VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ
DEPARTMENT OF INFORMATION SYSTEMS

BEZPEČNOSŤ A ÚTOKY CIELENÉ NA VIRTUÁLNYCH ASISTENTOV V PROSTREDÍ IOT

SECURITY AND ATTACKS AIMED AT VIRTUAL ASSISTANTS IN IOT ENVIROMENT

SEMESTRÁLNÍ PROJEKT
TERM PROJECT

AUTOR PRÁCE **RADOSLAV PÁLENÍK**
AUTHOR

VEDOUCÍ PRÁCE **Mgr. Ing. PAVEL OČENÁŠEK, Ph.D.**
SUPERVISOR

BRNO 2021

Abstrakt

Práca zaoberajúca sa popisom útokov na virtuálnych asistentov(Napr.: *Alexa* od firmy Amazon) v prostredí Internet of Things, ich motiváciou, princípom, a nebezpečenstvami

Abstract

Project describes IoT attacks aimed at virtual assistants (such as *Alexa* from Amazon company), their motivation, principles and risks.

Kľúčové slová

Internet vecí, Phishing, Virtuálny asistent

Keywords

Internet of Things, Phishing, Virtual assistant

Citácia

PÁLENÍK, Radoslav. *Bezpečnosť a útoky cielené na virtuálnych asistentov v prostredí IoT*. Brno, 2021. Semestrální projekt. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Mgr. Ing. Pavel Očenášek, Ph.D.

Bezpečnosť a útoky cielené na virtuálnych asistentov v prostredí IoT

Prehlásenie

Prohlašuji, že jsem tuto odbornou práci vypracoval samostatně pod vedením pana Očenáška
Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....
Radoslav Páleník
5. mája 2021

Poďakovanie

Ďakujem

Obsah

Kapitola 1

Úvod

Aj napriek vysokej popularite a konzistentnému trhovému rastu [1] je bezpečnosť IoT zariadení stále až kriticky nízka. Zatiaľ čo sa vo všetkých technológiách týkajúcich sa (nielen) nášho súkromia stále dbá na čoraz väčšiu bezpečnosť citlivých údajov, práve v oblasti IoT narastá počet útokov vysokým, až strmím tempom pričom medziročný nárast v rokoch 2018/2019 sa pohyboval skoro na deväťnásobku počtu útokov [7].

Popularita IoT priviedla rôzne formy útokov, ktoré sa snažia hlavne znemožniť správne fungovanie zariadení, alebo odpočuť ich komunikáciu. Výhodou pre útočníkov je aj to, že jedným z najdôležitejších faktorov vplývajúcim na tvorenie bezpečnostných chýb pri implementácii IoT zariadení je malé množstvo času, za ktorý majú byť tieto zariadenia navrhnuté [5].

Vďaka týmto chybám je pre útočníkov IoT prostredie ideálnym priestorom na používanie nových ale aj overených praktík na získanie citlivých dát, alebo aj znefunkčenia konkrétneho ekosystému. Útoky v tejto oblasti sú celkom rozmanité, od vytvárania botnet sietí pre DDoS útoky až po zámenu identifikátora peňaženky určenej pri vyplácaní odmien za vyťaženie kryptomien [7].

Tieto útoky sa nevyhli ani virtuálnym asistentom, odvetviu IoT zariadení zažívajúcim veľkú popularitu pri plnení funkcie hlavne domáceho pomocníka. Za prvých 5 rokov od vstúpenia zariadení *Amazon Alexa* na trh(2014) sa predalo vyše 100 miliónov zariadení [11], pričom sa odhaduje že sa tento počet do roku 2020 zdvojnásobil. Dobre sa darí taktiež momentálne najväčšiemu konkurentovi, platforme *Google Home* ktorá predala už vyše 50 miliónov vlastných asistentov [6].

Táto práca sa zaoberá technikami útokov zameraných práve na virtuálnych asistentov. Útoky, ktoré sú prezentované v tejto práci sa zameriavajú hlavne na prebranie kontroly nad samotným zariadením.

Kapitola 2

Definície pojmov

- **Virtuálny Asistent** Vrámci práce uvádzaný ako IoT zariadenie s prístupom na internet skonštruované ako smart reproduktor s funkcionalitou na ovládanie iných IoT zariadení pripojených hlavne v rovnakej LAN sieti alebo dosahu Bluetooth. Zariadenie je ovládané najmä hlasom[16].
- **Phishing** Podvodná technika vrámci sociálneho inžinierstva, pri ktorej sa snaží útočník získať citlivé údaje od obete, tým že predstiera inú ako svoju identitu. Zvyčajne sa jedná o identitu inštitúcie, vrámci ktorej chce zneužiť citlivé údaje obete(napr. prihlasovacie údaje do banky)[15].
- **Aplikácia** Všeobecné pomenovanie pre aplikácie vytvorené pre virtuálnych asistentov tretími stranami(Veľké spoločnosti majú tendenciu využívať vlastné pomenovania, napr.: „*Skill*“, „*Action*“,...).

Kapitola 3

Phishing s prebranou kontrolou nad virtuálnym asistentom

3.1 Nástup aplikácií pre virtuálnych asistentov

Od roku 2019[13] presahuje počet týchto aplikácií 100 tisíc pre najpopulárnejšiu platformu firmy Amazon *Alexa*. Pri platforme *Google Home* predstavuje ich počet aplikácií len podiel v jednotkách percent[2], no ich smart reproduktory dokážu komunikovať spolu s mobilnou aplikáciou *Google Assistant*, ktorá má príkazov už viac ako 1 milión[4]. Nezávisle od použitej platformy je možné vidieť vysoký trend rastu [1], [11], [6] v popularite týchto zariadení čomu sa prispôsobuje aj trh s aplikáciami ako je uvedené v [13] a [2]. Tento trend taktiež naznačuje s rastúcou popularitou aj nové metódy útokov [7], ktoré vznikajú najmä pre problémy spomenuté v 1.

3.2 Infiltrácia do virtuálnych asistentov

Jedným zo spôsobov ako dostať malware do virtuálneho asistenta budúcej obete sú Voice Squatting, resp. Masquerading útoky. Virtuálny asistenti používajú na inštaláciu a otváranie aplikácií tretích strán kľúčové slová, pomocou ktorých asistent manažuje operácie s jednotlivými aplikáciami. Jedná sa o exploitovacie techniky, pri ktorých útočníci registrujú svoje nové aplikácie pre virtuálnych asistentov s názvami, ktoré sa výslovnosťou približujú k názvom legitýmnych aplikácií, resp. môžu byť ich homonymá, synonymá, alebo sú publikované s preklepom v legitímnom názve aplikácie(napríklad pokiaľ by existovala aplikácia pre finančnú spoločnosť Goldman Sachs, útočník by sa mohol snažiť získať údaje ich zákazníkov publikovaním aplikácie s názvom „goldmine sacks“) [3].

Po publikovaní takejto aplikácie sa útočník spolieha na šancu, že Voice User Interface (VUI) daného asistenta v kombinácií s možnou zlou výslovnosťou obete pri vyhľadávaní stiahne útočníkovú aplikáciu namiesto tej legitímnej. Dôležitým poznatkom z výskumu týchto útokov [17] je aj to, že 60% užívateľov používa vrámci príkazov pre asistenta slovo „please“, pričom vyhľadávanie má tendenciu spájať hľadanú aplikáciu s čo najdlhším reťazcom, ktorý sa mu podarí nájsť. Pokiaľ by útočník pripojil na koniec názvu svojej aplikácie takéto slovo, značne by tým zvýšil šancu na spustenie práve jeho aplikácie voči požadovanej legitímnej.

Tím akademikov, ktorým sa v roku 2018 podarilo tieto nové metódy útokov objaviť informovali o ich nebezpečí firmy Google a Amazon, ktoré stoja za najpopulárnejšími virtuálnymi asistentmi na trhu. Pri týchto útokoch je kľúčová absencia autetntifikácie od asistenta smerom k užívateľovi. Taktiež ako sa uvádza v [17] je možné že takéto aplikácie sa už v obchodoch na týchto platformách už nachádzajú.

3.3 Phishing pomocou infiltrovaných aplikácií

3.3.1 Voice Squatting Attack

Aplikácia vyvíjaná za týmto účelom môže predstierať viac vzorov chovania. Najbežnejším sa môže javiť imitovanie správania legitímnej aplikácie namiesto ktorej bola podstrčená. Počas používania takejto aplikácie môže byť užívateľ vyzvaný, aby uviedol svoje údaje pre pokračovanie v danej operácii(napr. prihlasovanie sa). Tieto aplikácie môžu počas svojho behu imitovať aj správy od samotného asistenta, napríklad na stiahnutie novej aktualizácie, ktorú je potrebné potvrdiť heslom k správe celého zariadenia [10].

Okrem priameho získavania citlivých údajov cez asistenta môže aplikácia invokovať phishing aj pomocou podvrhnutých phishingových stránok, telefónnych čísel na falošnú podporu, alebo odkazovať na iné phishingové mechaniky. Takéto aplikácie môžu mať využitie aj na diskreditáciu reálnej spoločnosti.

Z danej štúdie [17] vyplýva, že pri takomto podhodení štyroch aplikácií zameraných na spúšťanie namiesto populárnej aplikácie „Sleep and Relaxation Sounds“[14] bol schopný výskumný tím odchytiť vyše 21 tisíc príkazov vrámci necelých 2700 otvorení nimi podvrhnutých aplikácií.

3.3.2 Voice Masquerading Attack

Voice Masquerading funguje na podobnom princípe ako Voice Squatting. Takáto aplikácia po svojom spustení predstiera určitý úkon, na ktorý bola zavolaná a následne imituje svoje ukončenie, tak ako by malo pri legitímnych aplikáciach prebiehať [10] [17].

Toto ukončenie môže prebehnúť buď automaticky alebo po prijatí niektorej z kľúčových fráz, ktoré používa asistent na legitímne vypnutie jeho aplikácií. Z množiny týchto fráz však väčšina slúži na imitáciu legitímneho vypnutia aplikácie, pričom daná aplikácia začne vystupovať ako samotná platforma zariadenia, cez ktorú sa zariadenie všeobecne ovláda.

Po predstieraní ukončenia aplikácie štandardnou audio-vizuálnou signalizáciou spustí aplikácia tichý audio súbor, aby sa sama neukončila po presiahnutí časovača ktorý má jednotlivé procesy asistenta ukončovať. Aplikácia je schopná na základe platformy odpočúvať užívateľov až do dĺžky nasledujúcich 384 sekúnd, pričom sa tento časovač obnovuje vždy, keď zahytí prichádzajúci audio vstup, a teda takto spustená aplikácia v ideálnych podmienkach môže byť spustená nepretržite [17].

Spustená aplikácia následne funguje ako rozhranie medzi užívateľom a aplikáciami ktoré chce spustiť, pričom im predáva audio vstup, ktorý je schopná uchovávať a teda sa správa ako pri voice squattingu.

3.3.3 Rozdiely v chovaní

Zatiaľ čo voice squatting aplikácie dokážu pracovať iba vo vnútri vlastného rámca a získavajú prevažne cielenú množinu dát, voice squatting metódy sú schopné akumulovať oveľa širší rozsah dát, ktorý je ale závislý na užívateľom spúšťaných aplikáciách. Aplikácie založené na týchto princípoch však nemusia slúžiť len na odpočúvanie a získavanie citlivých informácii, ale dokážu napríklad šíriť aj falošné správy.

Kapitola 4

Ovládanie asistenta pomocou laserového lúču

4.1 Princíp útoku

Princípom tohoto útoku je pomocou zvukového signálu pretransformovaného na svetelný signál vyvolať operáciu na virtuálnom asistentovi z diaľky. Asistent prijíma príkazy cez mikrofón s bránicou, ktorá je schopná prijímať okrem zvukových aj svetelné signály[9]. Vďaka tomuto útoku je útočník schopný ovládať virtuálneho asistenta do diaľky až 110 metrov. Hack, na ktorom je tento útok založený spočíva v konštrukčnej vlastnosti samotného zariadenia, resp. jeho mikrofónu.

4.2 Konštrukčný princíp MEMS mikrofónov

MEMS(Micro-Electro-Mechanical Systems) mikrofóny sa skladajú z dvoch podstatných častí [8]:

- **MEMS senzor** slúži na zachytenie zvukových vĺn dopadajúcich na mikrofónovú membránu
- **ASIC**(Application Specific Integrated Circuit) - Pomocou integrovaného obvodu sa konvertuje kapacitný rozdiel zachytený pomocou MEMS senzoru na analógový signál.

4.3 Problém s MEMS mikrofónmi

Problém pri zachytávaní „falošného“ signálu zariadením je v konštrukcii ASIC obvodu. Okrem požadovaného ovládania membránou v MEMS senzore, je totiž možné obvod ovládať aj na základe správne nastaveného a kontrolovaného lúču vďaka fotoelektrickému efektu. V pri dopade kontrolovaného lúču na obvod sa totiž indukuje foto-prúd, ktorého sila je úmerná intenzite svetla. Analógová časť ASIC rozpoznáva tento fotovoltaický prúd ako pravý signál z MEMS membrány, čo spôsobuje že mikrofón zaobchádza so svetlom ako s predpokladaným zvukovým signálom [12]. K úspešnému podvrhnutiu takéhoto signálu dopomáha aj fotoakustický efekt, ktorý počas dopadu na mikrofón okrem indukovania prúdu na ASIC taktiež vyvoláva mechanické vibrácie na MEMS membráne, čo ešte dopomáha ku kvalitnejšiemu spracovaniu injektovaného optického signálu.

4.4 Transformácia signálu

Signál lúčom injektovaný do mikrofónu sa správa rovnako zvuková vlna. Čím hlasnejšia má enkódovaná fráza byť odoslaná, tým väčšiu svetelnú intenzitu lúč nadobúda. Intenzita lúča, ktorá je nastavovaná prúdovým regulátorom pomocou amplitúdovej modulácie je výsledkom funkcie [12]

$$I_t = I_{DC} + \frac{I_{PP}}{2} \sin(2\pi f t)$$

,kde:

- I_t je prúd na dióde laseru
- I_{DC} je prúd jednosmernej zložky zosilneného vstupného audio súboru
- I_{PP} je prúd rozdielu amplitúd zložky zosilneného vstupného audio súboru

4.5 Obmedzenia

Keďže sa narozdiel od útokov v 3 jedná o hardvérovo založený útok, naskytuje sa viac možností, ako môže byť tento útok obmedzený. Keďže sa predpokladá, že sa útočník nenachádza v rovnakom obývacom priestore ako obeť, potrebuje mať na inkriminovaného virtuálneho asistenta priamy výhľad. Útočník musí byť teda vhodné umiestnený, a to nie len vzhľadom na potrebný výhľad, ale aj vzhľadom na maximálny dosah lúču, na ktorý je schopný asistenta ovládať. Pre správne fungovanie by mal byť taktiež vybraný laser, ktorý je schopný svojou funkcionalitou pokryť celé frekvenčné pásmo, ktorým je schopný útočník rozprávať [12].

Kapitola 5

Záver

Cieľom práce bolo vyzdvihnúť principiálnu jednoduchosť, na akej sú založené jednotlivé útoky ktoré boli spomenuté. V konkrétnych, niekedy až extrémnych, prípadoch nie je vylúčené, že pri vysokej motivácii by bolo možné spomenuté útoky aj kombinovať. Obidve metodiky na prístup ku kontrole virtuálneho asistenta ťažili hlavne na nedostatočnej autentizácii užívateľa, ktorý by vedel zabrániť nechceným operovaním útočníka s daným zariadením.

Je pochopiteľné že tieto zariadenia slúžia hlavne na komfortné spracovanie jednoduchých operácií týkajúcich sa domácností alebo získavania informácií a potvrdzovanie každého vykonávaného úkonu by hodnotu tohoto komfortu zrazili skoro na minimum, no potvrďovanie aspoň inštalovaných aplikácií by určite dopomohlo zvýšiť na túto dobu nízku úroveň zabezpečenia.

Literatúra

[1] Dahlqvist, F., Patel, M., Rajko, A. a Shulman, J. *Growing opportunities in the Internet of Things*. McKinsey & Company, Sep 2020. Dostupné z: https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things.

[2] Gebhart, A. *Everything you need to know about Google Home*. Sep 2020. Dostupné z: https://www.cnet.com/home/smart-home/everything-you-want-to-know-about-google-home/.

[3] Gillis, A. S. *What is voice squatting (skill squatting)? - Definition from WhatIs.com*. TechTarget, Jan 2019. Dostupné z: https://searchsecurity.techtarget.com/definition/voice-squatting-skill-squatting.

[4] Google. *Google Assistant*. Google, 2021. Dostupné z: https://assistant.google.com/explore.

[5] GUPTA, A. *The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things*. 1. vyd. Boston: Addison-Wesley, 2019. 14 – 16 s. ISBN 978-1-4842-4299-5.

[6] Kinsella, B. *RBC Analyst Says 52 Million Google Home Devices Sold to Date and Generating $3.4 Billion in 2018 Revenue*. Dec 2018. Dostupné z: https://voicebot.ai/2018/12/24/rbc-analyst-says-52-million-google-home-devices-sold-to-date-and-generating-3-4-billion-in-2018-revenue/.

[7] Mikhail Kuzin, V. K. *New trends in the world of IoT threats*. Sep 2018. Dostupné z: https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/.

[8] Min Qi, D.-h. Q. A High-Temperature, Low-Noise Readout ASIC for MEMS-Based Accelerometers. *Sensors*. 1. vyd. 2020, zv. 20, č. 1. ISSN 1424-8220. Dostupné z: https://www.mdpi.com/1424-8220/20/1/241.

[9] O'Donnell, L. *Alexa, Siri, Google Smart Speakers Hacked Via Laser Beam*. Nov 2019. Dostupné z: https://threatpost.com/alexa-siri-google-smart-speakers-hacked-via-laser-beam/149860/.

[10] Security Research Labs GmbH. *Smart Spies: Alexa and Google Home expose users to vishing and eavesdropping*. Dec 2019. Dostupné z: https://srlabs.de/bites/smart-spies/.

[11] Sterling, G. *More than 200 million smart speakers have been sold, why aren't they a marketing channel?* Feb 2020. Dostupné z: https://marketingland.com/more-than-200-million-smart-speakers-have-been-sold-why-arent-they-a-marketing-channel-276012.

[12] Sugawara, T., Cyr, B., Rampazzi, S., Genkin, D. a Fu, K. *Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems*. USENIX Association, 2020, s. 2631–2648. ISBN 978-1-939133-17-5. Dostupné z: https://www.usenix.org/conference/usenixsecurity20/presentation/sugawara.

[13] Vailshery, L. S. *Amazon Alexa: skill growth 2016-2019*. Jan 2021. Dostupné z: https://www.statista.com/statistics/912856/amazon-alexa-skills-growth/.

[14] Voice Apps, LLC. *Amazon.com: Sleep and Relaxation Sounds: Alexa Skills*. Google, 2021. Dostupné z: https://www.amazon.com/Voice-Apps-LLC-Relaxation-Sounds/dp/B06XBXR97N.

[15] Wikipedia contributors. *Phishing — Wikipedia, The Free Encyclopedia*. 2021. [Online; accessed 29-April-2021]. Dostupné z: https://en.wikipedia.org/w/index.php?title=Phishing&oldid=1020490637.

[16] Wikipedia contributors. *Virtual assistant — Wikipedia, The Free Encyclopedia*. 2021. [Online; accessed 29-April-2021]. Dostupné z: https://en.wikipedia.org/w/index.php?title=Virtual_assistant&oldid=1019988886.

[17] Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y. et al. *Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems*. 2019, s. 1381–1396. ISBN 978-1-5386-6661-6.