Examensarbete

HÖGSKOLAN I SKÖVDE

Internet of Things i smarta hemmet

En systematisk litteraturstudie för att kartlägga attackmetoder och verktyg

Internet of Things in the smart home

A systematic litterature study to map attack methods and tools

Examensarbete för kandidatexamen med huvudområdet informationsteknologi

Grundnivå 30 högskolepoäng
Vårtermin 2023

Student: Tommy Nylén

Handledare: Dennis Modig
Examinator: Ali Padyab

Förord

Detta är ett examensarbete som har genomförts på programmet Nätverks- och Systemadministration vid Högskolan i Skövde. I kursen hållbar utveckling gjordes en begränsad systematisk litteraturstudie om IoT inom industrin. Det var också där jag fick blodad tand för ämnet IoT. Efter en dialog med Dennis Modig kom jag fram till det ämne detta examensarbete omfattar.

Jag vill tacka min handledare Dennis Modig, som har bidragit med feedback men också en del anekdoter i ämnet. Jag vill tacka Ali Padyab, i sin roll som examinator, som har gett mig vägledning och konstruktiv feedback. Jag vill även tacka Martin Lundgren som har tagit sig tid och gett värdefulla råd under arbetets gång. Ett särskilt tack vill jag rikta till familj och vänner som har stöttat mig både under den tid detta examensarbete skrevs, och under de tre år som jag har studerat på högskolan.

Sammanfattning

Senaste åren har Internet of Things (IoT) haft en explosionsartad utveckling. En underkategori till IoT är det smarta hemmet, där smarta enheter kopplas samman med ett nätverk. Flera exempel på smarta enheter är smarta lampor, termostater, dörrlås, säkerhetskameror, smarta kylskåp och smarta tvättmaskiner. IoT i det smarta hemmet förbättrar både komforten och effektiviserar energiförbrukningen. Det är således en teknik som ökar användarnas livskvalitet. I takt med att IoT-enheter ökar i antal för det även med sig säkerhetsrisker. Cyberbrottslingar ser IoT-enheter som ett lukrativt mål och menar att de är enkla att attackera.

Den systematiska litteraturstudien hade som mål att identifiera och kartlägga vilka metoder samt verktyg som används i samband med en attack mot IoT-nätverk i hemmet. Ämnesspecifika sökord användes för att söka i vetenskapliga databaser. Artiklar som bedömdes uppfylla de fördefinierade urvalskriterierna lades till i en bibliografi. Omvänd snöbollsmetod användes för att hitta ytterligare artiklar. Artiklar genomgick en tematisk analys för att kartlägga vilka metoder och verktyg som förekom i litteraturen.

Studiens resultat visade att det förekom flera typer av metoder som kan riktas mot IoT-nätverk i hemmet. De flest omnämnda attackerna var Denial of Service (DoS), malware och Man-in-the-Middle (MitM). Resultatet visade även att det förekom många verktyg, där mångsidigheten gör att de kan användas till flera olika typer av attacker. De flest omnämnda verktygen var Hping3, Nmap och Wireshark.

Nyckelord: IoT, Internet of Things, smarta hemmet, attack, metod, verktyg

Abstract

In recent years, the Internet of Things (IoT) has experienced an uprising in the market. A subcategory of the IoT is the smart home, where smart devices are connected by a network. Several examples of smart devices are smart lights, thermostats, door locks, security cameras, smart refrigerators and smart washing machines. IoT in the smart home improves both comfort and makes energy consumption more efficient. Thus, it is a technology that increases the user's quality of life. As IoT devices increase in number, so does the security risks that come along with it. Cybercriminals see IoT as a lucrative target and find them easy to attack.

The aim of the systematic literature study was to identify and map which methods and tools are used in connection with an attack against IoT networks in the home. Subject-specific keywords were used to search in scientific databases. Articles judged to meet the predefined selection criteria were added to a bibliography. Reverse snowballing was used to find additional articles. Articles underwent a thematic analysis to map which methods and tools appeared in the literature.

The study's results showed that were several types of methods that can be targeted against IoT networks at home. The most mentioned attacks were Denial of Service (DoS), malware and Man-in-the-Middle (MitM). The result also showed that there were many tools, where the versatility allows them to be used for several different types of attacks. The most mentioned tools were Hping3, Nmap and Wireshark.

Keywords: IoT, Internet of Things, smart home, attack, method, tools

Innehållsförteckning

1 Introduktion

Termen “Internet of Things” myntades första gången år 1999 av Kevin Ashton under en presentation för Procter & Gamble. Han menade att människor var begränsade i att hantera data. Datorer skulle med all kunskap den samlat in, självständigt analysera och bearbeta data på ett effektivare sätt för att minska tidsåtgång och kostnader. Ett av de första exemplen av IoT introducerades i början på 1980-talet. Några programmerare anslöt sig, via internet, till en Coca Cola-maskin som stod i Carnegie Mellon University med syftet att kontrollera om dryck fanns tillgänglig och om den var kall (DataVersity, 2022).

Sedan dess har IoT utvecklats till att bli ett system där komponenter är sammankopplade och dataöverföringen oftast sker utan någon mänsklig inblandning. IoT använder sensorer och ställdon för generering och insamling av data, för att utföra effektiva anslutnings- och analysuppgifter (Sivapriyan et al., 2021).

Under de senaste åren har tillämpningen av IoT inom hemautomation setts som ett nytt paradigm som tillhandahåller tjänster till slutanvändaren. Hemautomation gör det möjligt att hantera ljus, klimat och säkerhet i hemmet. Tack vare sin potential har hemautomation blivit populärt i hela världen (Wang et al., 2022).

Meneghello et al. (2019) skriver att protokoll som används inom det smarta hemmet är många till antalet. De IoT-enheter som lanserats på marknaden, tillsammans med antalet protokoll, har lett till fler cyberattacker. Brottslingar ser dessa enheter som lukrativa mål och menar att attacker ofta är enkla att utföra. Attackerna kan utföras med målet att kränka användares integritet och läcka personlig information. Det kan omfatta allt från manipulering av rumstemperatur till att samla in information om en persons plats och levnadsvanor.

Syftet med denna studie är att kartlägga vilka typer av metoder som används, i samband med, en attack som utförs mot ett IoT-nätverk i hemmet. Det förekommer många olika typer av metoder och denna studie ska belysa hur de går till. Dessutom ska studien även kartlägga vilka typ av verktyg som används.

Tidigare artiklar som handlar om attacker kommer att granskas för relevant data. Målet med studien är att sammanställa vilka metoder samt verktyg som används när en angripare attackerar IoT-nätverk i hemmet.

Resterande rapport är strukturerad i flera kapitel, där vart och ett har ett specifikt syfte. Kapitel 2 ger läsaren en översikt av bakgrund, centrala koncept och tidigare forskning relaterat till ämnet. I kapitel 3 förklaras problemområdet och målet med studien. I kapitel 4 beskrivs forskningsmetodiken. Kapitel 5 beskriver hur forskningsmetodiken har implementerats i praktiken. Kapitel 6 presenterar resultatet av studien. I kapitel 7 förs en diskussion gällande studiens resultat i relation till tidigare forskning. Dessutom diskuteras validitet av resultat, genomförandet, framtida forskning, begräsningar med studien samt etiska och samhälleliga aspekter. Avslutningsvis, i kapitel 8, dras slutsatser utifrån studiens resultat.

2 Bakgrund

IoT är ett begrepp som används för att beskriva de föremål som utrustats med förmågan att ansluta till internet och andra nätverk (MSB, u.å.). Chanal och Kakkasageri (2020) beskriver IoT som ett nätverk av fysiska objekt inbäddade med beräknings- och kommunikationskapacitet, vilket möjliggör att dessa objekt kan kopplas samman och utbyta data via internet. Enheter som är uppkopplade mot internet är inget nytt i sig, då exempelvis datorer har varit uppkopplade mot internet de senaste decennierna. Dagens sensorer har krympt i storlek, vilket har lett till att de enheter som kopplas upp mot internet minskat i storlek.

Antalet IoT-enheter världen över förväntas nästan tredubblas från 9,7 miljarder år 2020 till drygt 29 miljarder år 2030 (Transforma Insights, 2022). Med en befolkning på cirka 8 miljarder, innebär det att varje person kommer, i genomsnitt, nyttja drygt 3 IoT-enheter.

Potentialen hos IoT är mångfaldig, då den går att tillämpa i olika typer av situationer och miljöer. Vanliga användningsområden är inom industri, jordbruk, sjukvård, smarta hemmet och transport (Al-Fuqaha et al., 2015). Under de senaste åren har smarta hemmets popularitet ökat världen över. Med hjälp av IoT har hemautomation kunnat byggas upp i det smarta hemmet, för att styra och övervaka exempelvis belysning, klimat och övriga apparater (Wang et al., 2022).

Skillnaden mellan IoT och IoT i smarta hemmet beskrivs av Ray och Bagwari (2020). De menar att IoT är sammankopplingen av fysiska enheter och objekt inbäddad med internetanslutning, beräkningskraft och andra komponenter. Det möjliggör att de kan kommunicera, skapa, samla in och utbyta data. IoT i det smarta hemmet är däremot en specifik tillämpning av IoT, där fokus ligger på hushållsapparater och andra enheter. Genom att använda sig av IoT kan dessa typer av apparater kopplas samman och bilda ett smart hemnätverk. IoT i det smarta hemmet kan ses som en underkategori till det större IoT-ekosystemet.

I takt med att IoT-enheter ökar i antal, för det även med sig säkerhetsrisker. Cybersäkerhetsföretaget Kaspersky rapporterade att de under första halvåret 2021, kunde se en fördubbling i antalet attacker mot IoT-enheter. Under de sex månaderna hade deras honeypots, en typ av fälla för hackare, blivit attackerade över 1,5 miljarder gånger. Detta kan jämföras med halvåret innan, då de attackerades drygt 600 miljoner gånger (Iottechnews, 2021).

2.1 Generisk IoT-arkitektur

IoT-enheter är uppbyggda på en unik arkitektur. Det finns många olika modeller, men den mest grundläggande arkitekturen består av tre lager: applikations-, nätverks- och perceptionslager (Swamy & Kota, 2020). Varje lager tillhandahåller sina egna funktioner och har samtidigt egna unika hot. Eftersom lagren är anslutna och förlitar sig till varandra, påverkar varje enskilt lager säkerheten i de andra lagren (Rizvi et al., 2018).

Applikationslagret är det lager som användaren interagerar med. Lagret kan på olika sätt anpassas för olika typer av IoT-applikationer (Gerodimos et al., 2023). Nätverkslagret ser till att upprätthålla en säker och tillförlitlig kommunikation mellan olika enheter med hjälp av standardiserade nätverksprotokoll (Wang et al., 2022). Kommunikationsmedium kan vara antingen av trådbunden eller trådlös karaktär. Vanligt förekommande protokoll inom IoT är Bluetooth Low Energy (Bluetooth LE), 802.15.4, LTE-Advanced (LTE-A), Near Field Communication (NFC), Wireless Fidelity (WiFi), ZigBee, Z-Wave (Al-Fuqaha et al., 2015; Al-Sarawi et al., 2017; Swamy & Kota, 2020). Perceptionslagret består av de fysiska enheterna och är det lager som har till uppgift att samla in information och omvandla till digitala data (Rizvi et al., 2018). De fysiska enheterna kan exempelvis vara sensorer, ställdon, RFID-taggar eller IP-kameror (Gerodimos et al., 2023).

2.2 IoT och dess utmaningar

Problemet med IoT är inte bara att de förväntas öka i antal väldigt snabbt, utan också att antalet kommunikationsvägar ökas ännu snabbare. Allt fler tillverkare kommer att konkurrera på marknaden vilket resulterar i att antalet varianter av hårdvara, mjukvara och protokoll växer. Det kommer innebära följdproblem med den systemkunskap som krävs för att säkra upp systemen (MSB, 2020).

Goswami et al. (2020) pekar på att standardisering är en av de största utmaningarna inom IoT. Flera standardiseringsorgan som ETSI, ITU, IETF och IEEE är involverade i att utveckla ramverket för IoT-utveckling. I och med att IoT fortfarande inte är tillräckligt moget ännu menar Sanaullah och Liu (2022) att experterna inom området inte kan definiera en välorganiserad tillverkningsstandard.

Iqbal et al. (2020) förklarar att skillnaden mellan ett traditionellt nätverk och ett IoT-nätverk är de resurser enheter på den yttersta änden har att jobba med. Enheter i ett IoT-nätverk består ofta av sensorer och taggar, där de jobbar med låg effekt, begränsat minne, lågt lagringsutrymme och begränsad beräkningskraft. Enheter i ett traditionellt nätverk jobbar däremot med större mängder resurser och består av bärbara datorer, stationära datorer, servrar samt smarttelefoner. Traditionella nätverk kan därför upprätthålla komplexa säkerhetsprotokoll. På grund av att IoT-enheter generellt har begränsade resurser menar MSB (2020) att det blir svårt att balansera säkerhetsmekanismer som exempel kryptering med funktionaliteten enheten förväntas leverera. Säkerheten tas inte på allvar och kan leda till att det blir svårt om inte omöjligt att i efterhand uppdatera och åtgärda säkerhetshål i enhetens mjukvara. Skulle en uppdateringsmekanism finns på plats anser Sanaullah och Liu (2022) att tillverkare är för långsamma att uppdatera och underhålla sina enheter och tjänster.

2.3 Smarta hemmet

Jabbar et al. (2018) skriver att det smarta hemmet är en nyckelkomponent i IoT. Allt har en tilldelad IP-adress och kan fjärrstyras samt övervakas på distans. Hushållsapparater och andra apparater är sammankopplade för att kontrollera alla aspekter av det smarta hemmet.

Hemautomation har blivit en av de viktigaste teknikerna inom det smarta hemmet. Den möjliggör styrning och övervakning av belysning, klimat och övriga apparater i hemmet (Wang et al., 2022). Det förbättrar både komforten och effektiviserar energiförbrukningen (Schurgot et al., 2015). Implementering av IoT i det smarta hemmet kan se ut på många olika sätt. Systemet består av flera sammankopplade komponenter som tillsammans bildar en problemfri och bekväm användarupplevelse.

En central gateway fungerar som hjärnan i hela systemet och har som uppgift att kommunicera och kontrollera alla andra komponenter i systemet. Den kan vara fristående eller integreras i en annan komponent. Gateway har flera olika funktioner som exempelvis enhetskonfiguration, identitetshantering, hantering av auktorisering och autentisering (Ray & Bagwari, 2020).

På enheter är sensorer och ställdon placerade, vilket har sin egen specifika funktion. Sensorer mäter olika saker som rörelse, temperatur, luftfuktighet, luftkvalitet, ljud och ljus. Ställdon däremot styr eller kör en enhet. Data som samlats in av en sensor skickas till en central gateway som i sin tur beräknar styrsignaler. Styrsignalerna skickas sedan till ett ställdon som utför åtgärden (Feng et al., 2017).

Smarta enheter är de enheter som kan styras via nätverk med olika trådlösa protokoll. Flera exempel på smarta enheter är smarta lampor, termostater, dörrlås, säkerhetskameror, smart kylskåp och smart tvättmaskin. Anslutning till en central gateway sker antingen genom trådbunden eller trådlös anslutning (Ray & Bagwari, 2020).

Med hjälp av ett användargränssnitt kan en användare integrera med ett IoT-system. Det sker vanligtvis med en mobilapplikation eller någon typ av pekplatta. Samtidigt har det tillkommit virtuella röstassistenter som slås samman med IoT för att bredda användningsområdet (Rahman et al., 2020).

Smarta hemnätverk är en sammankoppling mellan enheter, nätverksprotokoll och anslutningsmedium. Det skapar ett dynamiskt system med målet att effektivisera hanteringen av kommunikation och tillhandahålla tjänster till användarna (Ray & Bagwari, 2020). För att ett system ska kunna fungera korrekt behövs en stabil och pålitlig internetanslutning. Det gör att systemet kan fjärrstyras med hjälp av mobiltelefoner som är uppkopplad på samma nätverk (Sivapriyan et al., 2021).

2.4 Informationssäkerhet

Information är en byggsten för många organisationer i det digitala samhället. Information kan skapas, bearbetas, analyseras och lagras. Den behövs för det mesta som görs i vardagen (Informationssäkerhet, 2015). En del information kan vara värdefull både för en organisation och privatperson. Det kan omfatta allt från forskningsmaterial producerat av en organisation till fotografier tillhörande en person. Därför är det av stor vikt att informationen skyddas så att endast personer med rätt behörighet har tillgång till den, att informationen är riktig och att den är tillgänglig när den behövs (MSB, 2022).

Informationssäkerhet syftar till de säkerhetsåtgärder som verkställs för att skydda informationen från obehörig åtkomst. Det finns flera metoder som kan användas för att säkerställa att informationen skyddas. Några exempel är starka lösenord, kryptering av data (Sanaullah & Liu, 2022), implementering av brandväggar (Gupta et al., 2017) och IDS-system (Ghadeer, 2018).

2.5 Tidigare forskning

Med en snabb utveckling inom IoT har den letat sig in i allt fler områden som exempelvis det smarta hemmet. Mohammad et al. (2019) menar att det därför ställs högre krav på datainsamlingen och att den inte hamnar i händerna på illvilliga motståndare. Deras studie presenterade attacker inom olika IoT-applikationer. Resultatet visade att det smarta hemmet var sårbart mot avlyssnings-, imitations-, DoS- och malware-attacker.

IoT kopplas samman och utbyter data med hjälp av kommunikationsprotokoll. Tillämpning av IoT inom det smarta hemmet ses som ett av de viktigaste områdena. Ray och Bagwari (2017) diskuterar smarta hemmet och dess grundläggande komponenter samt hur IoT tillämpas inom smarta hemmet. De diskuterar även kommunikationsprotokoll som används vid kommunikation mellan enheter i det smarta hemmet och dess säkerhetsbrister. De föreslog en ny säkerhetsmodell med en brandvägg som används för att skydda nätverket mot angripare.

Många IoT-enheter som lanseras på marknaden är ofta billiga och saknar säkerhetsfunktioner. Det är viktigt att ta itu med dessa säkerhetsfrågor framför allt inom det smarta hemmet. Bastos et al. (2018) presenterar en heltäckande undersökning av IoT-teknik och säkerhetsfrågor riktat mot smarta hemmet och stadsmiljöer. Möjliga lösningar diskuteras för att förbättra IoT-säkerheten för nutida och framtida attacker mot dataprotokoll och anslutningar. Ett förslag var att utveckla ett nytt protokoll för att förbättra säkerheten. Problemet är att det är svårt för ett nytt protokoll att konkurrera ut befintliga protokoll. Deras lösning är istället att använda ett av de mest använda protokollen och utveckla säkerhetsfunktioner på det.

Rizvi et al. (2020) definierar attackytan för IoT-nätverk i hemmet. Attackytan i ett nätverk sammanfattar alla penetrationspunkter, eller attackvektorer som de också kallas. En angripare använder sig av dessa attackvektorer för att modifiera eller extrahera data i den utsatta miljön. De kom fram till att osäkra IoT-enheter i hemmet kan utgöra attackvektorer för större och dyrare attacker. De beskrev hur sårbarhetsskannrar kan automatisera och förenkla processen med att kartlägga attackytan. Verktyg som sniffar paket eller kartlägger nätverk används för att skanna IoT-nätverk och leta efter enheter som använder sig av klartext-lösenord, öppna portar eller andra sårbarheter.

Saxena et al. (2017) presenterar en undersökning av smarta hemnätverk och dess funktionalitet ur ett säkerhetsperspektiv. Studien tar upp vilka utmaningar smarta hemnätverk ställs inför och vilka säkerhetsproblem det kan ge. De utmaningar som beskrivs i studien är exempelvis att enheter i smarta hemnätverk är heterogena, systemen ofta är komplexa,

behovet av nya protokoll uppstår när heterogena enheter används i nätverken. De diskuterar även olika attacker som förekommer i smarta hemnätverk. Exempel på dessa attacker är avlyssning, DoS, MitM, replay, sinkhole, trafikanalys och wormhole.

Ali et al. (2017) har i sin studie undersökt säkerhetsattacker som riktas mot det smarta hemmet och har utvärderat inverkan på den övergripande systemsäkerheten. De klassificerade säkerhetsattackerna i två kategorier: passiva och aktiva attacker. De menar att vid passiva attacker försöker angripare få tag i systeminformation utan att påverka systemresurser. Exempel på passiva attacker är avlyssning och olika övervakningstekniker. Vidare menar de att vid aktiva attacker används information från den passiva attacken för att antingen ändra på systemresurser eller systemets operationer. Exempel på aktiva attacker är maskar, malware och DoS.

3 Problemformulering

Framväxten av hemautomationssystem ses som ett nytt och lovande paradigm, vilket tillhandahåller smarta hemmet-tjänster till användare (Wang et al., 2022). Samtidigt som IoT-enheter och hemautomatisering får en större utbredning ökar även säkerhetshot och sårbarheter för dessa system. Säkerhet riktat mot IoT har haft och kommer även i framtiden att ha en stor roll inom forskningen. I dagsläget existerar det en omfattande mängd litteratur som behandlar ämnet (Rizvi et al., 2018). Företag som tillverkar produkter inom IoT-segmentet har inte något incitament till att skapa produkter som har en hög säkerhet. Deras fokus ligger istället på funktionalitet och hålla kostnader nere. Detta har öppnat upp för angripare att utnyttja sårbarheter och attackera IoT-enheter (Neshenko et al., 2019).

År 2016 utförde cyberbrottslingar DDoS-attacker (Distributed Denial of Service) mot DNS-leverantören (Domain Name System) Dyn, och som konsekvens skapades det stora driftstörningar på flera stora företag som exempelvis Amazon, Netflix, PayPal, Spotify och Twitter. För att lyckas med denna bedrift utnyttjade cyberbrottslingarna svagheter i tusentals IoT-enheter som därefter kunde kapas och användas i attacken (Neshenko et al., 2019).

Under en fyra dagars lång period år 2017, registrerade Radware’s honeypots 1 895 PDoS-attacker (Permanent Denial of Service) runt om i världen. BrickerBot var en mjukvara som riktade in sig på att utföra brute-force-attacker mot telnet i IoT-enheter, för att därefter köra ett antal kommandon som korrumperade enheterna. Attackerna lyckades förstöra miljontals IoT-enheter (Radware, 2017).

Hemsäkerhetsföretaget Ring LLC är känd för sina produkter riktat mot det smarta hemmet. Exempel på produkter är övervakningskameror och smart dörrklocka med videofunktion. År 2019 blev en av deras övervakningskameror attackerad och kapad. Det visade sig att cyberbrottslingen hade skapat en egen mjukvara för att ta över övervakningskameror från Ring LLC. Mjukvaran utförde en brute-force-attack för att gå igenom användarnamn/email samt lösenord för att försöka logga in på konton kopplade till övervakningskameror (Vice, 2019).

Dessa typer av attacker är bara några exempel på hur utsatta IoT-enheter är i allmänhet och inom det smarta hemmet i synnerhet. Det får till följd att konsumenters attityd till IoT-enheter påverkas. Enligt en undersökning gjord av Microsoft och Greenberg Strategy, visade det sig att 90% av deltagarna trodde, i princip, att alla IoT-enheter kunde bli hackade. Lika stor andel svarade att tillverkarna måste se till att förbättra säkerheten på sina produkter (DarkReading, 2019).

Därför finns det ett behov av att kartlägga vilka attacker som förekommer i det smarta hemmet. Syftet med denna studie är att skapa en bild av hur en attack mot ett IoT-nätverk går till. Studien kommer att undersöka hur metodiken ser ut när en attack utförs. Vidare kommer studien även undersöka vilka typer av verktyg som används i samband med en attack.

Frågeställningen för studien ser ut enligt följande:

- Vilka metoder samt verktyg används vid en attack av IoT-nätverk inom hemmet?

3.1 Motivering

Sivapriyan et al. (2021) har analyserat vilka säkerhetsutmaningar och problem som finns med IoT-aktiverade hemautomatiseringssystem. Detta gav en överblick om de säkerhetshot, risker och krav en användare behöver vara medveten om. Chen et al. (2018) fokuserade på säkerhetshot och integritetsproblem. De valde att fördjupa sig i varje lager av IoT-arkitekturen. Det förekom klassificeringar av attacker mot IoT-arkitekturen och olika applikationsscenarier, däribland det smarta hemmet. Även Abdullah et al. (2019) har diskuterat hot mot IoT där de poängterar hur viktigt det är att ta reda på vilka hot som finns och hur de kan påverka det smarta hemmet. De delade upp hoten i fyra kategorier: DoS, avlyssning, imitation och äventyrande av system.

I takt med att IoT-enheter ökar i antal, kommer cyberbrottslingar lägga allt större fokus på att attackera dessa. Anledningen till detta är enligt Iqbal et al. (2020) att den inbyggda säkerhetsmekanismen är svag och att det saknas en standardiserad arkitektur. Nawir et al. (2017) konstaterar att säkerhetsbrister inom IoT kan resultera i negativa effekter för användarna. En stor mängd data placeras på IoT-enheter som kan nås på distans över hela världen. Deras studie sammanfattar olika typer av attacker som kan utföras mot IoT-enheter, däribland spoofing, replay, DoS, sybil. Davis et al. (2020) valde i sin studie att undersöka sårbarheter hos IoT-enheter i det smarta hemmet. De menar att attacker kan klassificeras enligt fyra olika kategorier: fysiska, nätverk, mjukvara och kryptering.

Mot bakgrund av ovan samt den tidigare forskningen i kapitel 2.5, belyser många artiklar vilka attacker som kan utföras mot IoT och det smarta hemmet. Det de har gemensamt är att dessa attacker inte diskuteras på ett djupare plan. Man belyser inte heller vilka verktyg som används för att utföra dessa attacker. Därför kommer denna studie att på ett djupare plan belysa attacker i kombination med de verktyg som finns att använda.

3.2 Forskningsmål

Målet med studien är att göra en sammanställning av de metoder och verktyg som används vid attacker mot ett IoT-nätverk i hemmet. Studien ämnar till att identifiera och analysera det gap som existerar i forskningen relaterat till forskningsfrågan ovan. För att svara på forskningsfrågan ska denna studie använda sig av en strukturerad litteraturstudie för att samla in data från artiklar. Det kommer sedan att ligga till grund för den sammanställning som kommer att göras.

4 Metod

Detta kapitel kommer redogöra för de metoder som valts för denna studie. Vidare omfattar kapitlet även de delmål som har utvecklats, vilka avgränsningar som har gjorts samt vilka validitetshot som finns relaterat till studien.

Berndtsson et al. (2008) skriver att när ett mål har utvecklats, behöver ett antal mindre delmål tas fram. För varje delmål behöver det väljas en metod. Det behöver inte nödvändigtvis betyda att samma metod används för att lösa samtliga delmål. Vad som är viktigt att tänka på är att valet av metod kan påverka kvaliteten samt slutsatsen som dras i studien.

Målet med studien är att kartlägga vilka typer av metoder samt verktyg som används när en attack utförs mot ett IoT-nätverk i hemmet. För att kunna besvara forskningsfrågan fastställdes det att en systematisk litteraturstudie är den mest tillämpbara metoden.

Enligt Snyder (2019) är en systematisk litteraturstudie att föredra när det gäller att utvärdera kunskapsläget om ett visst ämnesområde och kan användas för att identifiera kunskapsluckor i forskningen. Kitchenham och Charters (2007) skriver att en systematisk litteraturstudie kan undersöka i vilken utsträckning empiriska data stödjer eller motsäger en hypotes.

Det har genomförts mängder med forskning på området IoT det senaste decenniet. Genom att undersöka den existerande forskningen ska det vara tillräckligt för att kunna besvara forskningsfrågan på ett bra sätt. Andra metoder för insamling av data har övervägts. Exempelvis en intervju-metod skulle kunna fråga personer med god kännedom inom IoT, för att ta del av deras subjektiva empiriska kunskaper. Det finns dock en risk med detta förehavande, då det är möjligt att missa hur den objektiva skildringen ser ut. En annan metod som skulle kunna användas är en experimentell studie. Den ger flera fördelar jämfört med en systematisk litteraturstudie.

Wohlin et al. (2012) skriver att ett experiment ger forskare kontroll på de variabler som manipuleras och mäts. Studien kan utformas så de faktorer som är av intresse isoleras. Med hjälp av denna kontroll möjliggör det undersökning av orsakssamband mellan variabler. De skriver även att experiment kan vara antingen människoorienterade eller teknikorienterade. I denna studie hade ett teknikorienterat experiment varit att föredra, där olika verktyg appliceras mot specifika objekt, eller IoT-nätverk. Nackdelen med en experimentell studie är att det kan vara en lång process att skapa en miljö där undersökning av rätt variabler genomförs. Därför har experiment som metod valts bort i förmån för en systematisk litteraturstudie.

Vid användning av en systematisk litteraturstudie som metod, är det möjligt att vända sig till den forskning som har genomförts på ämnesområdet, för att erhålla en detaljerad bild av läget. Det är möjligt att använda många olika källor för att uppnå en opartisk skildring av ämnet.

Den data som blir insamlad i litteraturstudien kommer att genomgå en tematisk analys. Braun et al. (2006) slår fast att tematisk analys syftar till den analysmetod som används för att

identifiera, analysera och rapportera mönster inom data. De menar vidare att en stor fördel med tematisk analys är dess flexibilitet. Till skillnad från andra typer av analysmetoder, är inte tematisk analys kopplad till ett teoretiskt eller epistemologiskt ramverk. Genom sin flexibilitet kan metoden användas för att ge en detaljerad redogörelse för data.

4.1 Systematisk litteraturstudie

Kitchenham och Charters (2007) definierar systematisk litteraturstudie som ett sätt att identifiera, utvärdera och tolka forskning som är relevant för en specifik forskningsfråga. Syftet är att ge en heltäckande bild av befintliga bevis, vilket innebär att identifiering, analys och tolkning måste utföras på ett vetenskapligt sätt. Utförandet av en systematisk litteraturstudie är enligt (Jesson et al., 2011) en både tids- och resurskrävande metod. Oftast är det mer än en person involverad i denna typ av arbete.

En systematisk litteraturstudie kan enligt (Kitchenham & Charters, 2007) sammanfattas i tre generella faser: planera undersökning, genomföra undersökning och rapportera undersökning. Jesson et al. (2011) har sedan utvecklat mer detaljerade riktlinjer för hur en systematisk litteraturstudie utförs steg-för-steg:

1. Definiera forskningsfråga
2. Designa ett undersökningsprotokoll
3. Sökning av litteratur
4. Applicera urvalskriterier
5. Kvalitetsgranska utvald litteratur
6. Sammanställ resultat

Ett av de viktigaste stegen i en systematisk litteraturstudie är att definiera en eller flera forskningsfrågor. Det fungerar som en grundsten när övrigt arbete sedan ska utformas. Undersökningen inleds med att en forskningsfråga definieras. Därefter utformas ett undersökningsprotokoll för att hitta relevanta artiklar. Det omfattar exempelvis att välja söktermer som ska användas i databaser samt att utforma vilka urvalskriterier som ska appliceras på artiklar. Urvalskriterierna ska hjälpa till att kvalitetsgranska artiklar. De accepterade artiklarna kommer sedan att analyseras och därefter sammanställs resultatet av analysen.

4.1.1 Databaser

Jesson et al. (2011) konstaterar att det inte är tillräckligt att söka från endast en databas för att hitta alla relevanta artiklar. Databasen kan ha ett omfattande utbud av artiklar, men kan samtidigt sakna många artiklar relevanta för forskningsområdet. Akademiska artiklar som är referentgranskade är enligt (Jesson et al., 2011), den bästa datakällan till en systematisk litteraturstudie.

Högskolan i Skövde tillhandahåller fri tillgång till omkring 80 databaser med olika forskningsinriktning. Brereton et al. (2007) identifierade att de indexerade databaserna ACM Digital Library, IEEExplore och ScienceDirect är relevanta för mjukvaruutveckling

(Software Engineering). De bedöms vara tillämpbara även inom detta forskningsområde då informationsteknologi angränsar till mjukvaruutveckling.

Följande databaser kommer att användas:

- ACM Digital Library
- IEEExplore
- ScienceDirect

4.1.2 Söktermer

Det är viktigt att skapa en träffsäker sökstrategi, då hela studiens kvalité bygger på de artiklar som används. Snyder (2019) menar på att söktermer bör baseras på ord eller begrepp som är relaterade till forskningsfrågan. Ett vanligt tillvägagångssätt är att skapa en lista med akronymer, förkortningar och alternativa stavningar.

För att ytterligare förbättra sökresultatet kan logiska operatörerna AND, OR och NOT användas (Jesson et al., 2011). Logiska operatörer används för att begränsa antalet sökträffar (Berndtsson et al., 2008). Varje databas har sina egna regler hur sökningar får utföras. I och med att alla databaser inte klarar av att hantera komplexa söktermer, ställer det höga krav på att skapa söktermer som kan användas i olika databaser. Det får inte vara för komplexa söktermer, inte heller för enkla, med risk för att missa relevanta artiklar.

Sökord i tabell 1 nedan har testats i olika kombinationer i de valda databaserna. De sökningar som initialt utfördes visade på relevanta sökträffar och av den anledningen beslutades det att dessa sökord används i litteraturstudien.

Tabell 1 – Sökord (författarens egna)

Sökord	**Förklaring**
IoT Internet of Things	Studien bygger på att hitta relevanta artiklar där attacker utförs mot IoT-nätverk. IoT är en akronym till Internet of Things och syftar till att fånga upp relevanta artiklar med fokus på IoT.
Home automation Smart home	Studien är inriktad mot smarta hemmet. ”Home automation” och ”Smart home” syftar till att erhålla relevanta artiklar som fokuserar på smarta hemmet.
Attack Penetration Tool	Studien syftar till att hitta relevanta artiklar som nämner metoder och verktyg som används vid attacker.

4.1.3 Urvalskriterier för litteratur

När de potentiellt relevanta primärstudierna har erhållits är det dags att bedöma om de är faktiskt relevanta. Urvalskriterier är avsedda för att identifiera primärstudier som ger svar på forskningsfrågan (Kitchenham & Charters., 2007). Både Kitchenham och Charters (2007) samt Wohlin et al. (2012) menar att urvalskriterier bör utvecklas innan studiens start. De kan dock behöva justeras då alla aspekter av urvalskriterierna inte är helt uppenbara i planeringsstadiet. I tabell 2 nedan, finns de urvalskriterier som kommer att användas i denna litteraturstudie.

Tabell 2 – Urvalskriterier (författarens egna)

Inkluderingskriterier	IK1. Ska ha genomgått referentgranskning (peer-review)
	IK2. Publicerat i journal eller konferens
	IK3. Publicerat mellan 2018 och 2023
	IK4. Ska vara skrivet på engelska
	IK5. Ska vara relevant för ämnet i fråga
Exkluderingskriterier	EK1. Uppfyller inte inkluderingskriterierna
	EK2. Betalvägg eller krav på inloggning
	EK3. Dubbletter
	EK4. Bristande beskrivning av metod, implementation eller resultat

Referentgranskade artiklar genomgår en utvärderingsprocess för att garantera att de är kvalitativa. Det är inte förrän de uppfyller en viss standard som de accepteras för publicering. IK1 ser till att filtrera artiklar som håller en hög kvalité. För att bibehålla en hög kvalité, definierar IK2 att artiklar ska vara publicerade i antingen tidskrifter eller konferenser.

IK3 definierar den tidsram som gäller för artikelpubliceringarna i databaserna. De artiklar som ligger utanför tidsramen avfärdas. Anledningen till att just denna tidsram (2018–2023) har valts är att IoT utvecklas snabbt. Risken finns att äldre artiklar som erhålls i sökningarna, demonstrerar attacker som har hunnit bli utdaterade.

Majoriteten av artiklar som publiceras är skrivna på engelska. I en del databaser förekommer det artiklar på andra språk. IK4 definierar vilket språk en artikel ska vara skriven på.

IK5 definierar att artikeln ska innehålla relevant data relaterat till denna studie och dess forskningsfråga. Det innebär att artiklar som handlar om olika typer av metoder för att attackera IoT-nätverk i hemmet samt vilka verktyg som används i samband med det, är relevant för litteraturstudien. Däremot om artikeln handlar om attacker mot en annan typ av applikation, exempelvis sjukvård, bedöms den inte som relevant.

Sökträffarna granskas och filtreras i tre steg: titel, abstrakt och full text. Det innebär att sökträffarnas titel granskas i ett första steg. Återstående sökträffar granskas sedan i dess abstrakt. Till sist granskas de sista sökträffarna i sin helhet. De sökträffar som återstår efter dessa tre steg bedöms vara relevanta utifrån ämnet som valts för denna studie.

Utöver inkluderingskriterierna finns det dessutom exkluderingskriterier som syftar till att avfärda artiklar, vilket resulterar i en högre kvalité av de accepterade artiklarna. EK1 innebär att artiklar måste uppfylla samtliga inkluderingskriterier (IK1-IK5). Övriga artiklar avfärdas. EK2 definierar att det inte får finnas en betalvägg eller annan typ av inloggningskrav för att komma åt en hel artikel. EK3 definierar att det inte får förekomma dubbletter av artiklar. Enligt Kitchenham och Charters (2007) är det viktigt att inte inkludera flera publikationer av samma data då det kan påverka resultatet. Det ställer således krav på att filtrera bort identiska artiklar. Förekommer det dubbletter av artiklar ska den mest kompletta användas (Wohlin et al., 2012). EK4 definierar att om artiklar bedöms ha en bristande beskrivning av metod, implementation eller resultat ska de avfärdas.

4.1.4 Omvänd snöbollsmetod

När en systematisk litteraturstudie utförs är det viktigt att hitta relevanta primärstudier. Kitchenham och Charters (2007) skriver att inledande sökningar kan utföras i olika databaser men att det ofta inte är tillräckligt för en systematisk litteraturstudie. Andra källor behöver tas i beaktande när relevanta artiklar ska sökas fram.

Wohlin et al. (2012) påstår att omvänd snöbollsmetod (backward snowballing) är en användbar och kompletterande metod för att undvika att förbise artiklar som innehar relevans för studien. Metoden går ut på att systematiskt granska primärstudiernas referenslistor efter ytterligare primärstudier som kan användas i den egna studien. Det är samtidigt en avvägning mellan att hitta alla relevanta primärstudier och att inte få för många falskpositiva resultat, vilket skapar mer manuellt arbete.

Urvalskriterier appliceras på samtliga primärstudier i referenslistorna. Titel, abstrakt och full text granskas för sin relevans för ämnet i fråga. Anses en referens uppfylla alla urvalskriterier adderas den till listan över de accepterade artiklarna.

På grund av att det finns en begränsad tidsram för detta examensarbete samt att det endast är en person involverad kommer det att göras särskilda begränsningar i denna process. Endast titel och abstrakt kommer att granskas för sin relevans. Om en artikel beslutats uppfylla urvalskriterierna, läggs den till i listan för accepterade artiklar. Artikeln i sin tur kommer inte att granskas i dess referenslista för ytterligare artiklar.

4.1.5 Analysmetod

Artiklar kan genomgå en analys om de har blivit utvald och om de uppfyller samtliga urvalskriterier. Den data som blir insamlad i denna litteraturstudie kommer ha en kvalitativ karaktär. Därför har en tematisk analys valts som analysmetod. Metoden påminner till viss del om öppen kodning, där varje artikel läses igenom noggrant samt att text som kan vara relevant för forskningsfrågan markeras (Braun & Clarke., 2006).

Braun och Clarke (2006) menar att en tematisk analys är en bra metod för att identifiera, analysera och rapportera teman i den data som insamlats. Data som samlas in organiseras och beskrivs i detalj. Inom tematisk analys är det möjligt att jobba enligt två metoder, induktiv eller deduktiv. Skillnaden ligger i att den induktiva metoden låter insamlade data bestämma teman, medan den deduktiva metoden innebär att ett teoretiskt ramverk styr vad som förväntas att hittas i samma data (Braun & Clarke., 2006). I denna studie finns inga fördefinierade kategorier, därav används den induktiva metoden.

Det finns olika tillvägagångssätt för att utföra en tematisk analys. Den vanligaste formen är den sexstegsprocess som Braun och Clarke (2006) har utvecklat. Följs den processen hjälper det även till att undvika bekräftelsebias när analysen ska formuleras.

Den tematiska analysen kommer att utföras enligt följande:

1. **Bli bekant med insamlad data**
   Det första steget handlar om att lära känna sin data. Det kan innebära att läsa igenom texten helt och hållet minst en gång samt göra inledande anteckningar. Identifiering av mönster kan börja att formas under tiden texten läses igenom.

2. **Skapa initiala koder**
   I steg två påbörjas kodning av data. Kodning innebär att delar av text markeras. Det är vanligtvis fraser eller meningar som sedan tillges kortare etiketter eller koder som beskriver innehållet. Arbeta systematisk igenom hela datamängden och anteckna aspekter som kan ligga till grund för upprepade mönster. När datamängden har bearbetats samlas all data ihop i grupper som identifieras med kod. Koderna tillhandahåller en sammanfattad översikt av punkter/mönster som återkommer upprepade gånger.

3. **Sök efter teman**
   Efter föregående steg har en lista med koder erhållits. Bland dessa koder identifieras mönster, för att därefter skapa teman. Teman är i regel bredare än koder. Flera koder kan kombineras till ett tema. I detta steg kan det beslutas att vissa koder är för vaga och därför avfärdas. Det viktiga är att de potentiella teman som skapas ska berätta något om ens data.

4. **Utvärdera teman**
   Det här steget inleds när en uppsättning kandidatteman finns att tillgå. Teman måste vara användbara och korrekta. Ifall teman inte riktigt passar in kan de behöva delas upp, kombineras eller avfärdas. I slutet av detta steg ska det finnas en god uppfattning om vad de olika teman är och hur de passar ihop.

5. **Definiera och namnge teman**
   Efter de föregående stegen har en lista med teman utformats. Var och en av dessa teman ska nu definieras och namnges. Definiering av ett tema innebär att det förtydligas vad som menas med varje tema.

6. **Producera rapport**
   Till sist skrivs en analys av data. Varje tema tas upp i tur och ordning i rapporten. Exempelvis ska det beskrivas hur ofta teman dyker upp och vad de betyder. Det ska även inkluderas utdrag från det dataunderlag som har samlats in. I slutsatsen förklaras sedan de viktigaste aspekterna samt visar på hur analysen har besvarat forskningsfrågan.

4.2 Avgränsningar

Olika avgränsningar kommer att tillämpas, vilket utgör ramen för denna studie. Studien har begränsats till att undersöka området smarta hemmet. Det skulle bli ett allt för stort arbete, i denna typ av uppsats, om det skulle tas hänsyn till andra områden som exempelvis industri, sjukvård eller logistik- och transportsektorn.

Studiens syfte är att kartlägga metoder för hur attacker utförs mot IoT-nätverk inom det smarta hemmet. Dessutom ska studien kartlägga vilka verktyg som används vid en attack. Det kommer däremot inte ligga något fokus på de metoder som används för att angripa ett IoT-nätverk på ett fysiskt sätt.

4.3 Validitetshot

Wohlin et al. (2012) skriver att en studies validitet syftar till hur stor tillförlitlighet resultatet har. Det avser även i vilken utsträckning resultatet är korrekt. Berndtsson et al. (2008) menar att validitet är relationen mellan det som förväntas mätas och det som i slutändan mäts.

Problematiken med en systematisk litteraturstudie är att avgöra när tillräckligt med material har samlats in och om den är relevant. Det har en viktig betydelse i avseende med studiens validitet, det vill säga, om läsaren kan lita på resultatet (Berndtsson et al., 2008).

Berndtsson et al. (2008) poängterar att det är viktigt att i ett tidigt skede, tänka igenom och planera sin strategi av litteraturstudien, för att sedan hålla sig till den. Skulle det dyka upp avvikelser längs vägen ska det dokumenteras och förmedlas till läsaren, vilket förbättrar validiteten av studien.

Tillförlitlighet avser i vilken omfattning data och analys är beroende av en specifik forskare. Teoretiskt sätt om en annan forskare skulle utföra en replikering av studien, bör resultatet bli identiskt. Ifall en litteraturstudie och dess samlade resultat inte granskas kan det vara ett hot mot tillförlitligheten. Detta hot mildras genom att en handledare med jämna mellanrum granskar och tillhandahåller feedback för de metoder som utarbetas för studien. I denna studie ingår det att det färdiga examensarbetet genomgår en referentgranskning där andra studenter granskar resultatet. Dessutom ska examensarbetet granskas av en examinator. Ytterligare en åtgärd Jesson et al. (2011) föreslår för att mildra hot mot tillförlitligheten är att under hela arbetets gång dokumentera allt som görs. Det resulterar i att processen blir transparent och kan replikeras av andra forskare. Genomförandet av metoderna kommer att dokumenteras så långt det är möjligt. Det ska resultera i att processen blir transparent för läsaren.

5 Genomförande av metod

Föregående kapitel beskriver i flera steg hur litteraturstudien ska genomföras. Databaser som ska användas nämns i kapitel 4.1.1, medan kapitel 4.1.2 visar vilka sökord som har visat på relevanta sökträffar. I kapitel 4.1.3 finns urvalskriterierna som ska appliceras på sökträffarna.

Detta kapitel inleds med en databassökning med syftet att hitta relevanta artiklar. Därefter används omvänd snöbollsmetod för att finna ytterligare relevanta artiklar. Efter att urvalskriterier har applicerats på de funna artiklarna och de bedöms uppfylla alla kriterier adderas artiklarna till en bibliografi över accepterade artiklar. Artiklarna i bibliografin analyseras sedan och presenteras i ett senare kapitel.

5.1 Databassökning av artiklar

Söktermen är uppbyggd i tre block. I första blocket används ”Internet of Things” tillsammans med dess akronym IoT för att se till att fånga upp IoT-relaterade artiklar. I det andra blocket används sökordet ”home” för att fånga upp artiklar som omfattar ”home automation” och ”smart home”. I det tredje blocket används sökordet ”attack” som ska se till att fånga upp artiklar som handlar om olika typer av attacker.

Söktermen i sin helhet ser ut enligt följande:

- (IoT OR “Internet of Things”) AND home AND attack

Samtliga databaser tillhandahåller en avancerad sökfunktion. Databaserna som har valts ut har olika gränssnitt för sökfunktionen, vilket har resulterat i att sökningarna inte har kunnat utföras på ett identiskt sätt. I ACM Digital Library har sökningen utförts på abstrakt och publikationstitel. I IEEExplore har sökningen utförts på all metadata, där abstrakt, indexeringstermer och publikationstitel ingår. I ScienceDirect har sökningen utförts på abstrakt, nyckelord specificerade av författare samt publikationstitel. Sökningarna presenteras i tabell 3 nedan.

Tabell 3 – Artikelsökning (författarens egna)

Databas	**Sökfält**	**Datum**	**Sökträffar**
ACM Digital Library	Publication title, Abstract	2023-05-02	191
IEEExplore	All Metadata	2023-05-02	739
ScienceDirect	Title, abstract, author-specified keywords	2023-05-02	135
		Totalt	**1 065**

De initiala databassökningarna resulterade i totalt 1 065 sökträffar. Efter att inkluderingskriterier IK3 (tidsram för publicering: 2018–2023) och IK4 (skriven på engelska) applicerats, återstod 878 sökträffar. Ytterligare urvalskriterier utförs nedan för att filtrera bort artiklar som inte är relevanta för denna studie.

1. **Applicering av inkluderingskriterium IK2 (typ av material)**
   Materialet som samlas in ska vara av akademisk karaktär för att garantera en så hög kvalitet som möjligt. Det innebär enligt inkluderingskriterium IK2 att artiklar ska vara publicerat i journaler eller konferenser.

   I ACM Digital Library valdes även att material skulle vara av typen forskningsartiklar (Research Article). I ScienceDirect saknades möjlighet att filtrera på journal- eller konferenspublikation, men däremot valdes att material skulle vara av typen forskningsartiklar (Research articles). Det innebar att 79 artiklar filtrerades bort och att det återstod 799 sökträffar efter första steget.

2. **Applicering av exkluderingskriterium EK3 (dubbletter)**
   I och med att flera olika databaser används, kan det förekomma artiklar som är identiska. Med hjälp av referenshanteringsverktyget *EndNote Web* filtreras artiklar bort för att uppfylla exkluderingskriterium EK3. En artikel ansågs vara identisk med en annan och filtrerades bort. Det innebar att 798 sökträffar återstod efter andra steget.

3. **Applicering av inkluderingskriterium IK5 (relevans för ämnet i fråga)**
   För att inkluderingskriterium IK5 ska vara uppfyllt måste det insamlade materialet ha en relevans för ämnet i fråga. Det innebär att varje enskild artikel granskas för sin relevans. Efter att varje enskild titel granskats filtrerades 714 artiklar bort då det saknades relevans. Artiklar som filtrerades bort innehöll ord som exempelvis AI och blockchain i titeln.

   Därefter granskades abstrakten i de återstående 84 artiklarna. Det resulterade i att 54 artiklar filtrerades bort. Artiklar som filtrerades bort hade fokus på andra IoT-områden som exempelvis industri och sjukvård. I detta steg upptäcktes även att det fanns två artiklar som hade snarlika versioner publicerade med ett par års mellanrum. Efter att ha granskat artiklarna bedömdes det att de som var publicerade tidigast filtrerades bort som dubbletter. Efter att artiklar hade filtrerats bort för sin abstrakt samt att dubbletterna hade plockats bort återstod 28 artiklar.

4. **Applicering av inkluderingskriterium IK1 (referentgranskning)**
   Samtliga artiklar ska enligt inkluderingskriterium IK1 vara referentgranskade. Det innebär att tidskrifter och utgivare kontrolleras ifall referentgranskning utförs på det material som publiceras på deras plattform. Till hjälp kommer *Ulrichsweb* att användas som är en global katalog med fler än 300 000 publikationer. I katalogen är det möjligt att se om material är publicerat hos utgivare som utför referentgranskning. *Ulrichsweb* tillhandahålls av högskolan i Skövde kostnadsfritt. En viktig notering är att en artikel inte behöver ha genomgått en referentgranskning även om den tidskrift eller utgivare den är publicerad i har blivit det.

   Samtliga 28 artiklar granskades med hjälp av *Ulrichsweb*. I de fall där det saknades information utfördes manuella internetsökningar för att undersöka huruvida

referentgranskning genomförts. En artikel filtrerades bort då det saknades information om artikeln hade blivit referentgranskad. Efter detta steg återstod 27 artiklar.

5. **Applicering av exkluderingskriterium EK2 (betalvägg)**
   De återstående artiklarna granskades ifall de uppfyllde exkluderingskriterium EK2. Det innebär att artiklar ska hämtas i dess helhet. I och med att samtliga databaser som används i denna studie tillhandahålls av högskolan i Skövde, innebar det att inga ytterligare artiklar filtrerades bort. Efter detta steg återstod fortfarande 27 artiklar.

6. **Applicering av exkluderingskriterium EK4 (ofullständig)**
   Enligt exkluderingskriterium EK4 ska artiklar innehålla ett väldefinierat metod-, implementations eller resultatkapitel. Saknas det ska artikeln bedömas som ofullständig och därmed filtreras bort. Av 27 granskade artiklar var det en artikel som filtrerades bort då det saknades en metod-, implementations- eller resultatkapitel. Efter detta steg återstod 26 artiklar som lades till i den slutliga bibliografin för denna litteraturstudie. Bibliografin finns tillgänglig som bilaga, se ”*Bilaga A – Bibliografi över accepterade artiklar*”.

5.2 Omvänd snöbollsmetod

Den kompletterande metoden, omvänd snöbollsmetod, används för att se till att hitta så många relevanta artiklar som möjligt. Till skillnad från databassökningarna är utgångspunkten i detta fall, referenslistorna från de 26 accepterade artiklarna i föregående steg. Dessutom utförs denna metod helt manuellt då det saknas automatiska hjälpmedel som databaserna har.

Processen av omvänd snöbollsmetod utfördes 2023-05-03, och gick till enligt följande:

1. **Applicering av inkluderingskriterium IK3 (tidsram för publicering) och IK4 (skriven på engelska)**
   Inledningsvis samlades samtliga referenser in från referenslistorna från de 26 accepterade artiklarna. Det resulterade i totalt 1 227 artiklar. Artiklarna granskades utifrån när de blivit publicerade och vilket språk som använts. Efter granskningen filtrerades 699 artiklar bort. Det återstod 528 artiklar efter första steget.

2. **Applicering av inkluderingskriterium IK2 (typ av material)**
   I det andra steget filtreras artiklar för vilken typ av material det är. Inkluderingskriterium IK2 definierar att artiklar ska vara publicerade i antingen journaler eller konferenser. Efter att ha granskat de återstående artiklarna, visade det sig att 190 artiklar inte var publicerade i en journal eller konferens. Det återstod 338 artiklar efter det andra steget.

3. **Applicering av inkluderingskriterium IK5 (relevans för ämnet i fråga)**
   Artiklar måste uppfylla inkluderingskriterium IK5, vilket innebär att de ska ha en relevans för ämnet i fråga. Precis som i databassökningarna, filtrerades artiklar bort

om irrelevanta ord förekom i titeln eller om artikeln hade fokus på ett annat IoT-område än smarta hemmet. Efter att artiklarnas titlar och abstrakt hade granskats, filtrerades 235 respektive 78 artiklar bort. Det återstod 25 artiklar efter detta steg.

4. **Applicering av exkluderingskriterium EK3 (dubbletter)**
   Exkluderingskriterium EK3 innebär att artiklar som är dubbletter, ska filtreras bort. I och med att hela processen utförs manuellt kan inte *EndNote Web* användas. Istället har de återstående artiklarna granskats manuellt för att upptäcka eventuella dubbletter. Efter att de återstående artiklarna hade granskats, filtrerades fem artiklar bort. Det återstod 20 artiklar efter detta steg.

5. **Applicering av inkluderingskriterium IK1 (referentgranskning)**
   Artiklar har granskats så att de uppfyller inkluderingskriterium IK1, vilket innebär att artiklar ska ha genomgått en referentgranskning. Återigen har den globala katalogen *Ulrichsweb* använts. Dessutom har manuella internetsökningar utförts för de artiklar där det inte är möjligt att hitta information på *Ulrichsweb*. Efter denna granskning filtrerades två artiklar bort. Det återstod 18 artiklar efter detta steg.

6. **Applicering av exkluderingskriterium EK2 (betalvägg)**
   Enligt exkluderingskriterium EK2 måste artiklarna kunna hämtas i sin helhet. Det får inte finnas några inloggningskrav när artiklarna ska hämtas. Majoriteten av artiklarna förekom på databaser som tillhandahålls av högskolan i Skövde. Det visade sig att det fanns två artiklar som inte uppfyllde kriterierna. En av artiklarna fanns i databasen SpringerLink, där skolans prenumeration inte gav tillträde. Den andra artikeln befann sig bakom en inloggning. Efter detta steg återstod 16 artiklar.

7. **Applicering av exkluderingskriterium EK4 (ofullständig)**
   Exkluderingskriterium EK4 innebär att artiklar måste ha en väldefinierad metod-, implementation- eller resultatkapitel. Det var inga ytterligare artiklar som filtrerades bort i denna granskning. Efter detta steg återstod 16 artiklar som lades till i bibliografin över accepterade artiklar, se *”Bilaga A – Bibliografi över accepterade artiklar”*.

5.3 Analys av resultat

Efter att databassökningarna och den omvända snöbollsmetoden blev slutförd har en bibliografi med de accepterade artiklarna sammanställts, som återfinns i *”Bilaga A - Bibliografi över accepterade artiklar”*. Nästa steg är att utföra en tematisk analys av artiklarna som till antalet är 42. Processen av analysen är beskriven i kapitel 4.1.5 där den är uppdelad i flera steg.

Analysen inleddes med att läsa igenom artiklarna för att bekanta sig med texten. Det gjordes även anteckningar när intressant data dök upp i texten. Det stod klart snabbt att det fanns två tydliga teman som dök upp upprepade gånger i artiklarna. Det ena temat relaterar till vilka

typer av verktyg som beskrivs i exempelvis metod-delen i artiklarna. Det andra temat där det gick att se mönster upprepade gånger är vilka typer av attacker eller metoder som beskrivs i artiklarna.

Efter att samtliga artiklar hade lästs igenom påbörjades kodningen. Relevant text i relation till forskningsfrågan blev märkt och en beskrivande kod adderades till texten. När artiklarna hade blivit kodade sammanställdes alla koder i ett dokument. Därefter skapades underkategorier till respektive tema, där koderna sorterades in. Det förekom olika problem när teman skulle kategoriseras. En del av underkategorierna hade för få relevanta textpassager och det beslutades att dessa underkategorier skulle kasseras. Side-channel och sybilattacker var exempel på kategorier som blev kasserade av denna anledning. Det fanns underkategorier som var lika varandra men som behövde delas upp då koderna beskrev olika saker. Avlyssning, skanning och trafikanalys är exempel på underkategorier som delades upp. Till sist när teman och underkategorier har fastställts och granskats återstod att presentera analysen. En sammanställning av analysen återfinns i *”Bilaga B – Sammanställning av analys”*. Den illustrerar fördelningen av relevanta textpassager relaterat till attackmetoder och verktyg.

6 Resultat och analys

Syftet med detta kapitel är att beskriva och presentera den empiriska kunskapen som har erhållits från den tematiska analysen av bibliografin. Med hjälp av den tematiska analysen har totalt 18 kategorier identifierats. Nio kategorier med textpassager relaterat till verktyg har identifierats och återfinns i tabell 4 nedan. Nio kategorier med textpassager relaterat till typ av attack har identifierats och återfinns i tabell 5 nedan. Detta kapitel har delats upp i två underkapitel. Kapitel 6.1 omfattar vilka verktyg som har identifierats i litteraturen medan kapitel 6.2 omfattar vilka typer av attacker tillsammans med de metoder som har identifierats.

Tabell 4 – Identifierade textpassager i relation till verktyg (författarens egna)

Identifierade verktyg	Antal
Aircrack-ng	3
ARPspoof	4
Bettercap	3
Ettercap	3
Hping3	6
Metasploit	5
Nessus	3
Nmap	8
Wireshark	15

Tabell 5 – Identifierade textpassager i relation till attack/metod (författarens egna)

Identifierade attacker/metoder	Antal
Avlyssning	9
Denial of Service (DoS)	25
Distributed Denial of Service (DDoS)	9
Malware	16
Man-in-the-Middle (MitM)	14
Replay	8
Skanning	9
Sniffing	7
Trafikanalys	8

6.1 Verktyg

I detta kapitel beskrivs och presenteras vilka verktyg som har identifierats i litteraturen.

6.1.1 Aircrack-ng

Aircrack-ng är enligt A29 ett verktyg som kan användas till attacker, övervakning och knäckning av WiFi-nätverk. När det gäller attacker är det möjligt att utföra replay-attacker, de-autentiseringsattacker, fejka accesspunkter och paketinjektioner.

Verktyget är släppt som öppen källkod och fungerar på flera operativsystem som Linux, Mac och Windows. Verktyget används främst i kommandotolk men förekommer även i grafiskt gränssnitt (Aircrack. 2023). Då det är användarvänligt att använda och inga förkunskaper krävs, menar A29 att det blir ett farligt verktyg i händerna på illvilliga personer.

I A29 används verktyget för att utföra en variant av DoS-attack medan A18 och A34 diskuterar de-autentiseringsattacker samt övervakning av WiFi-nätverk.

6.1.2 ARPspoof

ARPspoof har visat sig vara ett verktyg som är allsidigt. I A01 används det till att utföra en MitM-attack mot IP-kameror, i A15 används det för att kapa en TCP-anslutning på en gateway till en Ring-enhet och i A17 används det till att utföra blackhole-attacker mot olika typer av smarta hem-enheter.

ARPspoof är ett verktyg som används för att lura en målmaskin, genom att skicka falska ARP-meddelanden (Address Resolution Protocol). Syftet är att övertala målet att skicka sin nätverkstrafik till antingen angriparens dator eller annan enhet i nätverket (Singh, 2019).

När ARPspoof används till en MitM-attack, förutsätter det att angriparen har gjort vissa förberedelser. Verktyget och metoden används i Kali Linux, vilket innebär att angriparen bör ha viss kännedom om operativsystemet för att underlätta nyttjandet av verktyget. Vidare krävs det ett nätverksgränssnitt installerat på värddatorn samt IP-adressen som används av målets router (Singh, 2019).

6.1.3 Bettercap

Bettercap (u.å.) beskriver Bettercap som ett kraftfullt och allsidigt verktyg skrivet i programmeringsspråket Go som har till syfte att användas vid spaning av nätverk samt MitM-attacker mot WiFi-nätverk, Bluetooth LE-enheter och IPv4/IPv6-nätverk. Verktyget ses som efterträdaren till verktyget Ettercap. Bettercap kan användas på tre olika sätt: genom ett grafiskt gränssnitt, en kommandotolk och med hjälp av skriptning. Verktyget är helt gratis och släppt som öppen källkod.

I A08 används Bettercap för att utföra både skanning och en MitM-attack. Nätverket skannas först genom att skicka UDP-paket till hela subnätet. Därefter kan angriparen utföra en ARP-spoof mot det lokaliserade målet och inta en MitM-position. A33 använder Bettercap i kombination med andra verktyg för att inta en MitM-position mellan en användares mobilapplikation och en server. Det visar på vilket användbart verktyg det är, som har ett flertal inbyggda funktioner.

6.1.4 Ettercap

Ettercap är enligt Ettercap-project (u.å.) ett omfattande verktyg som har till syfte att användas i MitM-attacker. Det är möjligt att både passivt och aktivt dissekera protokoll och utföra nätverksanalys. Ettercap tillhandahåller både ett grafiskt gränssnitt och kommandotolk. Vidare skriver Kali (2023) att det finns fyra olika sniffing-lägen: IP-baserad, MAC-baserad, ARP-baserad och PublicARP-baserad.

A10 nämner att Ettercap kan användas till att fånga paket, filtrera innehåll och dissekera protokoll. I deras studie används verktyget för att avlyssna trafik mellan en IP-kamera och en mobilapplikation kopplad till kameran. A37 utför experiment på samma modell av IP-kamera, en Tapo C200. Även i denna studie används Ettercap för att inta en MitM-position med hjälp av ARP-förgiftning.

A19 använde Ettercap för att testa flera olika typer av produkter som kopplas upp i det smarta hemmet. De lyckades erhålla känslig information från ett smart kylskåp. Paket som skickades till och från kylskåpet fångades upp med hjälp av Ettercap. I kombination med Wireshark analyserades paketen för att komma åt informationen.

6.1.5 Hping3

Hping3 är ett verktyg som är förinstallerad på Kali Linux. I artiklarna A13-A14, A19, A31, A36-A37 förekommer verktyget Hping3. I majoriteten av fallen, används verktyget till att utföra DoS-attacker. Artikel A36 nämner dock att Hping3 är ett avancerat verktyg som använder sig av TCP, UDP, ICMP och RAW-IP-protokoll och har möjligheten att kringgå brandväggsfilter. Således används Hping3 för brandväggstest men också till avancerad portskanning, fastställa OS-fingeravtryck och testning av nätverks prestanda.

Enligt Singh (2019) kan Hping3 användas till att lokalisera mål i nätverk, fastställa fingeravtryck för tjänster som används, sniffa nätverkstrafik, utföra DoS samt för filöverföring.

6.1.6 Metasploit

Metasploit är ett populärt ramverk för penetrationstestning som även används för att utveckla och utföra exploits mot mål på distans. Ramverket är förinstallerad på Kali Linux. A28 och A37 beskriver att, i likhet med Hping3, kan Metasploit användas som ett verktyg för att utföra DoS-attacker. A33 beskriver hur Metasploit kan användas för utveckling av exploits samt att kontrollera sårbarheter hos olika applikationer.

Nästintill all interaktion med Metasploit sker genom att använda moduler. Det finns tre olika typer av moduler: Exploits, Auxiliary och Payloads. Exploits innehåller moduler som använder sig av Payloads-moduler. Auxiliary-moduler innehåller portskannrar, fuzzers, sniffers med mera. Payloads-moduler innehåller kod som kan exekveras på distans (OffSec, u.å.).

6.1.7 Nessus

Innan en exploit används måste angripare identifiera vilka säkerhetsbrister som existerar på attackytan, vilket är det område en attack kommer att försöka utnyttja. Ett effektivt sätt att identifiera säkerhetsbrister är att använda en sårbarhetsskanner. En av de populäraste sårbarhetsskannrarna är Nessus (Singh, 2019).

A04 använde Nessus för att identifiera vilka tjänster som kördes samt vilka sårbarheter som existerade på 45 olika IoT-enheter i det smarta hemmet. A10 använder verktyget för att skanna efter sårbarheter på en IP-kamera (Tapo C200) medan A34 kör en sårbarhetsskanning på elva olika IoT-enheter vanligt förekommande i det smarta hemmet.

Det artiklarna har gemensamt är att de försöker identifiera CVE:s (Common Vulnerabilities and Exposures). Varje CVE har en unik identifierare. MITRE är en amerikansk organisation som jobbar bland annat med att identifiera, definiera och kategorisera dessa CVEs, vilket är publikt avslöjade sårbarheter (MITRE, u.å.).

6.1.8 Nmap

Nmap är ett gratisverktyg, med öppen källkod, vilket används för nätverksskanning och säkerhetsgranskning (Nmap, u.å.). Vidare använder Nmap RAW IP-paket för att avgöra:

- Vilka värdar som är tillgängliga
- Vilka tjänster som används (namn och versionsnummer)
- Vilket operativsystem som körs (namn och versionsnummer)
- Om brandväggar/paketfilter används

A01, A08, A10, A15, A28, A33-A34 och A37 nämner att Nmap används för att kartlägga hur nätverket ser ut. A10 skriver att det är ett av de första stegen som utförs när en angripare ska närma sig ett mål. A31 påpekar även att det även finns ett alternativ till Nmap som heter ZenMAP. Det som skiljer sig åt är att Nmap är en skanner som används med hjälp av kommandotolk medan ZenMAP har ett grafiskt gränssnitt.

6.1.9 Wireshark

Wireshark är ett gratisverktyg, fritt tillgängligt som öppen källkod och används för att analysera nätverkstrafik (Wireshark, u.å.). Med hjälp av Wireshark är det möjligt att fånga upp paket i realtid, filtrera data för att erhålla specifik information och slutligen visualisera den information som har filtrerats (CompTIA, u.å.).

A06 övervakar paket för att upptäcka DoS-trafik medan A13 jämför effekten av olika typer av DoS-trafik. A16 fångar upp Bluetooth-paket för att extrahera information som kan leda till att exploits utförs. I A30 fångas ZigBee-paket upp för vidare analys. Det visar på vilket kraftfullt och mångsidigt verktyg Wireshark utgör sig att vara.

6.2 Attack/Metod

I detta kapitel beskrivs och presenteras vilka attacker/metoder som har identifierats i litteraturen.

6.2.1 Avlyssning

Med nio textpassager identifierade i de accepterade artiklarna, placerade sig avlyssning på en fjärde plats tillsammans med DDoS och skanning. Avlyssning är en attack där angripare försöker ta sig in på en enhet eller ett nätverk på ett olovligt sätt utan att bli upptäckt. A12 beskriver hur avlyssning ses som en passiv attack där information samlas in. A05 skriver att huvudsyftet med att få tillgång till ett nätverk är att kunna ta kontroll och övervaka nätverkets aktiviteter. Ett av de vanligaste verktygen som används i samband med avlyssning är Wireshark. A32 förklarar hur det är ett populärt verktyg som används för att fånga upp trafiken.

A03 och A06 anser att avlyssning är en realtidsattack där angripare försöker stjäla information från trafik som enligt A26 fångas upp mellan olika IoT-enheter. A35 har en likartad uppfattning om attacken och menar att den kan spelas in eller pågå i realtid. A07 menar att en stor anledning till att trafik kan bli avlyssnad ligger i att kommunikationen sker i heterogena IoT-nätverk som innehåller ett stort antal enheter.

Genom att avlyssna trafik skriver A12 och A26 att användbar information kan exponeras. Viktig information som kan avslöjas är den fysiska lokaliseringen av nod eller gateway, enhetstyper, status på enheter, unika identitetsnummer, tidsstämplar, operativsystem och i stort sett all information som är okrypterad.

6.2.2 Denial of Service (DoS)

Den metod som hade enskilt flest antal identifierade textpassager i de accepterade artiklarna var DoS, med sina 25 textpassager. Det ger en indikation om vilken typ av attack som är den vanligast förekommande mot IoT-nätverk. DoS-attack beskrivs av A03 som en allvarlig attack som går ut på att blockera access till en enhet eller ett nätverk. Det uppnås genom att överflöda målet med många förfrågningar, vilket gör det omöjligt för legitima användare att nå fram. A21 definierar DoS-attack på ett liknande sätt, där nätverk bombarderas med stora mängder trafik som resulterar i att IoT-enheter inte kan utföra sina tjänster.

A07, A21 och A32 förklarar att DoS-attacken är en av de vanligast förekommande attackerna som utförs mot nätverk i allmänhet och IoT-nätverk i synnerhet. A35 förklarar vidare att DoS-attacker kan antingen vara aktiva attacker där en applikation eller uppgift blir avbruten kraftfullt, eller en passiv attack där en attack mot en applikation kan leda till att en annan uppgift stoppas.

A06 skriver att IoT-enheter med lätthet kan bli påverkade av DoS-attacker på grund av tidsbegränsningar, energiförbrukning och minnesbegränsningar. Enligt A32 har DoS-attacker inte syftet att bryta sig in i ett system, utan försöker snarare att göra nätverksresurser otillgängliga för autentiserade användare. DoS-attacker kan också användas som en typ av rökridå medan andra attacker utförs.

Det finns många olika metoder till att utföra DoS-attacker mot ett IoT-nätverk. A07, A21 och A37 diskuterar en metod som kallas “Land Attack”. A37 beskriver att ett TCP SYN-paket skapas där källans IP-adress samt TCP-port är inställd till samma som destinationens IP-adress och port. Paketet skickas till en öppen TCP-port på målets enhet. När målet sedan skickar ett svar, resulterar det i att paketet skickas i en oändlig loop. Målets enhet förbrukar resurser på obestämd tid och orsakar frysning, låsning eller krasch av enheten.

A07, A21, A39 diskuterar en metod som kallas “Ping of Death”. Det är en attack där ett missformat paket skickas till ett mål vilket kan resultera i en systemkrasch när paketet tas emot.

A07, A21 diskuterar TearDrop. Det är en attack vars syfte är att krascha ett nätverk, server eller enhet genom att skicka stora mängder modifierade paket. Överlappande fragmenterade paket skickas till ett mål. När målets enhet försöker att placera paketen i rätt ordning misslyckas det och så småningom kraschar systemet permanent (ClouDNS, 2022).

En av de vanligaste metoderna, diskuteras i A07-A08, A12-A14, A19, A31 och A36-A37 som kallas SYN-flooding. Det är en attack som utnyttjar en sårbarhet i TCP-protokollets tre-stegs-handskakning. Det beskrivs i A13, att en angripare skickar SYN-paket till ett mål, varpå målet bekräftar med ett SYN- och ACK-paket till angriparen. Angriparen låter bli att skicka ett ACK-paket till målet och låter anslutningen vara öppen. Angriparen fortsätter sedan att skicka ytterligare SYN-paket för att skapa ännu fler öppna anslutningar, tills målet får slut på resurser att dela ut till legitima anslutningar.

6.2.3 Distributed Denial of Service (DDoS)

Totalt nio textpassager identifierades i de accepterade artiklarna som kunde hänvisas till DDoS-attacker. DDoS står för Distributed Denial of Service. Som nämns i A23 är det en avancerad version av DoS-attacken. Den största skillnaden mellan DoS- och DDoS-attacker framhävs i A32, där en DoS-attack använder ett enda system för att attackera ett mål, medan DDoS-attack använder sig av flera system som tillsammans skickar mängder med trafik mot samma mål. A39 menar vidare att attacker från flera källor samtidigt, från början var en dyr metod. Med teknikens utveckling har det blivit både enklare och mer kostnadseffektivt att utföra DDoS-attacker.

DDoS-attacker kan enligt A32 kategoriseras utifrån volymbaserade-, protokollbaserade- och applikationsbaserade attacker. Syftet med volymbaserade attacker är att rikta in attacken mot bandbredden hos målet, för att se till att inga andra kan nyttja tjänsten. Exempel på dessa attacker är UDP-flooding, ICMP-flooding och andra typer av spoofade paket som översvämmar målet. Prokollbaserade attacker har som syfte att istället äventyra serverresurserna istället för bandbredden. Exempel på dessa attacker är SYN-flooding, fragmenterade paketattacker och Ping of Death. Applikationsbaserad attack däremot förbrukar lägre resurser än både volym- och prokollbaserade attacker. Det innefattar attacker som exempelvis Zero-Day-attacker, Slowloris-attacker och attacker som utnyttjar sårbarheter i Apache, OpenBSD och Windows.

Flera artiklar som exempelvis A01, A09, A23 samt A38-A39 innefattar en metod där botnet används för att utföra DDoS-attacker. A38 skriver om hur botnet, även kända som zombies, kontrolleras av en angripare med hjälp av en Command & Control-server (C&C) och kan enligt A09 användas för att utföra spamming, phishing och DDoS-attacker. IoT-enheter har blivit allt vanligare inom hem- och företagsnätverk. Det tillsammans med säkerhetsproblematiken har gjort att IoT-enheter har blivit ett idealiskt mål för botnet-attacker, främst dedikerade till att utföra DDoS-attacker. A39 ger ett exempel på ett botnet som skapas med hjälp av en malware-attack som kallas Mirai.

Likt DoS-attacken, förekommer identiska attacker även hos DDoS-attacker. A21 samt A32 diskuterar Ping of Death och hur attacken kan påverka system till att sluta svara på legitima förfrågningar. A03, A23 och A32 diskuterar den vanligare attacken SYN-flooding som utnyttjar sårbarheter i TCP-protokollet. A03 och A21 diskuterar reflektionsattacker, även kallade ”Land Attacks”, där angriparen skickar paket till ett mål, med målets IP-adress satt som källadress.

A03, A23 och A32 diskuterar UDP-attacker. Syftet med UDP-flooding är att skicka hög volym med UDP-paket riktat mot ett mål. Det påverkar i sin tur bearbetningskraften hos enheterna. En annan typ av UDP-attack är UDP-fragmentattack. UDP-paketen fragmenteras i minsta möjliga storlek, vilket gör att attacken blir mer utdragen för den enhet som blir utsatt.

6.2.4 Malware

Malware var den attack som hade näst flest antal textpassager. 16 textpassager kunde identifieras i de accepterade artiklarna. Sentor (2021) förklarar hur malware är en förkortning av orden malicious och software, vilket syftar på kod eller mjukvara som är utformad att skada enheter, nätverk och system. Både A03 och A06 skriver att malware är en metod som bistår angriparen med att stjäla data. A07 beskriver att malware är en generell term som omfattar exempelvis mask, ransomware, trojanska hästar och virus.

En vanlig malware-attack är kodinjektion, som diskuteras i A02-A03, A06-A07 och A11. A07 diskuterar hur en kodinjektion kan utnyttja kryphål i mjukvara. Det kan innebära att angriparen äventyrar en nod genom att injektera skadlig kod som kan orsaka nätverksproblem eller att angriparen får fullständig kontroll över nätverket. A02 visar hur ett skadligt JavaScript kan gömmas på en webbserver, förslagsvis i en annons. När en IoT-enhet sedan besöker webbservern kan det resultera i att angriparen kan ta kontroll över enheten. En annan typ av metod diskuteras i A21, där en mask anpassad för IoT kan infektera smartlampor från Philips Hue. Masken kan efter att ha infekterat en lampa spridas vidare till liknande enheter. A21 diskuterar även en metod där falsk data injekteras in i ett IoT-nätverk. Ett exempel är kameror med ansiktsigenkänning som installeras i anslutning till en entré för att skanna av ansikten och låsa upp dörren för rätt personer. En angripare skulle kunna injektera falsk data för att lura kameran att angriparen i själva verket är bostadsägaren och ge tillträde till bostaden.

Den vanligaste malware-attacken som har identifierats i litteraturen kallas Mirai, vilket diskuteras i A02, A09, A21, A23, A39 och A41. Mirai är en malware som riktar in sig på

IoT-enheter med öppna telnet-anslutningar. A39 och A41 beskriver Mirai-attacken på ett liknande sätt, där attacken delas upp i flera steg: skanna, inaktivera och attackera. En bot försöker att initiera en anslutning med slumpmässigt utvalda IP-adresser på port 23 och 2323. När en enhet med en öppen telnet-anslutning hittas försöker boten att logga in på enheten genom en brute-force. Om boten lyckas logga in på enheten sparas inloggningsuppgifterna och skickas till en server. Därefter upptar boten portarna 22, 23 och 80 för att förhindra att tjänsterna startas om. Enheten har nu blivit del av angriparens botnet. Angriparen kan sedan använda sig av sitt botnet för att utföra ytterligare attacker som exempelvis DDoS-attacker.

6.2.5 Man-in-the-Middle (MitM)

14 textpassager kunde identifieras där metoden omfattade Man-in-the-Middle-attacker. Flera av artiklarna, däribland A03 och A06-A08, definierar MitM-attack som en cyberattack där angriparen i hemlighet lyssnar på vad som kommuniceras mellan en sändare och mottagare. I A19 återges att OWASP definierar MitM-attacker som tillfällena där en angripare delar upp den ursprungliga TCP-anslutningen i två nya anslutningar, en mellan målet och angripare samt en mellan angripare och server. A06 skriver att när angriparen har fått tillgång till den fullständiga kommunikationen mellan två enheter, kan informationen som skickas där emellan manipuleras, och angriparens syfte uppfylls. Både A19 och A33 menar att MitM kan användas som en metod för att antingen avlyssna eller manipulera data. A19 tillägger dock att varje instans av avlyssning som metod, inte nödvändigtvis innebär att det är en MitM-attack.

Det är möjligt att kapa ett Z-Wave-nätverk med hjälp av en MitM-attack. A22 förklarar hur Z-Wave använder sig av ett parningsläge när en nod och en gateway paras samman. För att enheterna ska paras samman måste båda befinna sig i parningsläget. På noden hålls en knapp in i ett par sekunder för att aktivera parningsläget medan en gateway har möjlighet att aktivera läget via en användarapplikation. Angriparen kan på distans aktivera parningsläget på gateway och sedan para ihop den med angriparens egen nod. Attacken förutsätter att en router befinner sig mellan målets gateway och Z-Wave-servern samt att angriparen känner till inloggningsuppgifterna för routern. Metoden går ut på att angriparen placerar sig i en MitM-position på målets router och analyserar paketen som skickas mellan gateway och Z-Wave-servern.

A01, A08, A17, A33 och A37 utför MitM-attacken på ett liknande sätt, där metoden går ut på att använda ARP-spoofing/ARP-förgiftning. Attacken inleds med att angriparen korrumperar målens ARP-cache. MAC-adresser hos målen ersätts med angriparens MAC-adress. Trafik som går mellan exempelvis ett mål och en server omdirigeras via angriparen. Trafiken skickas sedan vidare till den legitima slutdestinationen.

När en angripare har utfört sin MitM-attack är det möjligt att utföra ytterligare attacker. I A08 beskrivs hur verktygen Bettercap och Xerosploit kan användas för att manipulera målets HTTP-trafik. A17 genomför en selektiv vidarebefordring av hjärtslag, där övrigt innehåll utelämnas. Det är en sårbarhet som en angripare kan utnyttja för att inaktivera ett säkerhetssystem i ett hem och bryta sig in i en bostad utan att bostadsägaren blir medveten om det. A33 utförde en nedgraderingsattack där HTTPS-trafik nedgraderades till HTTP-trafik.

Med hjälp av ett verktyg som heter SSLStrip, fångar angriparen upp TLS-autentiseringsinformation som är menat för målet. Alla HTTPS-länkar ersätts med HTTP-länkar som sedan skickas vidare till målet. A37 genomförde ett experiment där en MitM-attack utfördes för att utvärdera motståndskraften hos smarta hemsäkerhetskameror. I detta fall användes verktyget Ettercap för att fullborda attacken. Två enheter valdes ut som mål, en säkerhetskamera och en smarttelefon. Båda enheternas ARP-cache korrumperades och trafiken mellan dem omdirigerades till angriparen. Trafiken dirigerades sedan vidare till den legitima slutdestinationen och en MitM-attack hade genomförts.

6.2.6 Replay

Med åtta textpassager identifierade i de accepterade artiklarna, placerade sig metoden replay på en delad femte plats tillsammans med attacken trafikanalys. A03 beskriver replay-attack som en typ av avlyssningsattack. En angripare avlyssnar trafiken mellan en sändare och mottagare. Angriparen skickar informationen till den tilltänkta destinationen samtidigt som denne maskerar sig som den ursprungliga avsändaren. Mottagaren mottar meddelandet som ser ut att vara autentiskt och tolkar det som en giltig begäran. A26 beskriver en typ av replay-attack där angriparen modifierar ett mottaget meddelande som sedan skickas vidare till en IoT-enhet. Det resulterar i att IoT-enheten blir förvirrad när den ska hantera paketet.

A16 försöker i sin studie att bryta sig in i en Amazon Echo-enhet. Echo använder sig bland annat av Bluetooth vid kommunikation. Echo är normalt sätt osynlig för andra enheter tills parningsläget aktiveras. Det enda sättet att para ihop Echo med en annan enhet är att aktivera parningsläget röstkommandot *”Fråga Alexa”*. Det finns dock ett kryphål i implementationen av Bluetooth i Echo. Är Bluetooth aktiverat kommer Echo att svara på alla unicast-meddelanden som tas emot. En angripare skulle kunna använda en enhet och dess BDADDR (Bluetooth Device Address) och skicka unicast-meddelanden till en Echo. Echo-enheten kommer att svara på meddelandet även om den befinner sig i ett osynligt läge. Den här metoden blev uppkallad Blueborne. Parametrarna Blueborne använder sig av vid attacken är BDADDR, vilket är motsvarigheten till MAC-adresser inom nätverk, IP-adress på målet, HCI (Host Controller Interface) samt portinställning. För att få tag i adressen till Echo användes ett hårdvaruverktyg som heter Ubertooth, vilket är en 2,4 GHz trådlös transceiver. Den fångar upp Bluetooth-trafik som sedan analyseras med hjälp av Wireshark. Den extraherade informationen avvänds sedan tillsammans med Blueborne för att ta kontroll över Echo.

Även A18 diskuterar hur Bluetooth kan angripas genom en replay-attack. Ett smart lås kan angripas genom att inleda *”lås-upp-proceduren”*, varpå låset skickar en autentiseringsförfrågan. Angripare använder ett liknande verktyg som diskuterades i A16 och fångar upp meddelandet. Angriparen maskerar sig som låset och skickar autentiseringsförfrågan till bostadsägaren som i sin tur svarar på förfrågan. Angriparen fångar upp meddelandet som sedan kan användas vid ett senare skede och låsa upp låset.

En annan metod som diskuteras men även demonstreras i A18 är kombination av injektion-, sniffing och replay-attack. I denna metod används en uppkopplad leksaksdocka där mikrofonen aktiveras för att spela in samtal som innehåller känslig information. Det kan

exempelvis vara en kod som nämns i samtalet. Denna kod spelas sedan upp genom dockan till en Bluetooth-högtalare som vidarebefordrar kommandot till en gateway eller en röststyrd aktiveringsenhet. Kommandot utför sedan en aktivering av en sensor som kan vara exempelvis ett smart lås. A25 diskuterar en liknande metod där en angripare använder förinspelade röster från legitima användare för att lura röstaktiverade enheter. Det är möjligt att injektera dolda eller ohörbara röstkommandon som en människa inte hör men som fortfarande kan uppfattas av den röstaktiverade enheter.

6.2.7 Skanning

Nio textpassager kunde identifieras i de accepterade artiklarna, där metoden omfattade skanning. Skanning kan betecknas som en passiv attack och har till syfte att kartlägga hur ett nätverk ser ut. Innan en angripare ger sig på ett tilltänkt mål är det viktigt att definiera vad som är målet. A16, A28 och A33 beskriver på ett liknande sätt hur skanning används som ett sätt att kartlägga vilka enheter som finns anslutna till ett nätverk.

Flera av artiklarna är överens om att skanning anses vara ett av de första stegen när en attack ska utföras. Processen att skanna ett nätverk kan se lite olika ut beroende på vilka enheter som används inom nätverket. Den vanligaste metoden är att använda skannerverktyget Nmap. I A01, A10, A16, A28, A34 och A38 var det första steget att använda Nmap för att skanna efter öppna portar, vilket operativsystem en enhet använder samt om det finns exponerade tjänster. A33 använder sig av en kombination av Nmap och ZenMAP för att uppnå samma sak. A04 använder sig av ett annat skannerverktyg som heter Nessus. Syftet är snarlikt, där det går ut på att upptäcka och profilera körande tjänster på ett IoT-nätverk.

6.2.8 Sniffing

Sniffing är den attack som har minst antal textpassager, där sju textpassager identifierades i de accepterade artiklarna. Vid en sniffing-attack fångar en angripare upp paket som skickas i ett nätverk med syftet att antingen avlyssna eller stjäla känslig information som är okrypterad. A35 skriver att angripare kan sniffa den kommunikation som sker i den smarta miljön, och kan därför äventyra användarnas integritet. Genom att sniffa trafik kan angripare ta reda på om en enhet är aktiv eller inte.

A33 påstår att det finns flertal mobilapplikationer inom smarta hemmet som är extra känsliga mot attacker. Genom att kombinera flera olika attacker är det möjligt att sniffa trafik som inte är avsedd för angripare. Attacken inleds med att skanna nätverket med Nmap. Därefter utförs en ARP-spoofing för att placera angriparen i en MitM-position mellan användare och server. Verktyget SSLStrip används för att nedgradera HTTPS-trafik till HTTP-trafik. Angriparen kommunicerar med användaren över HTTP och med servern över HTTPS. När användaren anger känslig information som exempelvis användaruppgifter i mobilapplikationer, sniffas informationen av angriparen.

På ett liknande sätt utför A01 ett experiment för att testa säkerheten hos en IP-kamera. Kartläggning av nätverket sker med skannerverktyget Nmap. Paket som skickades mellan IP-kamera och smarttelefon fångades upp och analyserades med Wireshark. Genom att utföra en

ARP-spoofing placerar sig angriparen i en MitM-position och sniffar trafiken som passerar. Trafik som skickas mellan smarttelefon och IP-kamera samt mellan IP-kamera och server visade sig vara i klartext. Även autentiseringsinformation som skickades från smarttelefon till server var i klartext.

6.2.9 Trafikanalys

Det identifierades åtta textpassager i de accepterade artiklarna med relation till trafikanalys. Vid en trafikanalys-attack försöker angripare att olovligen få tillgång till ett nätverk för att sedan analysera trafiken. I ett IoT-nätverk kommunicerar de smarta enheterna alltid genom ett lokalt trådlöst nätverk. Oavsett om det är en enhet som använder sig av Bluetooth, WiFi, ZigBee, Z-Wave eller något annat protokoll, finns alltid risken för en trafikanalys-attack. A25 skriver att en angripare kan sniffa den trådlösa kanalen för att analysera nätverkstrafiken, rekonstruera kommunikationsprotokoll samt utföra spoofing-attacker mot IoT-nätverket. A10 beskriver att Wireshark är ett utmärkt verktyg för att erhålla en dynamisk bild av hur trafiken skickas och tas emot.

Identifiering av trafikflödet i ett nätverk är enligt A12 minst lika värdefullt som själva innehållet av ett paket. Noder som befinner sig närmre en gateway vidarebefordrar i regel fler paket än en nod längre ifrån. Information om var gateway och noder befinner sig i nätverket kan vara användbart för att ytterligare attacker som exempelvis DoS-attacker eller avlyssning av paket avsedda för just dessa enheter ska bli effektiva.

7 Diskussion

I detta kapitel diskuteras och reflekteras det kring implementationen och resultatet av den genomförda studien. Vidare diskuteras studiens etiska och samhälleliga effekter. Det ges förslag på hur studien kan användas för vidare forskning i framtiden. Avslutningsvis lyfts begränsningar med studien fram.

7.1 Resultat

Tidigare forskning har undersökt och visat att IoT-enheter i det smarta hemmet är sårbart mot flera olika typer av attacker. Mohammad et al. (2019) diskuterade olika IoT-applikationer i sin studie. Resultatet visade att det smarta hemmet är sårbart mot avlyssnings-, DoS-, imitations- och malware-attacker. Flera av dessa attacker förekommer i denna studie där både DoS- och malware-attacker har varit bland dem flest nämnda i artiklarna.

Nawir et al. (2017) konstaterar att säkerhetsbrister inom IoT kan leda till negativa effekter för användarna. Attacker som sammanfattades i deras studie var DoS, spoofing, replay och sybil. Det finns både likheter och olikheter med deras forskning och denna studie. Både DoS- och replay-attacker placerade sig bland de främst förekommande attackerna medan spoofing och sybil-attacker däremot, inte hade tillräckligt många omnämnanden i litteraturen.

Rizvi et al. (2020) har definierat vilka attackytor som finns i IoT-nätverk i hemmet. Det diskuteras verktyg som sniffar paket och kartlägger IoT-nätverk. I likhet med deras forskning har denna studie belyst attacker och deras olika metoder där angrepp sker mot IoT-nätverk. Verktyg som används har haft som syfte att ta reda på hur IoT-nätverk ser ut.

I tabell 4 är det möjligt att se hur många identifierade textpassager varje verktyg har. Medan Nmap och Wireshark har åtta respektive femton textpassager, har många av de andra verktygen endast några enstaka textpassager. Det har visat sig vara svårt att hitta tillräckligt många artiklar som omfattar verktyg. Flera studier som exempelvis (Beauchaine et al., 2021) och (Sallam et al., 2019), nämner verktygen vid namn men presenterar inte någon utförlig information om hur de används eller fungerar. Med det i åtanke blir det svårt att göra någon fördjupad analys utifrån litteraturen.

Flertalet attacker som förekommer i litteraturen är på många sätt lika varandra men kan ha olika syften när de används. Avlyssning, skanning och trafikanalys är exempel på passiva attacker. De är attacker som i grunden handlar om att samla in information. Granskas dessa attacker var för sig är det möjligt att se olikheter. Avlyssning används för att lyssna av trafik och få tag i känslig information. Skanning används för att kartlägga hur ett nätverk ser ut och hitta sårbarheter. Trafikanalys används för att analysera nätverk och ta reda på hur trafikmönstret ser ut.

Mohammad et al. (2019) diskuterar DoS och malware och nämner att det smarta hemmet är sårbart för dessa typer av attacker. I analysen har en metod varit mer framträdande än andra, där DoS och malware kombineras till en kraftfull attack. Malware i denna attack kallas Mirai och har till syfte att infektera så många IoT-enheter som möjligt och placera dessa i ett botnet. Det är sedan möjligt för angriparen att utföra DDoS-attacker med detta botnet.

Det finns en intressant koppling mellan MitM-, replay- och sniffingattacker. Innan en replay- eller sniffingattack utförs ser en angripare till att inta en MitM-position. MitM-attacken blir som en utgångspunkt innan en angripare påbörjar ytterligare attacker som exempelvis replay- eller sniffingattacker. Flera av dessa attacker är svåra för en användare att upptäcka då de sker passivt. Ali et al. (2017) diskuterade i sin studie att passiva attacker är ett tillvägagångssätt som används av angripare för att få tag i systeminformation utan att påverka systemresurser i sig. En förutsättning för att inte påverka ett system eller dra till sig uppmärksamhet vid en attack är att det sker passivt. Det kan styrkas utifrån den litteraturstudie som har genomförts.

Genom att sammanställa vilka attacker som förekommer i tidigare forskning och kombinera det med resultatet som har nåtts i denna studie, är det möjligt att få en samlad bild av vilka metoder samt verktyg, angripare använder sig av vid attacker mot det smarta hemmet. Resultatet visar också att vissa metoder samt verktyg förekommer mer frekvent än andra. Det kan dock ge en indikation om vilka metoder samt verktyg, angripare föredrar vid en attack.

7.2 Validitet av resultat

Den här studien har utförts som en litteraturstudie. I kapitel fyra beskrivs flera validitetshot som kan hota studien. Ett antal åtgärder har vidtagits för att mildra eller helt eliminera hoten. Ett protokoll har utformats som talar om hur studien ska genomföras. En handledare har vid ett flertal tillfällen granskat protokollet och lämnat feedback.

Det är svårt att avgöra när tillräckligt med relevant material har samlats in. I denna studie har både en databassökning och omvänd snöbollsmetod använts för att samla in så många relevanta artiklar som möjligt. Jesson et al. (2011) föreslår även att allt som har genomförts i studien ska dokumenteras, det gör att arbetet blir transparent och kan replikeras av andra forskare. Avvikelser i denna studie har dokumenterats utifrån bästa förmåga. Det färdiga examensarbetet kommer avslutningsvis att dels granskas av andra studenter i en referentgranskning, dels granskas av en examinator. Allt detta sammantaget resulterar i att studiens validitet upprätthålls.

7.3 Genomförandet

I ett av de första stegen av litteraturstudien ska ett undersökningsprotokoll utformas som beskriver hur den ska utföras. De söktermer som användes i denna studie uppfyllde sitt syfte i databassökningarna. Urvalskriterierna valdes utifrån att de skulle filtrera bort litteratur som inte nådde upp till en acceptabel nivå. Det kan dock diskuteras huruvida vissa kriterier var för snävt tilltagna vilket kan ha medfört att antalet artiklar blev för begränsat. Förslagsvis kunde publiceringsdatum på artiklar justeras något för att erhålla fler artiklar. Men det är samtidigt en balansgång med vart gränsen ska sättas, då det kan innebära att artiklar som uppfyller kriteriet visar sig vara utdaterat och attacker som beskrivs i artikeln inte längre är aktuella.

I studien användes referenshanteringsverktyg *EndNote Web* för att filtrera bort irrelevanta artiklar samt dubbletter. Trots att detta verktyg användes, visade det sig vara ett tidskrävande arbete att filtrera bort artiklar. Efter att artiklar hade filtrerats bort genom att granska titel och abstrakt var det fortfarande en del artiklar som var svåra att placera. Verktyget missade att

upptäcka ett par dubbletter som hade snarlikt innehåll. Dessa dubbletter filtrerades bort manuellt. Kriteriet gällande relevans är ett nödvändigt urvalskriterium för att endast behålla relevanta artiklar som kan bidra till studien. Det är ett kriterium som däremot är öppet för tolkning. Vad en specifik forskare anser vara relevant för en studie kan en annan forskare tycka är helt irrelevant.

Databassökningarna resulterade i 1 065 kandidatartiklar, där 26 artiklar slutligen hamnade i bibliografin. För att ytterligare bredda sökområdet och undvika att missa relevanta artiklar, användes den omvända snöbollsmetoden som ett komplement. Den omvända snöbollsmetoden ledde till 1 227 kandidatartiklar, där 16 artiklar sedan lades till i bibliografin. Av totalt 2 292 kandidatartiklar var det 42 artiklar som lades till i bibliografin. Strategin var att filtrera bort så många artiklar som möjligt för att det inte skulle bli alltför många artiklar som behövde granskas i sin helhet. Anledningen till det är att denna studie hade begränsade resurser i form av tid och mankraft.

Analysmetoden som valts för denna studie, tematisk analys, visade sig vara flexibel. Styrkan i tematisk analysmetod har varit hur den inte förhåller sig till något teoretiskt ramverk på samma sätt som andra analysmetoder (Braun & Clarke., 2006). Det gav ett användbart verktyg för att bearbeta data som samlats in från artiklarna. Samtidigt som metoden var användbar på många sätt var det också tidskrävande att gå igenom alla artiklar. Hade denna studie haft mer tid på sig hade en mer noggrann analys kunnat utförts.

7.4 Etiska & samhälleliga aspekter

Denna studie diskuterar flera typer av attacker och även vilka verktyg som används vid angrepp mot IoT-enheter och IoT-nätverk i det smarta hemmet. En etisk aspekt är att illvilliga personer skulle kunna utnyttja denna information i syfte att utföra attacker som kan anses vara oetiska. Studien diskuterar däremot inte några attacker på ett detaljerat sätt och berättar inte steg för steg hur en attack utförs eller verktyg används.

Smarta enheter finns i många hem, men det har samtidigt visat sig att säkerheten inte riktigt tas på allvar. Iqbal et al. (2020) har beskrivit hur säkerhetsmekanismer i dessa enheter är undermåliga eller inte existerar alls. Den här studien kan förhoppningsvis bidra till att människor med någon typ av säkerhetsroll kan dra nytta av att se vilka attacker som är vanligast förekommande i samband med angrepp mot IoT-nätverken och utforma säkerhetsmekanismer som står emot dem.

7.5 Framtida forskning

Den här studien har undersökt och kartlagt vilka metoder samt verktyg som används i samband med en attack mot IoT-nätverk. Detta har gjorts i kontexten av det smarta hemmet. Studien hade dragit fördel av att utföra ett praktiskt experiment för att testa de verktyg som har hittats i litteraturen. Fördelen är att det skulle vara möjligt att bilda sig en egen uppfattning om hur varje enskilt verktyg fungerar i realiteten. Ytterligare en utvidgning av detta skulle vara att sätta upp ett eget nätverk som motsvarar ett IoT-nätverk och sedan testa att utföra attacker med verktygen.

Skulle en litteraturstudie vara att föredra, skulle en annan ingång vara att rikta in studien på

ett annat område inom IoT. Ett förslag är att fokusera på den industriella miljön, där det finns helt andra motiv till att attackera och få tillgång till system.

7.6 Begränsningar

Resultaten av denna studie måste ses i ljuset av vissa begränsningar. En begränsning i denna studie gäller uteslutningen av ytterligare databaser som kunde ha inkluderats i forskningsprocessen. Även om den aktuella studien bygger på flera vetenskapliga databaser, där relevant data har samlats in, skulle införandet av fler databaser ha förbättrat det övergripande djupet och bredden av resultatet. På grund av tidsbristen och den omfattande karaktären av databassökning, omvänd snöbollsmetod samt analys, inkluderades inte ytterligare databaser utöver de som redan ingår. Som ett resultat av detta kan studiens slutsatser och generaliserbarhet ha påverkats vid utelämnandet av potentiellt relevant data från databaser som inte har inkluderats i forskningen.

8 Slutsats

Syftet med examensarbetet har varit att analysera och kartlägga de metoder och verktyg som används vid attacker riktade mot IoT-nätverk i hemmet. Det har uppnåtts genom att noggrant välja ämnesspecifika sökord för att bilda söktermer att använda vid sökningar i vetenskapliga databaser. De kandidatartiklar som har erhållits från databassökningarna genomgick en grundlig urvalsprocess med urvalskriterier som har utformats. De artiklar som uppfyllde samtliga urvalskriterier lades till i en bibliografi för accepterade artiklar. Referenslistorna från dessa artiklar användes som ett utgångsläge där en omvänd snöbollsmetod utfördes. De artiklar från referenslistorna som uppfyllde urvalskriterierna accepterades och lades till i bibliografin. Samtliga artiklar i bibliografin genomgick en analysmetod där tematisk analys användes.

Detta kapitel syftar till att redogöra för de slutsatser som har lyfts fram utifrån det resultat som har erhållits från analysen. Målet med denna studie var att besvara följande frågeställning:

”Vilka metoder samt verktyg används vid en attack av IoT-nätverk inom hemmet?”

Studien har identifierat nio verktyg och nio attacker med tillhörande metoder. Det går att konstatera att verktyg som förekommer i analysen kan användas till olika typer attacker. Aircrack-ng är mångsidigt då det kan användas till att både attackera och övervaka WiFi-nätverk. ARPspoof, Bettercap och Ettercap är exempel på verktyg som kan användas till MitM-attacker. Hping3 är ett verktyg som främst används i samband med DoS/DDoS-attacker. Metasploit är ett stort ramverk som används för att utnyttja exploits. Nessus och Nmap i kombination är effektiva verktyg som kan användas till att identifiera sårbarheter och kartlägga nätverk hos potentiella mål. Wireshark som förekom flest gånger i litteraturen är populärt för att analysera trafiken.

Ytterligare en slutsats som kan dras i relation till verktyg är att litteraturen innehåller få omnämnanden av verktyg som används vid angrepp. Vid ett flertal tillfällen har externa källor använts för att komplettera de luckor som har existerat. Det gör det svårt att dra någon djupare slutsats.

Av de attacker med tillhörande metoder som förekommer i analysen går det att konstatera flera saker. Avlyssning kan ske både i realtid och spelas in. Det huvudsakliga syftet är att försöka ta sig in på ett nätverk för att antingen exponera eller stjäla känslig information. DoS-attack är den attack som förekommer oftast i analysen. Det är en attack som kan utföras med olika metoder. Exempel på metoder som används vid DoS-attacker är land attack, ping of death, teardrop och SYN-flooding. I likhet med DoS-attacken kan DDoS-attacken använda sig av metoderna land attack, ping of death samt SYN-flooding. En kraftfull metod som används i kombination med DDoS är att använda stora nätverk med botnets. Efter att IoT-enheter har infekterats kan ett potentiellt mål attackeras genom att använda nätverket med

botnets för att utföra DDoS-attacker. DDoS-attacken blir svår att stoppa då källan till attacken kan komma från många olika riktningar på samma gång.

Malware är skadlig mjukvara som är utformad att skada enheter, nätverk och system. En vanlig metod som används är kodinjektion, där enheter äventyras genom att injektera skadlig kod. Den metod som är vanligast i analysen är Mirai-attacken. Det är en metod som riktar in sig på IoT-enheter med öppen telnet-anslutning. Enheter kan infekteras och läggas till i ett nätverk av botnets som kan utföra ytterligare attacker som DDoS-attacker. Andra metoder som förekommer är maskar som är anpassade för IoT-enheter samt falsk datainjektion som lurar ansiktsigenkänningskameror att ge obehörig åtkomst.

MitM är en vanligt förekommande attack mot IoT, där en angripare lyssnar på eller manipulerar trafiken, genom att placera sig mellan två enheter som kommunicerar. Den allra vanligaste metoden är att använda sig av ARP-förgiftning/ARP-spoofing för att genomföra attacken.

Replay-attack innebär att en angripare avlyssnar trafik mellan två parter. Vid ett senare skede maskerar sig angriparen som en sändare och skickar giltiga paket till en mottagare som uppfattar paketen som legitima. En metod som kan användas mot Echo-enheter är att utnyttja ett kryphål i implementationen av Bluetooth och utföra en attack döpt till Blueborne. Ytterligare en metod som angriper Bluetooth omfattar ett smart lås. Genom att använda ett verktyg som fångar upp Bluetooth-trafik är det sedan möjligt att utföra en replay-attack för att låsa upp låset. Det finns även en metod där ett förinspelat röstmeddelande spelas upp i en leksaksdocka med syftet att trigga en gateway eller röstaktiverad enhet att aktivera en sensor.

Skanning är en passiv attack som involverar kartläggning av nätverk för att identifiera enheter som är anslutna till det. Den vanligaste metoden är att använda Nmap, som söker efter öppna portar, fastställer enhetens operativsystem och identifierar exponerade tjänster. En annan metod som nämns är verktyget Nessus, som kan upptäcka och profilera körande tjänster på ett IoT-nätverk.

Sniffing är en attack där angripare fångar upp paket som skickas i ett nätverk, för att avlyssna eller stjäla känslig information som är okrypterad. Den vanligaste metoden är att skanna nätverket med verktyg som Nmap, utföra en ARP-spoofing för att placera angriparen i en MitM-position, för att därefter sniffa trafiken.

Vid en trafikanalys-attack försöker angripare att olovligen få tillgång till ett nätverk för att analysera trafiken. Den populäraste metoden är att använda sig av verktyget Wireshark för att få en dynamisk bild av hur trafiken skickas och tas emot.

Den slutsats som kan dras i relation till attacker är att det finns många metoder som kan riktas mot IoT och det smarta hemmet. Sett ur användarnas perspektiv i hemmet, är det en djungel i att leta fram relevant information samt en stor utmaning att skydda sig mot attacker och de olika metoder som förekommer.

Utöver de metoder som har presenterats i denna studie förekommer det metoder i litteraturen

som inte har inkluderats i studien. Precis som i fallet med verktygen, finns det flera metoder som har för få omnämnanden för att kunna dra någon slutsats. Ska även dessa metoder belysas behöver studien breddas för att erhålla större mängd artiklar.

Resultatet av studien kan förhoppningsvis bidra och ligga till grund när säkerhetspersonal ska utforma säkerhetsmekanismer som står emot dessa attacker. Vidare kan studien användas som en grund när vidare forskning ska utföras. Ett av förslagen var att praktiskt testa verktygen som hittats i litteraturen och göra det till ett experiment.

Referenser

Abdullah, T. A. A., Ali. W., Malebary, S. & Ahmed, A. A. (2019). *A Review of Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home*. International Journal of Computer Science and Network Security, 19(9), 139–146. https://www.researchgate.net/publication/336717887_A_Review_of_Cyber_Security_Challenges_Attacks_and_Solutions_for_Internet_of_Things_Based_Smart_Home

Aircrack. (2023, 16 januari). *Introduction*. Hämtad 14 maj, 2023, från https://www.aircrack-ng.org/doku.php

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. https://doi.org/10.1109/COMST.2015.2444095

Al-Sarawi, S., Anbar, M., Alieyan, K. & Alzubaidi, M. (2017, maj). *Internet of Things (IoT) communication protocols: Review*. 2017 8th International Conference on Information Technology (ICIT), Amman, Jordan, 685–690. https://doi.org/10.1109/ICITECH.2017.8079928

Ali, W., Dustgeer, G., Awais, M. & Shah, M. A. (2017, oktober). *IoT based smart home: Security challenges, security requirements and solutions*. 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield. https://doi.org/10.23919/IConAC.2017.8082057

Bastos, D., Shackleton, M. & El-Moussa, F. (2018). *Internet of Things: A survey of technologies and security risks in smart home and city environments*. Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 1–7. https://doi.org/10.1049/cp.2018.0030

Berndtsson, M., Hansson, J., Olsson, B. & Lundell, B. (2008). *Thesis Projects – A Guide for Students in Computer Science and Information Systems*. London: Springer. https://doi.org/10.1007/978-1-84800-009-4

Bettercap. (u.å.). *INTRODUCTION*. Hämtad 10 maj, 2023, från https://www.bettercap.org/intro/

Braun, V. & Clarke, V. (2006). *Using thematic analysis in psychology*. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brereton, P., Kitchenham, B., Budgen, D., Turner, M. & Khalil, M. (2007). *Lessons from applying the systematic literature review process within the software engineering domain*. Journal of Systems and Software, 80(4), 571–583. https://doi.org/10.1016/j.jss.2006.07.009

Chanal, P. M. & Kakkasageri, M. S. (2020). *Security and Privacy in IoT: A Survey*. Wireless Personal Communication 115, 1667–1693. https://doi.org/10.1007/s11277-020-07649-9

ClouDNS. (2022, 22 december). *What is a Teardrop attack, and how to protect ourselves?*. Hämtad 26 april, 2023, från https://www.cloudns.net/blog/what-is-teardrop-attack-and-how-to-protect-ourselves/

CompTIA. (u.å.). *What Is Wireshark and How Is It Used?*. Hämtad 25 april, 2023, från https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it

DarkReading. (2019, 10 januari). *Consumers Demand Security from Smart Device Makers*. Hämtad 24 februari, 2023, från https://www.darkreading.com/threat-intelligence/consumers-demand-security-from-smart-device-makers

DataVersity. (2022, 14 januari). *A Brief History of the Internet of Things*. Hämtad 30 mars, 2023, från https://www.dataversity.net/brief-history-internet-things/

Davis, B. D., Mason, J. C. & Anwar, M. (2020). *Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study*. IEEE Internet of Things Journal, 7(10), 10102–10110. https://doi.org/10.1109/JIOT.2020.2983983

Ettercap-project. (u.å.). *WELCOME TO THE ETTERCAP PROJECT*. Hämtad 10 maj, 2023, från https://www.ettercap-project.org/

Feng, S., Setoodeh, P. & Haykin, S. (2017). *Smart Home: Cognitive Interactive People-Centric Internet of Things*. IEEE Communications Magazine, 55(2), 34–39. https://doi.org/10.1109/MCOM.2017.1600682CM

Gamundani, A. M., Phillips, A. & Muyingi, H. N. (2019, juni). *An Overview of Potential Authentication Threats and Attacks on Internet of Things(IoT): A Focus on Smart Home Applications*. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada. https://doi.org/10.1109/Cybermatics_2018.2018.00043

Gerodimos, A., Maglaras, L., Ferrag, M. A., Ayres, N. & Kantzavelou, I. (2023). *IoT: Communication protocols and security threats*. Internet of Things and Cyber-Physical Systems, 3, 1–13. https://doi.org/10.1016/j.iotcps.2022.12.003

Ghadeer, H. (2018, november). *Cybersecurity Issues in Internet of Things and Countermeasures*. 2018 IEEE International Conference on Industrial Internet (ICII), Seattle, WA, USA. https://doi.org/10.1109/ICII.2018.00037

Goswami, S. A., Padhya, B. P. & Patel, K. D. (2020, mars). *Internet of Things: Applications, Challenges and Research Issues*. 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India. https://doi.org/10.1109/I-SMAC47947.2019.9032474

Gupta, H. & Sharma, S. (2021, augusti). *Security Challenges in Adopting Internet of Things for Smart Network*. 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India. https://doi.org/10.1109/CSNT51715.2021.9509698

Gupta, N., Naik, V. & Sengupta, S. (2017, juni). *A firewall for Internet of Things*. 2017 9th International Conference on Communication Systems and Networks (COMSNETS), Bengaluru, India. https://doi.org/10.1109/COMSNETS.2017.7945418

Informationssäkerhet. (2015, 19 augusti). *Detta är informationssäkerhet*. Hämtad 6 maj, 2023, från https://rib.msb.se/filer/pdf/29057.pdf

Iottechnews. (2021, 7 september). Kaspersky: Attacks on IoT devices double in a year. Hämtad 10 februari, 2023, från https://www.iottechnews.com/news/2021/sep/07/kaspersky-attacks-on-iot-devices-double-in-a-year/

Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B. & Bangash, Y. A. (2020). *An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security*. IEEE Internet of Things Journal, 7(10), 10250–10276. https://doi.org/10.1109/JIOT.2020.2997651

Jabbar, W. A., Alsibai, M. H., Amran, N. S. S. & Mahayadin, S. K. (2018, november). *Design and Implementation of IoT-Based Automation System for Smart Home*. 2018 International Symposium on Networks, Computers and Communications (ISNCC), Rome, Italy. https://doi.org/10.1109/ISNCC.2018.8531006

Jesson, J., Matheson, L. & Lacey, F. M. (2011). *Doing your literature review: Traditional and systematic techniques*. Sage Publications.

Kali. (2023, 8 mars). *Ettercap*. Hämtad 10 maj, 2023, från https://www.kali.org/tools/ettercap/

Kitchenham, B. & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in software engineering*. EBSE Technical Report EBSE-2007-01. https://www.researchgate.net/publication/258968007_Kitchenham_B_Guidelines_for_performing_Systematic_Literature_Reviews_in_software_engineering_EBSE_Technical_Report_EBSE-2007-01

Meneghello, F., Calore, M., Zucchetto, D., Polese, M. & Zanella, A. (2019). *IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices*. IEEE Internet of Things Journal, 6(5), 8182–8201. https://doi.org/10.1109/JIOT.2019.2935189

MITRE. (u.å.). *About the CVE Program*. Hämtad 10 maj, 2023, från https://www.cve.org/About/Overview

Mohammad, Z., Qattam, T. A. & Saleh, K. (2019). *Security Weaknesses and Attacks on the Internet of Things Applications*. 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 431-436. https://doi.org/10.1109/JEEIT.2019.8717411

Myndigheten för samhällsskydd och beredskap. (u.å.). *Internet of Things – IoT*. Hämtad 8 februari, 2023, från https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/sakerhet-i-cyberfysiska-system/internet-of-things--iot/

Myndigheten för samhällsskydd och beredskap. (2020, mars). *IoT-relaterade risker*. Hämtad 6 maj, 2023, från https://rib.msb.se/filer/pdf/29057.pdf

Myndigheten för samhällsskydd och beredskap. (2022, 31 maj). *Om systematiskt informationssäkerhetsarbete*. Hämtad 6 maj, 2023, från https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/om-systematiskt-informationssakerhetsarbete/

Nawir, M., Amir, A., Yaakob, N. & Lynn, O. B. (2017, januari). *Internet of Things (IoT): Taxonomy of security attacks*. 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand. https://doi.org/10.1109/ICED.2016.7804660

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G. & Ghani, N. (2019). *Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations*. IEEE Communications Surveys & Tutorials, 21(3), 2702–2733. https://doi.org/10.1109/COMST.2019.2910750

Nmap. (u.å.). *Nmap: Discover your network*. Hämtad 25 april, 2023, från https://nmap.org/

OffSec. (u.å.). *Metasploit Unleashed*. Hämtad 25 april, 2023, från https://www.offsec.com/metasploit-unleashed/

Radware. (2017, 4 april). *"BrickerBot" Results In Permanent Denial-of-Service*. Hämtad 23 februari, 2023, från https://www.radware.com/security/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/

Rahman, M. W., Islam, R., Hasan, M. M., Mia, S. & Rahman, M. M. (2020). *IoT Based Smart Assistant for Blind Person and Smart Home Using the Bengali Language*. SN Computer Science, 1(300), 1–13. https://doi.org/10.1007/s42979-020-00317-6

Ray, A. K. & Bagwari, A. (2017). *Study of smart home communication protocol's and security & privacy aspects*. 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), Nagpur, India, 240-245. https://doi.org/10.1109/CSNT.2017.8418545

Ray, A. K. & Bagwari, A. (2020). *IoT based Smart home: Security Aspects and security architecture*. 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India. https://doi.org/10.1109/CSNT48778.2020.9115737

Rizvi, S., Kurtz, A., Pfeffer, J. & Rizvi, M. (2018). *Securing the Internet of Things (IoT): A Security Taxonomy for IoT*. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, 163–168. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00034

Rizvi, S., Orr, RJ., Cox, A., Ashokkumar, P. & Rizvi, M. R. (2020). *Identifying the attack surface for IoT network*. Internet of Things, 9, 1–20. https://doi.org/10.1016/j.iot.2020.100162

Sanaullah, S. & Liu, B. (2022, augusti). *Information Security Challenges in the Internet of Things (IoT) Ecosystem*. 2022 International Symposium on Electrical, Electronics and Information Engineering (ISEEIE), Chiang Mai, Thailand. https://doi.org/10.1109/ISEEIE55684.2022.00029

Saxena, U., Sodhi, J. S. & Singh, Y. (2017). *Analysis of security attacks in a smart home networks*. 2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence, Noida, India, 431–436. https://doi.org/10.1109/CONFLUENCE.2017.7943189

Schurgot, M. R., Shinberg, D. A. & Greenwald, L. G. (2015). *Experiments with security and privacy in IoT networks*. 2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Boston, 1–6. https://doi.org/10.1109/WoWMoM.2015.7158207

Sentor. (2021, 29 mars). *Vad är malware?*. Hämtad 28 april, 2023, från https://www.sentor.se/artikel/malware/

Singh, G. D. (2019). *Learn Kali Linux 2019*. Packt Publishing. https://www.oreilly.com/library/view/learn-kali-linux/9781789611809/

Singh, H., Pallagani, V., Khandelwal, V. & Venkanna, U. (2018, juni). *IoT based smart home automation system using sensor node*. Konferensnamn, 2018 4th International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India. https://doi.org/10.1109/RAIT.2018.8389037

Sivapriyan, R., Sushmitha, S. V., Pooja, K. & Sakshi, N. (2021). *Analysis of Security Challenges and Issues in IoT Enabled Smart Homes*. 2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, 1–6. https://doi.org/10.1109/CSITSS54238.2021.9683324

Snyder, H. (2019). *Literature review as a research methodology: An overview and guidelines*. Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Swamy, S. N. & Kota, S. R. (2020). *An Empirical Study on System Level Aspects of Internet of Things (IoT)*. IEEE Access, 8, 188082–188134. https://doi.org/10.1109/ACCESS.2020.3029847

Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F. & Bilal, M. (2021). *Smart home security: challenges, issues and solutions at different IoT layers*. The Journal of Supercomputing, 77, 14053–14089. https://doi.org/10.1007/s11227-021-03825-1

Transforma Insights. (juli 1, 2022). *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030 (in billions)* [Graf]. In Statista. Hämtad 9 februari, 2023, från https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Vice. (2019, 11 december). *How Hackers Are Breaking Into Ring Cameras*. Hämtad 22 februari, 2023, från https://www.vice.com/en/article/3a88k5/how-hackers-are-breaking-into-ring-cameras

Wang, Z., Liu, D., Sun, Y., Pang, X., Sun, P., Lin, F., Lui, J. C. S. & Ren, K. (2022). *A Survey on IoT-Enabled Home Automation Systems: Attacks and Defenses*. IEEE Communications Surveys & Tutorials, 24(4), 2292–2328. https://doi.org/10.1109/COMST.2022.3201557

Wireshark. (u.å.). *Wireshark Frequently Asked Questions*. Hämtad 25 april, 2023, från https://www.wireshark.org/faq.html#_what_is_wireshark

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B. & Wesslén, A. (2012). *Experimentation in Software Engineering*. Springer Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-29044-2

Bilaga A – Bibliografi över accepterade artiklar

Tabell 6 nedan visar en lista över de accepterade artiklar som har passerat urvalskriterierna. Det ligger till grund för den analys som utförs i litteraturstudien. Varje artikel har tilldelats ett prefix. Anledningen till att prefix används är att underlätta när analysen redogörs.

Tabell 6 – Bibliografi över accepterade artiklar (författarens egna)

Prefix	**Titel**	**Författare & Publiceringsår**
A01	*Testing IoT Security: The Case Study of an IP Camera*	Abdalla, P. A. & Varol, C. (2020)
A02	*Web-based Attacks to Discover and Control Local IoT Devices*	Acar, G., Huang, D. Y., Li, F., Narayanan, A. & Feamster, N. (2018)
A03	*Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends*	Aldahmani, A., Ouni, B., Lestable, T. & Debbah, M. (2023)
A04	*SoK: Security Evaluation of Home-Based IoT Deployments*	Alrawi, O., Lever, C., Antonakakis, M. & Monrose, F. (2019)
A05	*Security Threats Against the Internet of Things at Home*	Alshammari, T. B. & Alanazi, A. S. (2021)
A06	*On the Feasibility of DoS Attack on Smart Door Lock IoT Network*	Asad, B. & Saxena, N. (2021)
A07	*A Study on IoT: Model, Communication Protocols, Security Hazards & Countermeasures*	Bagga, M., Thakral, P. & Bagga, T. (2018)
A08	*Security Attack on IoT Related Devices Using Raspberry Pi and Kali Linux*	Bakry, B. B. M., Adenan, A. R. B. & Yussoff, Y. B. M. (2022)
A09	*iBoT: IoT Botnet Testbed*	Beauchaine, A., Macchiaroli, M. & Yun, M. (2021)
A10	*PETIoT: PEnetration Testing the Internet of Things*	Bella, G., Biondi, P., Bognanni, S. & Esposito, S. (2023)
A11	*Firmware Update Attacks and Security for IoT Devices*	Bettayeb, M., Nasir, Q. & Talib, M. A. (2019)
A12	*Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures*	Butun, I., Österberg, P. & Song, H. (2020)

Tabell 6 – Bibliografi över accepterade artiklar (författarens egna), fortsättning

A13	*Denial of Service Attack on IoT System*	Chen, Q., Chen, H., Cai, Y., Zhang, Y. & Huang, X. (2018)
A14	*Evaluation of Several Denial of Service Attack Methods for IoT System*	Cui, Y., Liu, Q., Zheng, K. & Huang, X. (2018)
A15	*IoT Phantom-Delay Attacks: Demystifying and Exploiting IoT Timeout Behaviors*	Fu, C., Zeng, Q., Chi, H., Du, X. & Valluru, S. L. (2022)
A16	*Future Security of Smart Speaker and IoT Smart Home Devices*	Godwin, S., Glendenning, B. & Gagneja, K. (2019)
A17	*Selective Forwarding Attack on IoT Home Security Kits*	Hariri, A., Giannelos, N. & Arief, B. (2020)
A18	*A taxonomy of cyber-physical threats and impact in the smart home*	Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R.J., Filippoupolitis, A. & Roesch, E. (2018)
A19	*Penetration testing of connected households*	Heiding, F., Süren, E., Olegård, J. & Lagerström, R. (2023)
A20	*Vulnerabilities in IoT Devices with Software-Defined Radio*	Hung, P. D. & Vinh, B. T. (2019)
A21	*Study of Security and Privacy Issues in Internet of Things*	Khalid, M. H., Murtaza, M. & Habbal, M. (2020)
A22	*What's your protocol: Vulnerabilities and security threats related to Z-Wave protocol*	Kim, K., Cho, K., Lim, J., Jung, Y. H., Sung, M. S., Kim, S. B. & Kim, H. K. (2020)
A23	*DDOS prevention in IoT*	Kumar, S. & Chandavarkar, B. R. (2021)
A24	*Raspberry Pi Malware: An Analysis of Cyberattacks Towards IoT Devices*	Martin, E. D., Kargaard, J. & Sutherland, I. (2019)
A25	*Securing Consumer IoT in the Smart Home: Architecture, Challenges, and Countermeasures*	Meng, Y., Zhang, W., Zhu, H. & Shen, X. (2018)
A26	*Security Weaknesses and Attacks on the Internet of Things Applications*	Mohammad, Z., Qattam, T. A. & Saleh, K. (2019)

Tabell 6 – Bibliografi över accepterade artiklar (författarens egna), fortsättning

A27	*Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations*	Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G. & Ghani, N. (2019)
A28	*Penetration Testing of the Amazon Echo Digital Voice Assistant Using a Denial-of-Service Attack*	Overstreet, D., Wimmer, H. & Haddad, R. J. (2019)
A29	*Security Analysis and Prevention of Attacks on IoT Devices*	Raghuprasad, A., Padmanabhan, S., Babu, M. A. & Binu, P. K. (2020)
A30	*Systematic IoT Penetration Testing: Alexa Case Study*	Rak, M., Salzillo, G. & Romeo, C. (2020)
A31	*Securing Smart Home Networks with Software-Defined Perimeter*	Sallam, A., Refaey, A. & Shami, A. (2019)
A32	*An Analysis of DDoS Attacks in a Smart Home Networks*	Saxena, U., Sodhi, J. S. & Singh, Y. (2020)
A33	*Security Vulnerabilities in Consumer IoT Applications*	Shakdher, A., Agrawal, S. & Yang, B. (2019)
A34	*Security Testbed for Internet-of-Things Devices*	Siboni, S., Sachidananda, V., Meidan, Y., Bohadana, M., Mathov, Y., Bhairav, S., Shabtai, A. & Elovici, Y. (2019)
A35	*A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications*	Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T. & Uluagac, A. S. (2021)
A36	*Exploring The Security Issues in Home-Based IoT Devices Through Denial of Service Attacks*	Toutsop, O., Das, S. & Kornegay, K. (2021)
A37	*Investigating the Robustness of IoT Security Cameras against Cyber Attacks*	Trabelsi, Z. (2022)
A38	*IoT as a Land of Opportunity for DDoS Hackers*	Vlajic, N. & Zhou, D. (2018)
A39	*IoT based Mirai Vulnerability Scanner Prototype*	Vysakh, S. & Binu, P. K. (2020)

Tabell 6 – Bibliografi över accepterade artiklar (författarens egna), fortsättning

A40	*A Survey on IoT-Enabled Home Automation Systems: Attacks and Defenses*	Wang, Z., Liu, D., Sun, Y., Pang, X., Sun, P., Lin, F., Lui, J. C.S. & Ren, K. (2022)
A41	*Tracing MIRAI Malware in Networked System*	Xu, Y., Koide, H., Vargas, D. V. & Sakurai, K. (2018)
A42	*All Your Alexa Are Belong to Us: A Remote Voice Control Attack against Echo*	Yuan, X., Chen, Y., Wang, A., Chen, K., Zhang, S., Huang, H. & Molloy, I. M. (2018)

Bilaga B – Sammanställning av analys

Tabell 7 nedan, illustrerar fördelningen av relevanta textpassager relaterat till verktyg som identifierats i de accepterade artiklarna.

Tabell 7 – Relevanta textpassager relaterat till verktyg fördelat per accepterad artikel (författarens egna)

	Aircrack-ng	**ARPspoof**	**Bettercap**	**Ettercap**	**Hping3**	**Metasploit**	**Nessus**	**Nmap**	**Wireshark**
A01		**X**	**X**					**X**	**X**
A02									
A03									
A04							**X**		**X**
A05									
A06									**X**
A07									
A08			**X**					**X**	
A09									
A10				**X**			**X**	**X**	**X**
A11									
A12									
A13					**X**				**X**
A14					**X**				
A15		**X**						**X**	
A16									**X**
A17		**X**							**X**
A18	**X**								
A19				**X**	**X**				**X**
A20									
A21									
A22									

Tabell 7 – Relevanta textpassager relaterat till verktyg fördelat per accepterad artikel (författarens egna), fortsättning

	Aircrack-ng	**ARPspoof**	**Bettercap**	**Ettercap**	**Hping3**	**Metasploit**	**Nessus**	**Nmap**	**Wireshark**
A23									
A24									
A25									
A26									
A27									
A28						**X**		**X**	**X**
A29	**X**								
A30						**X**			**X**
A31					**X**				**X**
A32									**X**
A33		**X**	**X**			**X**		**X**	**X**
A34	**X**					**X**	**X**	**X**	**X**
A35									
A36					**X**				
A37				**X**	**X**	**X**		**X**	**X**
A38									
A39									
A40									
A41									
A42									

Tabell 8 nedan, illustrerar fördelningen av relevanta textpassager relaterat till attack/metod som identifierats i de accepterade artiklarna.

Tabell 8 – Relevanta textpassager relaterat till attack/metod fördelat per accepterad artikel (författarens egna)

	Avlyssning	**Denial of Service (DoS)**	**Distributed Denial of Service (DDoS)**	**Malware**	**Man-in-the-Middle (MitM)**	**Replay**	**Skanning**	**Sniffing**	**Trafikeanalys**
A01	**X**		**X**	**X**	**X**		**X**	**X**	**X**
A02	**X**			**X**					
A03	**X**	**X**	**X**	**X**	**X**	**X**			
A04					**X**		**X**		**X**
A05	**X**	**X**		**X**	**X**				
A06	**X**	**X**		**X**	**X**				
A07	**X**	**X**		**X**	**X**				
A08		**X**			**X**				
A09			**X**	**X**					
A10		**X**			**X**		**X**		**X**
A11				**X**					
A12	**X**	**X**							**X**
A13		**X**							
A14		**X**							
A15									
A16						**X**	**X**	**X**	
A17		**X**			**X**				
A18						**X**	**X**		
A19		**X**			**X**	**X**			
A20		**X**				**X**			**X**

Tabell 8 – Relevanta textpassager relaterat till attack/metod fördelat per accepterad artikel (författarens egna), fortsättning

	Avlyssning	Denial of Service (DoS)	Distributed Denial of Service (DDoS)	Malware	Man-in-the-Middle (MitM)	Replay	Skanning	Sniffing	Trafikeanalys
A21		X	X	X					
A22		X			X				
A23		X	X	X					
A24				X					
A25						X			X
A26	X	X		X	X	X			
A27		X		X				X	
A28		X					X		
A29		X							
A30								X	X
A31		X						X	
A32		X	X						
A33					X		X	X	X
A34							X		
A35	X	X						X	
A36		X							
A37		X			X				
A38			X				X		
A39		X	X	X					
A40				X					
A41			X	X					
A42						X			