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

Admis la susţinere
Şefă departament:
Tîrșu Valentina, conf. univ., dr
_____
„____”_____ 2024

ANALIZA COMPARATIVĂ A PROTOCOALELOR DE SECURITATE ÎN DISPOZITIVELE MOBILE

Teză de master

Student : **Arnaut Afanasie**
gr. SISRC-221M

Conducător : **Cerbu Olga**
conf.univ., dr.

Chișinău, 2024

ADNOTARE

Autorul: Arnaut Afanasie gr. SISRC-221M

Tema: Analiza comparativă a protocoalelor de securitate în dispozitivele mobile.

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

Cuvinte cheie: securitate mobilă, criptografie, securitate informațională, protocoale criptografice, protocol de comunicare.

Problematica studiului: Analiza comparativă a protocoalelor de securitate în dispozitivele mobile și elaborarea aplicației pentru metoda de criptare și hash-area criptografică utilizată în aceste protocoale .

Scopul lucrării: Este de a analiza protocoalele de securitate în dispozitivele mobile. Studierea generală a fiecărui protocol de securitate precum protocolul de autentificare a utilizatorului, protocolul de semnătură digitală, protocolul de stabilire a cheilor criptografice, protocolul de angajament, protocolul de autentificare a mesajelor, protocolul cu arbitru, protocolul aplicativ, protocolul de poștă electronică, protocolul de vot electronic și a altor protocoale de securitate. Implementarea sistemului de criptare și hash-are criptografică.

Obiectivele:

1. Studierea conceptului de protocol criptografic.
2. Analiza tipurilor de protocoale criptografice.
3. Efectuarea analizei protocoalelor de securitate în dispozitivele mobile.
4. Studierea schemei MAC și HMAC.
5. Implementarea sistemului de criptare și hash-are criptografică într-un limbaj de programare.

Metode aplicate: S-a utilizat metode de analiză a protocoalelor de comunicații, cercetare a unui vast fișier bibliografic și programare a aplicației cu metode de criptare simetrică și metode de hash-are criptografică.

Rezultatele obținute: A fost elaborată o aplicație în limbajul python pentru criptare și decriptare, cît și crearea unui hash prin metoda de hash-are criptografică cu algoritmul Whirlpool. S-a ajuns la concluzia că utilizarea acestui sistem de criptare în protocoalele de securitate pentru dispozitivele mobile este mai efectivă deoarece cu același sistem se efectuează și criptarea și hasharea criptografica.

ANNOTATION

Author: Arnaut Afanasie gr. SISRC-221M

Topic: Comparative analysis of security protocols in mobile devices.

Work structure: The work it consists of title pages, opinion, summary, introduction, 3 chapters, conclusions, bibliography and appendices.

Keywords: mobile security, cryptography, informational security, cryptographic protocols, communication protocol.

Research problem: Comparative analysis of the security protocols in mobile devices and the development of the application for the encryption method and the cryptographic hashing used in these protocols.

Purpose of the work: It is to analyze the security protocols in mobile devices. General study of each security protocol such as User Authentication Protocol, Digital Signature Protocol, Cryptographic Key Establishment Protocol, Commitment Protocol, Message Authentication Protocol, Arbiter Protocol, Application Protocol, Electronic Mail Protocol, electronic voting and other security protocols. Implementation of cryptographic encryption and hashing system.

Objectives:

1. Studying the concept of cryptographic protocol.
2. Analysis of the types of cryptographic protocols.
3. Conduct analysis of security protocols in mobile devices.
4. Study of MAC and HMAC scheme.
5. Implementation of the cryptographic encryption and hashing system in a programming language.

Methods applied: Communication protocol analysis methods, research of a vast bibliographic file and application programming with symmetric encryption methods and cryptographic hashing methods were used.

Results obtained: An application was developed in the python language for encryption and decryption, as well as the creation of a hash using the cryptographic hash method with the Whirlpool algorithm. It was concluded that the use of this encryption system in the security protocols for mobile devices is more effective because with the same system encryption and cryptographic hashing are performed.

CUPRINS

INTODUCERE

În prezent, comunicarea este necesară atît pentru sarcinile militare, cît și pentru cele civile. Organizațiile și întreprinderile avansate se caracterizează printr-o cantitate considerabilă de informații vaste, care penetrează zilnic rețelele în principal cele de telecomunicații.

Actualitatea temei

Securitatea rețelelor este acum o parte vitală a domeniului dispozitivelor mobile. Aceasta implică utilizarea de protocoale, tehnologii, sisteme, instrumente și tehnici pentru a asigura securitatea și a preveni atacurile rău-intenționate. În ultimii ani, atacurile cibernetice au avut o creștere semnificativă, cauzînd daune de peste 1 trilion de dolari anual conform rapoartelor Europol.

În ceea ce privește analiza comparativă a protocoalelor de securitate în dispozitivele mobile, există mai multe protocoale importante care sunt folosite pentru a asigura confidențialitatea și integritatea datelor în aceste dispozitive.

Protocoalele criptografice gestionează modul în care are loc procesul de criptare și decriptare. Ele stabilesc regulile pentru modul în care datele sunt transformate într-un cod secret și invers.

Iată cîteva protocoale de securitate comune în dispozitivele mobile:

1. Transport Layer (TLS): Acest protocol este utilizat pentru a asigura securitatea comunicațiilor pe internet. TLS oferă criptare și autentificare pentru a proteja datele transmise între dispozitiv și server.

2. Secure Sockets Layer (SSL): SSL este un protocol similar cu TLS și este utilizat pentru asigurarea securității comunicațiilor pe internet. Totuși, SSL este considerat învechit și înlocuit treptat de către TLS.

3. Virtual Private Network (VPN): VPN este o tehnologie care permite utilizatorilor să creeze o conexiune securizată între dispozitivul lor mobil și o rețea privată. Această oferă o criptare puternică și protecție împotriva atacurilor cibernetice.

4. Wi-Fi Protected Access (WPA): WPA este un protocol de securitate utilizat pentru a proteja rețelele Wi-Fi. Există mai multe versiuni ale acestui protocol, cum ar fi WPA2 și WPA3, care oferă niveluri diferite de securitate.

5. Secure Shell (SSH): SSH este un protocol de rețea utilizată pentru a permite administrarea securizată a dispozitivelor mobile și a altor sisteme. Acesta oferă autentificare și criptare pentru a proteja accesul la dispozitiv.

Acestea sunt doar cîteva exemple de protocoale de securitate în dispozitivele mobile. Este important să menționăm nivelul de securitate poate varia în funcția de implementare specifică a fiecărui dispozitiv și a configurației utilizate.

Recomandăm întotdeauna actualizarea dispozitivelor mobile cu cele mai recente actualizări de securitate și utilizarea unor parole puternice pentru a asigura o protecție adecvată a datelor.

Scopul lucrării constă în analiza comparativă a protocoalelor de securitate în dispozitivele mobile.

Studierea generală a fiecărui protocol de securitate precum protocolul de autentificare a utilizatorului, protocolul de semnătură digitală, protocolul de stabilire a cheilor criptografice, protocolul de angajament, protocolul de autentificare a mesajelor, protocolul cu arbitru, protocolul aplicativ, protocolul de poștă electronică, protocolul de vot electronic și a altor protocoale de securitate. Implementarea sistemului de criptare și hash-are criptografică.

Obiectivele:

1. Studierea conceptului de protocol criptografic.
2. Analiza tipurilor de protocoale criptografice.
3. Efectuarea analizei protocoalelor de securitate în dispozitivele mobile.
4. Studierea schemei MAC și HMAC.
5. Implementarea sistemului de criptare și hash-are criptografică într-un limbaj de programare.

BIBLIOGRAFIA

1. Wikipedia: Securitatea rețelelor de calculatoare [citat 04.12.2023]. Disponibil: https://ro.wikipedia.org/wiki/Securitatea_re%C8%9Belelor_de_calculatoare .
2. Wikipedia: TSL [citat 05.12.2023]. Disponibil: https://en.wikipedia.org/wiki/Transport_Layer_Security#SSL_1.0,_2.0,_and_3.0 .,
3. Wikipedia: Secure Sockets Layer (SSL) [citat 05.12.2023]. Disponibil: https://ro.wikipedia.org/wiki/Transport_Layer_Security .
4. Wikipedia: VPN [citat 05.12.2023]. Disponibil: https://ro.wikipedia.org/wiki/Re%C8%9Bea_privat%C4%83_virtual%C4%83 .
5. Wikipedia: Wi-Fi protected access (wpa) [citat 04.12.2023]. Disponibil: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access .
6. Wikipedia: Secure Shell [citat 04.12.2023]. Disponibil: https://en.wikipedia.org/wiki/Secure_Shell .
7. ȚURCANU, Dinu; SPINU, NATALIA; POPOVICI, Serghei; ȚURCANU, Tatiana. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. Journal of Social Sciences, Vol. IV, no. 1 (2021), pp. 74 – 83.
8. CAPCELEA, Titu; CAPCELEA Maria. Protocoale Criptografice. Partea I ; Universitatea de Stat din Moldova. Facultatea de Matematică și Informatică. Departamentul de Informatică. – Chișinău: CEP USM, 2020. – 198p. Bibliogr. p. 170-172 (63 tit.) – 50 ex. ISBN 978-9975-71-494-5.
9. CAPCELEA, Titu; CAPCELEA Maria. Protocoale Criptografice. Partea a II-a ; Universitatea de Stat din Moldova. Facultatea de Matematică și Informatică. Departamentul de Informatică. – Chișinău: CEP USM, 2020. – 139p. Bibliogr. p. 135-137 (54 tit.) – 50 ex. ISBN 978-9975-71-494-5.
10. Ludmila Peca, Dinu Țurcanu. Network security: Practical examples solved to be introduced in network security. Chișinău, Publisher „Tehnica-UTM”, 2023, pp. 7-232.
11. Ludmila Peca, Dinu Ţurcanu. Computer networks: Practical examples solved to be introduced in computer networks. ISBN 978-9975-45-812-2. Chișinău, Publisher „Tehnica-UTM”, 2022.
12. А. Черемушкин, Криптографические протоколы. Основные свойства и уязвимости, Москва: Академия, 2009.
13. A. Atanasiu, Securitatea informației. Protocoale de securitate, vol. 2, Cluj: Editura INFODATA, 2009.
14. С. Запечников, Криптографические протоколы и их применение в финансовой и коммерческой деятельности, Москва: Горячая линия - Телеком, 2007.
15. Federal Information Processing Standards Publication 198-1, "The Keyed-Hash Message Authentication Code (HMAC)," National Institute of Standards and Technology, 2008.
16. T. Krovetz, "UMAC: Message Authentication Code using Universal Hashing," Network Working Group. Request for Comments: 4418, 2006.
17. T. Krovetz and W. Dai, "VMAC: Message Authentication Code using Universal Hashing," CFRG Working Group, April 2007.
18. "The Transport Layer Security (TLS) Protocol Version 1.2," 2008.

19. N. Doraswamy and D. Harkins, IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 2006.
20. L. Carter and M. Wegman, "Universal hash functions," Journal of Computer and System Sciences, vol. 18, pp. 143-154, 1979.
21. W. Stallings, Cryptography and Network Security: Principles and Practice, 6th ed., Boston: Pearson, 2014.
22. National Institute of Standards and Technology (NIST), "FIPS Publication 180-4: Secure Hash Standard," March 2012.
23. Wikipedia: Whirlpool (хеш-функция) [citat 04.01.2024]. Disponibil: https://ru.wikipedia.org/wiki/Whirlpool_(%D1%85%D0%B5%D1%88-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F) .
24. Wikipedia: Whirlpool (funcție hash) [citat 04.01.2024]. Disponibil: https://en.wikipedia.org/wiki/Whirlpool_(hash_function) .
25. Wikipedia: Python [citat 04.01.2024]. Disponibil: https://ro.wikipedia.org/wiki/Python .
26. *Kyoji, Shibutani; Shirai, Taizo.* On the diffusion matrix employed in the Whirlpool hashing function (англ.) : journal. — 2003. — 11 March.
27. *Florian Mendel, Christian Rechberger, Martin Schläffer, Søren S. Thomsen.* The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl (англ.) (24 февраля 2009). — презентация нового способа криптоанализа и его применения для криптоанализа хеш-функций Whirlpool и Grøstl.
28. Li, W., Gao, Z., Gu, D., Ge, C., Liao, L., Zhou, Z., Liu, Y., & Liu, Z. (2017). Security Analysis of the Whirlpool Hash Function in the Cloud of Things. KSII Transactions on Internet and Information Systems, 11(1), 536–551. https://doi.org/10.3837/tiis.2017.01.028.
29. С.В.Дубров. Основы современной криптографии. — Новосибирск, 2012. — С. 65—67. — 260 с.
30. John Kelsey and Bruce Schneier. Second preimages on n-bit hash functions for much less than 2n work. — 2005. — С. 474–490.