Åbo Akademi

Försvarssystem för smarta hem

Sabina Bäck
Kandidatavhandling i Datavetenskap
Handledare: Marina Waldén
Fakulteten för naturvetenskaper och teknik
Åbo Akademi
Våren 2020

Referat

Genom att vardagliga objekt kopplas upp till internet har vi fått ett fenomen som kallas *Internet of Things* (IoT) eller sakernas internet. Smarta hem är en del av IoT, där hushållsapparater och andra objekt som finns i ett hem är uppkopplade. Allt detta bygger på ubik datateknik som betyder att objekt är lättrörliga in och ut från nätverk. I ett smart hem kopplas IoT-enheter upp och ned genom hemnätverket och detta sker ubikvitärt eller lättrörligt.

Ett smart hem kan sända potentiellt privat information till molntjänster och trots att både hemmet och molntjänsten är säkra så kan information läcka på vägen. För att skydda sig mot passiva nätverksobservatörer som extraherar, lyssnar av och tolkar informationen medan den sänds mellan hemmet och molnet kan man använda ett antal olika försvarssystem.

Det finns vedertagna försvarssystem så som brandvägg och Virtual Private Network VPN och sedan finns det mer specifika system så som Independent Link Padding (ILP), Stochastic Traffic Padding (STP) samt Attribute-Based Encryption (ABE). Det här arbetet går igenom alla dessa försvarssystem samt deras för- och nackdelar. Vilket försvarssystem en användare av smarta hem bör välja beror på vilka egenskaper hen söker i sitt system.

Innehållsförteckning

1 Introduktion

Sakernas internet eller *Internet of Things* (IoT) är ett koncept som blivit relevant tack vare utvecklingen av mobila enheter och ubik datateknik (eng. ubiquitous computing). IoT betyder i princip att saker, olika typer av vardagliga objekt, är kopplade till internet och IoT kan definieras som ett nätverk av enheter. När man pratar om nätverk är det naturligt att man tänker på ett nätverk av datorer, men IoT har utvecklats till att förutom vara ett nätverk av datorer också inkludera en mängd olika vardagliga objekt i olika storlekar. [1]

IoT består av olika enheter som kommunicerar och delar information sinsemellan, så som bilar, smarta mobiler, leksaker, hushållsapparater, kameror, multimediasystem med mycket mera. Dessa enheter samlar in och analyserar data för att kunna spåra och positionera ägarna. De kan till och med övervaka online samt uppgradera sig själva med mera. [1]

Ett smart hem är en del av IoT och kan definieras som en bostad som med hjälp av teknik samlar in information och reagerar därefter [2, 3]. Genom att styra över både tekniken i hemmet och uppkopplingen till världen utanför, sörjer det smarta hemmet för invånarens komfort, säkerhet och underhållning [2]. Det långsiktiga målet med utvecklingen av denna teknik har varit människans välbefinnande [3]. Allt från värme och luftkonditionering eller multimediasystem till ljusstyrka och hushållsmaskiner kan kontrolleras i ett smart hem [4].

Att få apparater att kommunicera sinsemellan har möjliggjorts genom innovationen av smarta produkter. Det här har i sin tur bidragit till utvecklingen av smarta hem [3]. Med smarta hem kommer också utmaningarna att bevara säkerheten i hemmet samt kontrollera vilken information passiva nätverksobservatörer kan komma åt [5].

Det är komplext att bygga mjukvara för att få helt automatiserade hem och det bygger på ubik datateknik. Det finns ännu utmaningar kvar att lösa innan man får detta att fungera helt. Då systemen bygger på öppenhet och dynamiska uppkopplingar behöver man också ta i beaktande invånarnas säkerhet och integritet

innan man bygger dessa system. För att få ett dynamiskt system kommer det smarta hemmets nätverk vara öppet för heterogena enheter vilket betyder att typer av enheter samt deras säkerhetsprotokoll kommer att variera. [4]

Ubik datateknik är, som tidigare nämnts, den teknik som används för att bygga automatiserade hem. Denna teknik bygger på att datoranvändning kan dyka upp var som helst och när som helst i ett nätverk med vilken typ av smart enhet som helst. Det finns tre karaktäristiska drag för ett ubikt datoranvändningssystem. Det första är att apparaten ska smälta in i sin omgivning. Det andra är att apparaten måste kunna kommunicera och interagera med andra apparater i omgivningen. Det sista är att apparaten måste ha egen energikälla för att kunna fungera autonomt. [4]

Eftersom smarta hem fungerar genom IoT så betyder det att hemmet är uppkopplat till ett nätverk och att de uppkopplade enheterna sänder information till molntjänster [5]. Smarta hem är en möjlighet för användaren att förenkla vardagen, men det innebär också risker att sända privat information över nätet [10].

Denna avhandling har som syfte att förklara teknologin bakom smarta hem samt undersöka vilka säkerhetsrisker och integritetsproblem som finns med denna teknologi. Dessutom syftar denna avhandling till att jämföra olika typer av försvarssystem som finns för att förhindra spridning av privat information.

2 Smarta hem

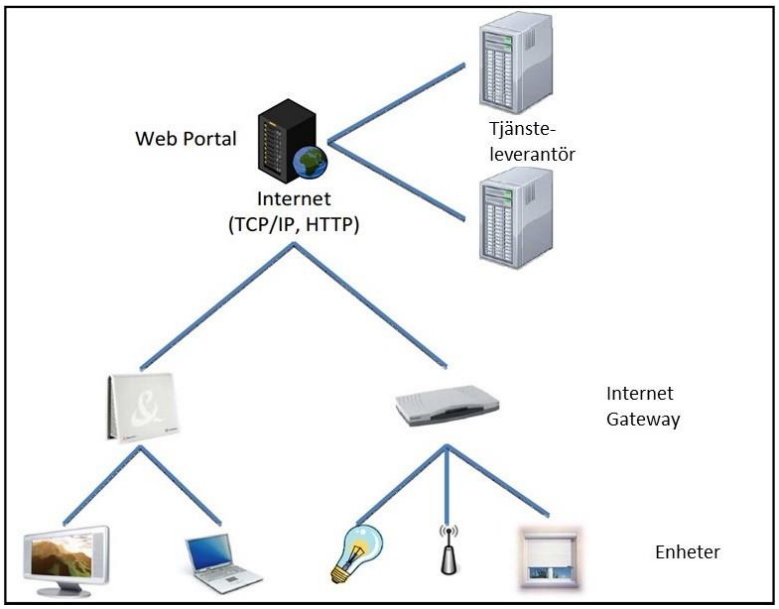
Forskare definierar smarta hem på många olika sätt och i sin definition fokuserar de på allt från tekniken bakom till användningen av smarta hem [3]. Enligt Marikyan et. al. [3], som gjort en sammanställning av litteraturen kring smarta hem, finns det ändå en viss koncensus bland forskarna om hur ett smart hem definieras. Teknik, tjänster och förmågan att tillfredsställa användarens behov är tre karaktäristiska drag för ett smart hem (Tabell 1) [2-4].

2.1 Karaktäristiska drag

2.1.1 Teknik

Tekniken består av både hårdvara och mjukvara, det vill säga till exempel hushållsapparater och sensorer samt programmen som styr dessa. Sensorer integreras i hushållsapparater och de kan via Wi-Fi kontrollera hemmiljön. Sensorerna spelar en speciellt viktig roll i ett smart hem, då dessa kan upptäcka förändringar i luften, ljuset, hos användaren samt annan stimuli från omgivningen och reagera på detta. [3,4,6,7]

I figur 1 visas hur arkitekturen bakom ett smart hem kan vara uppbyggt [4]. Det är en enkel struktur där en webbserver är kopplad till en nätsluss (eng. gateway) genom HTTP eller dylika protokoll. Genom att använda en nätsluss skapar man en brygga till ett lokalt nätverk eller Local Area Network (LAN) för att koppla ihop de smarta enheterna med de molntjänster, via vilka man styr enheterna i hemmet.



Figur 1. Ett enkelt schema över arkitekturen för ett smart hem. Hämtad från Lalanda et. al. [4], egen översättning.

2.1.2 Tjänster

Tjänster i smarta hem kan klassificeras på olika sätt. De Silva et. al. [6] anser att det smarta hemmet består av tre olika kategorier beroende på vilka tjänster det erbjuder, medan Marikyan et. al. [3] delar in det smarta hemmet i fem olika kategorier. Dessutom diskuterar de båda kring att addera en fjärde kategori till De Silvas et. al. [6] klassificering.

De Silva et. al. [6] beskriver den första kategorin av tjänster som att det smarta hemmet ger stöd till dess användare genom att försöka känna igen deras handlingar. I den andra kategorin försöker det smarta hemmet upptäcka och samla information om multimedia om användarens liv. I den tredje kategorin behandlar och analyserar det smarta hemmet insamlad data för att kunna varna användaren för kommande katastrofer, så som hot mot säkerheten eller naturkatastrofer. Den potentiella extra kategorin som Marikyan et. al. [3] och De Silva et. al. [6] beskriver är ett smart hem som försöker optimera energianvändning med mera för att vara ett ekologiskt hållbart hem.

Smarta hem kan graderas enligt en skala börjandes från traditionellt hem till och med fullständigt smart hem (eng. fully smart home) beroende på vilka enheter hemmet utrustats med [3]. Baserat på en mängd olika studier presenteras tjänster grupperat i fem olika kategorier, komfort, uppföljning, hälsoterapi (eng. health therapy), support och rådgivning (Tabell 1 nedan).

2.1.3 Användarens behov

Användarens behov, eller fördelar för användaren, grupperas i fyra olika kategorier; hälsorelaterade fördelar, fördelar för miljön, ekonomiska fördelar samt psykologiska fördelar [3].

Hälsorelaterade fördelar kan till exempel vara stöd för åldringar, personer med kroniska sjukdomar eller annars sårbara personer och kan innefatta tillgänglighet till vård eller hjälpmedel. Till exempel genom enheter i smarta hem som följer upp användarna och ger en varning om det finns avvikelser i hälsotillståndet eller virtuella besök till läkare eller annan vårdpersonal. [3,6,8]

Ett smart hem kan gynna miljön genom att minska konsumtionen av energi, använda energisnåla produkter samt övervaka energiförbrukningen [3,7,8]. Det här kan ha en långtidseffekt som att människor börjar leva mer ekologiskt hållbart samt minskat utsläpp av koldioxid [3].

De ekonomiska fördelarna kan samtidigt vara miljömässiga eller hälsorelaterade fördelar, till exempel genom att en effektivare energianvändning leder till lägre elräkning [3]. Det finns två tydliga sätt på vilket användaren av ett smart hem kan utnyttja enheter för att få ekonomiska fördelar. Dels genom en högre medvetandegrad om energikonsumtion samt dels genom möjligheten att själv följa upp energikonsumtionen gör att man kan konkurrensutsätta energibolag.

En användare av ett smart hem kan uppleva psykologiska fördelar genom att få denna att undvika social isolering till exempel genom att ge användaren

verktyg till social samvaro [3,8]. Däremot kan det finnas en risk för att ensamma individer får en minskad verklig kontakt med andra människor om de får sin sociala kontakt via smarta enheter [3].

Författare	*De Silva et. al. (2012)*	*Marikyan et. al. (2019)*
Teknik	Sensorer, integrerade system	Sensorer, enheter, integrerade system
Tjänster	Användarstöd Samla multimedia Varning för säkerhetsrisker och naturkatastrofer Miljövänligt	Komfort Uppföljning Hälsoterapi Support Rådgivning
Användarens behov / fördelar	Förhöjd livskvalitet	Hälsomässiga fördelar Miljömässiga fördelar Ekonomiska fördelar Psykologiska fördelar

Tabell 1. Översikt olika klassificeringar av smarta hem.

2.2 Utmaningar

Även om tekniken och tjänsterna som finns i smarta hem är till för användarens komfort och för att ge användaren en bekvämare vardag [2-4,9], så finns det också utmaningar med den utveckling som skett inom området [5,9].

I ett smart hem kan det finnas enheter som hela tiden är på och som registrerar användarens aktiviteter i hemmet och när enheterna är uppkopplade laddar de upp informationen till molntjänster [5]. Även om det

smarta hemmet och molntjänsterna är säkra genom kryptering kan en attack mot användaren ske genom analys av nätverkstrafiken [9].

Det är så kallade passiva nätverksobservatörer som genom att analysera mängden datatrafik, paketstorlek och timing kan få tillgång till känslig information om användaren [5,9]. En passiv nätverksobservatör är någon som observerar en användares nätverkstrafik och kan vara till exempel internetleverantörer eller någon annan med tillgång till nätverkstrafiken.

Maskininlärning (eng. machine learning) är en gren av datavetenskap där man försöker bygga datorsystem, som med erfarenhet automatiskt förbättrar sig självt [12]. Meidan et. al. [10] beskriver att angripare mycket effektivt kan identifiera enheter i smarta hem genom att analysera nätverkstrafiken med maskininlärningsalgoritmer. Träffsäkerheten för att identifiera olika typer av IoT-enheter låg i studien på 99,281%. Genom att komma åt information från till exempel en enhet som övervakar hälsan kan en attackerare extrahera information samt dra slutsatser om användarens hälsotillstånd [9]. Det kan i hemmets privata sfär finnas sådan information som man inte vill ska läcka ut till allmänheten. För att skydda sig mot detta finns det olika typer av försvarssystem man kan använda sig av.

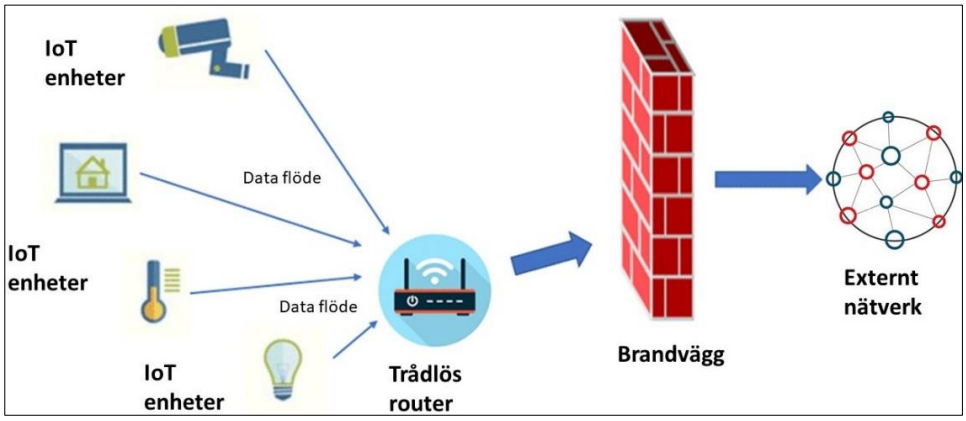
Vidare i detta arbete beskrivs i kapitel tre olika typer av försvarssystem som man kan använda mot passiva nätverksobservatörer. I kapitel fyra jämförs försvarssystemen sinsemellan.

3 Försvarssystem

Det finns olika typer av system för att dölja internettrafiken för passiva nätverksobservatörer. Som nämnts tidigare kan en passiv nätverksobservatör tyda sig till vad användaren gör i hemmet genom att analysera metadata och mer specifikt volymen datatrafik (eng. traffic volumes), paketstorlek och timing [5,9]. Det är möjligt att lära sig mycket om en användare enbart genom att analysera metadata från Internet. Det finns ett antal olika sätt att försöka dölja sin datatrafik och nedan beskrivs några av dessa.

3.1 Brandvägg

En brandvägg är en kombination av hårdvara och mjukvara som kontrollerar flödet av in- och utgående trafik [13]. Genom att kontrollera trafiken förhindrar en brandvägg obehörig kommunikation in till och ut från nätverket (Figur 2). Brandväggen identifierar namn, IP-adresser, applikationer och annan karaktäristisk inkommande trafik och den kontrollerar informationen mot tillgänglighetsreglerna som är programmerade in i systemet av nätverksadministratören.



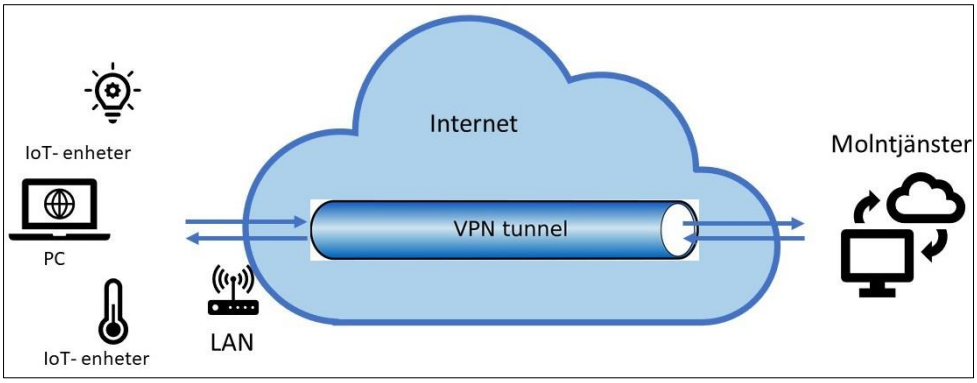
Figur 2. Schematisk bild över brandvägg i ett smart hem

En brandvägg är ett av de enklaste sätt att hindra sin attackerare (eng. adversary) från att över huvud taget samla nätverkstrafik från ett smart hem [5]. Genom att konfigurera en brandvägg blockerar man nättrafik till och från

sitt LAN, men det kan i sin tur vålla problem för IoT-enheter då många av dessa behöver uppkoppling till molntjänster för att fungera.

3.2 Virtual Private Network

Ett Virtual Private Network (VPN) eller virtuellt privat nätverk kan definieras som ett sätt att hemlighålla innehållet i kommunikationen över det öppna nätet genom att använda ett så kallat tunnlingsprotokoll, en VPN-tunnel (Figur 3) [14]. Ett VPN utvidgar LAN då man på distans kan ansluta sig till nätverket genom en krypterad VPN-tunnel. Den krypterade förbindelsen skyddar nätverkstrafiken mot avlyssning av passiva nätverksobservatörer.



Figur 3. Schematisk bild över VPN i ett smart hem.

Att styra nätverkstrafiken genom en VPN-tunnel är en möjlighet till skydd för användaren av smarta hem [5]. VPN sluter in all nätverkstrafik i ett transportlager för slutdestinationen. Att det från VPN blir ett enda flöde gör det svårt för en nätverksobservatör att avgöra vilka variationer i data som hör till vilken enhet. Det betyder i sin tur att det är svårt för observatören att dra slutsatser om användarens förehavanden hemma genom att analysera data från trafikflödet.

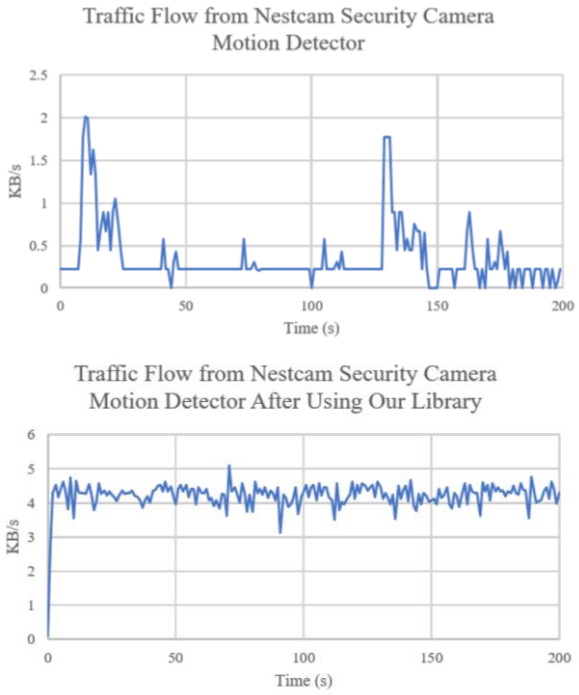
Enligt Apthorpe et. al. [5] beror VPN:s säkerhet på antalet enheter som sänder trafik. Det finns några olika scenarion som gör att en passiv nätverksobservatör kan lyssna som förut eller enkelt lista ut vilken enhet som används när. Det första är om man sänder med enbart en enhet för då

är mängden av nätverkstrafik densamma som vanligt. Det andra är om det är gles trafik, det vill säga att det är flera enheter som sänder men de sänder vid olika tillfällen. Det tredje och sista scenariot är om en enhet är dominerande i mängden trafik som sänds ut. Då kan en passiv nätverksobservatör lyssna och analysera trafiken från den dominerande enheten.

3.3 Independent Link Padding

För att förhindra passiva nätverksobservatörer från att tolka data som sänds ut från ett smart hem kan man använda sig av Independent Link Padding (ILP) eller oberoende länkutfyllning [5,7]. ILP begränsar trafiken i nätverket för att matcha ett förutbestämt schema eller hastighet [7]. För att försäkra sig om att den förutbestämda hastigheten hålls utförs fragmentering av paket så att de alla blir samma storlek eller så sänds överflödigt brus. På det här sättet döljs användarens beteende i det smarta hemmet då upp- och nedladdning av trafikfrekvensen (eng. traffic rate) formas (Figur 4) [5,7].

Då man krypterar meddelanden så förändrar man tillfälligt originalmeddelandet så att attackerare inte ska kunna läsa det [15]. Nyttolast (eng. payload) är den del av ett meddelande som är avsedd för mottagaren. Då meddelanden sänds sker en trafikkvotering (eng. traffic shaping) genom stoppning (eng. padding) eller fragmentering av nyttolasten samt genom att lägga till täckande paket (eng. cover packets).



Figur 4. Trafikflöde från en rörelsesensor i en Nestcam övervakningskamera. Övre bilden: När ILP inte används. Nedre bilden: När ILP används. Bild tagen från Datta et. al. [7].

För att kunna utföra detta har Datta et. al. [7] skapat ett bibliotek i Python, som kunde användas av tillverkare av IoT-enheter. I biblioteket finns metoden Sender.startPeriodicallySending() som startar en algoritm för att dölja trafik från enheten. Enligt algoritmen körs ILP så länge enheten är i sändningsläge. Först kontrolleras det att det finns meddelanden, därefter vilken längd det har. På basen av meddelandets längd sker antingen stoppning eller fragmentering. Om det inte finns meddelanden sänder ILP ut slumpmässigt brus (Algoritm 1).

```
while doSend do
    d ⇐ Sample from distribution D
    Pause for d seconds
    x ⇐ Sample from distribution X
    if q is not empty then
        m ⇐ first message in q
        len ⇐ size(m)
        if len ≤ x then
            Pad m to x bytes.
        else
            Put last len − x bytes of m at head of q
            m ⇐ first x bytes of m
        end if
    else
        m ⇐ Random cover traffic of length x
    end if
    m ⇐ m+ recovery header
    Send m
end while
```

Algoritm 1. ILP trafikkvoteringsalgoritm. Algoritmen tagen från Datta et. al. [7].

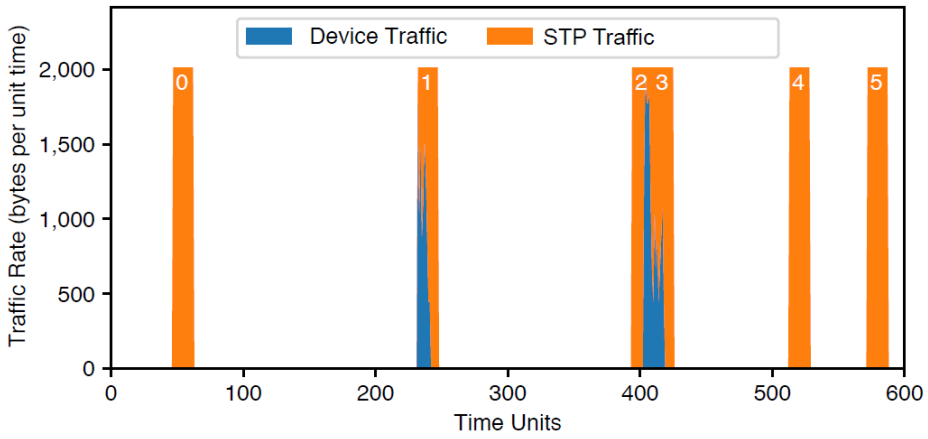
ILP belastar nätverket då det hela tiden sänder ut extra brus och det är estimerat att det tar cirka 4KB/s per enhet. ILP medför också en viss latens hos en enhet och det beror på att den försöker skicka data snabbare än ILP kan packa ihop det. Belastningen av nätverk samt latensen gör att det går att ifrågasätta användbarheten av det här försvarssystemet [5,7]. Det finns dock två scenarion där ILP fungerar för att skydda integriteten hos en användare i ett smart hem. Det första scenariot är då en enhet har ett konstant dataflöde. Det andra scenariot är då en enhet går att använda trots att den laggar.

3.4 Stochastic Traffic Padding

Ett nytt system för att skydda användaren av ett smart hem mot passiva nätverksobservatörer är Stochastic Traffic Padding (STP) eller stokastisk trafikutfyllnad [5]. STP är ett förslag för skydd av användarens integritet som Apthorpe et. al. [5] har byggt upp i sin studie. Det är precis som ILP ett system som bygger på trafikkvotering och det är byggt för att försvara användaren från passiva nätverksobservatörer. STP döljer trafiken från IoT-enheter

genom att skapa extra brus kring tiderna då en enhet sänder eller tar emot data. Genom att forma upp- och nedladdning av trafiken genom trafikkvotering skyddar försvarssystemet användarens integritet.

STP består av två olika strategier för att dölja användarens aktivitet i det smarta hemmet [5]. Första strategin är att STP laddar upp och ned trafikkvoteringar på ett ekvivalent sätt varje gång det sker en aktivitet (Figur 5, trafikperiod 1-3). På det här sättet hindras en passiv nätverksobservatör från att kunna skilja på olika aktiviteter som sker i hemmet. Den andra strategin går ut på att STP slumpmässigt laddar upp likadana trafikkvoteringar som vid användaraktivitet utan att det finns någon aktivitet att dölja (Figur 5, trafikperiod 0, 4-5). Det här gör att en passiv nätverksobservatör har svårt att skilja dessa perioder från perioder med riktig användaraktivitet.



Figur 5. Ett exempel på trafikfrekvens då STP är implementerat. En attackerare kan inte skilja på vilka perioder av utfyllnad som döljer trafik från en IoT-enhet och vilka som bara innehåller brus. Bild tagen från Apthorpe et. al. [5].

Enligt algoritmen för STP väljs först två fixerade värden för en sändningsperiod; varaktighet samt förekomstfrekvens (Algoritm 2) [5]. I början av varje sändningsperiod kontrolleras om en trafikkvotering (eng. traffic shaping) behöver göras. Om det behövs, så väljs det slumpmässigt ett likformigt startvärde och därefter utförs en trafikkvotering för att matcha det fasta trafikmönstret (eng. traffic pattern), enligt värdena som valdes i början. Om det däremot redan pågår en trafikkvotering på grund av

användaraktivitet eller att stoppningen (eng. padding) började redan på föregående period så upprepar sig detta steg en gång till. Modellen för trafikmönstret är slumpmässig och all användaraktivitet döljs enligt det förutbestämda trafikmönstret för att förhindra att en passiv nätverksobservatör ska kunna tolka användarens data.

```
1  padStart ← 0
2  padEnd ← 0
3  Function STP(t, q, T, R):
       /* Arguments: current time t, non-activity
          padding probability q, time period
          length T, padding rate R */
4      if t mod T = 0 and decisionFn(q, ...) then
           /* decisionFn() draws a random Boolean
              from a model parameterized on q and
              (optionally) previous user activity.
              */
5          padOffset ← uniformRandom(0, T)
6          if t + padOffset > padEnd then
7              padStart ← t + padOffset
8              padEnd ← padStart + T
9          else
10             padEnd ← padEnd + T
11     if padStart ≤ t ≤ padEnd then
12         padTraffic(R)
13     else if userActivityOccurring(t) then
14         padStart ← t
15         padEnd ← t + T
16         padTraffic(R)
```

Algoritm 2. Algoritm för STP.

Förutom att dölja den trafik som sänds ut från IoT-enheter så döljer STP även ingående trafik [5]. STP orsakar, beroende på vilken IoT-enhet som används, ingen eller liten extra belastning på nätverket och skapar ingen eller liten latens hos enheten [5].

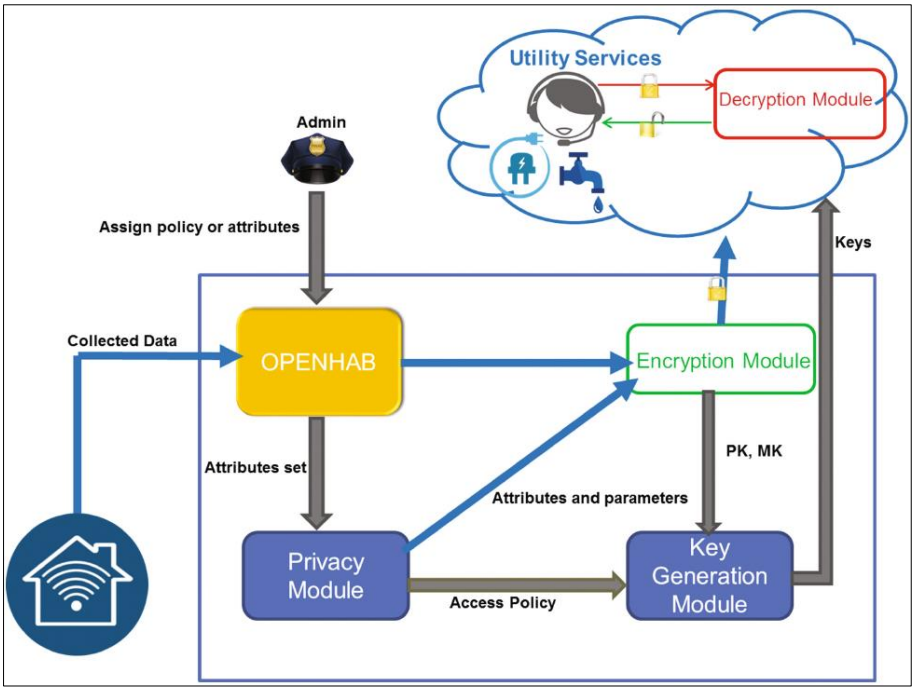
3.5 Attribute-Based Encryption

En metod för att skydda privat information är att kryptera den innan den skickas iväg från det smarta hemmet [11]. Attribute-Based Encryption (ABE) eller attributbaserad kryptering är en krypteringmetod som bygger på att använda publika nycklar. I ABE krypteras och dekrypteras data baserat på ett

antal attribut (till exempel postnummer, kön, ålder eller typ av sensor). ABE kan delas in i två olika scheman; Key-Policy ABE (KP-ABE) och Ciphertext-Policy ABE (CP-ABE).

Med ABE kan man ha en flexibel policy för åtkomstkontroll på sina krypterade data [11]. Det vill säga, det är enkelt att genom attributen specificera vem som får åtkomst till vilken data. Det här betyder att ABE respekterar principen om minimering av data, vilket är viktigt med tanke på till exempel allmänna dataskyddsförordningen eller som oftare används General Data Protection Regulation (GDPR).

Som nämndes ovan använder ABE ett slags krypteringssystem med publika nycklar [11]. Det här baseras på de olika attributen, som nämndes tidigare, för att få fram ett booleskt värde. Genom det booleska värdet dekrypteras meddelandena och mottagaren får tillgång till det data som skickats. De två olika scheman som används i ABE fungerar på lite olika sätt. I CP-ABE finns en åtkomstpolicy (eng. access policy) inbäddat i den krypterade texten och privata nycklar genereras genom en uppsättning attribut. I KP-ABE är åtkomstpolicyn sparad i en privat nyckel och den krypterade texten är beskriven genom en uppsättning attribut.



Figur 6. Arkitektur för ett försvarssystem med ABE och openHAB. Bild tagen från Chowdhury et. al. [11].

Chowdhury et. al. [11] använder ABE för att kryptera data som genereras i ett smart hem före det skickas iväg till en tredje part, det vill säga till ett användarkonto i molnet (Figur 6). I studien testades tre olika scheman; CP-ABE, KP-ABE och en förbättrad version av KP-ABE [11]. Dessutom användes ett mellanprogram (eng. middleware), openHAB.

ABE kan användas i ett smart hem för att skydda all data som sänds ut till olika molntjänster [11]. ABE i alla tre former kräver en del CPU samt minnesanvändning. Bäst kapacitet visade sig den förbättrade versionen av KP-ABE ha, men även där kan data inte samlas in oftare än var 20:e sekund.

4 Jämförelse mellan försvarssystem

De försvarssystem som behandlades ovan är ett urval av både befintliga system framtagna för andra syften samt nya system byggda specifikt för att skydda smarta hem. För att riktigt förstå skillnaderna behövs en jämförelse systemen sinsemellan (Tabell 2 nedan). Hur bra döljer systemet potentiellt privat information? Fungerar IoT-enheten utan latens om systemet används? Dessa frågor kommer att diskuteras och klarläggas nedan.

Som konstaterats kan en passiv nätverksobservatör extrahera, analysera och tolka data som skickas mellan IoT-enheter i smarta hem och molntjänster. För att hindra spridning av denna privata information kan användare av smarta hem implementera ett försvarssystem. De metoder som analyserats har olika tillvägagångssätt, men alla har samma målsättning; att försöka dölja personlig information.

Genom brandvägg stoppas förvisso all obehörig trafik till och från hemmet, men då det är påvisat att en stor del av IoT-enheterna också slutar fungera är det här inte ett reellt alternativ för ett smart hem [5]. En VPN tunnel fungerar mycket bra under vissa förutsättningar. Det måste vara mer än en enhet och trafik måste komma frekvent samtidigt som en enhet inte kan vara dominerande i mängden trafik som sänds ut.

ILP och STP använder sig båda av att fylla ut (eng. padding) eller sönderdela trafik samt att sända ut extra brus för att dölja användarens aktivitet. Det som skiljer dessa två metoder åt är att ILP frekvent sänder ut trafik och inne i detta finns användarens aktivitet inbakad. STP däremot har tidsperioder under vilka det sänds ut trafik och dessa tidsperioder kan innehålla användarens aktivitet eller vara tomt brus. ILP kräver mer av nätverket samtidigt som det finns en viss latens. Därför finns det begränsningar på när ILP kan användas och det är när det inte gör något att det finns en viss latens i IoT-enheten samt om enheten skapar ett konstant dataflöde.

Om den personliga informationen är väldigt känslig kunde ABE vara ett reellt alternativ eftersom det försvarssystemet krypterar all data som sänds ut till molntjänster. Nackdelen med ABE är dock att det finns begränsning på hur ofta en

IoT-enhet kan samla in data samt hur många IoT-enheter som kan vara i användning. Dock kunde man tänka sig att detta system kunde vara användbart på till exempel en hälsomonitor eller dylika enheter som samlar in privat information.

Apthorpe et. al. [5] föreslår att man kombinerar två av försvarsmetoderna ovan; STP samtidigt som man tunnlar trafiken genom en VPN. Det här skulle vara en metod för att helt och hållet dölja all information från attackerare. Detta eftersom STP enbart fokuserar på att dölja trafikfrekvensen (eng. traffic rate) medan protokoll, DNS värdnamn (eng. hostnames) och IP-adressers aktivitet inte döljs. Genom att kombinera STP och VPN skulle man ta bort begränsningen på antal enheter samt användningsfrekvens. Dessutom skulle man dölja även övrig metadata förutom trafikfrekvensen. Kombinationen av dessa två verkar därmed vara den försvarsmetod som döljer mest information på det mest effektiva sättet.

System	**Teknik**	**Hur det förhindrar avlyssning**	**Belastning på nät**
Brandvägg	Blockering	Blockerar all obehörig trafik	Mycket liten
Virtual Private Network (VPN)	Tunnel	Kanaliserar all trafik genom en tunnel, vilket gör det svårt att extrahera information från specifik IoT-enhet	Liten
Independent Link Padding (ILP)	Trafikkvotering (eng. traffic shaping)	Formar internettrafiken med stoppning (eng. padding), fragmentering eller genom att lägga till täckande paket. Konstant trafik även när IoT-enheter inte används	Måttlig - Stor 4KB/s och enhet
Stochastic Traffic Padding (STP)	Trafikkvotering (eng. traffic shaping)	Formar internettrafiken med stoppning (eng. padding), fragmentering eller genom att lägga till täckande paket. Slumpmässig trafik när IoT-enheter används	Mycket liten – Måttlig
Attribute-Based Encryption (ABE)	Kryptering	Krypterar data innan det sänds ut från hemmet.	Liten-Stor

Tabell 2. Jämförelse mellan olika försvarssystem

5 Diskussion och sammanfattning

I hemmets privata sfär kan det finnas saker en person inte vill ska komma till allmänhetens kännedom. I smarta hem finns IoT-enheter som per definition är uppkopplade till internet. Genom att koppla upp dessa enheter finns det risk att användarens integritet kränks och att uppgifter som läcker ut kan användas emot personen i fråga.

Noggrannhet med säkerheten i informationsgången mellan IoT-enheterna och molntjänsterna motverkar kränkning av användarens integritet. Det finns många olika metoder för att skydda den personliga informationen och det här arbetet har gått igenom några av dessa för att bringa klarhet i vilket försvarssystem som lämpar sig bäst att använda.

När en användare väljer ett försvarssystem till ett smart hem bör hen fundera på vilka egenskaper IoT-enheten ska ha. Får det förekomma latens? Hur känslig är informationen som enheten sänder ut?

När användaren funderat på dessa frågor borde hen ha svar på vilket försvarssystem som lämpar sig bäst för hens ändamål. VPN om det finns lagom många enheter i hemmet som används frekvent. ILP om sändningsfrekvensen är konstant eller om latens inte är ett hinder. ABE om informationen bör krypteras av sekretesskäl. Och till sist STP om inget av de övriga passar in. Även en kombination av olika försvarssystem kan vara ett reellt alternativ i vissa situationer, till exempel om man inte har så många enheter och därför valt STP, men samtidigt vill man även dölja kategorisk metadata så som DNS värdnamn eller IP-adresser.

Källor

[1] K.K. Patel, S. M. Patel. 2016. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. IJESC. V.6 Issue 5 pp 6122-6131. [Online] http://ostadr.ir/trans/iot/i4.pdf [hämtat 26.03.2020]

[2] Smart homes past present and future. Inside the smart home. [Online] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.661.3611&rep=rep1&type=pdf [hämtat 26.03.2020]

[3] D. Marikyan, S. Papagiannidis, and E. Alamanos. 2019. A systematic review of the smart home literature: A user perspective. Technological Forecasting & Social Change. V. 138 pp 139–154.

[4] P. Lalanda, J. Bourcier, J. Bardin and S. Chollet. 2010. Smart Home Systems. M. A. Al-Qutayri. Ed. INTECH Open Access Publisher. pp. 1-16. I. Book. [Online] https://www.intechopen.com/books/smart-home-systems/smart-home-systems [hämtat 26.03.2020]

[5] N. Apthorpe, D.Y. Huang, D. Reisman, A. Narayanan, N. Feamster. 2019. Keeping the Smart Home Private with Smart(er) IoT Traffic Shaping. Proceedings on Privacy Enhancing Technologies. vol. 2019, no. 3, pp. 128–148.

[6] L. C. De Silva, C. Morikawa, I. M. Petra. 2012. State of the art of smart homes. Engineering Applications of Artificial Intelligence. vol. 25, no. 7, pp. 1313–1321.

[7] T. Datta, N. Apthorpe, N. Feamster. 2018. A Developer-Friendly Library for Smart Home IoT Privacy-Preserving Traffic Obfuscation. Proceedings of the 2018 Workshop on iot security and privacy. pp. 43–48.

[8] M. Chan, D. Estève, C. Escriba, E. Campo. 2008. A review of smart homes- present state and future challenges. Computer methods and programs in biomedicine. vol. 91, no. 1, pp. 55–81.

[9] J. Liu, C. Zhang, Y. Fang. 2018. EPIC: A Differential Privacy Framework to Defend Smart Homes Against Internet Traffic Analysis. IEEE Internet of Things Journal. vol. 5, no. 2, pp. 1206–1217.

[10] Y. Meidan, M. Bohadana, A. Shabtai, J. D. Guarnizo, M. Ochoa, N. O. Tippenhauer, Y. Elovici. 2017. ProfilIoT: a machine learning approach for IoT device identification based on network traffic analysis. Proceedings of the Symposium on applied computing. vol. 128005, pp. 506–509.

[11] R. Chowdhury, H. Ould-Slimane, C. Talhi, M. Cheriet. 2017. Attribute-based encryption for preserving smart home data privacy. Lecture Notes in Computer Science. 10461 LNCS pp. 185-197.

[12] T. M. Mitchell. 2006. The discipline of machine learning. Vol. 9. Pittsburgh, PA: Carnegie Mellon University, School of Computer Science, Machine Learning Department. Book. [Online] Tillgänglig vid http://www-cgi.cs.cmu.edu/~tom/pubs/MachineLearningTR.pdf [hämtat 26.03.2020]

[13] J. A. O'Brien, G. M. Marakas. 2011. Management information systems. New York: McGraw-Hill/Irwin. Book. [Online] Tillgänglig vid http://fumblog.um.ac.ir/gallery/652/James_OBrien,_George_Marakas_Management_Information_Systems,_10th_Edition_____2010.pdf [hämtat 26.03.2020]

[14] A. A. Jaha, F. Ben Shatwan, M. Ashibani. 2008. Proper Virtual Private Network (VPN) Solution. 2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies. pp. 309–314.

[15] P. Christensson. 2006. Payload Definition. TechTerms. Sharpened Productions. [Online] https://techterms.com/definition/payload [hämtat 27.03.2020]