IOT Och Säkerhet I Smarta hem (arbetstitel)

Andreas Strandberg ,37960

Referat

Sakernas internet (IoT) blir allt vanligare i smarta hem,men hur ska datan skyddas och var exakt ska det krypteras?I denna avhandling undersöker och diskuterar jag om säkerhet inom smarta hem, med en inrikting av passiva attacker.
[TODO]

1. Inledning

[TODO]

2. IoT

Sakernas internet eller förkortningen IoT är lös samling av ändamålsdrivna nätverk som är sammankopplade för att ge säkerhet, att analysera och att hantera.[1]

IoT strävar efter tre K: Kommunikation, kontroll och automation och kostnadsminskning [2]

Kommunikation. Iot kommunicerar mellan människan och saker. Sensorer som skickar mätningar av maskiner och omgivning är kommunikation. Flera sensorer kan mäta temperaturen i alla rum för att få en översikt av husets uppvärmning. Företag kan använda gpssändare för att kontrollera försändelser . Med IoT kan vi få tillgång till information som inte har funnits tidigare eller information som mätes manuellt och sällan.

Kontroll och automation. Efter att man fått informationen från olika sändare ska det också vara lika enkelt att kontrollera och justera maskinerna på distans. Om man skapar en prestanda baslinje för hur en maskins information ska se ut går det att skapa en process som skickar ett meddelande vid avvikelser och även automatiserar kontrolländringarna för att svara på felmeddelandet.

Kostnadsminskning. För företag är IoT en kostnadsminskning, genom att de får noggranna data från sändare på maskinernas prestanda och status istället för uppskattningar . Sändare på fordon vilka ger data av bränsleförbrukning och temperaturer gör det lättare att få fram en mindre driftkostnad. Iot i hemmet ger data om värme och temperaturmätningar i hemmet för kontrollera värmare- och luftintag. Genom detta kan man hitta möjligheter till kostnadsminskningar och kan minska energiförbrukningen.

3. Smarta hem

Smarta hem är ett koncept med tre huvudpunkter: det externa nätverket, det interna nätverket och hemmets förmedlingsnod. Smart hem system uppbyggs för att enkelt kunna styra och monitorera all elektronik i hemmet. [3]

3.1 Externa nätverket

Det externa nätverket avser all elektronisk kommunikation som är uppkopplad till hemmet, som inkluderar internet och hemmets internetserviceförmedlare samt telefoner och plattor hemmets ägare använder för att styra elektroniken.

3.2 Interna nätverket

Kommunikationen som sker inne i hemmet kallas det interna nätverket och kan delas upp i fyra områden: hushållsmaskiner, ljus- och klimatkontrollsystem, underhållningssystem, kommunikationssystem och säkerhetssystem.

hushållsmaskiner-, ljus- och klimatkontrollsystem, är tre olika undersystem.
Hushållsmaskinssystemet kontrollerar och övervakar eluttagen för alla maskiner i hemmet. Detta ger möjlighet att både kontrollera elförbrukningen och att styra av och på maskinerna. Till hushållsmaskinssystemet hör också hulshållsmaskiner som kan kommunicera över internet.
Ljussystemet kontrollerar lamporna i smarta hemmet för att ge information om ljusstyrka och vilka rum som är belysta.

Klimatkontrollsystemet övervakar värmeelement , värmeledningar och luftsystem. Med klimatkontrollsystemet kan man styra att alla rum har ett behagligt klimat som är anpassat för människans trivsel.

underhållningssystem, inkluderar all ljud-, video- och spelunderhålling som kommunicerar och styrs genom internetkommunikation. Detta kan vara ett hemmabiosystem med ett kontrollcenter som styr suround-ljudsystemet och mediaspelaren och tv eller projektorn. Det kan också vara ett system som kopplar ihop internetradio med högtalare runt om i hemmet .

kommunikationssystem, handlar om telefoni, videosamtal, och intern rumtelefon. Till systemet hör också mobiltelefoner, datorer, printrar och plattor. Systemet erbjuder all sorts digital kommunikation från personer i hemmet till hela världen.

säkerhetssystem, inkluderar alla elektriska identifikationmedel och inbrottsalarmsystem. Till identifikationssystem hör biometrisk identifikation, röst identifikation, rfid-sensorer och kortläsare . Övervakningssystem som CCTV räknas till säkerhetssystemet. säkerhetssystemet kan också kopplas till ljussystemet för att tända och släcka lampor för att ge illusionen att någon är hemma. Hälsoövervakning av barn och äldre kan också höra under säkerhetssystemet.

3.3 Förmedlingsnod

Förmedlingsnoden är nätverks modulen som integrerar alla olika styrsystem i det interna nätverket , och ger tillgång till det externa nätverket åt det interna nätverket och tvärtom . Noden är den punkt styr all internet kommunikation i hemmet och all kommunikation mellan varje system i det interna nätverket. Förmedlingsnoden ger tillgång att styra systemen på distans genom applikationer

på telefoner eller datorer som kommunicerar över internet. Förmedlingsnoden verkar också som en gränsvakt, där säkerheten, i det här fallet, brandvägen identifierar och autentiserar alla användare som vill ha åtkomst till smarta hemmet.

4. Säkerhet

Säkerhet i smarthem går att dela upp i sju delkategorier: konfidentialitet, integritet, autentisering, auktorisering, icke förnekande och tillgänglighet.[3][5]

Konfidentialitet , menar att systemet skall hålla all information privat och inte ge tillgång åt icke-auktoriserade användare att läsa informationen. I en attack mot konfidentialitet så kan angriparen få indirekt övervakning av hemmets användare genom att läsa status information om hemmet.

Integritet i säkerheten är för att hindra modifiering av information av icke auktoriserade användare . I en attack mot integritet kan angriparen tjuvlyssna på datan till och från det interna nätverket för att ändra på data.

Autentisering, medel att verifiera användningen av systemet. Detta gör via ett lösenord eller en delad säkerhetsnyckel. En angripare kan låtsas vara en annan användare för att få åtkomst till data.

auktorisering, att bestämma rättigheter för användning av systemet och informationen. I en attack kan angripare använda sig av falska auktoriseringskoder för att komma åt viktiga system.

icke förnekande, ett system som sparar händelser och användare som deltar i händelserna för att hindra förnekande av meddelande eller mottagen fil. Arkivfilen kan använda av en tredje part för bestämma rätt i lagtvistningar.

tillgänglighet, säkerhetssystem ska ge tillgänglighet åt tjänster och resurser,som bredband, åt användaren. exempel på detta är : attacker som översvämmar nätverket med förfrågningar tills routern inte klarar av det mera eller batteridrivna sändare tömmer sina batteri snabbare.

4.1 Sårbarheter

Smarthemmet kan attackeras på distans ,genom direkt tillgång kontroll gränsnitt, till exempel pekskärmar, eller via nedladdning av sabotageprogram. I detta kapitel tas upp olika sårbarheter i smarthemmet.[5]

Smarthemmet är uppkopplat till utsidan, det externa nätverket. Hur väl avgränsat och säkert ett smarthem är kommer det alltid att finnas en risk via uppkopplingen till internet.

Begränsade resurser, sensorer styrs vanligtvis av mikrokontroller med begränsade utrymme och beräkningskapacitet. Detta leder till att man kan inte implementera för komplicerade säkerhets algoritmer för att skydda informationen som skickas från sensorerna.

Heterogena system, Smarthem är uppbyggda av flera olika system. Varje program eller maskin har sitt eget system och det finns ingen universell standard för IOT sensorer. En annan risk är att en del av systemen aldrig uppdaterar sina fasta program, så angripare kan utnyttja gamla kryphål i systemet.

Brist på professionella underhållningstjänster. Det saknas företag som erbjuder underhållning av alla system inom ett smarthem, och användare är själv tvungen att bygga och konfigurera sitt smarthem själv.

4.2 Hot

Hot mot säkerheten kan uppdelas i interna och externa hot. Externa hot delas sedan upp i passiva och aktiva attacker.

4.2.1 Interna hot

Interna hot kommer från inne i smarthemmet. Tidigare i kapitlet nämndes att användare själv oftast bygger upp sitt eget smarthems system, där kan hotet komma från att nätverket är felbyggt eller felkonfigurerat . Detta leder till att angripare kan hitta kryphål i ett annars säkert system. Ett annat liknande hot är en ofärdig rättighetsfördelning i smarthemmet, där vilken användare i huset kan

ändra och ta bort delar av systemet. Användaren kan också ladda ner skadliga program för datorn och systemet, vilket förbigår säkerhetssystemet.

4.2.2 Externa hot

Externa hot är alla hot som kommer från omvärlden utanför hemmet. Det klassificeras efter hur informationen blir upphämtade.

4.2.2.1 Passiva attacker

När ett smarthem är utsatt för passiva attacker sker det under en längre tid. Angriparen har tillgång till informationen utan att ändra på den,vilket gör det svårt att upptäcka. Passiva attacker är avlyssning av trafik eller trafikanalys.

Avlyssning av trafik betyder att angriparen har tillgång till att läsa informationen som skickas från hemmet till omvärlden, antingen via olagligt inskaffade säkerhetskoder eller via icke-krypterade meddelanden.

Angriparen kan också använda trafiken av kommunikationen mellan olika system för att analysera över en längre tid. vid trafikanalys ser man efter statusmeddelande från olika sändare och mängden trafik. Ur analysen kan man få fram lösenord och användarens position i hemmet under tider på dygnet. Hur angriparen får fram användarens position är till exempel att bara lyssna efter statusmeddelanden som lamporna i hemmet skickar, vilka lampor som är tända och vilka som är släckta.

4.2.2.2 Aktiva attacker

Andra sidan av externa hot är aktiva attacker, där angriparen gör attacker med direkt inverkan. Vanliga former av aktiva attacker är : maskerat meddelande, återskickning, ändring av meddelande, förnekning av tjänster och sabotageprogram.

Maskerat meddelande är en attack där angriparen skickar meddelande med falsk identifierings för att få manipulerat fram information. Det är ofta använt i en kombination med andra attacker som återskickning.

återskickning menar att angriparen samlar upp riktiga meddelande från sändare i systemet för att skicka meddelandet igen vid en annan tid och maskerat sig som den auktoriserade sändaren.

ändring av meddelande är att samla upp meddelanden och skicka en modifierad version vidare. Även att lägga till en försening på ett meddelande går under meddelande ändring.

förnekning av tjänster är när angriparen översvämmar ett system med meddelande för att neka användaren att använda systemet. Att översvämmna sändare för att minska ladning är nämnt tidigare och är en form av tjänsteförtnekning.

sabotageprogram är all kod som är skadlig för systemet.

4.3 Lösningar

dfsdsf

5. Diskussion

[TODO]

Referenser

[1]Dave Evans,2011:
The Internet of Things
How the Next Evolution of the Internet
Is Changing Everything

[2] Lopez research 2013,
"An Introduction to the Internet of Things(IoT)"Part 1. of "The IoT Series"

[3]G. mantas, D. Lymperopoulos, Nikos Kominos: Security in smart home environment.
https://www.researchgate.net/publication/232923869_Security_in_Smart_Home_Environm ent

[4]Attitudes and Perceptions of IoT Security in Critical Societal Services
Mikael Asplund ; Simin Nadjm-Tehrani

[5]Huichen Lin & Neil Bergmann: IoT Privacy and Security Challenges for Smart Home Environments. https://www.mdpi.com/2078-2489/7/3/44