MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microelectronică
Departamentul Inginerie Software și Automatică

Admis la susținere, Șef departament: conf. univ., dr. Fiodorov Ion

_____
„_____”_____ 20__

Tehnici de ofuscare pentru securitatea software-ului

Teză de master

Student: **Dolghieru Rodica, gr. SI-201M**

Coordonator: **Catanoi Maxim, asist. univ.**

Chișinău, 2022

ADNOTARE

Teza prezintă un studiu al tehnicilor de ofuscare în scopul asigurării unui nivel suplimentar de protecție și securitate a aplicațiilor software. Tehnicile de ofuscarea codului sursă reprezintă o practică promițătoare pentru securizarea software-ului. Acestea reprezintă o modalitate eficientă de a proteja software-ul împotriva intruziunilor și pentru a întări apărarea prin ofuscarea codului.

Scopul cercetării este prezentarea unui studiu al tehnicilor de ofuscare a software-lui în vederea asigurării unui nivel corespunzător al securității și care poate fi aplicat de către dezvoltatori pentru a facilita securitatea software-lui împotriva atacurilor de inginerie inversă, de manipulare și de acces neautorizat la codul sursă al aplicațiilor software.

Teza include patru capitole care prezintă considerațiile teoretice privind domeniul de cercetare al tehnicilor de ofuscare, analiza tehnicilor de ofuscare în conformitate cu taxonomia prezentată și structura stratificată a aplicațiilor software, de asemenea sunt descrise atacurilor cibernetice la care sunt supuse aplicațiile software fără aplicarea nivelului suplimentar de securitate a tehnicilor de ofuscare și prezentarea instrumentelor automatizate pentru efectuarea acestui proces.

ANNOTATION

The thesis presents a study of blurring techniques in order to ensure an additional level of protection and security of software applications. Source code obfuscation techniques in the field of promising software security. These effectively use intrusion-protected software and to prevent defenses by obfuscating the code.

The aim of the research is to present a study of software obfuscation techniques to ensure a high level of security and which can be applied by developers to facilitate the security of soft ware against reverse engineering attacks, manipulation and unauthorized access to software application source code.

The thesis includes four chapters that present theoretical considerations on the field of obfuscation research, analysis of obfuscation techniques according to the taxonomy presented and the stratified structure of software applications, also describes the cyber-attacks to which software applications are subjected without applying the additional level of security. blurring techniques and the presentation of automated tools for performing this process.

CUPRINS

INTRODUCERE

Actualitatea temei. Schimbul de informații a devenit o componentă esențială în era tehnologiilor informaționale. Zilnic utilizăm serviciul de e-mail, sistemele peer-to-peer, rețelele sociale și alte aplicații web pentru a facilitat schimbul de informații între noi. Avem încredere pe aplicațiile software incorporate în dispozitivele electronice pe care le utilizăm și ne sunt indispensabile. Evident, toate aceste aplicații software se bazează pe funcționarea corectă a software-ului și hardware-ului utilizat.

În anii 1980, securitatea aplicațiilor se realiza pe principiul hardware-ului securizat, exemplu sunt terminalele ATM sau set-top box-urile (STB). Cu toate aceste, în anii 1990 protecția software-lui a câștigat mai mult interes datorită flexibilității și costului său redus. În zilele, suntem înconjurați, practic, de aplicații software care ne facilitează viața, exemplu sunt site-urile comerciale cu plăți online, rețelele sociale, jocurile video, etc. Ca urmare au apărut amenințări precum pirateria, manipulări în cod, ingineria inversă, care sunt o adevărată problemă, de o importanță semnificativă. Din motiv, precum că majoritatea licențelor pentru unele aplicații software este foarte costisitoare, dar și din alte motive, o bună parte din utilizatori recurg la utilizarea ilegală a aplicațiilor software, descărcând de pe internet versiuni piratate și utilizându-le. De asemenea, în ultimul deceniu, a devenit foarte răspândită distribuirea în internet a unui număr impunător de aplicații software. Odată distribuit pe internet, un client (aplicație) proprietarul software-lui pierde controlul asupra acestuia, în plus majoritatea aplicațiilor și platformelor devin mobile, utilizându-se fără fir, prin intermediul rețelelor wireless. Acestea necesită un nivel adecvat de securitate, în primul rând, deoarece software-ul poate conține informații sensibile, confidențiale, exemplu fiind informații despre numerele de carduri. Pentru protecția acestora există algoritmi de criptare și autentificare, însă aceștia necesită ca și cheile secrete să fie protejate. În continuare trebuie protejat, de asemenea, codul aplicației, cea mai mare amenințare fiind ingineria inversă, analiza dinamică și manipulările în cod.

Scopul cercetării este prezentarea unui studiu al tehnicilor de ofuscare a software-lui în vederea asigurării unui nivel corespunzător al securității și care poate fi aplicat de către dezvoltatori pentru a facilita securitatea software-lui împotriva atacurilor de inginerie inversă, de manipulare și de acces neautorizat la codul sursă al aplicațiilor software.

BIBLIOGRAFIE

1. Collberg, C, Thomborson C, Low D (1997) A taxonomy of obfuscating transformations, Technical report. The University of Auckland Octavian COZNIUC [citat 24.09.2021]. Disponibil: https://www.dsi.unive.it/~avp/collberg97taxonomy.pdf
2. Barak, B, Goldreich O, Impagliazzo R, Rudich S, Sahai A, Vadhan S, Yang K (2001) On the (im) possibility of obfuscating programs In: Annual International Cryptology Conference [citat 25.09.2021]. Disponibil: https://link.springer.com/chapter/10.1007%2F3-540-44647-8_1
3. Chan, J-T, Yang W (2004) Advanced obfuscation techniques for java bytecode. J Syst Softw [citat 01.10. 2021]. Disponibil: https://www.sciencedirect.com/science/article/abs/pii/S0164121202000663?via%3Dihub
4. Vulnerabilities and threats in mobile banking Tehnologii Pozitive, Copyright 2002-2021 [citat 07.11.2021]. Disponibil: https://www.ptsecurity.com/ww-en/analytics/vulnerabilities-mobile-banks-2020/
5. Code Obfuscation: A Comprehensive Guide Against Reverse-Engineering Attempts, INKA Entworks Inc., Copyright 2002-2021 [citat 07.11.2021]. Disponibil: https://www.appsealing.com/code-obfuscation-comprehensive-guide/
6. Dalla Preda, M, Maggi F (2017) Testing android malware detectors against code obfuscation: a systematization of knowledge and unified methodology. J Comput Virol Hacking Tech [citat 01.10.2021]. Disponibil: https://link.springer.com/article/10.1007/s11416-016-0282-2
7. Collberg, C, Thomborson C, Low D (1998) Manufacturing cheap, resilient, and stealthy opaque constructs In: POPL [citat 14.10.2021]. Disponibil: https://dl.acm.org/doi/10.1145/268946.268962
8. Crane, SJ, Volckaert S, Schuster F, Liebchen C, Larsen P, Davi L, Sadeghi A-R, Holz T, De Sutter B, Franz M (2015) It's a TRaP: table randomization and protection against function-reuse attacks In: CCS [citat 04.10.2021]. Disponibil: https://dl.acm.org/doi/10.1145/2810103.2813682
9. Vmhunt: A verifiable approach to partially virtualized binary code simplification In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security [citat 30.10.2021]. Disponibil: https://dl.acm.org/doi/10.1145/3243734.3243827
10. Linn, C, Debray S (2003) Obfuscation of executable code to improve resistance to static disassembly In: CCS [citat 30.10.2021]. Disponibil: https://dl.acm.org/doi/10.1145/948109.948149
11. You, I, Yim K (2010) Malware obfuscation techniques: a brief survey In: International Conference on Broadband, Wireless Computing, Communication and Applications [citat 30.10.2021]. Disponibil: https://ieeexplore.ieee.org/document/5633410
12. Crane, SJ, Volckaert S, Schuster F, Liebchen C, Larsen P, Davi L, Sadeghi A-R, Holz T, De Sutter B, Franz M (2015) It's a TRaP: table randomization and protection against function-reuse attacks In: CCS [citat 30.10.2021]. Disponibil: https://dl.acm.org/doi/10.1145/2810103.2813682

13. Kovacheva, A (2013) Efficient code obfuscation for android In: International Conference on Advances in Information Technology.. Springer [citat 31.10.2021]. Disponibil: https://link.springer.com/chapter/10.1007%2F978-3-319-03783-7_10
14. White-Box Cryptography and an AES Implementation [citat 31.10.2021]. Disponibil: https://link.springer.com/chapter/10.1007%2F3-540-36492-7_17
15. M9: Reverse Engineering, OWASP Foundation, Inc., Copyright 2021, [citat 07.11.2021]. Disponibil: https://owasp.org/www-project-mobile-top-10/2016-risks/m9-reverse-engineering
16. Web Parameter Tampering, OWASP Foundation, Inc., Copyright 2021, [citat 07.11.2021]. Disponibil: https://owasp.org/www-community/attacks/Web_Parameter_Tampering#