samlas in och ger flera aspekter på samma data. Genom metodtriangulering stärks kvalitén i data samt skapar ett mer vetenskapligt och intressant resultat. Det blir möjligt att kontrollera resultat från den ena källan mot resultat från den andra. De dokument som analyserats har samlats in enligt informationssökningsstrategin som presenteras nedan. De utgör grunden för kunskapsinhämtningen om XMPP och distribuerade sociala nätverk.

3.3.1 Informationssökningsstrategi

Efter att arbetets forskningsfråga fastställts och information inhämtats från intervjuer påbörjades insamling av information från andra källor. Denna användes sedan för att kontrollera uppgifter från intervjuerna.

informationssökningen påbörjades med att målsättningen fastställdes enligt följande:

- Sök forskning publicerad inom säkerhet kopplad till Internet of Things.
- Sök information om hot och risker kopplat till IoT i dagsläget.
- Sök forskning som visar på hur man kan skydda sig emot eventuella hot och risker kopplade till IoT.
- Sök övergripande information som behandlar det teoretiska ramverket så som XMPP, IoT, säkerhet med mera.
- Finns publicerade fallstudier där XMPP har använts framgångsrikt eller inte framgångsrikt?

För att underlätta sökning användes en sökordsmatris. Begreppen användes både individuellt samt i kombination med varandra för att generera så många relevanta resultat som möjligt.

Sökord	IoT	Security	XMPP	Forskning	Distribuerade Sociala Nätverk	OWASP
Synonymer och närliggande termer	Internet of things	Integrity	Extensible Messaging and Presence Protocol	Research	DSN	Open Web Application Security Project
	Sakernas internet	Risks	XMPP extensions	Case study	Distributed Social Networks	OWASP Top 10 IoT Vulnerabilities
	Connected devices	Vulnerability	Jabber	Förberedelser	Federated Social Network	
	Machine to Machine	Threats	XEP	Assessment	Decentraliz-ed Social Network	

fig 5. Sökordsmatris

Med dessa verktyg genomsöktes databaserna Google scholar, scopus samt ub.uu.se. Dessa representerar stora databaser med relevanta och granskade artiklar som förväntas upprätthålla god vetenskaplig standard.

3.3.2 Insamling av dokumentation och forskning

Insamlingen av forskning och facklitteratur har följt den informationssökningsstrategi som beskrivs i föregående del. Den största delen information som inhämtats har dock inte kommit ifrån forskning utan istället ifrån den tekniska dokumentation som finns att tillgå via XMPP Standards Foundations hemsida XMPP.org samt deras lista över publicerade tillägg XMPP.org/Extensions.

För att kunna få fram rätt typ av dokumentation krävs först god kunskap om den punkt i OWASP som ska behandlas, sedan gallras rätt information manuellt fram ur den databas av dokumentation som finns tillgängligt på tidigare nämnda hemsidor.

Dokumentationen som samlats in är kvalitativ vilket betyder att den består av löpande text. Därför har informationen analyserats kvalitativt. Viss forskarreflexivitet kan därför ha förekommit. Informationen har dock hämtats för att besvara redan ställda påståenden så denna subjektivitet bör vara begränsad.

3.3.3 Intervjuer

En intervju är en strukturerad konversation där en part ställer frågor till en annan. Syftet är att insamla djupare kunskaper och information om det ämne man vill undersöka (Oates, 2006, s. 172-182). Personerna som intervjuades valdes med hjälp av bekvämlighetsurval då de var tillgängliga och innehade relevant kunskap. En intervjuguide togs fram enligt rekommendationer av Alan Bryman och de säger att frågor som ställs i en kvalitativ intervju ska hållas så öppna som möjligt för att konversationen inte ska begränsas utav förutfattade meningar utan följa en väg som uppkommer organiskt under samtalet (Bryman, 2011, s. 419-427). Således presenterades de olika OWASP punkterna för intervjuobjektet som sedan fick diskutera ämnet ur den synvinkeln som han själv tyckte passade. Detta i kombination med ett semistrukturerat intervjuupplägg gav balans mellan att ge intervjuobjekten frihet att förklara men ändå inte förlora fokus ifrån det relevanta. Nya frågor och följdfrågor tilläts uppkomma så länge de var relevanta för arbetet.

Intervjuer genomfördes både ostrukturerat samt semistrukturerat beroende på dess syfte. Inledningsvis önskades en bred diskussion om ämnet i allmänhet med experter. Följaktligen användes det ostrukturerade intervjuupplägget enligt Oates (2006, s. 173) för den första intervjun med Peter Waher. Först presenterades ämnet och vad arbetet var tänkt att behandla. Utifrån detta fördes en öppen diskussion för att uppnå en djupare förståelse.

- 2016-04-12: Intervju med Peter Waher via Skype. Enligt Oates (2006, s. 192) användes så kallade "Field Notes" genom anteckningar på dator.

Följande intervjuer genomfördes på ett semistrukturerat sätt där frågor och teman bestämdes i förväg men tid avsattes för diskussion och följdfrågor:

- 2016-04-28: Intervju med Joachim Lindborg via Skype. Ljudupptagning med hjälp av mobiltelefon.
- 2016-05-06: Intervju med Peter Waher via Skype. Ljudupptagning med hjälp av mobiltelefon

Då Peter Waher och Joachim Lindborg båda, på sidan om sitt vanliga arbete, aktivt arbetar som en del av XMPP Standards Foundation är de att betrakta som partiska vad gäller XMPPs duglighet i alla avseenden. Hänsyn har tagits till detta dels genom att förbereda intervjuerna med de frågor som skulle besvaras för att undvika allt för mycket utsvävande om för respondenterna relevanta aspekter. Waher och Lindborg valdes som intervjuobjekt, dels för enkelhetens skull då tid varit en faktor som spelat in och de varit lättillgängliga och ställt upp på kort varsel, men framförallt för att de besitter väldigt mycket expertis inom ett förhållandevis smalt område. Det hade varit en fördel att finna flera intervjuobjekt som kunnat anses som opartiska eller som till och med motarbetar XMPP. Fler utlåtanden om XMPP hade givetvis också varit önskvärt ifrån andra experter. Detta har dock av tidsskäl prioriterats bort till förmån för att skapa så djup förståelse som möjligt för ämnet. Arbetet hade med stor sannolikhet uppnått högre kvalité om mer tid hade kunnat spenderas på ytterligare intervjuer.

Efter att förståelse för de tekniska aspekterna av XMPP uppnåtts lades fokus både under intervjuerna samt i analysen av de andra källorna på att hitta säkerhetsproblem hos XMPP som föll under någon av punkterna i OWASPs lista.

Intervjuer som datainsamlingsmetodik har ett antal nackdelar enligt Oates. Dessa har dock mildrats i så stor utsträckning som möjligt. Bristen på reliabilitet som kan bli en följd av att de skildrar personers subjektiva åsikter eller att själva intervjuprocessen påverkar svaren bör inte påverka informationen då intervjuguiden utgår från OWASPs säkerhetsaspekter och uppgifter kontrolleras mot andra källor (Oates, 2006).

3.3.4 Metodik för dataanalys

Den insamlade informationen består av kvalitativ data och analyserades således med kvalitativa metoder enligt Oates (2006, s. 240-249). Materialet från andra källor i form av dokumentation och liknande sammanställdes till samma format i form av sammanfattningar digitalt för att göra den redo för dataanalys.

Intervjuernas anteckningar transkriberades genom tema- och nyckelordsanalys efter varje intervjutillfälle. Inledningsvis delades data in i tre teman. Det som var direkt irrelevant för arbetet, det som gav bakgrund och generell information om ämnet samt det som direkt gav information som möjliggjorde besvarandet av forskningsfrågan. Därefter användes deduktiv metod för temaanalys för att bestämma teman. Punkterna i OWASPs lista användes här som teman. Detta ansågs lämpligt då det var runt dessa som data söktes och intervjuguiden byggts utefter detta. Som underteman till dessa punkter sattes sedan styrkor och svagheter. personliga meriter var det sista temat och behandlade allt som hade med de intervjuades personinformation, arbete och liknande att göra. Teman blev alltså enligt följande (de sex huvudpunkternas underteman visas ej):

- Personliga meriter
- Insufficient authorization/authentication
- Insecure network services
- Lack of transport encryption
- Privacy concerns
- Insufficient security configurability
- Insecure software/firmware
- Övrigt

4. Resultat

Här presenteras först informanterna, sedan data som insamlats via intervjuer, litteratur och dokumentation. Datan presenteras under respektive punkt utefter OWASPs lista. Först behandlas det som framkommit under intervjuerna och sedan information som antingen stödjer eller motsäger detta från dokumentation och litteratur.

4.1 Presentation av informanter

Intervjudelen i detta kapitel är resultatet av intervjuer med två experter inom XMPP. Dessa personer är:

Peter Waher

Tidigare CTO på Clayster men innehar numera titeln Smart City Architect på konsultbyrån Giraff där han forskar på säkra och interoperabla lösningar för Internet Of Things. Han är också en aktiv medlem i XMPP Standards Foundation sedan 2012. Peter har tidigare författat boken “Learning Internet of Things” samt utvecklat elva extensions till XMPP.

Joachim Lindborg

CTO på Sustainable innovation med mångårig erfarenhet som systemarkitekt. Även Joachim är en aktiv medlem av XMPP standards foundation sedan 2012.

4.2 Insufficient authorization/authentication

4.2.1 Insufficient authorization/authentication i intervjuerna.

Enligt Peter Waher är SASL möjlig att använda även i små enheter med begränsad prestanda då enheten kan kontrollera alla förfrågningar som inkommer mot sin provisioneringsserver. Servern skickar då en lista med vilka metoder som är tillgängliga för den, enheten loopar igenom listan en gång och väljer autentiseringsmetoden (Waher, 2016-05-06). Även sessioner stöds vilket innebär att inaktivitet leder till att denna avbryts efter en bestämd tid och ny inloggning måste ske.

En specifik spoofing-attack mot SASL går ut på att låtsas vara en XMPP-server utan ett giltigt certifikat. Enheter som ansluter mot en servern kanske inte är tvingade via inställningar att kontrollera om servern har ett certifikat. Är klienten sedan vidare felinställd kan servern begära krypteringslös kommunikation och komma över inloggningsuppgifter i klartext (Waher, 2016-05-06).

För att säkerställa säker autentisering ligger alltså mycket av ansvaret på provisioneringsservern som måste vara konfigurerad på ett visst sätt för att vara säker. Vid autentisering av en enhet binds en resurs med ett resurs-ID. Om detta inte är inställt att tilldelas slumpvis och stort kan detta gissas. Man kan då kommunicera med enheten trots att man ej är auktoriserad. Det finns inget tekniskt hinder i XMPP för att ge sessioner korta specifika resurs-ID som är lätta att gissa. Klienter måste kontrollera servrars certifikat och får ej acceptera okrypterad kommunikation (Waher, 2016-05-06). Många servertillverkare har

dock förbundet sig att upprätthålla en viss krypteringsnivå vad gäller server-till-server-trafik via ett manifest som kallas Ubiquitous encryption. Där specificeras de minimumkrav som det federerade nätverket ställer på sina användares kryptering (github.com/stpeter/manifesto, 2014)

Uppbyggnaden av distribuerade sociala nätverk som en federation med användare och leverantörer gör det möjligt att använda sig av så kallade svartlistor och vitlistor (Lindborg, 2016-04-16). Svartlistor är listor med servrar som är känt dåliga eller illasinnade och som kommunikation inte accepteras ifrån. En vitlista är en ytterligare säkrare metod som består av en lista med endast de servrar som kommunikation accepteras ifrån. Inga andra servrar kan då kommunicera med ens server. Detta är möjligt tack vare de globalt autentiserade identiteter som kopplas till servrar, objekt och individer. Om en server missköter sig blir den alltså utesluten ur gemenskapen och problemet upphör.

För auktorisering finns också möjligheter i XMPP, med provisioneringstillägget. Provisioning sker i provisioneringsservern och den specificerar saker som hur enheter ska svara på vänskapsförfrågningar från olika källor. Dessa innehåller dels en lista med vem som äger enheter för att kunna veta vem som får svara på vänskapsförfrågningar till sin enhet samt en databas som uppdateras med vad ägaren önskar ska hända med en enhet i olika situationer. Servern behöver då bara fråga en gång om varje ny sak som händer och kan lära sig över tid vad som får och inte får göras. Auktorisering kan med provisioneringstillägget göras mycket granulärt vilket innebär att säkerhet inte blir ett skal som efter genomträngning inte ger något skydd innanför. Istället finns säkerhet på alla nivåer för att ge ett djup i försvaret. För varje ny aktivitet som ska utföras sker kontroller. (Waher, 2016-05-06).

För att detta ska fungera i små “dumma” enheter krävs en effektiv och resurssnål metod för att utföra detta. Lösningen som beskrivs i XMPP-tillägget provisioning använder en trovärdig tredje part i form av en provisioneringsserver för att flytta logik från enheten och på så sätt eliminera problemet med resursfattiga “dumma” enheter (Waher, 2016-05-06).

4.2.2 Insufficient authorization/authentication i dokumentationen

Den huvudsakliga funktionen för att åstadkomma autentisering och auktorisering är Simple Authentication and Security Layer (SASL). SASL är ett ramverk som används för att möjliggöra autentisering i användandet av connection based protocols (Zeilenga & Melnikov, 2016). Det upprättar ett abstraktionslager mellan den mekanism man vill skydda och kommunikationsprotokollets meddelande. Med detta är det möjligt att säkerställa autentisering på både klient och serversidan, säkerställa integritet på skickad data samt kryptera den. Kapitel 6 av XMPPs kärna behandlar SASL. Här fastslås i vilka lägen kommunikation skall tillåtas eller blockeras beroende på om olika kontroller misslyckas eller lyckas. Exempelvis kan inkommande kommunikation blockeras om den mottagande servern är inställd på att inte acceptera vissa tidiga versioner av SASL och en sådan förfrågan mottas. Kapitel 7 i XMPP core säger att efter att SASL använts binds en resurs till sessionen. Denna har en maxstorlek på 1023 byte men ingen undre gräns bestäms i dokumentationen. Detta visar att det går att sätta denna till ett litet värde som kan gissas (xmpp.org, 2016c).

Certifikat och hur dessa ska behandlas av klienter och servrar bestäms i XMPPs kärna. Där kan man läsa att alla typer av XMPP-entiteter, alltså både servrar och klienter, måste vid mottagandet av ett certifikat försöka autentisera dess riktighet. Vad som ska ske vid mottagandet av ett felaktigt certifikat kan i viss mån styras av implementeringen men rekommendationen är att kommunikationen skall upphöra (xmpp.org, 2016b).

Listor med entiteter som är tillåtna respektive blockerade för kommunikation över XMPP hanteras av så kallade "privacy lists". Standarden för hur dessa listor ska hanteras specificeras i XEP-0016: Privacy Lists. Denna extension möjliggör blockering och hantering av kommunikation med okända eller misstänkta entiteter på server-sidan. Blockering av en annan part kan baseras på tre olika kategorier: dess Jabber Identifier (JID), vilken typ av konto den andra parten har eller på kontots tillhörighet till exempelvis andra suspekta nätverk. Kommunikation med en oönskad part kan blockeras helt eller så kan olika typer av kommunikation hanteras på olika sätt beroende på användarens preferenser. Exempelvis kan användaren välja att inte ta emot chatt meddelanden ifrån en oönskad part men ändå tillåta att samma part kan fråga om användaren är online. Vad en oönskad part får för svar på en blockerad förfrågan kan också hanteras. Användaren kan välja att inte svara på förfrågningar alls eller svara på förfrågningar med ett felmeddelande. Även om användaren själv kan välja hur den vill svara på blockerad kommunikation finns det i XEP-0016 kap 2.14 beskrivet hur detta bör hanteras. (Millard & Saint-Andre, 2007)

4.3 Insecure network services

4.3.1 Insecure network services i intervjuerna

Internet är i grunden osäkert när det kommer till nätverkstjänster. För det första är kommunikationen anonym och för det andra är den helt öppen. Är du uppkopplad emot dagens Internet kan vem som helst kommunicera med dig. Detta medför att nätverksportarna du har kan, och med stor sannolikhet även kommer, att utsättas för påknackningar av potentiellt fientliga individer. Vem som helst med tillgång till en Internetuppkoppling kan helt anonymt använda port scanning, en metod för att utforska nätverksportarna på olika system och avgöra om några portar är öppna samt vilken trafik som går igenom dem, för att avgöra om ett system har luckor i den yttre säkerheten eller inte. En sådan lucka skulle kunna vara en osäker nätverkstjänst (Waher, 2016-05-06).

Den XMPP-baserade nätverksstrukturen som föreslås använder sig av globalt autentiserade identiteter och lagring av relationerna mellan dessa hos provisioneringsservrar för att lösa problemen. För att identitet A ska få kommunicera med enhet B krävs först att de skapar en relation med varandra. A gör då en förfrågan till sin provisioneringsserver om den får bli vän med B. Om As identitet är svartlistad, eller på något sätt inte matchar de krav som Bs ägare har för att tillåta kommunikation, tillåts inte A bli vän med B och på så sätt kan aldrig någon kommunikation inledas. Ytterligare säkerhet finns i form av att alla användare kopplar upp sig utåt emot XMPP-servrar för att etablera kommunikation. Dessa servrar är standardiserade och håller hög säkerhet. I och med att alla kopplar upp sig mot sådana servrar behöver man inte längre ha öppna portar på sina enheter. Om någon vill kontakta en enhet hanteras detta av servern. Detta gör att man inte längre kan använda sig av port scanning då enda sättet att

komma åt en enhet är att veta dess adress och sedan gå igenom en XMPP-server för att etablera en koppling. En illasinnad användare skulle efter att en koppling godkännts av servern kunna missbruka detta men i och med att man hela tiden vet från vem och var all kommunikation kommer går det effektivt att bryta kommunikation och sedan svartlista ett sådant konto. Detta gör också att spoofing och kapning av identiteter i XMPP-baserade nätverk blir oattraktivt då de snabbt blir svartlistade vid missbruk. För att undvika att en illasinnad användare eller bot autogenererar tusentals konton, och på så vis kan överbelasta system eller effektivt sprida spam, finns det begränsningar i XMPP-servrarna som standard. Dessa begränsningar gör att en mänsklig användare enbart kan skapa ett visst antal konton och att en bot inte kan skapa några alls (Waher, 2016-05-06).

4.3.2 Insecure network services i dokumentationen

Port scanning på internet är ett mycket utbrett problem som förekommer konstant. I ett experiment från 2008 sattes en försöksmiljö upp och exponerades för internet. Under en månads tid registrerades 445 utförda port scans. Med den information som inhämtas via dessa kan sedan attacker riktas mot upptäckta svagheter (Gadge & Patil, 2008).

En risk man utsätter sig för när man tillåter att vem som helst kan kommunicera med ens system är så kallade DoS-attacker (Denial of Service). En DoS-attack innebär att en angripare på något sätt skapar en överbelastning av det angripna systemets resurser vilket föranleder en kollaps. På så sätt stängs andra användare ute ur systemet. Det är nästintill omöjligt att skydda sig emot DoS-attacker då enbart ett överflöd av förfrågningar om att få öppna en kommunikationsväg kan räcka för att sänka ett system (www.us-cert.gov, 2016).

I XMPPs extension XEP-0205: Best Practices to Discourage Denial of Service Attacks återfinns potentiella lösningar på en mängd hot så som buffer-overflow attacker, TCP-kapning, attacker mot DNS-infrastruktur (infrastruktur som XMPP i hög grad är beroende av) samt överansträngning av applikations och operativsystems resurser (CPU-kraft, minneskapacitet mm). De potentiella lösningarna återfinns under kapitel 3: Potential Solutions och går ut på att man begränsar olika förfrågningar samt stryper storleken på viss kommunikation för att undvika överbelastningar. En användare kan begränsa antalet förfrågningar som skickas ifrån en specifik JID eller IP-adress, blockera kommunikation ifrån icke auktoriserade användare, blockera inkommande paket beroende på storlek och innehåll samt blockera användning av specifika tjänster som kan missbrukas. (Saint-Andre, 2009).

Spoofing och kapning av identiteter kan elimineras med tillägget XEP-0016: Privacy lists. Med detta är det möjligt att skapa tidigare nämnda svart- och vitlistor. Konton vars identitet misstänks ha kapats eller spoofats kan då blockeras i en svartlista. Alternativt kan all kommunikation från okända källor blockeras via vitlistor (Millard & Saint-Andre, 2007).

Problematiken med auto-generering av olika konton på XMPP-servrar hanteras av servertillverkaren själv. Ett exempel på hur detta görs återfinns hos tillverkaren TIGASE. De har per automatik en begränsning implementerad i sina produkter och de kan konfigureras med hjälp av följande kommando: `sess-man/plugins-conf/jabber\;iq\register/registrations-per-second=10`. I

detta specifika exempel har begränsningen satts till tio registreringar per sekund. (Account Registration Limits, juli-16)

4.4 Lack of transport encryption

4.4.1 Lack of transport encryption i intervjuerna

Det är inte alltid önskvärt med kryptering. Kryptering kan innebära en onödig kostnad i form av både prestanda hos enheter eller resurser för implementering och underhåll hos ägaren. Exempelvis mindre viktig data som transporteras trådbundet och internt hos ett företag eller i ett hem är inte nödvändigtvis i behov av kryptering. Det finns därför inga krav i själva protokollet att använda kryptering (Waher, 2016-05-06).

Ofta vid kommunikation mellan två servrar på XMPP-nätverket börjar kommunikationen med att parterna förhandlar fram vilken typ av kryptering som ska användas (Lindborg, 2016-04-16). Krypteringstekniker som AES (Advanced Encryption Standard) och Blowfish är vanliga alternativ. Den starkaste krypteringen som båda parter har tillgång till tillämpas sedan på det fortsatta dataflödet.

Utöver de rent tekniska lösningarna som återfinns i protokollet finns en annan åtgärd som också höjer säkerheten. I och med att XMPP-nätverk är decentraliserade innebär det att säkerheten är upp till var och en som användare. Det går inte att tvinga någon mot deras vilja att använda sig av säker kryptering. För att lösa detta publicerade xmpp.org ett manifest vid namn Ubiquitous Encryption (github.com/stpeter/manifesto, 2014). Målet med detta manifest är att säkerställa att all kommunikation mellan servrar på det federerade XMPP-nätet krypteras sin data. Detta manifest kan ses som ett kontrakt mellan aktörer på det federerade nätverket där de accepterar en viss säkerhetsstandard.

För att bevaka att dessa säkerhetskrav efterföljs har organisationen XMPP.net antagit rollen som "inspektör" av XMPP-servrarna som är uppkopplade i det federerade nätverket (Lindborg, 2016-04-16). XMPP.net är en hemsida som undersöker inte bara hur väl en XMPP-server hanterar kommunikation med andra servrar utan också hur väl kommunikation med klienter sköts. Dock är säkerhetskraven på den sistnämnda kommunikationen lägre på grund av att mängden data är mindre och inte lika utsatt för hot (Lindborg, 2016-04-16). XMPP.net säkerställer till exempel att de krypteringstekniker som förhandlas fram vid kommunikation mellan servrar är adekvata. Detta görs för att undvika att illasinnade servrar förhandlar bort kryptering eller förhandlar fram kryptering som är undermålig.

Det finns än så länge en lucka kvar som XMPP inte har åtgärdat. Krav finns som tidigare nämnts på att kommunikation mellan klienter och servrar samt mellan två servrar är skyddad. Än finns det dock inga krav på fullständig end-to-end kryptering. I dagsläget dekrypteras trafik som går över en XMPP-server för att hanteras av internminnet och krypteras sedan igen innan det skickas vidare till sin slutadress. Här finns en svaghet i säkerheten då en angripare som lyckats ta sig in i en server kan utläsa den trafik som passerar denna trots att datan ifrån början varit krypterad (Lindborg, 2016-04-16).

Denna lucka är något som snart kan komma att åtgärdas. XMPP har nämligen redan fullgott stöd för heltäckande end-to-end kryptering. Problemet grundar sig återigen i att XMPP-nätverk är decentraliserade och man därför måste nå konsensus för att något ska tillämpas av hela eller en tillräcklig majoritet av användarbasen. I dagsläget finns inte denna nödvändiga konsensus om vilken typ av metod som ska användas för end-to-end kryptering och därför kvarstår luckan. Ett antal lösningar är framtagna som förslag men förhandlingarna pågår fortfarande (Waher, 2016-05-06).

4.4.2 Lack of transport encryption i dokumentationen

XMPP-nätverk hanterar frågan om kryptering på ett antal sätt. Protokollet självt stöder användandet av Transport Layer Security (TLS) för att kryptera data vid transport. Den ström av data som skickas med protokollet kan då krypteras för att förhindra avlyssning. Det räcker inte enbart med att använda TLS utan man använder också SASL, en metod för att autentisera avsändare hos mottagare vid kommunikationens ändpunkt. TLS fungerar alltså som eskort av meddelandet och SASL som inpasseringskontroll vid destinationen (xmpp.org, 2016).

XMPP core kapitel 5 specificerar hur TLS ska användas innan SASL kan tillämpas. där står att en administratör KAN kräva TLS medan klienter BÖR göra det. Även kommunikation mellan servrar BÖR använda sig av TLS. Om den initierande parten kräver TLS måste krypteringen upprättas innan kommunikation inleds i syfte att skydda inloggningsdata som sedan ska användas av SASL. Vilken krypteringsalgoritm som skall användas definieras inte i XMPP core (xmpp.org, 2016).

Det manifest som undertecknats av de största aktörerna specificerar att minst version 1.2 av TLS bör användas men i syfte att säkerställa bakåtkompatibilitet tillåts klienter att förhandla fram TLS version 1.0 samt 1.1. Manifestet tillåter alltså TLS 1.0 och 1.1 vilka har brister i säkerheten. Om en administratör inte vill tillåta TLS 1.0 och 1.1 kan denne stänga av detta och uppnå ökad säkerhet på bekostnad av kompatibilitet. TLS 1.0 och 1.1 har visat sig bära på olika svagheter enligt Internet Engineering TaskForce (Dierks & Rescorla, 2008) (github.com/stpeter/manifesto, 2014).

Xmpp.net ger betyg till servrar bland annat utefter längdkrav på publika krypteringsnycklar, bit-storleken på kryptering och vilka TLS-versioner de stödjer. Sidan tillhandahåller också en lista på publika servrar där vem som helst kan registrera sig för att använda XMPP som messagingprotokoll. Betyg på säkerhet uppdelat på server-till-server samt klient-till-server kan ses (xmpp.net, 2016).

Det har nyligen publicerats en extension som ämnar lösa problemet med end-to-end encryption. XEP-0373: OpenPGP for XMPP har i nuläget statusen "experimental" och är alltså ingen antagen standard. Tanken är att denna extension ska kunna användas av andra extensions i framtiden för mer specifika användningsområden. Genom att använda det redan existerande krypteringsparadigmet Open Pretty Good Protection(OpenPGP) skapar man fullständig end-to-end kryptering mellan två eller flera kommunicerande användare. OpenPGP är ett hybridkryptosystem som använder sig av olika hashnings-algoritmer i kombination med public-key kryptering och sessions nyckelkryptering för att göra det

omöjligt för en obehörig att läsa information som skickas (How PGP Works, juli-16). Tanken är att varje användare exponerar sin publika nyckel, som är kodad med Base64, emot andra användare genom ett xml-element. När två parter har erhållit varandras publika nycklar kan kommunikationen ta sin början. (Schmaus, Schurmann & Breitmoser, 2016)

4.5 Privacy concerns

4.5.1 Privacy concerns i Intervjuerna

En distribuerad och federerad arkitektur via distribuerade sociala nätverk och unika identiteter lagrar inte stora mängder personuppgifter på centrala platser vilket minskar nyttan med att attackera en enhet (Waher, 2016-05-06). Enbart relationer mellan objekt finns på provisioneringsservrar. Inte heller någon metadata existerar, enbart listor med XMPP-adresser. För att underlätta förståelsen för hur detta bidrar till säkerhet, föreställ dig att det tar en månads arbete att hacka en server med 10 000 personuppgifter och lika lång tid att hacka ett hem med 4 så tydliggörs att incitamentet att utföra sådana attacker minskar menar Waher. De globalt autentiserade identiteter som systemet nyttjar behöver inte heller vara kopplade till juridiska personer rent tekniskt vilket anonymiserar systemet. Detta kan göra det svårare för exempelvis stater som skulle vilja övervaka sin befolkning. En person i ett sådant land kan då välja en server som erbjuder adekvat skydd. Detta kan givetvis också nyttjas av kriminella element på liknande sätt som det görs idag då en förövaras identitet förblir anonym.

De provisioneringsservrar som lagrar listor med relationer mellan klienter måste kunna skydda dessa både från utomstående attacker men också helst från auktoriserade administratörer som ej bör kunna extrahera uppgifter som inte behövs i deras arbete. Detta skulle kunna lösas med fullständig end-to-end-kryptering men svårigheten att nå konsensus i communityn förhindrar detta. I dagsläget existerar alltså även innehållet i meddelanden ofta i klartext på en servers internminnen då kryptering sker mellan servrar och klient till server (Lindborg, 2016-04-16).

XMPP och distribuerade sociala nätverk kan inte rent tekniskt styra vilka data som enheter samlar in, det är upp till tillverkaren. Denna lösnings jobb är att skydda den insamlade datan från obehöriga. Som nämnts ovan görs detta via autentisering, auktorisering och kryptering samt hur data lagras.

4.5.2 Privacy concerns i Dokumentationen

Ingen information i dokumentationen behandlar direkt den personliga integriteten som ett separat intresse.

4.6 Insufficient security configurability

4.6.1 Insufficient security configurability i Intervjuerna

Att själv kunna konfigurera säkerhetsinställningar underlättas då IoT-system byggs på öppna, ej proprietära lösningar och standarder. Användare kan själva välja lösning efter säkerhetsnivå som de önskar. Man kan också om man inte är nöjd med säkerhetsmöjligheterna själv driva en XMPP-server och konfigurera denna som man själv önskar (Waher, 2016-05-06). Detta är inget som genomsnittliga användare kommer att göra men möjligheten existerar. Säkerhetsnivån är som tidigare nämnts till stora delar implementationsspecifikt.

Om man antar att de flesta inte kommer att välja leverantör utefter säkerhet utan snarare saker som användarvänlighet, pris och liknande blir denna punkt främst av intresse för administratörer av provisioneringsservrar och tillverkare av IoT-produkter. Fördelen XMPP har mot andra protokoll är att det är från grunden byggt för att vara säkert. Man kan förvisso aktivt konstruera system som är osäkra men dess säkerhetsmöjligheter underlättar för administratörer och tillverkare att lägga mer fokus på säkerhet än många andra teknologier så som HTTP som inte har säkerheten inbyggd. Osäkert konfigurerade servrar kommer också att svartlistas vilket minskar problem med medvetet osäkert konfigurerade servrar (Waher, 2016-04-16).

4.6.2 Insufficient security configurability i dokumentation

Det finns förslag på att automatisera processen att konfigurera en XMPP-server automatiskt då detta har beskrivits som en icke trivial och tidsödande process för en administratör (Foley & Adams, 2011). Detta bedöms kunna öka säkerheten i federationen genom att eliminera den mänskliga faktorn till en viss del.

På XMPP hemsida finns en lista med open source-mjukvara som kan användas för att själv konfigurera en XMPP server på alla plattformar så som exempelvis Windows, Mac och Linux. I och med detta kan säkerheten anpassas till behoven för alla typer av användare och implementationer (xmpp.org, 2016c).

Ett exempel på säker användning av XMPP är företaget ISODE som erbjuder kommunikationstjänster åt sjö-, luftfarts- och försvarsindustri baserade på protokollet. Kunder till företaget består till exempel av välkända Oracle (isode.com, 2016).

4.7 Insecure Software/Firmware

4.7.1 Insecure software/firmware i intervjuerna

Det finns i dagsläget ingen implementerad lösning för att uppdatera enheter via XMPP-kommunikation och inte heller är någon under utveckling. En anledning till detta är att stort ansvar läggs på tillverkare av IoT-produkter att själva utveckla lösningar för hur de vill uppdatera sina enheter. I och med den heterogena naturen hos IoT kan det bli svårt att komma överens om en standardiserad metod som passar alla produkter (Waher, 2016-05-06). Det finns alltså ingen möjlighet i lösningen att uppdatera de enheter som ingår i nätverk med ny programvara för att åtgärda sårbarheter.

4.7.2 Insecure Software/Firmware i dokumentation

Det är fullt möjligt att skicka binär data, alltså filer, via XMPP tack vare ett tillägg, XEP-0234: Jingle File Transfer (Saint-Andre & Stout, 2016). Dock är det inte helt enkelt då XMPP-kommunikation i grunden är XML-objekt som består av taggar samt klartext och binär data skickas som ett flöde av ettor och nollor. Filöverföringslösningen som existerar är mest för mindre filstorlekar och lämpar sig inte för exempelvis stora uppdateringsfiler även om ingen storleksgräns finns i själva protokollspecifikationen (Ludwig, 2016).

5. Analys

Här utvärderas hur väl informationen från intervjuerna kan styrkas. Utvärderingen görs utifrån den information om risker och åtgärdsförslag som hittas i OWASPs lista och de underrubriker som finns där. Underlaget är den data som presenteras i kapitel 4, Resultat.

5.1 Insufficient authorization/authentication

Autentisering och auktorisering är det område som har gått att skapa det största teoretiska underlaget runt. De intervjuer som genomförts har också spenderat mest tid på detta. Skyddet består både av tekniska funktioner samt av det federerade nätverkets självkorrigerande natur. De tre huvudaspekterna som behandlar detta är SASL, svart- och vitlistor samt provisionering.

All information om SASL som framkommit via intervjuer har gått att direkt härleda till dokumentationen för XMPP och förefaller också vara korrekt. SASL har starkt stöd i XMPP core där många kapitel utöver enbart SASL-kapitlet behandlar detta på olika sätt (xmpp.org, 2016b). Ett korrekt implementerat SASL-protokoll hjälper dock inte om användares lösenord inte är tillräckligt säkra. Det är upp administratörer av XMPP-servrar att bestämma minsta nivå för att uppnå tillräckligt säkra lösenord.

Både intervjuer och dokumentation säger att en sessions identifierare kan vara en svaghet i teorin (Waher, 2016-05-06) (xmpp.org, 2016b). Men möjligheten finns att konfigurera servrar att enbart acceptera tillräckligt långa resursidentifierare vilket eliminerar denna sårbarhet. Det finns inga uppenbara fördelar med att inte kräva säkra resursidentifierare annat än att medvetet göra en server osäker.

Användning av svart- och vitlistor får stöd av både intervju och litteratur (Millard & Saint-Andre, 2007). Att med hjälp av listor explicit kunna kontrollera vem som får kommunicera med en användare och hur detta sker är ett effektivt vapen för ökad säkerhet då man hela tiden kan vara säker på att den man pratar är välvillig. Man kan dessutom lätt tänka sig hur effektivt det skulle vara med användning av offentliga svartlistor där konton som tidigare betett sig illa finns registrerade.

Waher nämner i sin intervju att provisionering är ett effektivt redskap för att säkerställa autentisering och auktorisering (Waher, 2016-05-06). På XMPP.org återfinns XEP-0324: Provisioning. Anledningen till att denna inte finns med i resultatdelen är att den är skriven av Waher själv och har statusen "Experimental". Att använda denna extension i resultatdelen vore enbart upprepning av Wahers tidigare information. Att denna XEP har publicerats, om än som experimentell, tyder på att det finns ett visst intresse hos XMPP communityn och att det i framtiden kan bli en officiell standard. I nuläget är detta dock så inte fallet. Enligt XMPP Standards Foundation är en experimentell XEP inte att ses som godkänd av dem utan är enbart publicerad i syfte att flera parter skall kunna utvärdera och kommentera innehållet. Allt bruk av en experimentell XEP i annat syfte än utvärdering avråds således (Waher, 2015).

Det har varit tydligt under intervjuer och i litteratur att detta är ett område som anses betydande då mycket vikt verkar läggas på detta av XMPP standards foundation. Stora delar av XMPP core behandlar olika delar av autentisering och auktorisering. Alla nödvändiga verktyg verkar alltså finnas på plats för att uppnå säkerhet i detta avseende.

5.2 Insecure network services

Port scanning löses enligt intervjuerna av att låta provisioneringsservern agera mellanhand i syfte att skydda klienterna (Waher, 2016-05-06). Detta skydd kommer från den extension för provisionering, XEP-0324: Provisioning, som Peter Waher själv har skrivit och som enligt tidigare är experimentell (Waher, 2015). Själva uppbyggnaden av XMPP med distribuerade sociala nätverk gör dock att antalet portar som kan scannas minskar vilket tyder på att XMPP har fördelar när det kommer till att motverka port scanning (Waher 2016-05-06).

Under intervjuerna framkom ingen djupare information om Denial of Service-attacker men då detta är ett välkänt fenomen söktes senare information i dokumentationen angående detta. Den extension, XEP-0205: Best practices for discouraging denial of service attacks, som listar best practices för att motarbeta dessa attacker är accepterat och implementerat av XMPP standards foundation. Dess status är "active" vilket betyder att XMPP.org fullt ut stödjer och förespråkar användning av denna extension. Enligt dokumentationen är DoS-attacker dock inget som drabbat XMPP-nätverk ännu (Saint-Andre, 2009). Arbetet med att förhindra detta görs alltså i förebyggande syfte. Det blir dock svårt att bedöma hur väl skyddat XMPP är innan försök till attacker verkligen gjorts.

Skyddet mot spoofing och identitetskapning med hjälp av privacy lists i XEP-0016 har statusen draft standard vilket innebär att dess användande rekommenderas av XMPP standards foundation men att ändringar kan komma att ske i framtiden. Skyddet kan dock i dagsläget anses vara implementerat (Millard & Saint-Andre, 2007).

Som det ser ut i dagsläget har XMPP visst stöd för hantering av osäkra nätverkstjänster. Dock hanteras problematiken på traditionellt sätt vilket gör att risken för attacker minskas men inte helt kan avskrivs. Om det visar sig att Wahers vision med användning av provisioneringsservrar och identiteter blir lyckad och en fullskalig implementation görs kommer skyddet att öka markant. För att detta ska ske krävs dock acceptans av XMPP Standards Foundation och communityn i stort. Det är alltså en lång väg kvar för att denna metod kan anses vara en lösning på det aktuella problemet och inte, som i nuläget, mer en spekulation och önskan om att så är fallet. Mycket av säkerheten ligger i nuläget på användare av tekniken. XEP-0205 som behandlar DoS-attacker och kontoregistrerings problemet är bra exempel på detta. Det enda som finns är riktlinjer för HUR man ska göra men under studien har ingenting framkommit som tyder på ATT det måste implementeras. Att den mänskliga faktorn kommer spela en viktig roll för säkerhetens nivå är alltså ett rimligt antagande man kan göra.

5.3 Lack of transport encryption

Att XMPP core inte definierar vilken krypteringsalgoritm som ska användas i TLS utan lämnar detta upp till implementeraren och administratören kan orsaka problem då man kan välja en äldre och sårbar krypteringsalgoritm (xmpp.org, 2016). Administratörer kanske prioriterar kompatibilitet före säkerhet i vissa lägen vilket kan öppna för attacker.

xmpp.net gör egentligen inget annat än att presentera betyg på vissa aspekter av publika servrars säkerhet. Dess största bidrag till säkerheten är att ge varje användare möjligheten att själv utvärdera säkerheten för servrar (Lindborg, 2016-04-16). Genom att göra denna information publik kan man exponera osäkra tjänsteleverantörer och därmed stärka säkerheten.

I nuläget finns en svaghet vad gäller end-to-end kryptering då ingen konsensus finns över vilken teknik som ska tillämpas (Waher, 2016-05-06). Detta är en lucka som bör åtgärdas innan man kan säga att XMPP har fullgott skydd vad gäller kryptering. XMPP stöder visserligen end-to-end kryptering och används säkerligen av många redan idag men att få med det som en punkt i en ny version av Ubiquitous Encryption vore ändå ett viktigt steg för att öka säkerheten. Visserligen finns det nu en XEP som ämnar bli standard för end-to-end kryptering, XEP-0373, men i likhet med tidigare nämnda extensions som också befinner sig i det experimentella stadiet kan inga slutsatser dras av detta (Schmaus, Schurmann & Breitmoser, 2016). Det finns alltså en ansats att åtgärda problemet men det är en bit kvar för att OpenPGP ska bli standard för XMPP.

Totalt sett har XMPP en hög nivå av säkerhet rörande kryptering. Med fullgott stöd för de flesta former av stark kryptering och med Ubiquitous Encryption, manifesterat alla användare godtar, tvingar man dessutom fram en hög säkerhet i det federerade nätverket. Det saknas dock fortfarande en standardiserad metod för end-to-end kryptering vilket enligt OWASP kan utgöra ett hot emot protokollets totala säkerhet.

5.4 Privacy concerns

Då ingen dokumentation kunde hittas som behandlar personlig integritet kommer denna analys att utgå från informationen som framkommit under intervjuerna då det finns ett värde i att spekulativt analysera de metoder som föreslås i OWASP listan.

Med Peter Wahers föreslagna provisionering i kombination med funktionerna i kapitel 4.1, 4.2 och 4.3 skulle den personliga integriteten per automatik bli väl tillgodosedd (Waher, 2016-05-06). En lösning med XMPP över distribuerade sociala nätverk är med sin decentraliserade natur lämpad för att värna den personliga integriteten. Som tidigare nämnts är provisioneringstillägget experimentellt vilket gör att det än inte finns en vetenskaplig grund som pekar på att denna funktion fungerar.

Spridningen av känslig data är en fördel för att förhindra stora läckor av personuppgifter. Detta kräver dock att alla de olika serverleverantörer som kommer att utgöra IoT-nätverket upprätthåller en miniminivå av säkerhet. Risken är annars att majoriteten av lösningarna

erbjuder en god säkerhet men ett stort antal inte lever upp till tillräckliga nivåer. Lyckligtvis är detta åtminstone relativt enkelt att kontrollera ifall XMPP används som standard då det går att konstruera automatiska kontrollprogram, som tidigare nämnda xmpp.net, där olika inställningar kan kontrolleras (Lindborg, 2016-04-16).

En möjlig risk är att exempelvis stater med tillräckliga resurser implementerar bra och säkra servrar som dock loggar information och meddelanden som passerar genom dem om inte end-to-end encryption skyddar data. De måste dock explicit få tillstånd att kommunicera med de som de vill övervaka så detta möjliggör inte övervakning av vilka nätverk som helst. Med korrekt auktorisering kan detta förhindras då inte ens autentiserade servrar får tillstånd att inhämta data från enheter.

Stora läckor av personuppgifter kan elimineras men enskilda individer med mindre säkra lösningar riskerar att vara utsatta i stället. Kan man säkerställa en minsta nivå är detta ett område som XMPP och distribuerade sociala nätverk kan göra mycket säkert. Specifika rekommendationer som beskriver sätt att stärka den personliga integriteten skulle underlätta för administratörer och implementerare. Det finns dock inga hinder för att skapa säkerhet vilket kan ses som en styrka hos lösningen.

5.5 Insufficient security configurability

Möjligheterna att modifiera säkerhetsinställningar är mycket goda för XMPP-servrar och provisioneringstjänster (Waher 2016-05-06). All önskvärd säkerhet förefaller möjlig att implementera och har stöd i XMPP-protokollet. Det krävs väldigt få tredjepartslösningar ovanpå XMPP-kommunikation för att lösa de vanligaste säkerhetsproblemen då mycket finns implementerat. Med svartlistor och vitlistor på säkra och osäkra servrar kommer medvetet osäkert konfigurerade servrar att blockeras snabbt och problem med dessa upphöra.

Den metod som föreslagits för att automatisera säkerhetskfigurationen av nya XMPP-servrar kan innebära både fördelar och risker (Foley & Adams, 2011). Genom att automatisera processen och på så sätt eliminera den mänskliga faktorn kan det säkerställas att alla servrar som nyttjar en sådan tjänst upprätthåller den minsta nivå som krävs för att undvika attacker. Om detta inte görs korrekt uppstår dock nya risker som skulle kunna resultera i att ett stort antal servrar som nyttjar en felaktig applikation konfigureras osäkert och öppnas upp för attacker.

Som nämnts tidigare så går XMPP och distribuerade sociala nätverk att göra mycket säkert så detta område löses mycket väl. Inga hinder finns som skulle kunna stå i vägen för valfriheten i möjligheterna till säkerhetskfiguration. OWASPs rekommendationer i detta avseende specificerar enbart att säkerhet skall gå att konfigurera vilket det gör i XMPP.

5.6 Insecure software/firmware

Firmware-och mjukvaruuppdateringar är något som ingen riktigt verkar ha tänkt på. Dels verkar problematiken grunda sig i att XMPP i dagsläget rent praktiskt lämpar sig dåligt för överföring av större filer men också för att XMPP inte riktigt verkar göra anspråk på att lösa detta problem. Den enda metoden som i nuläget finns tillgänglig för filöverföringar är som tidigare nämnts Jingle File Transfer (Saint-Andre & Stout, 2016). Även om det är enklare att låta det vara upp till varje tillverkare av IoT-produkter att på eget bevåg lösa frågan om uppdatering borde det finnas någon form av stöd för säker uppdatering via XMPP. Framtagen data, ifrån både informanter och litteraturstudien, säger att XMPP-ämnen vara en helhetslösning för IoT-kommunikation. Med detta i åtanke är det rimligt att tycka att protokollet borde ha en lösning för att åtgärda problemet med säkra uppdateringar.

Osäker uppdatering blir enligt OWASP XMPPs största svaghet. Att lämna detta problem helt i händerna på tillverkare kan i många fall fungera. Kopplar man dock upp en enhet tillverkad av en mindre seriös aktör emot det federerade nätverket och denna aktör använder sig av undermålig säkerhet vid uppdatering så har man skapat en lucka. Om man inte finner något behov att utveckla ett standardiserat sätt att uppdatera enheter på via XMPP, utan står fast vid att det är upp till de olika tillverkarna, kan det finnas ett värde i att införa rekommendationer för detta i en framtida version av det nuvarande manifestet. Det kan också, om praktiskt möjligt, vara en poäng att exempelvis XMPP.net utvecklar metoder för att undersöka olika enheter och tillverkares förmåga att på ett säkert sätt hantera uppdateringar. De intervjuades ovilja att diskutera problematiken djupare kan vara ett tecken på en svaghet i XMPPs förmåga.

6. Slutsats och diskussion

Här presenteras ett antal slutsatser utifrån en diskussion av resultatet och analysen. Slutligen ges förslag på vidare forskning.

Arbetet syftade till att svara på om XMPP i kombination med distribuerade sociala nätverk kan användas framgångsrikt för att lösa säkerhetsproblematiken som nämnts tidigare. Att svara på detta anses vara av vikt för att bidra till att bedöma lösningens trovärdighet som fullgod IoT-standard.

För att mäta säkerheten hos den tidigare nämnda metoden tillämpades OWASP Topp 10 IoT sårbarheter. Där listades de tio största säkerhetsriskerna hos Internet of Things.

Frågeställningen som arbetet ämnade svara på löd:

- Hur väl kan XMPP över Distribuerade Sociala Nätverk som IoT-standard lösa de relevanta problem som OWASP listar.

6.1 Slutsats

Efter en slutförd analys av förmågan hos XMPP och distribuerade sociala nätverk att agera som ett säkert kommunikationsparadigm inom IoT konstateras att denna metod med stor sannolikhet lämpar sig väl för detta ändamål. Resultatet visar att fyra av sex punkter behandlas i någon grad av lösningen.

Insufficient authorization/authentication hanteras effektivt genom användning av SASL, sessions hantering och provisioneringsservrar. För att lösa Insecure network services drar konceptet nytta av det faktum att alla användare är registrerade och all kommunikation går genom standardiserade och autentiserade XMPP-servrar. Lösningen för lack of transport encryption återfinns både i starkt stöd för kryptering och i manifestet ubiquitous encryption där användare binder sig att alltid använda adekvat kryptering vid kommunikation i det federerade nätverket. Konsensus skulle behöva nås för vilken typ av end-to-end kryptering som ska användas för att fullt ut tillfredsställa denna punkt. Privacy Concerns tas upp av intervjuobjekten men det finns ingen konkret implementation som idag tillämpas. Genom att uppmuntra ett federerat nätverk och öppna för proprietära lösningar får Insufficient security configurability bra lösningsalternativ. Insecure software/Firmware behandlas inte alls. Det finns för närvarande inget som helst standardiserat sätt för olika användare att på ett säkert sätt uppdatera sina enheter.

Metoden som undersöks består, som tidigare beskrivits, av två delar: XMPP-protokollet och konceptet med distribuerade sociala nätverk och globalt autentiserade identiteter. Det går att tillämpa konceptet utan XMPP och det går att tillämpa XMPP utan konceptet. Lösningen på de problem som analyserats kommer dock i vissa fall ifrån protokollet själv, ibland ifrån konceptet med sociala nätverk och ibland ifrån en kombination av de båda. Detta gör att en slutsats kan dras. För att de båda delarna ska prestera optimalt i en IoT-miljö krävs att de implementeras tillsammans för att skapa den kombination av interoperabilitet och säkerhet

som i inledningen nämns som ett krav för att uppnå “den smarta staden” och Web 3.0. IoT-aktörer som väljer att använda sig av proprietära lösningar och skapa isolerade nätverk kommer i framtiden få problem med skalning vilket i sin tur kan riskera företags existens (Waher, 2016). I framtiden kommer alltså en lösning som på ett bra sätt hanterar interoperabilitet och säkerhet att vara ett krav. Det kanske inte blir just den metod som undersökts i detta arbete men något som drar inspirationen därifrån.

Slutsatsen blir att XMPP har goda egenskaper vad avser säkerheten enligt OWASPs lista och löser de flesta av dessa väl. XMPP skulle därför kunna användas som IoT-standard ur ett säkerhetsmässigt perspektiv.

I figur 6 ges en sammanfattning av resultatet i de sex punkterna från intervjuer och dokumentation. Om båda källorna är överens och inga allvarliga brister upptäckts anses punkten mycket väl hanterad. De punkter där brister har identifierats eller de två källorna motstrider varandra men det övergripande hanteringen är god anses vara väl hanterade. Den punkt som inte hanterades alls av någon av källorna anses ej hanterad.

Område	Intervjuresultat	Dokumentationsresultat
Insufficient authorization/authentication (Otillräcklig autentisering/auktorisering)	Mycket väl hanterat.	Mycket väl hanterat.
Insecure network services (Osäkra nätverkstjänster)	Mycket väl hanterat.	Väl hanterat, dock beroende av implementation och hantering av användaren.
Lack of transport encryption (Brist på kryptering vid transport)	Väl hanterat, dock ingen konsensus runt end-to-end encryption.	Väl hanterat, dock saknas konsensus runt end-to-end encryption.
Privacy concerns (Integritetsproblem)	Mycket väl hanterat.	Inget i dokumentationen hanterar privacy concerns specifikt men lösningens konstruktion ger goda möjligheter att hantera detta väl.
Insufficient security configurability (Otillräcklig säkerhetskongfigurabilitet)	Mycket väl hanterat.	Mycket väl hanterat.
Insecure software/firmware (Osäker mjukvara/mjukvara inprogrammerad i enheter)	Ej hanterat.	Ej hanterat.

fig 6. Slutgiltigt resultat av studien.

6.2 Reflektioner

Att Internet of Things i framtiden kommer att etablera sig som det nya teknikparadigmet pekar det mesta på. Allt ifrån hemmet till industrin kommer med allra största sannolikhet att vara genomsyrat av maskiner som kommunicerar med andra maskiner helt autonomt. Som tidigare har nämnts uppskattas antalet IoT-relaterade enheter i världen nå 20 miljarder år 2020 (gartner.com, 14/1 -16). Detta kommer ställa oerhört stora krav på säkerheten. För att möta dessa krav beräknas summan som spenderas på IT/ITC/IoT-säkerhet runt om i världen att öka drastiskt. Enligt forbes.com beräknar marknadsundersökningsbolaget Markets and Markets att den totala spenderingen kommer att öka ifrån \$75 miljarder 2015 till hela \$170 miljarder år 2020 (Morgan, S. 2016). Ökningen enbart på IoT-fronten beräknas enligt Gartner.com mellan åren 2015 och 2018 att gå ifrån \$281,5 miljoner till \$547,2 miljoner (gartner.com, 25/4 -16). Denna information tyder på att det finns en vilja i branschen att säkra upp sina IT/IoT-miljöer och en förståelse för att det måste göras.

Att enbart spendera pengar är dock ingen garanti för framtida framgångar. Metoderna som undersöks i detta arbete, XMPP och distribuerade sociala nätverk, är bara en del av en helhet för att skapa en säker värld. Det krävs att utvecklare och tillverkare väljer en säker väg i framtiden och att konsumenterna ställer höga krav på dessa aktörer att leverera säkerhet. Resultatet av arbetet tyder på att XMPP kombinerat med distribuerade sociala nätverk kan vara den väg som båda parter söker. Säkerhet, skalbarhet och interoperabilitet måste kombineras och även om det inte blir just XMPP som till slut används inom IoT tror vi att det blir något liknande då protokollet är något på spåret. Det kommer krävas standardisering, interoperabilitet och hög säkerhet, oavsett vilket protokoll som till slut segrar kommer detta vara de krav som ställs.

Som tidigare nämnts är de två källorna som intervjuats Peter Waher och Joakim Lindborg som själva arbetar aktivt som en del av XMPP standards foundation. Detta gör att de kan anses vara partiska vilket kan ha försvårat upptäckandet av negativa aspekter av XMPP och distribuerade sociala nätverk. Trots att tid har lagts på att granska deras information kunde andra åtgärder ha vidtagits för att öka informationens neutralitet och tillförlitlighet. Till exempel kunde kommentarer ha sökts från företrädare för andra standarder som utgör konkurrensen till XMPP. Detta har dock inte hunnits med då fokus har lagts på att få så djup förståelse för XMPP som tidsramen tillåter. I de fall där information som framkommit under intervjuer inte kunnat styrkas med andra källor blir det svårt att dra någon slutsats. I fallet Privacy concerns där enbart de intervjuades åsikter fanns att tillgå gjordes valet att analysera punkten ur en spekulativ synvinkel och reflektera över hur en tillämpning av deras rekommendationer skulle fungera. Det har dock oftast varit möjligt att finna källor som stödjer eller motsäger påståenden tack vare att XMPPs kärna är open source.

Att enbart två personer har intervjuats får ses som en brist i resultatet. Detta motiveras dock av att de intervjuade är framstående experter inom ett område som i nuläget är relativt litet. Det är alltså inte en garanti att kvalitén på uppsatsen hade blivit avsevärt bättre med flera personers synvinklar. Dock hade det kunnat bidra en del till uppsatsens trovärdighet och bredd.

Den första intervjun som gjordes var en upptäcktsintervju. Anledningen till detta var att vi på förhand inte hade så god kunskap om ämnet. Om vi hade haft mer tid att bygga upp en förståelse för ämnet skulle denna första intervju varit mer givande då bättre frågor kunde ställts. Optimalt sett hade en upptäcktsintervju inte behövts utan det första tillfället hade

istället kunnat läggas på en grundlig strukturerad intervju. Som sagt blev det inte så då tidsramen inte tillät detta.

6.3 Förslag på ytterligare forskning

Mycket finns fortfarande att göra ur ett vetenskapligt perspektiv inom området. Joachim Lindborg arbetar med ett företag som är tänkt att sälja solcellsenergi i mindre kvantiteter där XMPP används för att kommunicera mellan dessa. För att utvärdera XMPP skulle detta kunna vara ett mål för en fallstudie som skulle kunna inriktas på säkerhet.

För att praktiskt testa XMPP över Distribuerade sociala nätverk skulle en experimentstudie kunna utföras genom att ett begränsat system byggs upp i en miljö där det kan utsättas för olika typer av attacker. Detta vore ett utmärkt sätt att testa den tekniska säkerheten i lösningen. Detta skulle kräva större kunnande rörande teknik och IT-säkerhet än denna studie.

7. Källförteckning

7.1 Muntliga Källor

Joachim Lindborg, CTO på Sustainable Innovations AB, Medlem XMPP standards foundation, 12/4 2016.

Peter Waher, Smart City Architect På Stockholmsbaserad konsultfirma, Medlem XMPP standards foundation. 16/4 2016.

Peter Waher, Smart City Architect På Stockholmsbaserad konsultfirma, Medlem XMPP standards foundation. 6/5 2016.

7.2 Skriftliga Källor

1. Acharya, S., Ehrenreich, B., & Marciniak, J. (2015) OWASP inspired mobile security. I: *2015 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)* (pp. 782–784). DOI: <http://doi.org/10.1109/BIBM.2015.7359786>
2. Adedayo, L., Butakov, S., Ruhl, R., & Lindskog, D. (2013) E-Government web services and security of Personally Identifiable Information in developing nations a case of some Nigerian embassies. I: *Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference* (pp. 623–629).
3. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015) Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys Tutorials*, 17(4), 2347 – 2376.
4. Bann, L. L., Singh, M. M., & Samsudin, A. (2015) Trusted Security Policies for Tackling Advanced Persistent Threat via Spear Phishing in BYOD Environment. *Procedia Computer Science*, 72, 129 – 136.
5. Bendel, S., Springer, T., Schuster, D., Schill, A., Ackermann, R., & Ameling, M. (2013). A service infrastructure for the Internet of Things based on XMPP. I: *2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, (pp. 385–388).
6. Bowerman, B., Braverman, J., Taylor, J., Todosow, H., & Von Wimmersperg, U. (2000) The vision of a smart city. I: *2nd International Life Extension Technology Workshop, Paris* (Vol.28).
7. Bryman, A. & Nilsson, B. (2011) *Samhällsvetenskapliga metoder*. Malmö, Sverige: Liber.
8. Conzon, D., Bolognesi, T., Brizzi, P., Lotito, A., Tomasi, R., & Spirito, M. A. (2012) The VIRTUS Middleware: An XMPP Based Architecture for Secure IoT Communications.

- 2012 21st International Conference on Computer Communications and Networks (ICCCN) (pp. 1–6).
9. Dierks, T., Rescorla, E. (2015). The Transport Layer Security (TLS) Protocol Version 1.2. *ietf.org*. Hämtad 26 april från <http://tools.ietf.org/html/rfc5246>
 10. Encyclopedia Britannica (2015). Protocol. Encyclopedia Britannica. Hämtad 22 april 2016 från <http://global.britannica.com/technology/protocol-computer-science>
 11. Foley, S. N., & Adams, W. M. (2011). Trust management of XMPP federation. I: *12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops*, (pp. 1192–1195). DOI: <http://doi.org/10.1109/INM.2011.5990581>
 12. Gadge, J. & Patil, A.A. (2008). Port scan detection. I: *16th IEEE International Conference on Networks*, (pp. 1-6). doi:10.1109/ICON.2008.4772622
 13. Gartner.com (25.4.2016) *Gartner Says Worldwide IoT Security Spending to Reach \$348 Million in 2016*. Hämtad 17 maj 2016 från <http://www.gartner.com/newsroom/id/3291817>
 14. Gartner.com (14.1.2016). *Gartner Says By 2020, More Than Half of Major New Business Processes and Systems Will Incorporate Some Element of the Internet of Things*. Hämtad 13 maj 2016 från <http://www.gartner.com/newsroom/id/3185623>
 15. Greenberg, A. (2015). How the Internet of Things Got Hacked. *Wired.com* Hämtad 16 maj 2016 från <https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/>
 16. Guamán, D., Guamán, F., Jaramillo, D., & Correa, R. (2016). *Implementation of Techniques, Standards and Safety Recommendations to Prevent XSS and SQL Injection Attacks in Java EE RESTful Applications*. New Advances in Information Systems and Technologies (s. 691–706). Berlin: Springer International Publishing.
 17. Hanseth, O., & Lyytinen, K. (2004). Theorizing about the design of Information Infrastructures: design kernel theories and principles. *Sprouts: Working Papers on Information Environments, Systems and Organizations*, 4(4), 207 – 241.
 18. Hanseth, O., & Lyytinen, K. (2010). Design theory for dynamic complexity in information infrastructures: the case of building internet. *Journal of Information Technology*, 25(1), 1–19. <http://doi.org/10.1057/jit.2009.19>
 19. Hildebrand, J., Millard, P., Eatmon, R., & Saint-Andre, P. (2008). *XEP-0030: Service Discovery*. Hämtad april 26 2016 från <http://xmpp.org/extensions/xep-0030.html>
 20. HP (2014). HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. *HP-News*. Hämtad 13 maj 2016, från http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.VzWU_pOyOko
 21. International Telecommunications Union (2012). Y.2060: Overview of the Internet of things. *International Telecommunications Union*. hämtad 2 maj från <https://www.itu.int/rec/T-REC-Y.2060-201206-I/en>
 22. IoTSverige (2016). Om IoT. *IoTSverige*. Hämtad 16 april 2016 från <http://iotsverige.se/internet-things-2/http://iotsverige.se/internet-things-2/>
 23. Jan-Olof Andersson. (2015). *Inledning* [PowerPoint-presentation]. Hämtad från Informations- och IT-säkerhet, 7.5p kurs, Uppsala Universitet.

24. Ludwig, S., Beda, J., Saint-Andre, P., McQueen, R., Egan, S., & Hildebrand, J. (2016). XEP-0166: Jingle. Hämtad maj 25, 2016 från <http://xmpp.org/extensions/xep-0166.html>
25. Isode (2016). Military Instant Messaging. *Isode*. Hämtad 11 maj 2016 från <http://www.isode.com/solutions/military-xmpp.html>
26. Koliass, C., Stavrou, A., & Voas, J. (2015, september 23). Securely Making Things Right. Hämtad 14 april 2016 från <http://doi.org/10.1109/MC.2015.258>
27. Kungl. Ingenjörsvetenskapsakademien. (2013). Nationell agenda Internet of things: summering av projektet IoT Sverige. *Kungliga Ingenjörsvetenskapsakademien*. Hämtad april 16 2016 från http://www.vinnova.se/PageFiles/751290452/Internet_of_things_agenda.pdf
28. Microsoft (2016a). *Authentication*. Hämtad 10 maj 2016 från [https://msdn.microsoft.com/en-us/library/windows/desktop/aa374735\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa374735(v=vs.85).aspx)
29. Microsoft (2016b). *Authorization*. Hämtad 10 maj 2016 från [https://msdn.microsoft.com/en-us/library/windows/desktop/aa375769\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa375769(v=vs.85).aspx)
30. Millard, P., Saint-Andre, P. (2007). *XEP-0016: Privacy Lists*. Hämtat Juli 17 2016 från <http://xmpp.org/extensions/xep-0016.html>
31. Mohammed, J. (15 december, 2015). *5 predictions for the Internet of Things in 2016*. Hämtad april 14, 2016, från <https://www.weforum.org/agenda/2015/12/5-predictions-for-the-internet-of-things-in-2016/>
32. Morgan, S. (2016, mars 9). Worldwide Cybersecurity Spending Increasing To \$170 Billion By 2020. *Forbes.com*. Hämtad 17 maj 2016 från <http://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/>
33. Oates, B.J. (2006). *Researching information systems and computing*. 1st ed. London.
34. OWASP (2016a). OWASP Internet of Things Project. *OWASP.org* Hämtad 14 april 2016 från https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
35. OWASP (2016b). About The Open Web Application Security Project. *OWASP.org*. Hämtad 22 april 2016 från https://www.owasp.org/index.php/About_OWASP
36. PGP International (Läst 2016). How PGP Works. Hämtad juli 17 2016 från <http://www.pgpi.org/doc/pgpintro/#p10>
37. Press, G. (2014, juni 18). A Very Short History Of The Internet Of Things. *Forbes.com*. Hämtad 7 april 2016 från <http://www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things/>
38. Sahu, S. (2014). An Analysis of WhatsApp Forensics in Android Smartphones. *International Journal of Engineering Research*, 3(5), 349–350.
39. Saint-Andre, P. (2009). *XEP-0205: Best Practices to Discourage Denial of Service Attacks*. Hämtad juli 17 2016 från <http://xmpp.org/extensions/xep-0205.html>
40. Saint-Andre, P. (2014). *Manifesto*. Hämtad 10 maj 2016 från <https://github.com/stpeter/manifesto>

41. Schmaus, F., Schürmann, D. & Breitmoser, V. (2016). *XEP-0373: OpenPGP for XMPP*. Hämtad juli 17 2016 från <http://xmpp.org/extensions/xep-0373.html>
42. Schuster, D., Grubitzsch, P., Renzel, D., Koren, I., Klauck, R., & Kirsche, M. (2014). Global-Scale Federated Access to Smart Objects Using XMPP. I: *2014 International Conference on, and Green Computing and Communications (GreenCom), IEEE and Cyber, Physical and Social Computing (CPSCom), IEEE*. (pp. 185–192).
43. Shadbolt, N., Hall, W., & Berners-Lee, T. (2006). The semantic web revisited. *IEEE Intelligent Systems*, 21(3), 96-101
44. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164.
45. Tan, L., & Wang, N. (2010). Future internet: The internet of things. I: *Advanced Computer Theory and Engineering (ICACTE)*, 2010 3rd International Conference on (Vol. 5, pp. V5–376).
46. Tigase Administration Guide (Läst 2016). Account Registration Limits. *Tigase.org*. Hämtad juli 17 2016 från docs.tigase.org/tigase-server/snapshot/Administration_Guide/webhelp/accountRegLimit.html
47. Tramp, S., Frischmuth, P., Ermilov, T., Shekarpour, S., & Auer, S. (2014). An architecture of a distributed semantic social network. *Semantic Web Journal*, 5(1), 77–95.
48. US-CERT (2009). Understanding Denial-of-Service Attacks. *US-CERT.gov*. Hämtad 23 maj 2016 från <https://www.us-cert.gov/ncas/tips/ST04-015>
49. Viswanathan, G. (2009). *From Web 1.0 to Web 2.0 and beyond: Reviewing usability heuristic criteria taking music sites as case studies*. Hämtad februari 27 2015 från https://www.academia.edu/8381037/From_Web_1.0_to_Web_2.0_and_beyond_Reviewing_usability_heuristic_criteria_taking_music_sites_as_case_studies
50. Waher, P. (2015). *XEP-0324: Internet of Things – Provisioning*. Hämtad 3 maj 2016 från <http://xmpp.org/extensions/xep-0324.html#usecases>
51. Want, R. (2006). *An introduction to RFID technology*. *Pervasive Computing, IEEE*, 5(1), 25–33.
52. xmpp.org (2016a). Technology overview. *XMPP.org*. Hämtad 8 april från xmpp.org/about/technology-overview.html 2016/02/11
53. xmpp.org (2016b). Extensible Messaging and Presence Protocol (XMPP): Core. *XMPP.org*. Hämtad 26 april 2016 från <https://xmpp.org/rfcs/rfc3920.html>
54. xmpp.org (2016c). Extensible Messaging and Presence Protocol Servers. *XMPP.org*. Hämtad 7 juli 2016 från <https://xmpp.org/rfcs/rfc3920.html>
55. Zeilenga, K. D., & Melnikov, A. (2016). *Simple Authentication and Security Layer (SASL)*. Hämtad 26 april 2016 från <http://tools.ietf.org/html/rfc4422>

7.3 Figurer

1. Schuster, D., Grubitzsch, P., Renzel, D., Koren, I., Klauck, R., & Kirsche, M. (2014). *Global-Scale Federated Access to Smart Objects Using XMPP*. s. 188. IEEE.

Bilagor

Bilaga 1 - Intervjumall

Den mall som användes vid de två semistrukturerade intervjuerna med Peter Waher och Joachim Lindborg.

Inledning

1. Presentera dig själv och vad du har arbetat och arbetat med?
2. Vad har du för erfarenhet av XMPP?

Huvudfrågor

3. Hur kan XMPP användas för att lösa följande huvudproblem och delproblem?
Vilka tekniker eller principer existerar?
 - A. Insufficient authentication/authorization
 - B. Insecure network services
 - C. Lack of transport encryption
 - D. Privacy concerns
 - E. Insufficient security configurability
 - F. Insecure software/firmware
4. Ser du några andra aspekter av säkerhet inom IoT som inte tas upp av OWASPs IoT topp 10?
 - A. Hur kan de i så fall lösas eller inte lösas av användandet av XMPP?
5. Vad anser du om säkerheten för XMPP i allmänhet
6. Finns det något annat du vill nämna när det gäller säkerheten i XMPP?
7. Vad är det största hotet mot säkerheten i XMPP enligt dig?

Bilaga 2 - OWASP top 10

I2 | Insufficient Authentication/Authorization

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the web interface, mobile interface or cloud interface including internal and external users.	Attacker uses weak passwords, insecure password recovery mechanisms, poorly protected credentials or lack of granular access control to access a particular interface. Attack could come from external or internal users.	Authentication may not be sufficient when weak passwords are used or are poorly protected. Insufficient authentication/authorization is prevalent as it is assumed that interfaces will only be exposed to users on internal networks and not to external users on other networks. Deficiencies are often found to be present across all interfaces. Many issues with authentication/authorization are easy to discover when examining the interface manually and can also be discovered via automated testing.		Insufficient authentication/authorization can result in data loss or corruption, lack of accountability, or denial of access and can lead to complete compromise of the device and/or user accounts.	Consider the business impact of compromised user accounts and possibly devices. All data could be stolen, modified, or deleted. Could your customers be harmed?

I3 | Insecure Network Services

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence UNCOMMON	Detectability AVERAGE	Impact MODERATE	Application / Business Specific
Consider anyone who has access to the device via a network connection, including external and internal users.	Attacker uses vulnerable network services to attack the device itself or bounce attacks off the device. Attack could come from external or internal users.	Insecure network services may be susceptible to buffer overflow attacks or attacks that create a denial of service condition leaving the device inaccessible to the user. Denial of service attacks against other users may also be facilitated when insecure network services are available. Insecure network services can often be detected by automated tools such as port scanners and fuzzers.		Insecure network services can result in data loss or corruption, denial of service or facilitation of attacks on other devices.	Consider the business impact of devices which have been rendered useless from a denial of service attack or the device is used to facilitate attacks against other devices and networks. Could your customers or other users be harmed?

I4 | Lack of Transport Encryption

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the network the device is connected to, including external and internal users.	Attacker uses the lack of transport encryption to view data being passed over the network. Attack could come from external or internal users.	Lack of transport encryption allows data to be viewed as it travels over local networks or the internet. Lack of transport encryption is prevalent on local networks as it is easy to assume that local network traffic will not be widely visible, however in the case of a local wireless network, misconfiguration of that wireless network can make traffic visible to anyone within range of that wireless network. Many issues with transport encryption are easy to discover simply by viewing network traffic and searching for readable data. Automated tools can also look for proper implementation of common transport encryption such as SSL and TLS.		Lack of transport encryption can result in data loss and depending on the data exposed, could lead to complete compromise of the device or user accounts.	Consider the business impact of exposed data as it travels across various networks. Data could be stolen or modified. Could your users be harmed by having their data exposed?

15 | Privacy Concerns

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the device itself, the network the device is connected to, the mobile application and the cloud connection including external and internal users.	Attacker uses multiple vectors such as insufficient authentication, lack of transport encryption or insecure network services to view personal data which is not being properly protected or is being collected unnecessarily. Attack could come from external or internal users.	Privacy concerns generated by the collection of personal data in addition to the lack of proper protection of that data is prevalent. Privacy concerns are easy to discover by simply reviewing the data that is being collected as the user sets up and activates the device. Automated tools can also look for specific patterns of data that may indicate collection of personal data or other sensitive data.		Collection of personal data along with a lack of protection of that data can lead to compromise of a user's personal data.	Consider the business impact of personal data that is collected unnecessarily or isn't protected properly. Data could be stolen. Could your customers be harmed by having this personal data exposed?

18 | Insufficient Security Configurability

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact MODERATE	Application / Business Specific
Consider anyone who has access to the device.	Attacker uses the lack of granular permissions to access data or controls on the device. The attacker could also use the lack of encryption options and lack of password options to perform other attacks which lead to compromise of the device and/or data. Attack could potentially come from any user of the device whether intentional or accidental.	Insufficient security configurability is present when users of the device have limited or no ability to alter its security controls. Insufficient security configurability is apparent when the web interface of the device has no options for creating granular user permissions or for example, forcing the use of strong passwords. Manual review of the web interface and its available options will reveal these deficiencies.		Insufficient security configurability could lead to compromise of the device whether intentional or accidental and/or data loss.	Consider the business impact if data can be stolen or modified and control over the device assumed. Could your customers be harmed?

19 | Insecure Software/Firmware

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability DIFFICULT	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the device and/or the network the device resides on. Also consider anyone who could gain access to the update server.	Attacker uses multiple vectors such as capturing update files via unencrypted connections, the update file itself is not encrypted or they are able to perform their own malicious update via DNS hijacking. Depending on method of update and device configuration, attack could come from the local network or the Internet.	The lack of ability for a device to be updated presents a security weakness on its own. Devices should have the ability to be updated when vulnerabilities are discovered and software/firmware updates can be insecure when the updated files themselves and the network connection they are delivered on are not protected. Software/Firmware can also be insecure if they contain hardcoded sensitive data such as credentials. Security issues with software/firmware are relatively easy to discover by simply inspecting the network traffic during the update to check for encryption or using a hex editor to inspect the update file itself for interesting information.		Insecure software/firmware could lead to compromise of user data, control over the device and attacks against other devices.	Consider the business impact if data can be stolen or modified and devices taken control of for the purpose of attacking other devices. Could your customers be harmed? Could other users be harmed?