THE MINISTRY OF EDUCATION AND RESEARCH OF THE REPUBLIC OF MOLDOVA

THE TECHNICAL UNIVERSITY OF MOLDOVA. FACULTY OF COMPUTERS, COMPUTER SCIENCE AND MICROELECTRONICS. DEPARTMENT OF SOFTWARE ENGINEERING AND AUTOMATION

Admitted by Head of the Department:

_____

/Family name, Given name, scientific-didactic title / "

_____"_____ 2021

CYBER DEFENSE AND ARTIFICIAL INTELLIGENCE

MASTER'S THESIS

Student: Masiutin Maxim

Thesis director: Catanoi Maxim

Chisinau 2022

ABSTRACT (ENG)

(rezumat/adnotare)

CYBER DEFENSE AND ARTIFICIAL INTELLIGENCE

Author: Masiutin Maxim

The problem of the study is the application of artificial intelligence to automatically detect and deal with cyberattacks. The study's objectives are to analyze the current trends in applying artificial intelligence for cyber defense, provide examples of using artificial intelligence in cyber defense, and develop a tool to detect and mitigate cyber-attacks. The final objective is the tool that would predict and detect network compromises by using machine learning. The hypothesis is that by using a transparent proxy server before a real application server, the proxy can analyze traffic, detect malicious requests and break the connection, thus protecting the real server. The author used observation and experiments to obtain the results. The thesis also describes the most significant attacks on incorrect RSA implementations that have occurred in practice and the software code on Python programming language to reproduce the attacks, such as the Coppersmith attack, the Boneh & Durfee attack, and Howgrave-Graham, and the ROCA attacks, all of them aim to decrypt a message and Bleichenbacher's signature forgery. The current thesis also provides real examples of avoiding these attacks by using RSA correctly to ensure secure data transmission and digital signatures. As a result, in the final section of the thesis, the author came up with two computer programs. The first program implements MonteCarlo simulation to get a good move for a computer player in a Hex Board Game, thus demonstrating an implementation of an artificial intelligence algorithm. The Monte-Carlo simulation is implemented very efficiently, so it takes just about a second to make a move from a million trials on an average notebook on a 7x7 field or about 5 seconds on an 11x11 field. The second program is a proxy stub to check incoming TCP connections in real-time and break malicious connections. It is the cyber-defense server-side (reverse) proxy server application which is presented by the author.

Keywords: cyberdefence, artificial intelligence, Monte-Carlo simulation, RSA, Python.

ABSTRACT (ROM)

(rezumat/adnotare)

APĂRARE CIBERNETICĂ ȘI INTELIGENȚĂ ARTIFICIALĂ

Autor: Masiutin Maxim

Problema studiului este aplicarea inteligenței artificiale (AI) pentru a detecta și a proteja împotriva atacurilor cibernetice în mod automat. Scopul este utilizarea AI pentru detectarea și gestionarea automată a atacurilor cibernetice. Obiectivele studiului sunt de a analiza tendințele actuale în aplicarea AI pentru apărarea cibernetică, de a oferi exemple de utilizare a AI în apărarea cibernetică și de a dezvolta un instrument pentru detectarea și atenuarea atacurilor cibernetice. Obiectivul final este instrumentul care ar prezice și detecta compromisurile rețelei prin utilizarea învățării automate. Ipoteza este că prin utilizarea unui server proxy transparent înaintea unui server de aplicații real, proxy-ul poate analiza traficul, detecta cererile rău intenționate și întrerupe conexiunea, protejând astfel serverul real. Autorul a folosit observația și experimentele pentru a obține rezultatele. De asemenea, în prezenta teza sunt descrise cele mai semnificative atacuri asupra implementărilor incorecte a criptosistemului RSA care au avut loc în practică și codul software pe limbajul de programare Python pentru a reproduce atacurile, cum ar fi atacul Coppersmith, atacul Boneh & Durfee și Howgrave-Graham și ROCA. Toate atacuri demonstrate au scopul de a decripta un mesaj și falsificarea semnăturii lui Bleichenbacher. Teza oferă, de asemenea, exemple reale de evitare a acestor atacuri prin utilizarea corectă a RSA pentru a asigura transmisia sigură a datelor și semnăturile digitale. Drept urmare, în secțiunea finală a tezei, autorul a venit cu două programe de calculator. Primul program implementează simularea Monte-Carlo pentru a obține o mișcare bună pentru un jucător de calculator într-un joc de masă Hex, demonstrând astfel o implementare a unui algoritm de AI. Simularea MonteCarlo este implementată foarte eficient, așa că durează aproximativ o secundă pentru a trece de la un milion de încercări pe un notebook mediu pe un câmp 7x7 sau aproximativ 5 secunde pe un câmp 11x11. Al doilea program este un proxy stub pentru a verifica conexiunile TCP de intrare în timp real și pentru a întrerupe conexiunile rău intenționate. Este aplicația server proxy de apărare cibernetică (reverse proxy) care este prezentată de autor.

Cuvintele-cheie: cyberdefence, artificial intelligence, Monte-Carlo simulation, RSA, Python.

Table of Contents

1. Analysis of the current trends

1.1. Introduction

Cyber defense and artificial intelligence is new, emerging study. Cyber attacks lead to unauthorized access to systems connected to Internet networks anywhere in the world. As a result, cyber attacks ultimately lead to controlling these systems. With the introduction of artificial intelligence technology, these attacks continue to increase exponentially, and artificial intelligence technology has been effectively applied in the fields of health care, computer science and mechanical engineering. However, artificial intelligence can be used as a defense measure as well. With the application of artificial intelligence in the network field, traditional network attacks have begun to appear in the form of intelligent network attacks. Software development using standard, traditional algorithms is not sufficient to defend against attacks. In the present master's thesis, the literature research on artificial intelligence methods in the field of network security is studied, reviewed, and the knowledge applied. For topics discussed from different perspectives, solutions for defense and attack, applications used, backgrounds between different disciplines, analysis, and country-based examples will be introduced.

Artificial Intelligence (AI) aims to mimic real human intelligence. Intelligence, in its turn, is based on imagination. The phenomenon of imagination contributed to the creation of humankind. What also contributed to the creation of humankind is the development of one's sense of invention combined with the impulses of competition, ambition, creativity, and curiosity. As a matter of fact, before somebody even knows how to do it, it is only imagined. Artificial intelligence, which was first the subject of movies and now causes one of the biggest transformations in the world, is one of them. This transformation, which begins with a dream, will be presented to the service of humanity it brings with it a relentless service. AI deals with complex problems by enabling machines to find solutions like humans. The system, people's decision to simulate the mechanism, modeling is made with some algorithms.

A sub-stage of AI is machine learning. Machine learning is the name given to methods that make inferences from existing data using mathematical and statistic methods and make predictions about the unknown with these inferences. In a sub-stage

of machine learning, there is a deep learning technique. This technique is based on learning data functions with an artificial neural network approach. In summary, Figure 1 shows the relationship between artificial intelligence, machine learning, and deep learning. Today, artificial intelligence techniques are actively used in many fields, from automation to machine translation, from medical images to sound synthesis. One of the areas where the most active research areas actually take place is artificial intelligence in cybersecurity.

REFERENCES

1. M. Kuzlu, C. Fair, O. Guler. "The Role of the Artificial Intelligence in the Internet of Things (loT) Cybersecurity", Discover Internet of Things, vol. 1, no. 1,7, pp. 1-14, 2021.
2. Y. Senkaya, U. G. Adar, "Review of Artificial Intelligence Systems in Cyber Defense," Academic Informatics, Mersin, February 2014.
3. E. Şeker, "Use of Artificial Intelligence Techniques/Applications in Cyber Defense," International Journal of Information Security Engineering, vol. 6, No. 2, pp. 108-115.
4. Ş. N. Reşitoglu, "Artificial Intelligence Effect in Cybersecurity," TUIC Academy, March 26, 2021.
5. B. Aytan and N. Peacemaker, "Artificial Intelligence Based Attack Detection and Analysis in Cyber Defense," in Proceeding of the 2nd International Symposium on Innovative Approaches in Scientific Studies, Samsun, December 2018.
6. N. R. Moshteanu, K. Galea, "Artificial Intelligence and Cyber Security - Face to Face with Cyber Attack - A Maltese Case of Risk Management Approach," Ecoforum, vol. 9, no. 2, pp. 1-8, 2020.
7. K. Bresniker, A. Gavrilovska, J. Holt, D. Milcjicic and T. Tran, "Grand Challenge: Applying Artificial Intelligence and Machine Learning to Cybersecurity," Computer, vol. 52, no.12, pp. 45-52, 2019.
8. P. Patil. "The Artificial Intelligence In the Cyber Security" International Journal of Research in Computer Applications and Robotics, vol. 4, no. 5, pp. 1-5, 2016.
9. Sheyabni, Javidi, "Seminars in Proactive Artificial Intelligence for Cybersecurity (SPAIC): Consulting and Research," Systemics, Cybernetics and Informatics, vol. 17, no. 1, pp. 297-305, 2019.
10. R. V. Yampolskiy, M. S. Spellchecker, "Artificial Intelligence Safety and Cybersecurity: A Timeline of AI Failures", 2016.
11. A. P. Veiga, "Applications of Artificial Intelligence (AI) to Network Security," ITEC 625- Information Systems Infrastructure, March 2018.
12. S. Zeadally, E. Adi, Z. Baig, I. A. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," IEEE Access, vol. 8, pp. 23817-23837, 2020.
13. V. D. Soni, "Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA," SSRN, 3624487, 2020.
14. E. Proko, A. Hyso, D. Gjylapi, "Machine Learning Algorithms in Cyber Security,"Proceedings of the 3rd International Conference on the Recent Trends and the Applications in the Computer Science and the Information Technology,pp. 203-207, 2018.
15. V. Ford and A. Siraj, "Applications of machine learning in cyber security," in Proceedings of the 27th International Conference on the Computer Applications in the Industry and the Engineering, Kota Kinabalu, 2014.
16. AI In cyberspace: Miracle or Threat? https://ccip.khas.edu.tr/post/20/siber-dunyada-vapay-intelligence-use-miracle-mi-threat-mi
17. Murphy, Edmond J. "Assorted Attacks on the RSA Cryptographic Algorithm." (2014).
18. Boneh, D.. "Twenty years of the attacks on the the RSA Cryptosystem". Notices of American Mathematical Society, #46 (1999): 203-212.
19. Hinek, M. "The Cryptanalysis of the RSA cryptosystem and Its Variants" (2009).

20. Matus Nemec, Marek Sys, Petr Svenda, Dusan Klinec, and Vashek Matyas.The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. Published in the Proceedings of 2017 ACM SIGSAC Conference on the Computer and Communications Security, CCS '17, pages 1631-1648, New York, NY, USA, 2017. ACM.
21. NIST National Vulnerability Database. CVE-2017-15361.https://nvd.nist.gov/vuln/detail/CVE-2017-15361, October 2017.
22. Infineon. SLJ52GCA150 JavaCard, https://secure.smartcard- source.com/slj52gdl150cl-java-smart-card.html, May 2019.
23. Bruno Produit, "Optimization of the ROCA (CVE-2017-15361) Attack", University of Tartu, Estonia, May 2019.
24. Don Coppersmith. “Finding the Small Root of the Bivariate Integer Equation; Factoring with High Bits Known”. In Ueli Maurer, editor, Advances in Cryptology — Eurocrypt '96, pages 178-189, Berlin, Heidelberg, 1996. Springer, Berlin Heidelberg.
25. Dan Boneh and Glenn Durfee. “Cryptanalysis of the RSA cryptosystem with private key d less than $N^{0.292}$”. Published in the Lecture Notes in the Computer Science. This includes subseries Lecture Notes in the Artificial Intelligence and Lecture Notes in Bioinformatics, 1999.
26. Howgrave-Graham, Nicholas A. "Computational mathematics inspired by RSA" (1998).
27. Herrmann, Mathias and Alexander May. "Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA." Public Key Cryptography (2010).
28. Ronald L. RivestAdi ShamirLeonard M. Adleman, US patent US4405829A, "Cryptographic communications system and method", filed on December 14 1977, by Massachusetts Institute of Technology, US.
29. Robinson, Sara (June 2003). "Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders" (PDF). SIAM News. 36 (5).
30. John M. Delaurentis, “The further weakness in common modulus protocol for RSA cryptographic algorithm", Cryptologia (1984), vol. 8, nr. 3, pag. 253-259, doi 10.1080/0161-118491859060, Taylor & Francis;
31. Wen-Guey Tzeng "Common modulus and chosen-message attacks on public-key schemes with linear recurrence relations", Information Processing Letters (1999), vol. 70, Issue 3, Pages 153-156, ISSN 0020-0190,
32. Hinek, M. and Charles C. Y. Lam. "Common modulus attacks on small private exponent RSA and some fast variants (in practice)." J. Math. Cryptol. (2010).
33. M. Bellare, P. Rogaway. "Optimal Asymmetric Encryption -- How to encrypt with RSA". Extended abstract in Advances in Cryptology - Eurocrypt '94 Proceedings, Lecture Notes in Computer Science Vol. 950, A. De Santis ed, Springer-Verlag, 1995.
34. Bardou, Romain et al. "Efficient Padding Oracle Attacks on Cryptographic Hardware." IACR Cryptol. ePrint Arch. 2012 (2012): 417.
35. Bleichenbacher, D. "Forging some RSA signatures with pencil and paper." presentation in the rump session, CRYPTO 2006, August (2006).