MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Electronică şi Telecomunicaţii

Departamentul Telecomunicații și Sisteme Electronice

Admis la susţinere

Şefă departament TSE:

V. Tîrșu dr., conf.univ.

„___” _____ 2025

Metode de autentificare și control al accesului în rețelele de comunicații

Student: **Crețu Călin, SISRC-231M**

Conducător: **Dinu Țurcanu. dr.conf.univ**

Chișinău 2025

REZUMAT

La teza de master

Tema : „Metode de autentificare și control al accesului în rețelele de comunicații”

Actualitatea și importanța temei - este extrem de importantă, având în vedere creșterea continuă a numărului de dispozitive conectate la internet, a volumului de date schimbate și a amenințărilor cibernetice tot mai complexe. Într-un context global digitalizat, tema „Metode de autentificare și control al accesului în rețelele de comunicații” rămâne esențială pentru a asigura securitatea informațiilor și continuitatea operațiunilor. Implementarea unor soluții moderne și proactive nu este doar o necesitate tehnologică, ci și o obligație socială și economică.

Cuvinte cheie: Autentificare,control acces, protocol,securitate,dispozitive ACS.

Scopul tezei – este identificarea, analiza și propunerea unor soluții eficiente pentru metodele de autentificare și control al accesului în rețelele de comunicații, având ca obiectiv principal asigurarea unui nivel ridicat de securitate, confidențialitate și protecție împotriva accesului neautorizat.

Obiective specifice sunt**:**

Analiza generală a metodelor actuale de autentificare și control al accesului:

Studiul provocărilor actuale în securitatea rețelelor:

Evaluarea tehnologiilor emergente:

Proiectarea și testarea unor soluții inovatoare:

Elaborarea unui set de bune practici pentru implementare:

Evaluarea impactului soluțiilor propuse:

Scopul și obiectivele tezei sunt orientate către dezvoltarea unui cadru teoretic și practic care să contribuie la îmbunătățirea securității rețelelor de comunicații, având în vedere tendințele actuale și provocările viitoare în domeniul cibernetic.

Semnificația și valoarea aplicativă constă în :

Analizarea metodelor de autentificare și control al accesului pentru evidențierea punctelor forte și slabe datorită cărora este posibil îmbunătățirea securității de control acces la datele stocate in interprinderi mari cît și în cele mici pentu evitarea pătrunderilor nedorite și scurgerea de informație răufăcătorilor.

SUMMARY

Master thesis

Theme :„Authentication and access control methods in communication networks”

The topicality and importance of the topic - is extremely important, given the ever-increasing number of devices connected to the internet, the volume of data exchanged and the increasingly complex cyber threats. In a digitized global context, the topic of "Authentication and access control methods in communication networks" remains essential to ensure information security and business continuity. Implementing modern and proactive solutions is not only a technological necessity, but also a social and economic obligation.

Keywords: Authentication, access control, protocol, security,ACS devices.

The aim of the thesis - is to identify, analyze and propose effective solutions for authentication and access control methods in communication networks, with the main objective of ensuring a high level of security, confidentiality and protection against unauthorized access.

Specific objectives are:

General analysis of current authentication and access control methods:

Study of current challenges in network security:

Evaluation of emerging technologies:

Design and test innovative solutions:

Developing a set of best practices for deployment:

Impact assessment of the proposed solutions:

The aims and objectives of the thesis are oriented towards the development of a theoretical and practical framework to contribute to the improvement of the security of communication networks, taking into account current trends and future challenges in the cyber domain.

The significance and application value consists of :

Analyzing authentication and access control methods in order to highlight the strengths and weaknesses due to which it is possible to improve the security of access control to data stored in large and small enterprises to avoid unwanted intrusions and leakage of information to the wrongdoers.

CUPRINS

INTRODUCERE

În era digitală actuală, unde informația circulă rapid și eficient, securitatea rețelelor de comunicații a devenit o preocupare majoră pentru organizații de toate dimensiunile și din toate domeniile. Creșterea volumului de date gestionate, împreună cu diversificarea metodelor de acces, a generat o expunere semnificativă la amenințări cibernetice. Astfel, asigurarea unui control eficient al accesului și implementarea unor metode solide de autentificare au devenit esențiale pentru protejarea resurselor informaționale.

Autentificarea reprezintă procesul prin care se verifică identitatea utilizatorilor sau a sistemelor care solicită acces la resurse. Aceasta poate include metode tradiționale, cum ar fi parolele, dar și soluții mai avansate, cum ar fi autentificarea biometrică sau autentificarea multifactorială (MFA). Pe de altă parte, controlul accesului se referă la setarea unor politici și reguli care determină cine poate accesa ce resurse, în ce condiții și pentru ce scopuri. Modelele de control al accesului, cum ar fi DAC (Discretionary Access Control), MAC (Mandatory Access Control) și RBAC (Role-Based Access Control), sunt utilizate pentru a gestiona permisiunile și a preveni accesul neautorizat.

Importanța acestor metode nu poate fi subestimată. Un sistem de autentificare robust și un control al accesului bine implementat pot preveni breșele de securitate care ar putea conduce la pierderi financiare semnificative, daune reputaționale și compromiterea informațiilor sensibile, precum datele personale identificabile (PII) și proprietatea intelectuală. De asemenea, aceste măsuri sunt esențiale pentru conformitatea cu reglementările legale și standardele de securitate, care impun protejarea datelor utilizatorilor.

Pe măsură ce tehnologiile avansează, noi provocări și oportunități apar în domeniul autentificării și controlului accesului. De exemplu, trecerea de la soluțiile tradiționale de autentificare unică (Single Sign-On) la gestionarea unificată a accesului reflectă o tendință de integrare a securității în diverse medii IT, inclusiv în cloud. Aceste evoluții oferă organizațiilor soluții mai flexibile și scalabile, dar vin și cu propriile riscuri și complexități.

Obiectivele tezei:

1. **Analiza generală a metodelor actuale de autentificare și control al accesului:**
    - Clasificarea tehnologiilor existente (autentificare prin parolă, autentificare biometrică, autentificare cu doi factori etc.).
    - Evaluarea avantajelor și limitărilor acestor metode în diverse contexte.
2. **Studiul provocărilor actuale în securitatea rețelelor:**
    - Identificarea amenințărilor și vulnerabilităților care afectează metodele de autentificare și control al accesului.

- Analiza impactului atacurilor cibernetice asupra rețelelor și a datelor sensibile.

3. **Evaluarea tehnologiilor emergente:**
   - Explorarea potențialului unor tehnologii precum blockchain, inteligența artificială, și autentificarea fără parolă (passwordless authentication).
   - Analiza eficienței lor în reducerea riscurilor și îmbunătățirea performanței sistemelor de securitate.
4. **Proiectarea și testarea unor soluții inovatoare:**
   - Propunerea unui model de autentificare hibrid sau a unui algoritm de control al accesului adaptabil.
   - Realizarea unui prototip sau simularea funcționării soluției propuse în diverse scenarii.
5. **Elaborarea unui set de bune practici pentru implementare:**
   - Crearea unui ghid care să includă recomandări pentru implementarea metodelor de autentificare și control al accesului în organizații de diferite dimensiuni.
   - Identificarea aspectelor legate de costuri, scalabilitate și conformitate cu reglementările.
6. **Evaluarea impactului soluțiilor propuse:**
   - Compararea performanței soluției propuse cu metodele tradiționale.
   - Analiza beneficiilor aduse din punct de vedere al securității și al eficienței operaționale.

Această lucrare își propune să exploreze în profunzime metodele de autentificare și controlul accesului în rețelele de comunicații. Vor fi analizate diferitele tehnici disponibile, avantajele și dezavantajele fiecărei metode, precum și impactul lor asupra securității organizației. Printr-o înțelegere detaliată a acestor concepte și a provocărilor asociate, organizațiile pot dezvolta strategii eficiente de securitate, esențiale pentru a face față amenințărilor cibernetice în continuă evoluție și pentru a asigura protecția datelor sensibile într-un peisaj digital dinamic.

BIBLIOGRFIE:

1. https://www.geeksforgeeks.org/authentication-in-computer-network/[Authentication in Computer Network, Last Updated : 16 Jun, 2022]
2. 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. – Chişinău: Tehnica-UTM, 2023. – 243 p. ISBN 978-9975-45-941-9. http://repository.utm.md/handle/5014/22819
3. https://frontegg.com/blog/authentication [Complete Guide to Authentication in 2024, August 19, 2024]
4. https://www.techtarget.com/searchsecurity/definition/access-control [What is access control?, Gavin Wright,Ben Lutkevich, Site Editor]
5. 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. – Chişinău: Tehnica-UTM, 2022. – 188 p. ISBN 978-9975-45-8122. http://repository.utm.md/handle/5014/20549
6. https://www.spy-shop.ro/blog/metode-autentificare-pentru-control-acces?srsltid=AfmBOorLyN7MPbInBimCylh_yXY3U2i496wubuMI3wdTtK7XVcWasHai [Ghid - metode de autentificare pentru control acces, 06.08.2019]
7. https://moodle.kstu.ru/mod/page/view.php?id=10126 [7 Лекция. Аутентификация. Криптографические методы аутентификации. 25 августа 2016, 09:17]
8. https://blog.synology.com/romania/dedicate-vs-bazate-pe-browser-de-parole-care-este-cel-mai-potrivit-pentru-pentru-dumneavoastra [Dedicate vs. bazate pe browser de parole: Care este cel mai potrivit pentru pentru dumneavoastră?,Synology Team 23 June 2023]
9. Carolina Timco, Larisa Bugaian, Dinu Țurcanu. Governance of the Technical University of Moldova in the digital era. Journal of Social Sciences, Vol. II, no. 2 (2019), pp. 19 - 27.
10. https://www.spiceworks.com/it-security/identity-access-management/articles/what-is-biometric-authentication-definition-benefits-tools/
11. https://www.delta.ru/blog/chto-takoe-skud/#:~:text=СКУД%20–%20аббревиатура%2C%20которая%20расшифровывается%20как,с%20помощью%20специализированного%20программного%20оборудования. [Что такое СКУД? 09.09.2022 Компания «DELTA системы безопасности»]
12. https://tatprofing.com/uslugi/montazh-i-obsluzhivanie-skud/proektirovanie-skud/

13. Dinu Ţurcanu, Rodica Siminiuc, Tatiana Ţurcanu. Role of the University Management System in the digitalization of Technical University of Moldova. The 12th International Conference on Electronics, Communications and Computing. 20-21 October, 2022, Chisinau, Republic of Moldova. IC ECCO-2022. pp. 268 – 275.
14. http://accesscontrolconsult.in/Controllers/solus-sacs-sw-s.html
15. https://zkteco.com.hk/download/Biometric%20Authorization%20Product%20and%20Solution%20Brochures.pdf
16. https://scanport.ru/blog/
17. https://russian.fullsmarthomesystem.com/sale-10733642-pin-code-and-rfid-card-access-control-reader-metal-cover-with-ip68-waterproof-and-anti-vandal-featur.html
18. https://bigdataschool.ru/blog/biometrics-cybersecurity-big-data.html
19. https://www.deeterelectronics.com/reed-switch-how-it-works/
20. https://www.energometrika.ru
21. https://www.bezopasnost.ru/service/367/proektirovanie-sistemy-kontrolya-i-upravleniya-dostupom/
22. https://www.simplilearn.com/what-is-kerberos-article [What Is Kerberos? How Does Kerberos Work: Everything You Need to Know. Last updated on Jul 2, 2024]
23. https://www.keepersecurity.com/ru_RU/resources/glossary/what-is-kerberos/[Что такое Kerberos?. © Keeper Security, Inc., 2025]
24. https://www.fortinet.com/resources/cyberglossary/radius-protocol#:~:text=What%20Is%20RADIUS%3F,how%20something%20communicates%20or%20operates. [RADIUS (Remote Authentication Dial-In User Service) Protocol. Copyright © 2025 Fortinet, Inc. All Rights Reserved.]
25. https://www.geeksforgeeks.org/tacacs-protocol/[TACACS+ Protocol, Last Updated : 05 Nov, 2021]
26. https://habr.com/ru/companies/vk/articles/115163/[OAuth 2.0 простым и понятным языком. Сайт team.vk.company,9 августа 2008, *Дмитрий Битман*
27. 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/
28. 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

29. 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.