MINISTERUL EDUCAŢIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Electronica și Telecomunicații
Departamentul Telecomunicații și Sisteme Electronice

Admis la susţinere
Şefă departament TSE:
Tîrșu Valentina, conf. univ., dr.

20 ianiarie 2025

Analiza securității rețelelor fără fir și protecția lor împotriva atacurilor cibernetice de tip man-in-the-middle

Teză de master

Student: **Gorceag Vasile,**
gr. SISRC-231M

Conducător: **Șestacova Tatiana,**
conf., univ., dr.

Chișinău, 2025

REZUMAT

Autorul: Gorceag Vasile, SISRC-231M

Titlul tezei de master: " Analiza securității rețelelor fără fir și protecția lor împotriva atacurilor cibernetice de tip man-in-the-middle"

Structura lucrării: constă din pagini de titlu, aviz, rezumat, introducere, 3 capitole, concluzii, bibliografie.

Cuvinte cheie: rețele wireless, securitate, atacuri Man-in-the-Middle (MITM), vulnerabilități, criptare, protecție.

Problematica studiului: Analiza vulnerabilităților rețelelor wireless și evaluarea măsurilor de protecție împotriva atacurilor de tip Man-in-the-Middle (MITM).

Scopul lucrării: Evaluarea securității rețelelor wireless prin identificarea vulnerabilităților critice și a metodelor de atac, cu accent pe atacurile MITM, și propunerea unor soluții pentru îmbunătățirea protecției acestora.

Obiectivele:

1. Caracteristica generala a securității rețelelor fără fir
2. Analiza detaliată a atacurilor cibernetice de tip Man-In-The-Middle
3. Examinarea măsurilor de protecție împotriva atacurilor MITM
4. Analiza rețelelor de acces false si rețelelor Wi-Fi publice nesecurizate
5. Studierea educației utilizatorilor și a rolului acesteia in prevenirea atacurilor
6. Elaborarea măsurilor pentru îmbunătățirea securității rețelelor fără fir

Metode aplicate: Studiul utilizează analiza comparativă a vulnerabilităților rețelelor wireless și a mecanismelor de protecție disponibile. A fost realizată o cercetare detaliată a atacurilor MITM, incluzând metode și instrumente utilizate. Studiul experimental a inclus simularea unui atac MITM și testarea unor algoritmi de criptare avansată, evaluând eficiența acestora în scenarii practice. Datele rezultate au fost analizate pentru a determina impactul măsurilor de protecție asupra securității și experienței utilizatorilor.

Rezultatele obținute: În urma acestei lucrări s-a elaborat un model de evaluare a vulnerabilităților rețelelor wireless, cu accent pe atacurile de tip Man-in-the-Middle (MITM). De asemenea, s-a propus un set de soluții practice pentru îmbunătățirea securității acestora, inclusiv algoritmi de criptare avansată, politici de acces și recomandări pentru educarea utilizatorilor și prevenirea riscurilor în diverse medii informatice.

SUMMARY

Author: Gorceag Vasile, SISRC-231M

Master's Thesis Title: "Analysis of Wireless Network Security and Protection Against Cyber Attacks of the Man-in-the-Middle Type" Security analysis of wireless networks and their protection against" protecția lor man-in-the-middle" cyberattacks

Structure of the Thesis: Consists of the title pages, approval, summary, introduction, three chapters, conclusions, and bibliography.

Keywords: wireless networks, security, Man-in-the-Middle (MITM) attacks, vulnerabilities, encryption, protection.

Research problem: Analysis of wireless network vulnerabilities and evaluation of protection measures against Man-in-the-Middle (MITM) attacks.

Thesis purpose: Evaluate the security of wireless networks by identifying critical vulnerabilities and attack methods, focusing on MITM attacks, and proposing solutions to improve their protection.

Objectives:

1. General feature of wireless network security
2. Detailed analysis of Man-In-The-Middle cyber attacks
3. Examining of MITM attack protection measures
4. Analysis of fake access networks and unsecured public Wi-Fi networks
5. Studying user education and its role in preventing attacks
6. Development of measures to improve the security of wireless networks

Applied Methods:

The study employs a comparative analysis of wireless network vulnerabilities and available protection mechanisms. A detailed investigation of MITM attacks, including methods and tools used, was conducted. The experimental study simulated a MITM attack and tested advanced encryption algorithms, evaluating their efficiency in practical scenarios. The resulting data were analyzed to determine the impact of protection measures on security and user experience.

Results Obtained:

The study developed a model for evaluating wireless network vulnerabilities, with a focus on Man-in-the-Middle (MITM) attacks. A set of practical solutions was proposed to enhance network security, including advanced encryption algorithms, access policies, and recommendations for user education and risk prevention in various computing environments.

CUPRINS

INTODUCERE

În era digitală, rețelele wireless au devenit o componentă esențială a infrastructurii de comunicație, facilitînd accesul rapid la informație și interconectarea dispozitivelor. Aceste rețele sunt utilizate în diverse domenii, de la rețelele domestice la aplicații industriale și instituționale, oferind un nivel de flexibilitate și mobilitate greu de realizat prin intermediul conexiunilor cablate. Cu toate acestea, proliferarea rețelelor wireless a adus cu sine o serie de provocări în materie de securitate, vulnerabilitățile acestora fiind exploatate de atacatori pentru a compromite confidențialitatea și integritatea datelor transmise.

Atacurile de tip man-in-the-middle (MitM) reprezintă o metodă frecvent utilizată de infractorii cibernetici pentru a intercepta și modifica comunicațiile între două părți fără ca acestea să fie conștiente de intervenția neautorizată. Aceste atacuri pot avea consecințe devastatoare, inclusiv furtul de informații sensibile, accesul neautorizat la conturi sau servicii online, și chiar compromiterea întregii infrastructuri de rețea.

Scopul tezei de master constă în analiza securității rețelelor fără fir și metodelor de protecție împotriva atacurilor MITM.

Pentru a atinge acest scop, este necesar să se rezolve următoarele ***obiective***:

1. Caracteristica generala a securității rețelelor fără fir
2. Analiza detaliată a atacurilor cibernetice de tip Man-In-The-Middle
3. Examinarea măsurilor de protecție împotriva atacurilor MITM
4. Analiza rețelelor de acces false si rețelelor Wi-Fi publice nesecurizate
5. Studierea educației utilizatorilor și a rolului acesteia in prevenirea atacurilor
6. Elaborarea măsurilor pentru îmbunătățirea securității rețelelor fără fir

Sunt analizate mecanismele care permit atacatorilor să intercepteze și să modifice datele transmise între dispozitive, precum și metodele eficiente de prevenire a acestor atacuri.

Avînd în vedere utilizarea pe scară largă a rețelelor wireless (Wi-Fi, Bluetooth etc.) pe dispozitivele personale și corporative, securitatea acestor rețele devine o sarcină critică. Atacurile MITM reprezintă o amenințare gravă, deoarece atacatorul poate interveni neobservat în comunicații, ceea ce duce la furtul de date, modificarea traficului sau accesul la informații confidențiale. În ciuda dezvoltării tehnologiilor de criptare, atacurile MITM rămîn unul dintre cele mai periculoase tipuri de atacuri asupra rețelelor wireless.

Lucrarea va analiza diferite protocoale de comunicație wireless, vulnerabilitățile acestora și mecanismele de protecție. O atenție deosebită va fi acordată atacurilor de tip MITM: tipurilor acestora, metodelor de implementare, consecințelor și metodelor de protecție. O parte importantă a analizei va fi dedicată revizuirii metodelor moderne de detectare și prevenire a acestor atacuri, precum și recomandărilor pentru îmbunătățirea securității rețelelor.

BIBLIOGRAFIE

1. Stallings, W. (2017). *Network Security Essentials: Applications and Standards*. Pearson. Bază solidă în securitatea rețelelor și informații detaliate despre atacuri MITM și soluții de protecție.

2. Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks*. Pearson. Înțelegere cuprinzătoare a rețelelor de calculatoare și a principiilor de securitate, inclusiv protecția împotriva atacurilor MITM.

3. Peca, L., Țurcanu, D. Network security: Practical examples solved to be introduced in network security. Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Department Software Engineering and Automatics. – Chișinău: Tehnica-UTM, 2023. – 243 p. ISBN 978-9975-45-941-9. http://repository.utm.md/handle/5014/22819

4. Peca, L., Țurcanu, D. Computer networks: Practical examples solved to be introduced in computer networks. Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Department Software Engineering and Automatics. – Chișinău: Tehnica-UTM, 2022. – 188 p. ISBN 978-9975-45-812-2. http://repository.utm.md/handle/5014/20549

5. Bennett, J. A. (2014). *Wireless Security: Models, Threats, and Countermeasures*. Springer. Vulnerabilitățile rețelelor wireless și măsurile de securitate, incluzând protecția împotriva atacurilor MITM.

6. Mahmoud, M. M., & Hawari, M. A. (2020). *Mitigation of Man-in-the-Middle Attacks in Wireless Networks: A Survey*. *IEEE Access*, 8, 132299-132313. Revizuire a tehnicilor de protecție împotriva atacurilor MITM în rețelele wireless.

7. Chavan, S. P., & Joshi, D. R. (2018). *Security Issues and Attacks in Wireless Networks*. *International Journal of Computer Applications*, 180(2), 11-18. Articol despre diferitele atacuri de securitate în rețelele wireless și soluțiile de protecție.

8. Yu, H., & Wen, J. (2017). *Prevention and Detection of Man-in-the-Middle Attacks in Secure Wireless Communications*. *Journal of Wireless Communications and Networking*, 2017(1), 1-15. Metodele de prevenire și detecție a atacurilor MITM în comunicațiile wireless.

9. OWASP (Open Web Application Security Project) – *OWASP Wireless Security*. https://owasp.org. Ghiduri și recomandări pentru securizarea rețelelor wireless și protecția împotriva atacurilor MITM.

10. RFC 5246 – *The Transport Layer Security (TLS) Protocol Version 1.2*. https://tools.ietf.org/html/rfc5246. Descrierea protocolului TLS, utilizat pentru protecția comunicațiilor împotriva atacurilor MITM prin criptare.

11. Wi-Fi Alliance – *Wi-Fi Security Whitepaper*. https://www.wi-fi.org. Informații detaliate despre standardele de securitate Wi-Fi și protecția rețelelor wireless.

12. IEEE 802.11 – *Wi-Fi Security Standards*. Standardele pentru securitatea rețelelor Wi-Fi, incluzând WPA3.

13. RFC 2818 – *HTTP Over TLS*. https://tools.ietf.org/html/rfc2818. Utilizarea TLS pentru protejarea comunicațiilor HTTP și prevenirea atacurilor MITM.

14. ISO/IEC 27001 – *Information Security Management Systems*. Măsuri pentru protecția rețelelor împotriva atacurilor MITM.

15. RFC 7616 – *HTTP/2 Security Considerations*. https://tools.ietf.org/html/rfc7616. Securitate în implementarea HTTP/2 și protecția împotriva atacurilor MITM.

16. Gautam, V., & Meena, S. (2020). *Mitigation of Man-in-the-Middle Attacks Using Secure Socket Layer (SSL) in Wireless Communication*. *Journal of Network and Computer Applications*, 157, 102577. Implementarea protocolului SSL pentru protecția împotriva atacurilor MITM în comunicațiile wireless.

17. Zhao, K., & Li, Y. (2017). *A Survey on Man-in-the-Middle Attacks in Wireless Networks: Techniques, Challenges, and Solutions*. *Wireless Communications and Mobile Computing*, 2017, 1-18. Tehnicile și soluțiile pentru protecția împotriva atacurilor MITM în rețelele wireless.

18. Tîrșu V., Sava L. Integrating elasticsearch and kibana in ict management *processes for economic efficiency in multimedia content administration.* In: The scientific heritage. Economic Sciences., Vol.1 № 142 (142), 2024, p.15-20 . Budapest, Hungary. ISSN 9215 — 0365, Cosmos Impact Factor - 3.336 SJIF Impact Factor - 5.78 DOI: , Categoria B+. Disponibil: http://www.scientific-heritage.com/ru/arhiv/

19. Tîrșu V., Cerbu O. *Interactive visualization of geographical data using proxmox and modern technologies.* In: The scientific heritage. Economic Sciences., Vol.1 № 142 (142), 2024, p.21-26. Budapest, Hungary. ISSN 9215 — 0365, Cosmos Impact Factor - 3.336 SJIF Impact Factor - 5.78 DOI: , Categoria B+. Disponibil: http://www.scientific-heritage.com/ru/arhiv/

20. Sava L., Tîrșu V., Plămădeală C. *Performance evaluation of microtik routers according to electromagnetic compatibility testing standards.* În: Electrotehnica, Electronica, Automatica, vol.72/4, p.57-61. Romania, Sibiu: ISSN: 2392-828X, categoria B+. Disponibil: https://eea-journal.ro/articles-and-issues/current-issues/

21. Tîrșu, V., Cristea E. Baze de date : Ghid metodic pentru lucrările de laborator. Chișinău: Ed. "Tehnica-UTM", 2024, 112 pag. ISBN 978-9975-64-392-4. Disponibil: https://library.utm.md/items/?biblionumber=2628876

22. Tîrșu, V. Programare : Ghid metodic pentru lucrări de laborator. Chișinău: Ed. "Tehnica-UTM", 2022, pag.130, ISBN 978-9975-45-861-0. Disponibil: https://library.utm.md/items/?biblionumber=2619626

23. Sava, L., Vortolomei, D. Organizarea şi analiza activităţii economice în domeniul telecomunicaţiilor. Note de curs, Chişinău, Editura UTM, 2022, ISBN: 978-9975-45-805-4.

24. Sava, L., Țurcanu, T., Răuleț, D. Statistica în domeniu. Note de curs. Universitatea Tehnică a Moldovei, Facultatea Electronică și Telecomunicații, Departamentul Telecomunicații și Sisteme Electronice, Chişinău: Tehnica-UTM, 2024. ISBN 978-9975-64-394-8. – 124 p. https://utm.md/wp-content/uploads/2024/02/statistica-in-domeniu.pdf