Cyber Security - Current and Future Trends

Raluca-Elena VASILOIU
Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest,
Romania
rvasiloiu4@gmail.com

Abstract

During recent years, many researchers and professionals have revealed the endangerment of wireless communication technologies and systems from various cyberattacks, these attacks cause detriment and harm not only to private enterprises but to the government organizations as well. The attackers endeavor new techniques to challenge the security frameworks, use powerful tools and tricks to break any sized keys, security of private and sensitive data is in the stale mark. There are many advancements being developed to mitigate these attacks. In this conjunction, this paper gives a complete account of survey and review of the various exiting advanced cyber security standards along with challenges faced by the cyber security domain. The new generation attacks are discussed and documented in detail and the advanced key management schemes are also depicted. The quantum cryptography is discussed with its merits and future scope of the same. Overall, the paper would be a kind of technical report to the new researchers to get acquainted with the recent advancements in Cyber security domain.

Index terms: cybersecurity, DES, RSA, key management, side channel attacks

References

[1]. B. Arora, "Exploring and analyzing Internet crimes and their behaviours," Perspect. Sci. 8 (7), 540–542, https://doi.org/10.1016/j.pisc.2016.06.014, 2016.

[2]. B. Schneier, "Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish).," Proceedings of the International Workshop on Fast Software Encryption, https://doi: 10.1007/3-540-58108-1_24, 1993.

[3]. S. E. Jasper, "US cyber threat intelligence sharing frameworks," Int. J. Intell. Count. Intell. 30 (1), 53–65, https://doi.org/10.1080/08850607.2016.1230701, 2017.

[4]. Emmanuel, S., Thomas, T., Vijayaraghavan, "Machine learning and cybersecurity," Machine Learning Approaches in Cyber Security Analytics, Springer, Singapore, pp. 37–47, https://doi.org/10.1007/978-981-15-1706-8_3, 2020.

[5]. Niekerk, Johan V., Solms, Rossouw V., "rom information security to cyber security," Comput. Sec. 38 (7), 97–102., https://doi.org/10.1016/j.cose.2013.04.004, 2013.

[6]. Apostolopoulos, T., Gritzalis, D., Mitrou, L., Pipyros, K., Thraskias, C., "A new strategy for improving cyber-attacks evaluation in the context of tallinn manual," Comput. Sec. 74 (3), 371–383., https://doi.org/10.1016/j.cose.2017.04.007.

[7]. Fiedelholtz, "Incident Response and Recovery.," The Cyber Security Network Guide. Studies in Systems, Decision and Control, vol 274. 2021.Springer, https://doi.org/10.1007/978-3-030-61591-8_4, 2021.

[8]. D. Smit, "Cyber bullying in south african and american schools: a legal comparative study.," S. Afr. J. Educ. 35 (2), 1076–1087, https://doi.org/10.15700/saje.v35n2a1076, 2015.

[9]. Aslam N., Chowdhury C., Roy M, "Security and privacy issues in wireless sensor and body area networks," Handbook of Computer Networks and Cyber Security.173-200.2020.Springer, https://doi.org/10.1007/978-3-030-22277-2_7, 2020.

[10]. J. Ruohonen, "An acid test for europeanization: public cyber security procurement in the European union," Eur. J. Sec. Res., 1–29, https://doi.org/10.1007/s41125-019-00053-w, 2019.

[11]. Dagmar, B., Gabor, E., Jorg, R., Tim, M., Tobias, R., "Quantum cryptography: a survey.," ACM Comput. Surv 39 (2), 6., https://doi.org/10.1145/1242471.1242474, 2007.

[12]. A. S. Djekic, "Cryptography of the Ancient Sparta," Australian Science, no. http://www.australianscience.com.au/technology/a-scytale-cryptography-of-the-ancient-sparta/, 2013.

[13]. NIST., "Announcing Approval of the Withdrawal of Federal Information Processing Standard (FIPS) 46–3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation," FIPS 46-3 FIPS 74 and FIPS 81, https://csrc.nist.gov/news/2005/withdrawal-of-fips-46-3-fips-74-and-fips-81, 2005.

[14]. E. Biham, "New types of cryptanalytic attacks using related keys," J. Cryptols. 7 (4), 229–246, https://doi.org/10.1007/BF00203965, 1994.

[15]. M. Matsui, "Linear Cryptanalysis Method for DES Cipher," Proceedings of International Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg. 386-397., https://doi.org/10.1007/3-540-48285-7_33, 1993.

[16]. Bhanot, R., Hans, R., "A review and comparative analysis of various encryption algorithms.," Int. J. Sec. Its Appl. 9 (4), 289–306, https://doi.org/10.14257/ijsia.2015.9.4.27, 2015.

[17]. Kapczynski, A., Lawnik, M., "The application of modified Chebyshev polynomials in asymmetric cryptography," Comput. Sci. 20 (3), https://doi.org/10.7494/csci.2019.20.3.3307, 2019.

[18]. B. Gómez, "Hidden Irreducible Polynomials: A Cryptosystem Based on Multivariate Public Key Cryptography," Cryptology ePrint Archive, Report, 2009

[19]. Chowhan, S. S, Jaju, S. A., "A Modified RSA Algorithm to Enhance Security for Digital Signature," Proceedings of International Conference and Workshop on

Computing and Communication. IEEE, Vancouver, BC, Canada. 1-5., https://doi.org/10.1109/IEMCON.2015.7344493, 2015.

[20]. Huang, X., Liu, J., Ma, J., Xiang, Y., Zhou, W., "Data Authentication with Privacy Protection. In Advances in Cyber Security," Principles, Techniques, and Applications.115-142. 2019. Springer, Singapore, https://10.1007/978-981-13-1483-4_6, 2019.

[21]. E. Fujisaki, "All-but-many encryption," J. Cryptol. 31 (1), 226–275, https://doi.org/10.1007/s00145-017-9256-x, 2018.

[22]. H. Chie, "Using the modified Diffie-Hellman problem to enhance client computational performance in a three-party authenticated key agreement," Arab. J. Sci. Eng. 43 (2), 637–644, https://doi.org/10.1007/s13369-017-2725-6, 2018.

[23]. Ardehali, M., Ardehali, M., Lo, H.K., "Efficient quantum key distribution scheme and a proof of its unconditional security.," J. Cryptol. 18 (2), 133–165, https://doi.org/10.1007/s00145-004-0142-y, 2005.

[24]. C. B. C. Brassard, "Quantum cryptography: public key distribution and coin tossing.," Comput. Sci. 560 (P1), 7–11., https://doi.org/10.1016/j.tcs.2014.05.025, 2014.

[25]. Chen, W., Du, W., Ma, W., Li, J., Li, N., Zhang, Y., "A survey on quantum cryptography.," Chin. J. Electron. 27 (2), 223–228, https://doi.org/10.1049/cje.2018.01.017, 2018.

[26]. A. Nitaj, "Quantum and post quantum cryptography," https://pdfs.semanticscholar.org/25d9/82dfdaa93976dda7fd8dfdae8e12c7b28bb4.pdf, 2012.

[27]. C. Elliott, "Quantum cryptography," IEEE Sec. Privacy 2 (4), 57–61, https://doi.org/10.1109/MSP.2004.54, 2004.

[28]. Polak, W., Rieffel, E., "An introduction to quantum computing for nonphysicists," ACM Comput. Surv. 32 (3), 300–335, https://doi.org/10.1145/367701.367709, 2000.

[29]. S. Lomonaco, "A quick glance at quantum cryptography," Cryptologia 23 (1), 1–41, https://doi.org/10.1080/0161-119991887739, 1999.

[30]. Shen, J., Shen, J., Wang, C., Zhou, T., "Quantum cryptography for the future internet and the security analysis," Sec. Commun. Netw.. Article 8214619, https://doi.org/10.1155/2018/8214619, 2018.

.