Säkerhet i smarta hem

Kandidatavhandling i datateknik

Nicolas Ragnell

Handledare: Jerker Björkqvist

Fakulteten för naturvetenskap på teknik

Åbo Akademi

Våren 2018

Abstrakt

[TODO]

Innehållsförteckning

1. Introduktion

1.1 Sakernas Internet och intelligenta miljöer

Termen ”Sakernas Internet” (IoT, som är en förkortning av det engelska uttrycket ”Internet of Things) kan användas för att beskriva anslutningen av icke-traditionella enheter till internet, som fabriksmaskiner, medicinsk utrustning eller hushållsapparater, som t.ex. en kaffekokare eller tvättmaskin [1]. Flera enheter som är anslutna till internet och därmed till varandra, kan tillsammans bilda en intelligent miljö eller en s.k. smart miljö, där de alla förmedlar information om omgivningen. Med denna information kan man vid behov ändra på omständigheterna i den intelligenta miljön till ett önskat läge. Ett klassiskt exempel är att man ökar på temperaturen i ett rum med ett kommunikationsnätverk.

1.2 Smarta hem

Ett smart hem är en intelligent miljö där flera enheter och system är anslutna till varandra. Dessa enheter kan t.ex. vara sensorer eller andra elektroniska komponenter. Med hjälp av kommunikationsnätverk kan man få tillgång till dessa enheter, monitorera dem eller fjärrstyra dem. Hemmets ägare kan vid behov kontrollera enheterna och ändra på omständigheterna i miljön till ett önskat läge med hjälp av den information som enheterna förser. Smarta hem har också möjligheten att automatiskt ändra på miljön utan att hemägaren själv måste ingripa. Till exempel om en gassensor märker att det finns en gasläcka, så kan systemet automatiskt stänga av gasen [2].

1.3 Datasäkerhetsproblem

Med den nuvarande tekniken i smarta hem finns det massor av sårbarheter som kan utnyttjas av oväntade intränglingar.

Smarta hem är hela tiden anslutna till internet, vilket betyder att de kan bli utsatta för olika säkerhetshot och anfall. Missbruk av känslig information som t.ex. lösenord eller hemägarens personliga information kan lätt hamna i fel händer och orsaka stora problem.

För att förstå de olika riskerna som ett smart hem utsätts för kan man dela in de olika hoten som allmänt existerar på internet i tre huvudkategorier.

Spridning av känslig information: Den första kategorin är där känslig information oönskat sprids ut. Det kan vara allt från lösenord till medicinsk information om hemmets ägare. Även

information om hemmets temperatur kan vara till nytta för en inträngling, eftersom man med hjälp av informationen kan bestämma huruvida hemmets ägare är hemma eller ej.

Identifieringshot kan leda till att en inträngling manipulerar de anslutna enheterna, kontrolleringsenheterna eller annan känslig information. Till exempel kan en utomstående manipulera kontrolleringsinformation och skapa ett falskt scenario där vanligtvis låsta dörrar öppnas.

Kontroll över hela systemet: Det största hotet är där en inträngling får full kontroll över systemet, vilket gör hela smarta hemmet osäkert. Full kontroll över systemet skulle ge en utomstående möjlighet att göra t.ex. en Denial of Service (DoS) attack eller en ”energy depletion attack” (en form av DoS-anfall), där attackeraren tömmer energin i enheter som fungerar med batteri.

Med hjälp av de ovannämnda kategorierna kan man lättare förstå de olika faktorerna som påverkar säkerheten i ett smart hem. De säkerhetsriskerna som specifikt påverkar ett smart hem tas upp senare.

1.4 Avgränsningar

Avhandlingen kommer mest att beakta de externa hoten som påverkar ett smart hem, eftersom det finns flera av dem. De interna hoten kommer dock kort att nämnas.

2. Smarta hem och säkerhetsrisker

2.1 Introduktion

Smarta hem består av olika sensorer, enheter och andra system, där alla är anslutna till ett kommunikationsnätverk. Man kan dela in ett smart hems system i tre olika områden: De fysiska komponenterna, kontrollsystemet och kommunikationssystemet.

De fysiska komponenterna består av elektroniska komponenter som t.ex. sensorer. De fysiska komponenternas uppgift är att mäta och samla information om omgivningen.

Kontrollsystemet mottar informationen från de fysiska komponenterna. Beroende av vad för form av aktivitet som sker, så klassificerar systemet även den mottagna informationen.

Kommunikationssystemet kan antingen vara trådbundet eller trådlöst. Systemets uppgift är att möjliggöra kommunikation mellan de fysiska komponenterna on kontrollsystemet. Ett exempel scenario är där ett gasläckage upptäcks av en sensor som skickar informationen till kontrollsystemet via ett trådlöst kommunikationsnätverk som t.ex. ZigBee. Kontrollsystemet gör sedan beslutet att stänga av gasen i huset och skickar beslutet till ett ställdon (en komponent som används för att styra en mekanism eller ett system [5]) som stänger av gasventilen [4].

Utöver de tre olika områden kan man dela in smarta hemmets funktionalitet i det interna nätverket, det externa nätverket och en residental gateway (RG). Det interna nätverket består av de ovannämnda områdena och av de trådbunda- och trådlösa nätverk som finns inom hemmet. Det externa nätverket består av hemmets nätverksleverantör som förser hemmet med en internetanslutning. RG är en enhet i smarthemmet som alltid är ansluten till internet och den kopplar ihop smarthemmets interna nätverk med det externa. [5]

2.2 Faktorer som påverkar säkerheten

De faktorer som påverkar hemmets säkerhet är till största del hur säkra de olika enheterna är. De fysiska komponenterna kan vara av olika komplexitetsgrad och ha olika funktioner och krav, vilket även påverkar på hur åtkomliga de är av en utomstående. En dator kan enkelt stöda flera olika säkerhetsprogram, medan en liten sensor inte eventuellt är kapabel att stöda mer en ett enkelt säkerhetsprogram.

För att ett smart hem skall funktionera krävs det att det hela tiden är anslutet till internet, vilket ökar på riskerna att bli utsatta för cyber attacker. Den konstanta anslutningen till internet betyder att smarta hemmet har en statisk IP-adress, vilket innebär att utomstående har tid att försöka gissa sig fram till rätta IP-adress och därmed komma åt systemet [5].

Personerna som bor i huset påverkar även på säkerheten i hemmet. Mänskliga misstag kan bidra till att säkerheten blir sämre. De flesta installerar själva sina enheter i hemmet vilket kan bidra till att man glömmer någon viktig säkerhetsåtgärd. Vissa bryr sig inte heller om säkerheten och förstår inte eventuellt vad för risker det finns.

2.3 Säkerhetskrav

För att ett smarthem skall vara säkert finns det allmänna säkerhetskrav som skall uppfyllas. De olika kraven är Sekretesskrav, integritetskrav, autentiseringskrav, auktoriseringskrav, icke-förkastningskrav (non-repudiation) och tillgänglighetskrav. [5]

Med hjälp av sekretesskraven håller man data privat, dvs. enbart auktoriserade användare (som kan vara både människor och andra enheter) har tillgänglighet till informationen. Sekretesskrav uppnås med t.ex. kryptografi.

Integritetskraven bygger på sekretesskraven och innebär att enbart auktoriserade användare kan modifiera data. Integritet bygger på att man upprätthåller konsistens, exakthet och trovärdighet av data. Integritet upprätthålls med t.ex. Message Authentication Code (MAC).

Autentisering i smarthem bygger på att data inte har ändrats av en utomstående, och att data som skickas och används faktiskt kommer från en auktoriserad användare. I smarthem är autentisering speciellt viktigt, eftersom mycket autentiseringsmekanismer används. Det finns användare till enhet, användare till det interna nätverket, enhet till enhet, enhet till det interna nätverket osv.

Auktorisering ger enheter och användare rättigheter inom smarta hem och bestämmer vad olika användare får göra och vad som inte får göras. Det finns även olika grader av auktoritet, t.ex. kan vissa enheter kan ha rättigheter som andra inte har.

Non-repudiation bygger på autentisering, och innebär att någon eller någonting inte kan förneka information som har skickats av en autentiserad användare. Man kan åstadkomma detta krav med hjälp av digitala underskrifter.

Tillgänglighetskrav finns för att skydda nättjänster och resurser inom smarta hemmet och för att se till att de alltid är tillgängliga. Smarta hem är alltid anslutna till nätet och därför utsätter tillgängligheten risker, som olika attacker.

2.3 Säkerhetshot

Man kan enligt tidigare forskning [6] dela in de olika hoten som finns i passiva- och aggressiva attacker.

Attacker	Externa	Interna	Detektering	Skada
Aggressiva	Node compromise, wormhole	Node replication, selective forwarding, Sybil, Rushing, Sinkhole, Black hole, wormhole	medium	höga
Passiva	Eavesdropping, traffic analysis, wormhole	Eavesdropping, traffic analysis, wormhole	harder	lower
Detektering	harder	medium		

Attack Klassificiering [7]

2.3.1 Passiva attacker

Passiva attacker är attacker där man en inträngling monitorerar eller avlyssnar information och data som skickas inom smarta hemmet utan att det påverkar eller förändrar på systemet. Dessa attacker är svåra att upptäcka och sker oftast utan att ägaren märker. För att undvika dessa former av attacker är det viktigt att förebygga dem.

Avlyssning (eng. Eavesdropping) är en attack där en oväntad utomstående fångar upp information om hemmet utan att hemmets ägare märker. Den trådlösa kommunikationen sänder konstant ut information i hemmiljön till andra enheter, och gör det därför enkelt för attackeraren att komma åt informationen med t.ex. en bra mottagare [7]. Med tillräcklig information om hemmet kan attackeraren vidare utföra mera attacker, eftersom avlyssning är grunden för andra attacker [2].

TrafikAnalys (eng. Traffic analysis) är en liknar mycket avlyssning, men nu analyserar attackeraren olika kommunikationsmönster mellan enheter, för att få information om dem. Detta kan göras även då data är krypterat. Eftersom det inte sker några modifikationer, så är trafikanalys väldigt svårt att detektera.

Wormhole eller *maskhål* är en attack där paket mottas av attackeraren i ett skede av nätverket skickas framåt genom en trådlös eller trådbunden länk med mindre latens än nätverket, och sedan vidarebefordras till ett annat skede i nätverket [8]. Detta orsakar sedan ostabilitet i trådlösa sensor-nätverk, och kan i värsta fall inaktivera hela nätverket.

2.3.2 Aggressiva attacker

Aggressiva attacker är i motsats till passiva attacker menade att förändra och modifiera på systemet. Detta kan ske genom att man modifierar på data som skickas och gör den felaktig, vilket därmed leder till problem eller förändringar i systemet. Ett exempel på en aggressiv attack kan vara förnekande av tjänst eller en s.k. Denial-of-Service attack (DoS).

Node compromise är en attack där attackeraren får kontroll över noder i nätverket och kan med hjälp av det pressa ut material, som är allt som behövs för att komma åt nätverket och sedan utföra interna attacker. [7] Med hjälp av dessa övertagna noder kan man även utföra trafikanalys, dvs. analysera trafik inom nätverket.

Node replication är en attack där man gör kopior av viktigt material från en av det övertagna noderna och sedan introducerar nya noder med det kopierade materialet. Attacken kan påverka hela systemet med att man lägger till falska data eller tar bort data.

Selective forwarding innebär att man skickar vidare enbart en del av det packet som mottas medan resten av paketen förkastas. Skulle man förkasta alla av de mottagna paketen skulle det vara en *black hole attack.*

Replay attacks innebär att man låtsas vara en giltig användare genom att fånga upp ett meddelande som skickats mellan två giltiga användare, och sedan skickar meddelandet pånytt, vilket ger bilden av att man är den giltiga användaren [2].

Sybil attack är en attack där en illvillig nod tar åt sig flera identiteter och representerar sig själv som en grupp av giltiga noder för komma åt nätverket.

Denial-of-Service (DoS) är en attack där en utomstående försöker överbelasta nätverket med att överflöda det med trafik från andra enheter. När nätverket är överbelastat hindras det ifrån att hantera befogade begäran från berättigade enheter. Denna form av attack hör till en av de vanligare attackerna [6].

En liknande attack är *Distributed-Denial-of-Service (DDoS)* där den inkommande trafiken som överflödar nätverket kommer från flera olika enheter, vilket gör det svårare att hindra attacken. En av de större problemen är att enheterna i det smarta hemmet kan bli utsatta för att bli del av ett bot-net (flera enheter som blivit övertagna av en attackerare) som utför dessa överbelastningsattacker. Tidigare var attackeraren tvungen att överta datorer för att få ihop ett tillräckligt stort bot-net, vilket var krävande, men nu kan sårbara IoT-enheter lätt kommas åt [10].

Masquerade attacks (“Maskerade attacker”) är där en utomstående får oberhöriga rättigheter inom hemmet med en falsk identitet. Med denna falska identitet kan man sedan få tillgång till det interna nätverket på avstånd eller komma åt känslig information. Med en lyckad masquerade attack är det möjligt att göra andra former av attacker.

2.4 Motiv

För att lättare förstå varför säkerheten är viktig i smarta hem kan man analysera motiven till varför en person skulle vilja attackera ett smart hem, och därifrån sedan befrämja problemet. Attackerna mot ett smart hem har delvis samma motiv som de allmänna attacker som sker på internet.

Det mest allmänna orsaken varför någon skulle vilja attackera ett smart hem är för ekonomisk vinst. Får man tag på känslig information om hemmets ägare kan den känsliga informationen säljas vidare till personer som vill begå bedrägeri. Även identitetsstölder kan ske om någon lyckas tränga in sig i smarta hemmets system. Ett annat sätt att göra ekonomisk vinst är genom utpressning. En attackerare kunde till exempel låsa någon del av hemmet och begära en liten summa från ägaren för att åter ge tillgång igen.

Den andra orsaken till varför attacker mot ett smart hem skulle ske är på grund av politiska eller sociala motiv. Cyber-attacker som utförs på grund av dessa motiv brukar kallas för ”hacktivism”. ”Hacktivisterna” attackerar sina mål för att läcka någon slags information om

dem som kan vara skadligt, eller på grund av att ge ett dåligt rykte om dem om t.ex. deras produkter plötsligt upphör att fungera. I ett smart hem är det dock ganska osannolikt att någon skulle bryta in sig i systemet på grund av politiska motiv om inte målet är att specifikt läcka information om någon speciell person.

Den tredje orsaken som driver människor till att bryta sig in i system är på grund av självaste utmaningen. Man kan göra det för att det är intressant eller för att få en adrenalinkick. Dessa hackare menar ofta inget farligt och är eventuellt inte kriminella. De kan t.ex. vara personer som hjälper företag att upptäcka brister i systemet så att det kan åtgärdas.

Orsakerna till varför man skulle anfalla ett smart hem är väldigt varierande och är en komplex fråga. Utöver de ovannämnda orsakerna kunde det vara hämnd, eller på grund av att man vill övervaka eller spionera på någon. Med att förstå motiven bakom attackerna kan de lättare befrämjas [17].

3. Teknik för att förverkliga smarta hem

Ett smart hem består av både trådlösa och trådbundna teknologier som tillsammans arbetar för att förverkliga den smarta miljön. De alla har olika komplexitet, olika räckvidd, snabbheter, olika överföringsmedium, energikonsumption mm. Alla har de även olika för- och nackdelar gällande säkerheten och bristerna i säkerhet. Det finns en stor mängd olika trådlösa tekniker som används för att att förverkliga smarta miljöer: ZigBee, BlueTooth, Z-Wave WiFi, IEEE 802.11, HiperLAN [6]. Eftersom ett smarthem även består av trådbundna nätverk, såsom X10, USB, och IEEE1394 med mera, så kan säkerhetshoten komma både från det trådbundna såväl som det trådlösa nätverket.

3.1 ZigBee

ZigBee är en trådlös kommunikationsteknik med låg kostnad som är kapabel att skapa WPANs (Wireless Personal Area Network) mellan olika typer av trådlösa enheter. Den är designad för enheter som kräver låg ström och låg hastighet, vilket betyder att den förser en batterilivstid på flera år. Exempel på enheter är ljus-, regn- och röksensorer och ”actuators”. ZigBees specifikationer tillämpar sig bra i smarta hem, eftersom hemmet i huvudsak består av olika sensorer och ”actuators” som helatiden skall vara i bruk. Zigbee kan ha upp till 65 000 noder / nätverk, vilket passar in i smarta hem som består av många enheter.

ZigBee opererar på frekvenserna 2.4GHz, 900MHz och 868MHz för WPANs med låga hastigheter. Zigbee stöder datahastigheter på 250kb/s på 915MHz vilket är lägre än vad BlueTooth stöder [2]. Zigbee är designad för RF kommunikation (Radio Frequency), vilket i princip är samma som trådlös kommunikation.

Zigbee innehåller fyra olika säkerhetskoncept [12] som möjliggör säkerhet inom ZigBee nätverket:

Det första konceptet är att Zigbee består av två olika nivåer av säkerhet, som kallas hög säkerhet (eller kommesiell säkerhet) och standard säkerhet. De två olika säkerhetsnivåerna hanterar nycklar, samt distribution olika.

Det andra konceptet är att Zigbee baserar sig på en centraliserad infrastruktur som förser kontroll över säkerheten. Trust Center (TC) är är en enhet inom ZigBee nätverket som hanterar säkerheten. Den förser tre olika säkerhetsnycklar: *network key, link key* och *master key. Link Key* försäkrar kommunikationen mellan två olika enheter. *Master key* används för att generera *link keys* och är färdigt installerad på TC. *Network key* är en allmän nyckel som används av alla enheter i systemet och används för att försäkra alla kommunikationer i nätverket som sänder ut information.

Det tredje säkerhetskonceptet Autentisering och datakryptering. Zigbee använder 128-bit Advanced Encryption Standarad (12-bitAES) som använder den allmänna *network key* för kryptering av nätverket och *link keys* för kryptering av enheter [research NOTE: kolla ännu upp denna punkt -> lite olika i olika texter].

Det sista konceptet av säkerhet i Zigbee är att integriteten och *freshness* av data hålls. Detta åstadkomms med olika säkerhetsnycklar och metoder. Message Integrity Code (MIC) håller reda på att data som sänds inte har modifierats.

3.2 Bluetooth (IEEE 802.15.1)

Bluetooth är en av de standardprotokollen inom trådlös kommunikation idag och används hemmaapparaturer som mobiler, hörlurar, tangentbord mm. Bluetooth har även blivit mera populär inom IoT och man använder protokollet i bland annat smarta hem.

BlueTooth möjliggör trådlös dataöverföring mellan enheter med en licensfri ISM- bandbredd (Industrial, Scientific, and Medical) på 2.4GHz frekvens. Detta är en fördel eftersom den kan operera på denna bandbredd, men också en nackdel eftersom det kan skapa möjliga störningar [13-14]. Bluetooth kräver låg ström och fungerar på korta distanser (10cm – 100m). Den kan överföra data på 24Mbps, vilket är en stor ökning jämfört med när bluetooth introducerades, och enbart hade en överföringshastighet på 1Mbps [usb urn]. Mera specifikationer kan hittas i **figur 1**.

När två eller flera bluetooth enheter kommunicerar med varandra skapas ett piconät. Dessa enheter fungerar sedan som *slaves* eller *Masters.* Piconätet är begränsat till att det finns endast en *Master* per nät, och resten är slavar. Masterenheten kan bilda ett piconät med att skicka inbjudan till andra enheter som är i närheten. Enheter kan höra till flera piconät, och

kombinationen av två eller flera piconät kallas för *scatternet.* Första gången en anslutning görs sker en *pairing* där de delar på en hemlig nyckel som produceras genom en serie av protokoller. En masterenhet kan *paira* sig med upp till 7 andra enheter [13]. Mera specifikationer kan hittas i **figur 1.**

CHARACTERISTICS	ZIGBEE	BLUETOOTH	WIFI
Standard	802.15.4	802.15.1	801.11b
Transmission range	10-100m	1-10m	1-100m
Battery life	100-1000 days	1-7 days	0.5-5.0 days
Number of nodes in network	>65000	7	many
Stack size	<64Kb	>250Kb	>1000Kb
Throughput	20-250Kbps	720Kbps	11,000Kbps
Bandwidth	250Kbps	1000Kbps	>11000Kbps
Cost	$3	$5	$9
Security	128 bit AES	64 bit, 128 bit	nil
Operating Frequency	868MHz, 902-928MHz, 2.4GHz ISM	2.4GHz	2.4GHz & 5GHz
Network Topology	Star, peer to peer mesh, adhoc, hybrid	Adhoc piconets	Point to hub
Complexity	low	high	high
Scalability	Very high	low	high
Flexibility	Very high	medium	high
Reliability	Very high	medium	high
Applications used in	Monitoring & control, building automation	Wireless connectivity between phones, laptops	Web, email, video

Figur 1: Jämförsele av specifikationer mellan olika trådlösa tekniker [11].

3.3 KNX

KNX är en förkortning av det latinska ordet *connexo* (förbindelse) och är ett internationellt kommunikationsprotokoll för intelligenta byggnader. KNX är en godkänd ISO-standard (ISO/IEX 14543-3) såväl som en europeisk standard (CENELEC EN 500090 och CEN EN 13321-1) och kinesisk standard (GB/T 20965) [15]. Det finns över 370 företag internationellt som är KNX medlemmar och de erbjuder ca. 7000 certifierade KNX produktgrupper.

KNX har låga opereringskostnader och erbjuder en energisparande lösning med hjälp av att enbart slå på ljus och värme då det behövs. KNX sammanfogar alla kommunicerande enheter med endast en bus och deras huvuduppgift är att erbjuda interoperabilitet mellan produkter, applikationer och system.

För att vidare skydda KNX produkter, har de utvecklat KNX Secure enligt ISO-standarden 18033-3, och använder kryptering enligt AES 128 CCM. KNX Secure består av två typer av säkerhet: KNX IP Secure och KNX Data Secure. KNX IP Secure skyddar kommunikationen och KNX Data Secure skyddar runtime kommunikationen. Dessa två säkerheter körs parallellt. [16]. ETS (Engineering Tool Software) används vid designen och installationen, och försäkrar kommunikationen mellan enheterna.

3.4 Z-Wave (ska jag ha med?)

4. Analys av säkerhet i protokoll

4.1 Zigbee sårbarheter

Zigbee har dock sina styrkor även svagheter som kan uttnyttjas av utomstående för att komma åt smarta hemmet. Exempel på attacker som är hot mot Zigbee-system är eavesdropping (avlyssning), packet decoding och datamanipulering [12]. En RZUSB (AVR RZ Raven USB Stick) kan användas för att komma åt Zigbee trafik inom smarta hemmet och kan agera som en del av Zigbee Personal Area Network (PAN) cordinator eller som en ZED (ZigBee End-device). En RZUSB är en special hårdvara som är designad för att utföra attacker, och kostar ca. 40 dollar / 33 euro. Till exempel skulle attackeraren kunna använda sig av två RZUSB:s samtidigt, där den ena innehåller ett *KillerBee software suite (innehåller en modifierad version av RZUSB och andra verktyg för att utföra attacker mot ZigBee säkerhet), för att* för att parallelt utföra en paketmodifiering/injektion mot ZigBee. *KillerBee* är ett gratis program som är publicerat under Berkley Software Distribution licenset, och förväntas utvecklas i framtiden, vilket gör att vem som helst i praktiken kan utföra en attack mot smarta hem med Zigbeeprotokollet.

En annan sårbarhet i ZigBee-enheter är att ”Acutators” och sensorer är batteridrivna, och för att spara energi, har de uppväckningsinterval som är fördefinierade. Detta kan utnyttjas med DoS-attacker, som kontinuerligt blockerar Contention Access Period (CAP) och Contention Free Period (CFP), vilket leder till en oändlig överföringsloop. Det leder till att batterierna i enheterna minskar eller töms.

4.1.1 Eventuella åtgärder

[TODO]

I en säkerhetsevaluering [12] demonstrerades två potentiella attacker mot ett ZigBee system där sårbarheter utnyttjades.

Zigbee End-Device Sabotage Attack:

ZigBee Network Key Sniffing Attack:

4.2 Bluetooth sårbarheter

Användare av Bluetooth kan ses som det första lagret av säkerhet, eftersom de själva kan välja i vilket anslutnings- och synlighetsläge deras bluetooth-enhet fungerar på. Användaren kan välja mellan dessa lägen:

- *Silent:* enheten tar inte emot några anslutningar utan övervakar Bluetoothtrafik.
- *Private:* enheten är privat, dvs. syns inte för andra. Inga anslutningar tas emot om inte addressen är känd för *master.*
- *Public:* enheten syns och tar emot anslutningar från *masters.*
- *LE (Low-Energy):* meddelanden kan i ett trådlöst läge levereras av enheten till andra Bluetooth enheter.

Pairing-funktionen bestämmer respektive lägenas säkerhetsnivåer [18].

Det finns säkerhetsrisker beroende på vilken version av bluetooth som används. Till exempel, upp till bluetooth 2.0+EDR (Enhanced Data Rate) används i *pairing* enbart en 4-siffrig kod som den hemliga nyckeln. 4-siffriga koder är inte svåra att gissa med hjälp av olika program, vilket är en säkerhetsrisk. Till exempel finns det risk för att en *Man-In-The-Middle* (MITM) attack utförs.

4.2.1 MITM Attack och SSP

Med Bluetooth enheter upp till Bluetooth 2.0+EDR finns det en stor risk att de uttnyjttas av aktiva MITM-attacker (aktiv *Eavesdropping*) på grund av den bristande säkerheten. I Bluetooth 2.1+EDR introducerades Secure Simple Pairing (SSP) som bygger på krypering av den allmänna nyckeln och på visuell bekräftning. SSP använder sig av fyra konecpt, beroende på input/output möjligheterna för enheten, för att förse en hög säkerhet när *pairing* sker.

[TODO]

Det har visats med laboratorietester att bluetooth dock SSP har sina säkerhetsbrister.

4.2.2 Eventuella åtgärder

5. Slutsatser

[TODO]

Källförteckning:

[1] Huichen Lin & Neil Bergmann: *IoT Privacy and Security Challenges for Smart Home Environments.* Tillänglig här (fanns vissa problem med linken där ”error 404” förekommer): www.mdpi.co/2078-2489/7/3/44/htm

[2] Olayemi Olaolu Olawumi: *Data security in smart environments for assisted living.* Tillgänglig här: http://epublications.uef.fi/pub/urn_isbn_978-952-61-2578-7/urn_isbn_978-952-61-2578-7.pdf

[4] R. Kavitha, Dr. G. M. Nasira, Dr. N. Nachamai: - *smart home system using wireless sensor network – a comparative analysis.* Tillgänglig här: https://www.scribd.com/document/113204592/Smart-Home-Systems-Using-Wireless-Sensor-Network-a-Comparative-Analysis

[5] G. mantas, D. Lymperopoulos, Nikos Kominos: *Security in smart home environment*. Tillgänglig här:

https://www.researchgate.net/publication/232923869_Security_in_Smart_Home_Environment

[TODO: Utveckla dessa källor]

[5] https://en.wikipedia.org/wiki/Actuator

[6] http://www.diva-portal.org/smash/get/diva2:909200/FULLTEXT01.pdf

[7] http://kt.ijs.si/markodebeljak/Lectures/Seminar_MPS/2012_on/Seminars/Seminar_1_Erzen.pdf

[8] https://rd.springer.com/chapter/10.1007/978-0-387-75462-8_19

[9] https://erepo.uef.fi/bitstream/handle/123456789/5124/PUBLICATION%20I.pdf?sequence=2&isAllowed=y

[10] https://www.iotsecurityfoundation.org/why-you-need-to-worry-about-your-smart-homes-security/

IEEE artiklar:

http://ieeexplore.ieee.org/document/6480466/?anchor=authors

[11]http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=6658018

[12] http://ieeexplore.ieee.org/document/6480466/?part=undefined%7Csec2#sec2

[13] http://ieeexplore.ieee.org/document/7868416/

[14] https://www.researchgate.net/publication/267200901_Bluetooth_Security_Threats_And_Solutions_A_Survey

zigbee och bluetooth:

http://ieeexplore.ieee.org/document/7513647/

https://www.researchgate.net/publication/267200901_Bluetooth_Security_Threats_And_Solutions_A_Survey

https://www.sciencedirect.com/science/article/pii/S0167404817300615

[15] https://www.knx.org/in/knx/association/what-is-knx/index.php

[16] https://www.knx.org/knx-en/Landing-Pages/KNX-Secure/introduction/index.php

[17] http://www.fico.com/en/blogs/fraud-security/why-do-hackers-commit-cyber-attacks/

http://www.oppi.uef.fi/uku/vaitokset/vaitokset/2009/isbn978-951-781-992-3.pdf

[18] https://www.researchgate.net/publication/323956636_BLUETOOTH_PAIRING_SECURITY_THREATS_AND_COUNTERMEASURES