MINISTERUL EDUCAŢIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microelectronică
Departamentul Microelectronică și Inginerie Biomedicală

Admis la susținere
Șef interimar departament MIB:
conf.univ., dr. Serghei RAILEAN

_____
„ ____ ” _____ 2022

Dezvoltarea unei aplicații VPN utilizând tehnologia OpenVPN

Teză de master

Student: **Onofraș Dionisie, MN-201M**
Conducător: **Railean Serghei, conf. univ, dr.**

Chișinău, 2022

REZUMAT

La teza de master a studentului Onofraș Dionisia

Tema „Dezvoltarea unei aplicații VPN utilizând tehnologia OpenVPN.”

Lucrarea cuprinde: 4 capitole, 32 figuri, 11 tabele, 20 surse bibliografice și 4 anexe.

Cuvinte-cheie: Aplicație; OpenVPN; Rețea privată virtuală; iOS; Cripatre.

Scopul lucrării constă în dezvoltarea unei aplicații mobile VPN, cu utilizarea tehnologiei OpenVPN în limbajul Swift, aplicația este destinată pentru utilizatorii de telefoane pe platforma iOS și scopul ei este de a proteja datele personale a utilizatorului.

Obiectivele generale – analiza bibliografică în domeniu aplicațiilor VPN, proiectarea și dezvoltarea aplicației, simularea datelor și testarea aplicației, testarea securității datelor utilizatorului pentru diferite servere.

Domeniul de cercetare îl constituie aspectele teoretice și practice de dezvoltare a aplicațiilor VPN securizate, tipurile de cripatare a datelor transmise prin internet. Tunelarea datelor pentru securizarea rețelelor publice.

Originalitate științifică, în aplicație sunt prezente o gamă largă de servere disponibile cu diferite tipuri de criptare a datelor. Utilizarea tehnologiei OpenVPN care permite combinarea a mai mult tipuri de criptare într-o singură aplicație cu gestionare automată.

Teza cuprinde în sine introducere, trei capitole, concluzii, bibliografie și 4 anexe.

Capitolul 1 descrie aspecte teoretice despre aplicațiile VPN, tipurile de protocoale folosite în aceste aplicații, cele cai populare tehnologii VPN și metode de criptare.

Capitolul 2 descrie tehnologiile folosite la dezvoltarea aplicației, colectarea serverelor, crearea configurărilor vpn, efectuarea conexiunii și tunelarea datelor.

Capitolul 3 conține testele și rezultatele obținute, analiza securității aplicației, eficiența funcționării și gradul de protejare a acesteia plus sunt afișate și rezultatele implementării interfeței utilizatorului.

În concluzie se remarcă că scopul principal al proiectului s-a atins, sunt prezentate punctele forte ale aplicației în comparație cu produsele deja existente. Sunt prezentate punctele ce pot fi îmbunătățite în viitor.

În anexe sunt reprezentate clasele de bază legate de funcționalitățile cheie ale aplicației.

ANNOTATION

On the master's thesis of the student Onofraș Dionisie.

Theme "Developing a VPN application using OpenVPN technology"

The thesis includes: 4 chapters, 32 figures, 11 tables, 20 bibliographic sources and 4 annexes.

Keywords: Application; OpenVPN; Virtual private network; iOS; Encryption.

The purpose of the work is to develop a mobile VPN application, using OpenVPN technology in Swift language, the application is intended for users of phones on the iOS platform and its purpose is to protect the user's personal data.

General requirements – bibliographic analysis in the field of VPN applications, application and development of the application, simulation of data and security of the data, test of the user's application.

The research field is the theoretical and practical aspects of the development of secure VPN applications, the types of encryption of data transmitted over the Internet. Tunneling data to secure public networks.

Scientific originality, the application includes a wide range of servers available with different types of data encryption. Use OpenVPN technology that allows you to combine multiple types of encryption into one self-managed application.

Thesis contains introduction, three chapters, conclusions, a bibliography list and 4 annex.

Chapter one contains theoretical aspects of VPN applications, the types of protocols used in these applications, the popular ways VPN technologies and encryption methods.

The second chapter describes the technologies used to develop the application, connect to servers, create vpn configurations, connect and tunnel data.

The third chapter contains the tests and results obtained, the analysis of the security of the application, the efficiency of its operation and its degree of protection plus are displayed and the results of the implementation of the user interface.

In conclusion it is noted that the main purpose of the project has been achieved, the strengths of the application are presented compared to existing products. the points that can be improved in the future are presented.

In annexes the basic classes related to the key functionalities of the application are represented.

CURPINS

INTRODUCERE

Lumea de astăzi a devenit din ce în ce mai conectată în ultimul deceniu. Odată cu introducerea telefoanelor inteligente, aproape toată lumea are la îndemână un dispozitiv conectat la internet de cele mai multe ori. Noile paradigme, cum ar fi Internetul lucrurilor (IoT) și tehnologii precum standardul 5G pentru comunicațiile celulare mobile nu vor face decât să crească numărul de dispozitive conectate. Introducerea cloud computing-ului a adus provocări suplimentare. Rețelele existente la nivel local trebuie extinse și conectate la rețelele virtuale cloud. Pentru o integrare perfectă, toate cloud-urile majore oferă gateway-uri IPsec pentru a crea VPN-uri de la site la site.

În special, aceste cazuri de utilizare de la site la site impun cerințe uriașe în ceea ce privește debitul unei soluții VPN. Cercetările noastre inițiale din Secțiunea 3 sugerează că implementările VPN open-source nu sunt suficient de rapide pentru a gestiona legăturile multi-gigabit la viteza de linie pe hardware-ul COTS. Administratorii de rețea se bazează în schimb pe soluții hardware dedicate VPN, care sunt adesea costisitoare și nu pot fi auditate din punct de vedere al securității.

Rețelele private virtuale (VPN) sunt o tehnologie care facilitează comunicarea securizată printr-o rețea nesigură (cum ar fi internetul). Soluțiile VPN pot fi clasificate în mai multe tipuri, fiecare având propria abordare a securității, avantaje și dezavantaje și dependență de diferite combinații de protocoale și standarde. Cele trei tipuri majore sunt soluțiile VPN bazate pe IPSec, PPTP și TLS. Având în vedere complexitatea soluțiilor VPN și faptul că există diverse implementări diferite de aceste tipuri, nu este de neconceput ca unele dintre aceste implementări să aibă vulnerabilități de securitate nedescoperite. Această lucrare se va concentra pe testarea uneia dintre aceste implementări, VPN-ul bazat pe TLS numit OpenVPN.

Metoda de testare folosită va fi fuzzing. Aceasta înseamnă că vom trimite mesaje de protocol confuze către un server OpenVPN pentru a vedea cum răspunde. Prin monitorizarea comportamentului serverului și a traficului de rețea dintre client și server și plasând aceste informații lângă mesajele neclare care au cauzat acest comportament, este posibil să găsim defecte în implementarea OpenVPN. De asemenea vot testa aplicația la scurgeri de date DNS și vor verifica pachetele transmise la conținutul de date vulnerabile cum ar fi parole, poze, etc.

Organizarea acestei lucrări va fi după cum urmează. Capitolul 1 va oferi o privire de ansamblu asupra tehnologiilor care se folosesc pentru aplicații VPN, tipurile de criptare a datelor. Capitolul 2 va descrie detaliat tehnologiile, instrumentele, librăriile utilizate la dezvoltarea aplicației. Toți pașii parcurși de la stabilirea cerințelor tehnice până la obținerea aplicației finale. Capitolul 3 va prezenta rezultatele testelor efectuate, care neajunsuri au fost identificate, metodele utilizate pentru testarea aplicației. Și, în sfârșit, concluzia, unde pe scurt este redat rezumatul lucrării, care sunt beneficiile față de alte aplicații și cum poate fi îmbunătățită aceasta.

BIBLIOGRAFIE

1. SHEILA, Frankel; KAREN, Kent; LEWKOWSKI Ryan; OREBAUGH Angela D.; RITCHEY Ronald W. and SHARMA Steven R. *Guide to IPsec VPNs*. NIST Special Publication, 800-77, 2005. 126 p.
2. VACCA, John R. Virtual private network security. In: *Complete Book of Remote Access: Connectivity and Security*, Auerbach Publications, 2002, pagini 251–267.
3. TANENBAUM Andrew S. și WETHERALL David J.. *Computer Networks. Pearson*, 5th edition, 2011. 920 p.
4. HAMZEH Kory; PALL Grueep; VERTHEIN William; TAARUD Jeff, LITTLE W. and ZORN Glen. *Point-to-point tunneling protocol (PPTP).* RFC 2637, 1999. 57 p.
5. HUYGHE Stijn. OpenVPN 101: introduction to OpenVPN. 2017 [citat 17.09.2021]. Disponibil: https://openvpn.net/papers/openvpn-101.pdf.
6. FRANKEL Sheila; HOFFMAN Paul; OREBAUGH Angela și PARK Richard. *Guide to SSL VPNs*. NIST Special Publication, 800-113, 2008. 87 p.
7. OpenVPN Security Overview. 2018 [citat 17.09.2021]. Disponibil: https://openvpn.net/index.php/ open-source/documentation/security-overview.html
8. OpenVPN Manual. 2018 [citat 13.09.2021]. Disponibil: https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage.
9. SCHNEIER Bruce; David WAGNER și Mudge. *Cryptanalysis of Mi- crosoft's PPTP Authentication Extensions (MS-CHAPv2)*. In Secure Networking—CQRE [Secure]'99, Springer, 1999. pagini 192–203.
10. Ebo van der Laan. **OpenVPN-NL protocol specification,** 2017. 28 p.
11. OpenVPN network protocol overview documentation file. 2018 [citat 17.09.2021]. Disponibil: https://github.com/OpenVPN/openvpn/blob/master/doc/doxygen/doc_protocol_overview.h.
12. The OpenVPN post-audit bug bonanza. 2017 [citat 17.09.2021]. Disponibil: https: //guidovranken.wordpress.com/2017/06/21/ the-openvpn-post-audit-bug-bonanza/.
13. Pedram Amini and Aaron Portnoy. Sulley: Fuzzing frame- work. 2017. [citat 17.09.2021]. Disponibil: http://www.fuzzing.org/wp-content/SulleyManual.pdf.

14. JOERI DE RUITER. *Lessons learned in the analysis of the EMV and TLS security protocols.* PhD thesis, Radboud University Nijmegen, 2015. 129 p.

15. DIERKS Tim si RESCORLA Eric. *The transport layer security (TLS) protocol.* Technical report, RFC 5246, 2008. 101 p.

16. DURUMERIC Zakir; KASTEN James; ADRIAN David; HALDERMAN Alex J.; BAILEY Michael; LI Frank; WEAVER Nicolas; AMANN Johanna; BEEKMAN Jethro si PAYER Mathias. *The matter of heartbleed. In Pro- ceedings of the 2014 Conference on Internet Measurement Conference*, pagini 475–488. ACM, 2014.

17. HOEKSTRA Berry; MUSULIN Damir su KEIJSER Jan Just. *Comparing TCP performance of tunneled and non-tunneled traffic using Open- VPN*. Master's thesis, Universiteit Van Amsterdam, System & Network Engineering, 2011. 56 p.

18. MEYER Christopher si SCHWENK J¨org. *Lessons learned from previous ssl/tls attacks-a brief chronology of attacks and weaknesses*. IACR Cryptology EPrint Archive, 2013:49, 2013. 15 p.

19. M¨OLLER Bodo; DUONG Thai si KOTOWICZ Krzysztof. This POODLE bites: exploiting the SSL 3.0 fallback. 2014 [citat 17.09.2021]. Disponibil: https://www.openssl.org/~bodo/ssl-pood le.pdf.

20. The best architecture for the iOS app. 2020 [citat 18.10.2021] Disponibil: https://medium.com/flawless-app-stories/the-best-architecture-for-ios-app-does-it-even-exist-3af357ac62e7