**UNIVERZITA OBRANY**

**FAKULTA VOJENSKÝCH TECHNOLOGIÍ**

**Studijní program: Vojenské technologie**

Studijní obor: Kybernetická bezpečnost

Ev. číslo: xxxx/22



**DIPLOMOVÁ PRÁCE**

Název: Nástroj pro testování a zvyšování odolnosti organizací proti phishingu

Zpracoval: Tomáš Hujňák

Vedoucí práce: mjr. Ing. Tomáš Šlajs

BRNO 2025

**PODĚKOVÁNÍ**

**ČESTNÉ PROHLÁŠENÍ**

Prohlašuji, že jsem zadanou diplomovou práci na téma „Využití lehké kryptografie k provedení autentizace“ vypracoval samostatně, pod odborným vedením vedoucího mjr. Ing. Pavla Kozaka, Ph.D. a použil jsem pouze literární zdroje uvedené v práci.

Dále prohlašuji, že jsem seznámen s tím, že se na moji diplomovou práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména skutečnosti, že Univerzita obrany má právo na uzavření licenční smlouvy o užití této diplomové práce jako školního díla podle § 60 odst. 1 výše uvedeného zákona, a s tím, že pokud dojde k užití této diplomové práce mnou nebo bude poskytnuta licence o užití díla třetímu subjektu, je Univerzita obrany oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladu, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše. Souhlasím se zpřístupněním své diplomové práce pro prezenční studium v prostorách knihovny Univerzity obrany.

V Brně, dne xx. dubna. 2022

..........................................

Tomáš Hujňák

**ABSTRAKT**

**Klíčová slova:**

**ABSTRACT**

**Key words:**

**OBSAH**

[SEZNAM POUŽITÝCH ZKRATEK 8](#_Toc167298636)

[SEZNAM OBRÁZKŮ 10](#_Toc167298637)

[SEZNAM TABULEK 11](#_Toc167298638)

[ÚVOD 12](#_Toc167298639)

[1 Teoretická část 13](#_Toc167298640)

[1.1 Internet věcí 13](#_Toc167298641)

[1.1.1 Architektura Internetu věcí 13](#_Toc167298642)

[1.1.2 Aplikace Internetu věcí v domácnostech 15](#_Toc167298643)

[1.2 Zabezpečení v Internetu věcí 16](#_Toc167298644)

[1.2.1 Bezpečnostní výzvy 17](#_Toc167298645)

[1.2.2 Současné bezpečnostní techniky 19](#_Toc167298646)

[1.3 Úvod do kryptografie 20](#_Toc167298647)

[1.3.1 Základní principy kryptografie 21](#_Toc167298648)

[1.3.2 Moderní kryptografie 22](#_Toc167298649)

[1.3.3 Lehká kryptografie 26](#_Toc167298650)

[1.3.4 Základní principy lehké kryptografie 26](#_Toc167298651)

[1.4 Bezpečnostní mechanismy z lehké kryptografie 27](#_Toc167298652)

[2 Cíle a omezení 28](#_Toc167298653)

[3 Analýza rizik 29](#_Toc167298654)

[4 30](#_Toc167298655)

[ZÁVĚR 31](#_Toc167298656)

[SEZNAM POUŽITÉ LITERATURY 32](#_Toc167298657)

[SEZNAM PŘÍLOH 34](#_Toc167298658)

SEZNAM POUŽITÝCH ZKRATEK

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# SEZNAM OBRÁZKŮ

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Strana |
| Obrázek 1 | − | Aplikace IoT zařízení |  |
| Obrázek 2 | − | Celkový počet připojených zařízení IoT a globální trh IoT doposud a předpověď budoucnosti |  |
| Obrázek 3 |  | Šifrování a dešifrování pomocí sdíleného klíče |  |
| Obrázek4 |  | Šifrování a dešifrování pomocí veřejného a tajného klíče |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# SEZNAM TABULEK

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Strana |
| Tabulka 1 | − | Popis tabulky | … XX |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# ÚVOD

V

# Teoretická část

V teoretické části bude objasněn pojem Internet věcí, známý pod zkratkou IoT (z anglického „Internet of Things“), a jeho význam a role, se zaměřením na bezpečnostní aspekty těchto zařízení. Budou popsány běžné bezpečnostní hrozby, kterým čelí IoT zařízení v domácnostech, a představeny specifické typy útoků, které jsou pro tato zařízení nejrelevantnější. Speciální pozornost bude věnována zranitelnostem, které vyplývají z omezené výpočetní kapacity a energetické náročnosti těchto zařízení.

Následně bude diskutováno o různých metodách zabezpečení, které lze použít k ochraně IoT zařízení, se zvláštním důrazem na využití kryptografie a zejména lehké kryptografie. Jelikož se lehká kryptografie jeví jako preferované řešení pro ochranu dat v IoT, tak tato část zahrne přehled hlavních principů a algoritmů, které jsou vhodné pro implementaci na IoT zařízeních.

## Internet věcí

Internet věcí představuje koncept, kde fyzické předměty a zařízení jsou propojeny pomocí internetu, aby mohly komunikovat a vzájemně interagovat. Tyto „chytré“ předměty mohou sbírat a vyměňovat data automaticky, což otevírá nové možnosti pro efektivnější řízení a automatizaci v různých oblastech života.

Pojem „Internet of Things“ byl poprvé použit Kevinem Ashtonem v roce 1999 během jeho prezentace pro Procter & Gamble. Ashton zdůraznil potenciál propojených zařízení, které by mohly revolucionizovat každodenní procesy tím, že propojí fyzický svět s počítačovými systémy bez potřeby lidského zásahu [1]. S postupem času se IoT stalo klíčovým prvkem v mnoha průmyslových odvětvích, včetně zdravotnictví, kde umožňuje sledování pacientů na dálku, v zemědělství pro monitorování a automatizaci procesů, ve výrobních průmyslu pro optimalizaci výrobních linek, ve správě měst pro inteligentní dopravní systémy, v energetice pro efektivní správu zdrojů a zejména v domácnostech, kde IoT zařízení pomáhají zvyšovat pohodlí a efektivitu (viz Obrázek 1).

Obsah obrázku text, snímek obrazovky, diagram, Písmo

Popis byl vytvořen automaticky

Obrázek 1 – Aplikace IoT zařízení

# Cíle a omezení

# Analýza rizik

# 

# ZÁVĚR

Je nutné věnovat stejnou, ne-li větší pozornost jako úvodu. V závěru musíte podat shrnutí, vyzvednout nejdůležitější postřehy a také vyhodnotit, zdali jste naplnili cíle, které jste si stanovili v úvodu své práce.

# SEZNAM POUŽITÉ LITERATURY

**ELEKTRONICKÉ ZDROJE**

1. Ali, Zainab & Ali, Hesham & Badawy, Mahmoud. (2015). Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions. International Journal of Computer Applications. 128. 975-8887
2. <https://www.deviceauthority.com/blog/unpacking-iot-architecture-layers-and-components-explained/>
3. Yaqoob, Ibrar & Ahmed, Ejaz & Hashem, Ibrahim & Ahmed, Abdelmuttlib Ibrahim Abdalla & Gani, Abdullah & Imran, Muhammad & Guizani, Mohsen. (2017). Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. IEEE Wireless Communications. 24. 10.1109/MWC.2017.1600421.
4. Detienne, M. (2022). *Master thesis : MQTT broker with in-line, real-time data visualiser for the Internet of Things (IoT).*(Unpublished master's thesis). Université de Liège, Liège, Belgique. Retrieved from <https://matheo.uliege.be/handle/2268.2/14496>
5. <https://www.analyticssteps.com/blogs/9-applications-iot-home-automation>
6. IDC's U.S.IoT Decision Maker Survey, July 2021
7. Taherdoost, H. Security and Internet of Things: Benefits, Challenges, and Future Perspectives. Electronics **2023**, 12, 1901. <https://doi.org/10.3390/electronics12081901>
8. DDoS
9. <https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security>
10. <https://www.splunk.com/en_us/blog/learn/cryptography.html>
11. Noor, Shab E & Ahmad, Ali. (2022). Learning the basics of cryptography with practical examples. Revista Electrónica de Investigación y Docencia (REID). 10.30827/Digibug.74740.
12. Kryptologie, šifrování a tajná písma přehled Pavel Vondruška
13. Al-Vahed, Ahmed and Haddad Sahhavi. “An overview of modern cryptography.” (2011).
14. <https://sandbox.cz/~varvara/El_podpis/index.html>
15. <https://research.ijcaonline.org/icaet2016/number2/icaet036.pdf>
16. Aumasson, Jean-Philippe. (2017). The impact of quantum computing on cryptography. Computer Fraud & Security. 2017. 8-11. 10.1016/S1361-3723(17)30051-9.
17. <https://is.muni.cz/www/ostadal/hash_overview.pdf>
18. Thakor, V.A., Razzaque, M.A., and Khandaker, M.R.A.Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison andresearch opportunities. IEEE Access. 2021; 9: 28177-28193.
19. <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8454.pdf>
20. <https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices>
21. (PDF) Lightweight Cryptography for Internet of Things: A Review. Available from: https://www.researchgate.net/publication/379349394\_Lightweight\_Cryptography\_for\_Internet\_of\_Things\_A\_Review [accessed May 27 2024].

* Pozn. ČSN ISO 690 Informace a dokumentace – Pravidla pro bibliografické odkazy a citace informačních zdrojů

|  |  |
| --- | --- |
|  |  |
|  |  |

# SEZNAM PŘÍLOH

|  |  |  |  |
| --- | --- | --- | --- |
| Příloha č. 1 | − | Popis přílohy (→ styl Odstavec) |  |
| Příloha č. 2 | − | Popis přílohy (→ styl Odstavec) |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

(→ Styl Příloha – číslování) Příloha 1

Popis přílohy (→ styl Příloha – popis)

|  |
| --- |
|  |