VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ
DEPARTMENT OF INFORMATION SYSTEMS

BEZPEČNOST A ÚTOKY V PROSTŘEDÍ IOT

SECURITY AND ATTACKS IN THE IOT ENVIRONMENT

IBS - ODBORNÁ PRÁCE NA VYBRANÉ TÉMA
IBS - TECHNICAL WORK ON A SELECTED TOPIC

AUTOR PRÁCE **ANDREI SHCHAPANIAK**
AUTHOR

BRNO 2022

Obsah

Kapitola 1

Úvod

Internet věcí (**Internet of things**, **IoT**) popisuje síť fyzických objektů obsahujících senzory, software a další technologie, které jsou nutné k propojení a výměně dat s jinými zařízeními přes internet. „Věci“ ve světě IoT mohou být člověk se srdečním implantátem, fotoaparát, automobil, lednička, žárovka, kuchyňské spotřebiče, dětské monitory nebo jakýkoli jiný přírodní nebo umělý objekt, kterému lze přiřadit IP adresu a je schopen přenášet data po síti [8].

IoT je centralizovaný systém, který poskytuje možnost přístupu k informacím odkudkoli a kdykoli na jakémkoli zařízení, které je připojeno k síti. Ve většině případů lidé mají hubové zařízení nebo aplikaci, ke kterým jsou připojena ostatní IoT zařízení.

Hlavní výhodou takového systému je automatizace úkolů, která snižuje potřebu lidského zásahu. "Paměť"zařízení pomáhá nastavovat mu periodické úkoly, které je nutné nastavit pouze jednou. Například lze nastavit chytrou konvici tak, aby každý den v osm ráno vařila vodu, pokud v konvici je více než 500 mililitrů vody.

Ale IoT jako i jiný sytém má své nevýhody. Takový velký počet připojených zařízení může znamenat, ze pokud je v systému chyba, každé připojené zařízení se může pravděpodobně poškodit. Ještě k tomu lze přidat, že v současné době neexistuje mezinárodní standard kompatibility pro IoT, což komplikuje vzájemnou komunikaci zařízení různých výrobců.

Jako i jiné systémy IoT podvržen různým typům kybernetických útoků. Cílem této práce je seznámit čtenáře s problematikou různých typů útoků na IoT zařízení a ukázat vhodné a efektivní způsoby ochrany proti nim.

Kapitola 2

Útoky v prostředí IoT

Zabezpečení IoT systémů není snadné. IoT propojuje miliardy zařízení mezi sebou přes internet a je třeba zabezpečit každé z nich. Propojení velkého počtu zařízení dovoluje hackerům zneužít pouze jednu zranitelnost, aby se dostali ke všem datům a učinili je nepoužitelnými. V dalších sekcích budou popsány nejrozšířenější typy útoků na IoT zařízení.

2.1 Odmítnutí služby

Odmítnutí služby (**Denial of Service**, **DoS**) je typ útoku, jehož cílem je znefunkčnit nebo znepřístupnit napadenou službu legitimním uživatelům. Při použití DoS útoků mohou být ohroženy tři věci – důvěrnost, integrita a dostupnost.

Jeden známý malware, který generuje DoS útoky, je BrickerBot[1]. Používá slovníkové útoky hrubou silou k získání přístupu k IoT zařízením a po přihlášení spustí řadu škodlivých příkazů, které vedou k trvalému poškození zařízení. Mezi tyto příkazy patří:

- Špatná konfigurace úložiště a parametrů jádra zařízení.
- Vymazání všech souborů na zařízení.
- Omezení připojení k internetu.

Tento útok často vyžaduje reinstalaci hardwaru nebo kompletní výměnu zařízení. Dále budou popsány dva neznámějších typů útoků, avšak existuje jich mnohem více a každý z nich je zaměřen na určité protokoly a kriteria určitého IoT systému.

2.1.1 Smurf útok

Vytváří se falešný paket, který má zdrojovou IP adresu nastavenou na adresu cílového serveru a cílovou IP adresu nastavenou na broadcast routeru. Až paket dorazí na směrovač, ten odešle ho všem hostitelským zařízením v síti, která odpoví odesláním paketů ICMP na podvrženou adresu cíle. V důsledku toho bude cílový server přetížen [1].

2.1.2 SYN flood útok

Tento útok je založen na principu TCP handshaku [5]. TCP pracuje synchronně s IP a udržuje pořadí dat mezi odesílatelem a příjemcem. Při handshaku server obdrží SYN paket

[1] https://www.radware.com/security/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/

od klienta k inicializaci spojení. Odpoví odesláním potvrzení ACK a pak znovu obdrží ACK od klienta. Při útoku SYN flood útočník neodesílá odpověď serveru a pokračuje posílat SYN pakety, dokud nevyčerpá všechny dostupné síťové porty serveru. Pak bude služba legitimním klientům odepřena a server může dokonce spadnout.

2.2 Umělá inteligence

V poslední době využití umělé inteligence v různých IT oblastech velmi rychle roste. Pro hackery je velmi důležité sledovat aktuální trendy, proto se umělá inteligence používá v kybernetických útocích již více než deset let. Nejčastější oblast pro její využití je sociální inženýrství.

Nástroje potřebné pro budování a používání umělé inteligence při kybernetických útocích se prodávají na temném webu. Systémy umělé inteligence mohou provádět opakované úkoly k rychlému škálování hrozeb IoT a jsou schopny napodobovat běžný provoz uživatelů.

Jedna ze známých testovacích metod je **Fuzzing**, generující různé vstupy, které mohou způsobit selhání cílového softwaru [6]. Příkladem takovéhoto vstupu může být SQL injekce, velké číslo, speciální znak a jiné. Umělá inteligence na základě formátu softwaru a chyb generuje nové vstupní hodnoty. Vývoj efektivního inteligentního fuzzing algoritmu však vyžaduje odborné znalosti a ladění. Tato metoda pomáhá automatizovat hledání slabých míst v systému a udělat toto hledání chytřejším.

2.3 Botnety

Hackeři mohou využít IoT zařízení, která jsou připojena k internetu, pro provádění hromadných útoků. Takové útoky se nazývají distribuované odmítnutí služby (**Distributed Denial of Service**, **DDoS**). Liší se od DoS tím, že k útoku je využita velká skupina zařízení, kterým se říká botnety. Počet botnetů ve skupině může být tvořen stovkami tisíc nebo dokonce miliony IoT zařízení.

Když útočníci nainstalují malware na tato zařízení, mohou využít svůj kolektivní výpočetní výkon k tomu, aby se postavili na větší cíle. Proto tyto útoky jsou mnohem závaznější než DoS útoky.

Útočníci mohou:

- Posílat spam.
- Krást informace.
- Dělat záznamy zvuku nebo videa.

Jeden z nejznámějších botnetu, červ Mirai, byl použit k provedení jednoho z největších dosud známých DDoS útoku a byl zaměřen na infikování IoT zařízení, jako jsou DVR[2], CCTV[3] kamery a domácí routery [4]. Virus byl skrytý, protože byl poměrně malý a ve skutečnosti se nenacházel na pevném disku zařízení. Zůstával v paměti a po restartování zařízení byla provedena reinfekce. Zajímavé je, že BrickerBot, o kterém bylo zmíněno v sekci 2.1, byl navržen se záměrem na zařízení, na která cílil botnet Mirai. Cílem BricketBotu bylo zničení zařízení po provedení DDoS útoku.

[2]Digital Video Recoder https://en.wikipedia.org/wiki/Digital_video_recorder
[3]Closed Circuit Televisionhttps://en.wikipedia.org/wiki/Closed-circuit_television

2.4 Muž uprostřed

Slabá metoda šifrování mezi klientem a serverem usnadňuje provedení útoku typu muž uprostřed (**Man in the Middle**, **MITM**). Útočník se snaží tajným odposlechem komunikace mezi dvěma stranami oklamat klienta, aby si myslel, že dostává legitimní zprávu. V případě úspěšného provádění útoku útočník bude moct manipulovat zařízeními. Příkladem může byt SSL stripping[4], ARP spoofing a jiné [7].

Mnoho IoT zařízení neověřuje úroveň důvěryhodnosti certifikátů, proto metoda certifikátu s vlastním podpisem je někdy užitečná. Například chytrý kávovar s funkcí zobrazení Google kalendáře uživatele může být lehce prolomen, když útočníci zjistí, že systém neověřuje SSL certifikáty.

2.5 Vyděračský software

Vyděračský software (**Ransomware**) je forma malwaru určená k uzamčení zařízení, blokování systému nebo šifrování dat, dokud nebude zaplaceno výkupné. Cílem hackerů je pokusit uzamknout samotné zařízení, čím omezí přístup autorizovaného uživatele. Problém je v tom, že se zbavit tohoto viru lze správným resetováním zařízení nebo instalací opravy. Kvůli tomu systémy, které jsou podvrženy útokem pomoci tohoto malwaru, jsou kritické. To znamená, ze zaplatit výkupné ve velmi krátkém časovém období je výhodnější, než čekat na opravu. Například kritickým zařízením může být IoT zařízení používané v průmyslovém prostředí.

[4] https://www.keyfactor.com/blog/what-are-ssl-stripping-attacks/

Kapitola 3

Zabezpečení proti útokům

Jak lze vidět z kapitoly 2, existuje velké množství útoků. Některé z nich mohou ukrást soukromá data, jiné zničit celý systém. Odborníci v kybernetické a informační bezpečnosti pravidelně vyvíjí nové nástroje a metody bránění proti počítačovým útokům. Dále budou uvedeny populární způsoby, jak udělat váš firmware a software bezpečnějším.

3.1 Pravidelná aktualizace softwaru a firmwaru

Většina bezpečnostních nástrojů pro zjištění útoků používají databáze virů a malwaru – soubory, které softwaru umožňují detekovat konkrétní viry. Příkladem takové databáze je MalwareBazaar[1]. Pokud zařízení nebudou aktualizována, nástroj nebude vědět o posledních a aktuálních malwarech, co může způsobit snížení bezpečnosti IoT zařízení. Zajištěním pravidelné aktualizace vašich IoT zařízení se vám pomůže vyhnout infekce malwarem.

Aktualizovat firmware lze dvěma způsoby:

1. Dálkově. Tato metoda zahrnuje pravidelnou komunikace zařízení s claudovým úložištěm a čekáni na zprávy o aktualizaci. Zařízení, které bylo aktualizováno, může poslat oznámení sousedním zařízením v síti, že je dostupna nová verze firmwaru. V případě takové aktualizace DoS útok představuje velké riziko, proto je vhodné přidat další bezpečnostní úroveň během aktualizace.

2. Přímo. Typ takové aktualizace firmwaru je využít v kritických IoT systémech, kde je nutné udržení nejvyšší možné úrovně zabezpečení. Proběhne kontrola integrity firmwaru ověřeným uživatelem, která snižuje možnost nahrazení legitimní firmware zařízení škodlivým.

3.2 Systém detekce narušení

Systém detekce narušení (**Intrusion Detection System**, **IDS**) je skupina nástrojů a mechanismů k identifikaci a hodnocení jakýchkoli druhů neschválených nebo neoprávněných aktivit v síti nebo systému. Většina z nich funguje na základě porovnání aktuálních souborů datových vzorů s předdefinovaným souborem základních kritérií [2].

IDS nejčastěji je využít pro detekci zneužití a anomálií. V prvním případě se zaměřuje na vzory dříve známých útoků, ve druhém naopak na normální chování systému.

[1] https://bazaar.abuse.ch/

Důležitou roli v systémech detekce narušení hraje umělá inteligence [3].

- Učení s učitelem.
  - **Naïve Bayes**. Určuje jaká je pravděpodobnost, že dojde k určitému druhu útoku, s ohledem na pozorované aktivity systému.
  - **Umělá neuronová síť (Artificial neural network)**. Jedna z nejrozšířenějších metod strojového učení, ale detekce u méně častých útoků potřebuje zlepšení, protože pro ně testovací datová sada je malá.
  - **Skrytý Markovův model (Hidden Markov Model)**. Je statistický Markovův model, ve kterém se předpokládá, že modelovaný systém je Markovův proces s neviditelnými daty. Tato metoda může být použita k identifikaci konkrétních druhů malwaru.
- Učení bez učitele.
  - **K-means**. Často se používá k identifikaci různých profilů chování hostitele.
  - **Pravděpodobnostní a hierarchické shlukování (Probabilistic and hierarchical clustering)**.
- Hluboké učení.
  - **Rekurentní neuronová síť (Recurrent neural network)**. Používá informace o svém předchozím stavu jako vstup pro svou aktuální předpověď. Díky této funkci je velmi vhodná pro vytváření IDS s vysokou přesností a jeho výkon je lepší než u tradičních klasifikačních metod strojového učení.
  - **Konvoluční neuronová síť (Convolutional neural network)**.

3.3 Kryptografická schémata

Kryptografie je jeden ze způsobů zabezpečení komunikačních kanálů. Existují různé možnosti pro zajištění bezpečného doručení zpráv v síti:

- Symetrická kryptografie(AES, IDEA, RC4).
- Asymetrická kryptografie (RSA, digitální podpis, Diffie–Hellman).
- Infrastruktura veřejného klíče.

Avšak v IoT systému vyskytují problémy, které komplikují implementaci šifrovacích standardů. Neexistuje standard, podle kterého by v celém světě byla vyvíjena IoT zařízení. Každý výrobce je implementuje s využitím různého hardwaru. Zajistit pro takové systémy jediný bezpečný šifrovací standard je velmi obtížné. Kvůli tomu se kryptoanalytici a odborníci v oboru kybernetické bezpečnosti zabývají testováním nových šifrovacích algoritmů, které by mohly poskytnout důvěrnost v odlehčených prostředích jako je IoT prostředí. V současné době se testuje odlehčený šifrovací algoritmus **LEA**[2], který je jedenapůlkrát až dvakrát rychlejší než pokročilý standard šifrování **AES**[3].

[2]Lightweight Encryption Algorithm https://en.wikipedia.org/wiki/LEA_(cipher)
[3]Advanced Encryprion Standard https://cs.wikipedia.org/wiki/Advanced_Encryption_Standard

Ale i tady jsou své zvláštní problémy, jako například čekáni na zpřístupnění odlehčené šifrovací technologie. Může být obtížné dodatečně vybavit existující technologie IoT novými bezpečnostními standardy, protože uživatele budou muset buď vyměnit stará zařízení nebo mít omezené zabezpečení dat.

3.4 Změna továrních nastavení

Při nastavování nového zařízení do IoT světu je dobrou praxí změnit tovární nastavení, protože některá z nich nikdy nebudete používat a necháte je zapnutá. Možná jsou vhodná pro vytváření chytré domácí sítě, avšak taková zařízení mohou vytvořit významnou bezpečnostní mezeru. Pomoci jednoho nezabezpečeného IoT zařízení se hackeři mohou snadno připojit k síti. Jednou z takových nebezpečných funkcí v IoT zařízeních je vzdálený přístup.

Většina zařízení je chráněná heslem, které uživatelům sítě zabrání měnit nastavení zabezpečení nebo používat zařízení bez správného hesla. Tato zařízení se však často dodávají s továrními hesly. Hackeři mohou často uhádnout výchozí hesla pomocí slovníků s častými hesly nebo použít zdroje výrobce k vyhledání hesla pro zařízení.

Změna výchozího hesla na něco jedinečného a bezpečného pomůže udržet IoT zařízení v bezpečí.

Kapitola 4

Závěr

V kapitole 1 byl probrán koncept Internetu věcí, co to je, jak funguje, výhody a nevýhody. Čtenář byl seznámen s objektem další práce. V kapitole 2 byly ukázány různé typy útoků na IoT systémy. Každý z útoků byl krátce popsán a byla vysvětlena jeho hlavní myšlenka a na čem je založen. Následně v kapitole 3 byly popsány neznámější typy bránění proti takovým útokům.

Literatura

[1] Abughazaleh, N., Bin, R., Btish, M. a M., H. DoS Attacks in IoT Systems and Proposed Solutions. *International Journal of Computer Applications*. Červen 2020, sv. 176, s. 16–19. DOI: 10.5120/ijca2020920397.

[2] Ahanger, T. Defense Scheme to Protect IoT from Cyber Attacks using AI Principles. *International Journal of Computers Communications Control*. Listopad 2018, sv. 13, s. 915–926. DOI: 10.15837/ijccc.2018.6.3356.

[3] Ansam, K. a Ammar, A. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity*. Březen 2021. DOI: 10.1186/s42400-021-00077-7. Dostupné z: https://doi.org/10.1186/s42400-021-00077-7.

[4] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E. et al. Understanding the Mirai Botnet. In: *Proceedings of the 26th USENIX Security Symposium*. 2017. Dostupné z: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

[5] Conrad, E., Misenar, S. a Feldman, J. Chapter 3 - Domain 2: Telecommunications and Network Security. In: Conrad, E., Misenar, S. a Feldman, J., ed. *CISSP Study Guide (Second Edition)*. Second Edition. Boston: Syngress, 2012, s. 63–141. DOI: https://doi.org/10.1016/B978-1-59749-961-3.00003-0. ISBN 978-1-59749-961-3. Dostupné z: https://www.sciencedirect.com/science/article/pii/B9781597499613000030.

[6] Murat, K., Corinne, F. a Ozgur, G. Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*. Únor 2021. DOI: 10.1007/s43926-020-00001-4. Dostupné z: https://doi.org/10.1007/s43926-020-00001-4.

[7] Sukkar, G. A., Saifan, R., Khwaldeh, S., Maqableh, M. a Jafar, I. Address Resolution Protocol (ARP): Spoofing Attack and Proposed Defense. *Communications and Network*. Červenec 2016. DOI: 10.4236/cn.2016.83012. Dostupné z: https://doi.org/10.4236/cn.2016.83012.

[8] Urbanovský, J. *Bezpečnost a útoky v prostředí IoT*. Brno, CZ, 2018. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Dostupné z: https://www.fit.vut.cz/study/thesis/21256/.