Universitatea Tehnică a Moldovei

ANALIZA VULNERABILITĂȚILOR ȘI EFICIENȚA MECANISMELOR DE SECURITATE ÎN CADRUL LORAWAN

Student:
BRUMARIUC Maxim

Conducător:
conf.univ.,dr. NAZAROI Ion

Chişinău – 2019

Ministerul Educaţiei, Culturii Şi Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Electronică şi Telecomunicaţii

Programul de masterat "Sisteme și Comunicații Electronice"

Admis la susţinere

Şef departament, conf.univ.dr.

_____ P.NICOLAEV

____ _____ 2019

Analiza vulnerabilităților și eficiența mecanismelor de securitate în cadrul LoRaWAN

Teză de master

Student: _____ (**BRUMARIUC M.**)

Conducător: _____ (conf.univ.,dr. **NAZAROI I.**)

Chişinău – 2019

A D N O T A R E

În cadrul curentei teze au fost analizate vulnerabilitățile și mecanismele de securitate în cadrul LoRaWAN.

Capitolul întâi prezintă informații referitoare la studiul comparativ al tehnologiilor utilizate în IoT, stiva de protocol LoRaWAN, metode de securizare și tipuri de atacuri.

În capitolul doi are loc crearea unui workbench pentru realizarea testelor de verificare a vulnerabilităților, realizarea atacutilor Jamming, Eavesdropping, Flooding, Reply Attack, Bit-Fliping și în final analiza rezultatelor de răspuns la atac.

Teza de master contine 60 pagini, 42 ilustrații, 4 tabele și sunt citate 27 surse bibliografice.

A N N O T A T I O N

Within the current thesis, the vulnerabilities and security mechanisms within LoRaWAN were analyzed.

The first chapter presents information on the comparative study of technologies used in IoT, LoRaWAN protocol stack, security methods and types of attacks.

In chapter two, a workbench is created to perform vulnerability testing, Jamming, Eavesdropping, Flooding, Reply Attack, Bit-Fliping and finally analyzing the response results to the attack.

The master's thesis contains 60 pages, 42 illustrations, 4 tables and 27 bibliographic sources are cited.

CUPRINS

INTRODUCERE

În prezent ne aflăm la trecerea spre o nouă epocă – epoca IoT (Internet of Things). IoT este utilizat pe scară larga în conectarea dispozitivelor și colectarea informațiilor. Una din tehnologiile care în ultimii ani se impune pe piață este LoRaWAN.

De ce anume LoRa? Fiindcă LoRa poate fi ușor implementată cu o infrastructură minimă și un cost redus, funcționează în diapazonul frecvențelor nelicențiate (ceea ce înseamnă că nu costă nimic, sau costă foarte puțin), permite de a transmite date pe o distanță destul de mare cu un consum de putere în regimul de emisie mic. Și nu în ultimul rând trebuie de menționat că LoRa suportă criptarea datelor AES 128 biți, are o rată de date adaptabilă și o scalabilitate perfectă. Deci LoRa reprezintă compromisul dintre preț, calitate și acesibilitate.

În acestă teză vor fi analizate vulnerabilitățile și concomitent mecanismele de securitate în cadrul rețelei LoRaWAN.

Obiectivele impuse în cadrul tezei curente sunt:

• Studiul și analiza stivei de protocoale din cadrul LoRaWAN;

• Studiul și analiza particularităților de securitate pentru fiecare nivel din stivă;

• Crearea unui workbench pentru realizarea testelor de verificare a vulnerabilităților;

• Realizarea atacurilor de tip jamming și selective jamming, prin generarea semnalelor pe aceeași frecvență ca și a dispozitivului LoRa din rețeaua LoraWAN;

• Realizarea atacurilor de tip eavesdropping (man-in-the-midle), prin interceptarea semnalelor de la un dispozitiv LoRa din rețeaua LoRaWAN;

• Realizarea atacurilor de tip flooding, prin saturarea gateway-ului din cadrul LoRaWAN cu pachete pentru blocarea comunicării;

• Realizarea atacurilor de tip bit-flipping;

• Analiza răspunsurilor la atac;

BIBLIOGRAFIE

1. https://machinaresearch.com/news/agricultural-iot-will-see-a-very-rapid-growth-over-the-next-10-years/
2. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5579920/
3. http://www.ieee802.org/15/pub/TG4.html
4. http://www.ieee802.org/15/pub/TG1.html
5. http://www.ieee802.org/11/
6. http://www.ieee802.org/15/pub/TG4g.html
7. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5579920/
8. https://www.digikey.be/nl/articles/techzone/2016/nov/lorawan-part-1-15-km-wireless-10-year-battery-life-iot
9. https://stackoverflow.com/questions/55461604/how-to-set-a-specific-lora-spread-factor-in-mbed-os
10. https://smartmakers.io/en/security-in-lorawan-applications/
11. https://sirinsoftware.com/blog/lorawan-mac-layer/
12. http://www.techplayon.com/lora-device-activation-call-flow-join-procedure-using-otaa-and-abp/
13. https://www.researchgate.net/publication/329858421_Security_Risk_Analysis_of_LoRaWAN_and_Future_Directions
14. https://www.researchgate.net/publication/303253115_Software_Defined_Radio_Basic_Principles_and_Applications
15. https://www.ettus.com/all-products/ub210-kit/
16. https://wiki.gnuradio.org/index.php/InstallingGR
17. https://arxiv.org/pdf/1712.02141.pdf
18. https://www.researchgate.net/publication/307965130_A_Study_of_LoRa_Long_Range_Low_Power_Networks_for_the_Internet_of_Things
19. https://docplayer.fr/71046243-C-esar-computer-electronics-security-applications-rendez-vous-internet-des-objets-vous-avez-dit-securite.html
20. https://www.researchgate.net/publication/332402515_Protecting_Gateway_from_ABP_Replay_Attack_on_LoRaWAN
21. https://www.researchgate.net/publication/316176437_Risk_analysis_and_countermeasure_for_bit-flipping_attack_in_LoRaWAN

22. Handbook of Research on Wireless Security, author: Yan Zhang, Jun Zheng, Miao Ma, Information Science Reference (March 14, 2008)
23. Precision: Principles, Practices and Solutions for the Internet of Things, author: Timothy Chou, Lulu.com (October 20, 2016)
24. Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IoT attacks, author: Alexey Kleymenov, Amr Thabet, Packt Publishing (June 6, 2019)
25. Interoperability, Safety and Security in IoT, editor: Nathalie Mitton, Hakima Chaouchi, Thomas Noel, Thomas Watteyne, Alban Gabillon, Patrick Capolsini, Springer; 1st ed. 2017 edition (February 13, 2017)
26. Security and Privacy in Wireless and Mobile Networks, author: Georgios Kambourakis, Felix Gomez Marmol, Guojun Wang, Mdpi AG (April 13, 2018)
27. Future Network Systems and Security, editor: Robin Doss, Selwyn Piramuthu, Wei ZHOU, Springer; 2015 edition (May 22, 2015)