December 2024: Top 10 Read Articles in Network Security and Its Applications

International Journal of Network Security & Its Applications (IJNSA)
ERA, WJCI Indexed

ISSN: 0974 - 9330 (Online); 0975 - 2307 (Print)

https://airccse.org/journal/ijnsa.html

Citations, h-index, i10-index

Citations 11309 h-index 50 i10-index 211

SECURITY & PRIVACY THREATS, ATTACKS AND COUNTERMEASURES IN INTERNET OF THINGS

Faheem Masoodi[1] Shadab Alam[2] and Shams Tabrez Siddiqui[2]

[1]Department of Computer Science, University of Kashmir, J&k, India [2]Department of Computer Science, Jazan University, KSA

ABSTRACT

The idea to connect everything to anything and at any point of time is what vaguely defines the concept of the Internet of Things (IoT). The IoT is not only about providing connectivity but also facilitating interaction among these connected things. Though the term IoT was introduced in 1999 but has drawn significant attention during the past few years, the pace at which new devices are being integrated into the system will profoundly impact the world in a good way but also poses some severe queries about security and privacy. IoT in its current form is susceptible to a multitudinous set of attacks. One of the most significant concerns of IoT is to provide security assurance for the data exchange because data is vulnerable to some attacks by the attackers at each layer of IoT. The IoT has a layered structure where each layer provides a service. The security needs vary from layer to layer as each layer serves a different purpose. This paper aims to analyze the various security and privacy threats related to IoT. Some attacks have been discussed along with some existing and proposed countermeasures.

KEYWORDS

Internet of Things, privacy, attacks, security, threats, protocols.

For More Details : **http://aircconline.com/ijnsa/V11N2/11219ijnsa05.pdf**

Volume Link : **http://airccse.org/journal/jnsa19_current.html**

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.

[2] Roman, R., Najera, P., Lopez, J., 2011. Securing the internet of things. Computer 44 (9), 51_58.

[3] Horrow, S., and Anjali, S. (2012). Identity Management Framework for Cloud-Based Internet of Things. SecurIT '12 Proceedings of the First International Conference on Security of Internet of Things, 200– 203. 2012

[4] Whitmore, A., Agarwal, A., and Da Xu, L. (2014). The Internet of Things: A survey of topics and trends. Information Systems Frontiers, 17(2), 261– 274.

[5] Aazam, M., St-Hilaire, M., Lung, C.-H., and Lambadaris, I. (2016). PRE-Fog: IoT trace based probabilistic resource estimation at Fog. 2016 13th IEEE Annual Consumer Communications and Networking Conference (CCNC), 12– 17.

[6] Jiang, H., Shen, F., Chen, S., Li, K. C., and Jeong, Y. S. (2015). A secure and scalable storage system for aggregate data in IoT. Future Generation Computer Systems, 49, 133–141.

[7] Li, S., Tryfonas, T., and Li, H. (2016). The Internet of Things: a security point of view. Internet Research, 26(2), 337– 359.

[8] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys Tutorials, 17(4):2347–2376, Fourth quarter 2015.

[9] Pongle, P., and Chavan, G. (2015). A survey: Attacks on RPL and 6LoWPAN in IoT. 2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015, 0(c), 0–5

[10] Tsai, C.-W., Lai, C.-F., and Vasilakos, A. V. (2014). Future Internet of Things: open issues and challenges. Wireless Networks, 20(8), 2201–2217.

[11] V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," Transaction on IoT and Cloud Computing, vol. 3, no. 1, pp. 11-17, 2015

[12] D. Locke, "MQ telemetry transport (MQTT) v3. 1 protocol specification," IBM Developer WorksTechnicalLibrary,2010, http://www.ibm.com/developerworks/webservices/library/wsmqtt/index.html

[13] M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure MQTT for the Internet of Things (IoT)," in Fifth International Conference on Communication Systems and Network Technologies (CSNT 2015), April 2015, pp. 746-751.

[14] OASIS, "OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0," 2012, http://docs.oasis-open.org/amqp/core/v1.0/os/amqp-core-complete-v1.0-os.pdf

[15] T. Winter, et al., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," IETF RFC 6550, Mar. 2012, http://www.ietf.org/rfc/rfc6550.txt

[16] A. Aijaz and A. Aghvami, "Cognitive machine-to-machine communications for internet-of-things: A protocol stack perspective," IEEE Internet of Things Journal, vol. 2, no. 2, pp. 103-112, April 2015,

[17] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=7006643

[18] Z. Zhou, B. Yao, R. Xing, L. Shu, and S. Bu, "E-CARP: An energy-efficient routing protocol for UWSNs on the internet of underwater things," IEEE Sensors Journal, vol. PP, no. 99, 2015, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7113774

[19] D. Dujovne, T. Watteyne, X. Vilajosana, and P. Thubert, "6TiSCH: Deterministic IP-enabled industrial internet (of things)," IEEE Communications Magazine, vol. 52, no.12, pp. 36-41, December 2014, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6979984

[20] M. Hasan, E. Hossain, D. Niyato, "Random access for machine-to-machine communication in LTEadvanced networks: issues and approaches," in IEEE Communications Magazine, vol. 51, no. 6, pp.86-93, June 2013, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6525600

[21] Z-Wave, "Z-Wave Protocol Overview," v. 4, May 2007, https://wiki.ase.tut.fi/courseWiki/imges/9/94/SDS10243_2_Z_Wave_Protocol_Overview.pdf

[22] ZigBee Standards Organization, “ZigBee Specification,” Document 053474r17, Jan 2008, 604 pp., http://home.deib.polimi.it/cesana/teaching/IoT/papers/ZigBee/ZigBeeSpec.pdf

[23] O. Cetinkaya and O. Akan, "A dash7-based power metering system," in 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Jan 2015, pp. 406-411, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=7158010

[24] Zhang, Zhi-Kai, et al. ”IoT security: ongoing challenges and research opportunities.” ServiceOriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on. IEEE, 2014.

[25] D. Migault, D. Palomares, E. Herbert, W. You, G. Ganne, G. Arfaoui, and M. Laurent, “E2E: An Optimized IPsec Architecture for Secure And Fast Offload,” in Seventh International Conference on Availability, Reliability and Security E2E: 2012.

[26] Abomhara, Mohamed, and Geir M. Køien. ”Security and privacy in the Internet of Things: Current status and open issues.” Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on. IEEE, 2014.

[27] B. L. Suto, "Analyzing the Accuracy and Time Costs of Web Application Security Scanners," San Fr., no. October 2007, 2010.

[28] O. El Mouaatamid, M. LahmerInternet of Things security: layered classification of attacks and possible countermeasures Electron J (9) (2016).

[29] Seda F. Gürses/Bettina Berendt/Thomas Santen, Multilateral Security Requirements Analysis for Preserving Privacy in Ubiquitous Environments, in Bettina Berendt/Ernestina Menasalvas (eds), Workshop on Ubiquitous Knowledge Discovery for Users (UKDU '06), at 51–64;

[30] Stankovic, J. (2014). Research directions for the internet of things. IEEE Internet of Things Journal, 1(1), 3–9

[31] Sicari, Sabrina, et al. "Security, privacy and trust in the Internet of Things: The road ahead." Computer Networks76 (2015): 146-164.

[32] https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/ Accessed on 15-03-2019

[33] Bokhari, Mohammad Ubaidullah, and Faheem Masoodi. "Comparative analysis of structures and attacks on various stream ciphers." Proceedings of the 4th National Conference. 2010.

EVALUATION OF A BLOCKCHAIN-ENABLED RESOURCE MANAGEMENT MECHANISM FOR NGNS

Michael Xevgenis[1], Dimitrios G. Kogias[2], Ioannis Christidis[1], Charalampos Patrikakis[2] and Helen C. Leligou[1]

[1]Dept. of Industrial Design and Production Engineering, University of West Attica, 122 43 Attica, Greece
[2]Dept. of Electrical and Electronics Engineering, University of West Attica, 122 43 Attica, Greece

ABSTRACT

A new era in ICT has begun with the evolution of Next Generation Networks (NGNs) and the development of human-centric applications. Ultra-low latency, high throughput, and high availability are a few of the main characteristics of modern networks. Network Providers (NPs) are responsible for the development and maintenance of network infrastructures ready to support the most demanding applications that should be available not only in urban areas but in every corner of the earth. The NP's must collaborate to offer high- quality services and keep their overall cost low. The collaboration among competitive entities can in principle be regulated by a trusted 3rd party or by a distributed approach/technology which can guarantee integrity, security, and trust. This paper examines the use of blockchain technology for resource management and negotiation among NPs and presents the results of experiments conducted in a dedicated real testbed. The implementation of the resource management mechanism is described in a Smart Contract (SC) and the testbeds use the Raft and the IBFT consensus mechanisms respectively. The goal of this paper is two-fold: to assess its performance in terms of transaction throughput and latency so that we can assess the granularity at which this solution can operate (e.g. support resource re-allocation among NPs on micro-service level or not) and define implementation-specific parameters like the consensus mechanism that is the most suitable for this use case based on performance metrics.

KEYWORDS

Blockchain, NGNs, Resource management, Consensus, Performance

For More Details : **https://aircconline.com/ijnsa/V13N5/13521ijnsa01.pdf**

Volume Link : **https://airccse.org/journal/jnsa21_current.html**

REFERENCES

[1] Website: Cisco Annual Internet Report (2018–2023) White Paper, link: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html ,Accessed on 31/03/2021

[2] Redana, S., Bulakci, Ö., Zafeiropoulos, A., Gavras, A., Tzanakaki, A., Albanese, A., ... & Zhang, Y. (2019). 5G PPP Architecture Working Group: View on 5G Architecture.

[3] Website: OSM MANO, link: https://osm.etsi.org/ Accessed on 31/03/2021

[4] Panagiotis Trakadas, Panagiotis Karkazis, Helen-Catherine Leligou, Theodore Zahariadis, Felipe Vicens, Arturo Zurita, Pol Alemany, Thomas Soenen, Carlos Parada, Jose Bonnet, Eleni Fotopoulou, Anastasios Zafeiropoulos, Evgenia Kapassa, Marios Touloupou, Dimosthenis Kyriazis, «Comparison of Management and Orchestration solutions for the 5G Era», Journal of Sensor and Actuator Networks, 2020, Vol. 9, No 4; doi:10.3390/jsan9010004.

[5] T. Soenen et al., "Insights from SONATA: Implementing and integrating a microservice-based NFV service platform with a DevOps methodology," NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, 2018, pp. 1-6, doi: 10.1109/NOMS.2018.8406139.

[6] Website: IBM Foodtrust, link: https://www.ibm.com/blockchain/solutions/food-trust Accessed on 01/04/2021

[7] Website: IOTA, link: https://www.iota.org/ Accessed on 01/04/2021

[8] Website: CryptoKitties, link: https://www.cryptokitties.co/ Accessed on 01/04/2021

[9] Xevgenis, M., Kogias, D. G., Karkazis, P., Leligou, H. C., & Patrikakis, C. (2020). “Application of Blockchain Technology in Dynamic Resource Management of Next Generation Networks”, Information, 11(12), 570.

[10] Togou, M. A., Bi, T., Dev, K., McDonnell, K., Milenovic, A., Tewari, H., & Muntean, G. M. (2020, June). A distributed blockchain-based broker for efficient resource provisioning in 5g networks. In 2020 International Wireless Communications and Mobile Computing (IWCMC) (pp. 1485-1490). IEEE.

[11] Maksymyuk, T., Gazda, J., Volosin, M., Bugar, G., Horvath, D., Klymash, M., & Dohler, M. (2020). Blockchain-Empowered Framework for Decentralized Network Management in 6G. IEEE Communications Magazine, 58(9), 86-92.

[12] Xu, H., Klaine, P. V., Onireti, O., Cao, B., Imran, M., & Zhang, L. (2020). Blockchain-enabled resource management and sharing for 6G communications. Digital Communications and Networks, 6(3), 261-269.

[13] Papadakis-Vlachopapadopoulos, K., Dimolitsas, I., Dechouniotis, D., Tsiropoulou, E. E., Roussaki, I., & Papavassiliou, S. (2021, March). On Blockchain-Based Cross-Service

Communication and Resource Orchestration on Edge Clouds. In Informatics (Vol. 8, No. 1, p. 13). Multidisciplinary Digital Publishing Institute.

[14] Hewa, T., Gür, G., Kalla, A., Ylianttila, M., Bracken, A., & Liyanage, M. (2020, March). The role of blockchain in 6G: challenges, opportunities and research directions. In 2020 2nd 6G Wireless Summit (6G SUMMIT) (pp. 1-5). IEEE.

[15] Praveen, G., Chamola, V., Hassija, V., & Kumar, N. (2020). Blockchain for 5g: A prelude to future telecommunication. IEEE Network, 34(6), 106-113.

[16] Website: 5G Zorro, link: https://www.5gzorro.eu/ Accessed on 01/04/2021

[17] Website: https://docs.soliditylang.org/en/v0.8.3/ ,Accessed on 05/05/2021

[18] Website: GoQuorum, link: https://docs.goquorum.consensys.net/en/stable/ Accessed on 03/04/2021

[19] Ongaro, D., & Ousterhout, J. (2014). In search of an understandable consensus algorithm. In 2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14) (pp. 305-319).

[20] Lamport, L. (2001). Paxos made simple. ACM Sigact News, 32(4), 18-25.

[21] Moniz, H. (2020). The istanbul BFT consensus algorithm. arXiv preprint arXiv:2002.03613.

[22] Website: Hyperledger Caliper, link: https://hyperledger.github.io/caliper/ Accessed on 03/04/2021

[23] Website: Provable, link: https://provable.xyz/ Accessed on 04/04/2021

[24] Website: Chainlink, link: https://chain.link/ Accessed on 04/04/2021

[25] Al-Breiki, H., Rehman, M. H. U., Salah, K., & Svetinovic, D. (2020). Trustworthy blockchain oracles: review, comparison, and open research challenges. IEEE Access, 8, 85675-85685.

[26] Leligou, H.C., Kanonakis, K., Angelopoulos, J., Pountourakis, I., Orphanoudakis, T.(2006). Efficient burst aggregation for QoS-aware slotted OBS systems. European Transactions on Telecommunications, 17(1), 93-98.

AUTHORS

Michael Xevgenis is a Ph.D. Candidate at the Department of Industrial Design and Production Engineering of the University of West Attica. The subject of his Ph.D. research is Secure Resource Management in Next Generation Networks, where Blockchain technology is one of the main fields of this study. In addition, he is a Research Associate at the Computer Network and Services Research Team (CONSERT) of the University of West Attica. His research concerns are on the Networking and Cloud Computing sector. In the last few years he has participated in two EU projects: the TRILLION and the STORM of H2020. Finally, he holds the Master in Data and Networking Communications of Kingston University in collaboration with TEI of Piraeus.

Dimitrios G. Kogias was born in Athens in 1978. He received his diploma in Physics from the National and Kapodistrian University of Athens in 2001. In December 2004 he received his M.Sc. in Electronics and Radioelectrology and in May 2010 his Ph.D. degree from the National and Kapodistrian University of Athens on Algorithms for dissemination of information in Unstructured Networking Environments. He works as an Adjunct Lecturer in the Department of Electrical & Electronics Engineering of the University of West Attica (UniWA).

Ioannis Christidis has graduated from the University of West Attica while also participated in ASSET Learning Community & Ecosystem. He is currently a postgraduate student at the University of West Attica and the subject of his research is Blockchain as real-time monitoring system. His research interests focus on blockchain and distributed ledger technologies, data freshness, and gamification.

Charalampos Z. Patrikakis is a Full Professor at the Dept. of Electrical & Electronics Engineering of the University of West Attica. He has participated in more than 32 National, European and International programs, in 16 of which he has been involved as technical coordinator or principal researcher. He has more than 100 publications in chapters of books, international journals, and conferences, and has 2 contributions in national legislation. He is a member of the editorial committee of more than 50 international journals and conferences and has acted as editor in the publication of special issues of international journals, conference proceedings volumes, and coedited three books. He is a senior member of IEEE, Assistant Editor In Chief (Special Issues) of IEEE IT Pro Magazine, member of the Technical Chamber of Greece, the European Association for Theoretical Computer Science, ACM, and counselor of the IEEE student department of University of West Attica.

Helen C. Leligou received the Dipl.Ing. and Ph.D. degrees, both in electrical and computer engineering, from the National Technical University of Athens (NTUA), Athens, Greece, in 1995 and 2002, respectively. Her research interests lie in the area of protocol design for communication systems, access control mechanisms in optical access/metro/core networks, with emphasis on their implementation in hardware using state-of-the-art primarily FPGA but also ASIC technologies. She has also been active in security, routing, and application layer protocols for wireless sensor networks and their implementation in embedded systems. Currently, her research interests lie in blockchain technologies and in the application of novel sensor applications for affect detection in learning environments. She is currently an assistant professor at the University of West Attica while from 2007-2017 she is acting as Assistant Professor at the Technological Educational Institute of Central Greece teaching “Digital Design” and “Computer Networks”. Her research results have been published in more than 100 scientific journals and conferences. She has participated in several EU-funded ACTS, IST and ICT and H2020 research projects in the above areas.

AN EFFICIENT SECURE CRYPTOGRAPHY SCHEME FOR NEW ML-BASED RPL ROUTING PROTOCOL IN MOBILE IOT ENVIRONMENT

Kishore Golla[1] and S. PallamSetty[2]

[1]Research Scholar, Dept. of CSE, Andhra University, Visakhapatnam, Andhra Pradesh, India
[2]Dept. of CSE, Andhra University, Visakhapatnam, Andhra Pradesh, India

ABSTRACT

Internet of Things (IoT) offers reliable and seamless communication for the heterogeneous dynamic low-power and lossy network (LLNs). To perform effective routing in IoT communication, LLN Routing Protocol (RPL) is developed for the tiny nodes to establish connection by using deflaut objective functions: OF0, MRHOF, for which resources are constraints like battery power, computation capacity, memory communication link impacts on varying traffic scenarios in terms of QoS metrics like packet delivery ratio, delay, secure communication channel. At present, conventional Internet of Things (IoT) are having secure communication channels issue for transmission of data between nodes. To withstand those issues, it is necessary to balance resource constraints of nodes in the network. In this paper, we developed a security algorithm for IoT networks with RPL routing. Initially, the constructed network in corporates optimization-based deep learning (reinforcement learning) for route establishment in IoT. Upon the establishment of the route, the ClonQlearn based security algorithm is implemented for improving security which is based onaECC scheme for encryption and decryption of data. The proposed security technique incorporates reinforcement learning-based ClonQlearnintegrated with ECC (ClonQlearn+ECC) for random key generation. The proposed ClonQlearn+ECCexhibits secure data transmission with improved network performance when compared with the earlier works in simulation. The performance of network expressed that the proposed ClonQlearn+ECC increased the PDR of approximately 8% - 10%, throughput of 7% - 13%, end-to-end delay of 5% - 10% and power consumption variation of 3% - 7%.

KEYWORDS

ECC, security, Optimal path, Routing, Reinforcement learning

For More Details : **https://aircconline.com/ijnsa/V14N2/14222ijnsa01.pdf**

Volume Link : **https://airccse.org/journal/jnsa22_current.html**

REFERENCES

[1] Srilakshmi, A., Rakkini, J., Sekar, K. R., & Manikandan, R. (2018). A comparative study on Internet of Things (IoT) and its applications in smart agriculture. Pharmacognosy Journal, 10(2).

[2] Samie, F., Bauer, L., & Henkel, J. (2019). From cloud down to things: An overview of machine learning in internet of things. IEEE Internet of Things Journal, 6(3), 4921-4934.

[3] Shadroo, S., & Rahmani, A. M. (2018). Systematic survey of big data and data mining in internet of things. Computer Networks, 139, 19-47.

[4] Accettura, N., Grieco, L. A., Boggia, G., & Camarda, P. (2011, April). Performance analysis of the RPL routing protocol. In 2011 IEEE International Conference on Mechatronics (pp. 767-772). IEEE.

[5] Saad, L. B., Chauvenet, C., & Tourancheau, B. (2011, September). Simulation of the RPL Routing Protocol for IPv6 Sensor Networks: two cases studies. In International Conference on Sensor Technologies and Applications SENSORCOMM 2011. IARIA.

[6] Airehrour, D., Gutierrez, J. A., & Ray, S. K. (2019). SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Future Generation Computer Systems, 93, 860-876.

[7] Tripathi, J., de Oliveira, J. C., & Vasseur, J. P. (2010, March). A performance evaluation study of rpl: Routing protocol for low power and lossy networks. In 2010 44th Annual Conference on Information Sciences and Systems (CISS) (pp. 1-6). IEEE.

[8] Zhao, M., Ho, I. W. H., & Chong, P. H. J. (2016). An energy-efficient region-based RPL routing protocol for low-power and lossy networks. IEEE Internet of Things Journal, 3(6), 1319-1333.

[9] Gaddour, O., Koubâa, A., Baccour, N., & Abid, M. (2014, May). OF-FL: QoS-aware fuzzy logic objective function for the RPL routing protocol. In 2014 12th International symposium on modeling and optimization in mobile, ad hoc, and wireless networks (WiOpt) (pp. 365-372). IEEE.

[10] Kim, H. S., Kim, H., Paek, J., & Bahk, S. (2016). Load balancing under heavy traffic in RPL routing protocol for low power and lossy networks. IEEE Transactions on Mobile Computing, 16(4), 964-979.

[11] Djedjig, N., Tandjaoui, D., Medjek, F., & Romdhani, I. (2017, April). New trust metric for the RPL routing protocol. In 2017 8th International Conference on Information and Communication Systems (ICICS) (pp. 328-335). IEEE.

[12] Xie, H., Zhang, G., Su, D., Wang, P., & Zeng, F. (2014, June). Performance evaluation of RPL routing protocol in 6lowpan. In 2014 IEEE 5th International Conference on Software Engineering and Service Science (pp. 625-628). IEEE.

[13] Abdel Hakeem, S. A., Hady, A. A., & Kim, H. (2019). RPL routing protocol performance in smart grid applications based wireless sensors: Experimental and simulated analysis. Electronics, 8(2), 186.

[14] Conti, M., Kaliyar, P., Rabbani, M. M., & Ranise, S. (2018, October). SPLIT: A Secure and Scalable RPL routing protocol for Internet of Things. In 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (pp. 1-8). IEEE.

[15] Alvi, S. A., ul Hassan, F., & Mian, A. N. (2017, June). On the energy efficiency and stability of RPL routing protocol. In 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC) (pp. 1927-1932). IEEE.

[16] Glissa, G., Rachedi, A., & Meddeb, A. (2016, December). A secure routing protocol based on RPL for Internet of Things. In 2016 IEEE Global Communications Conference (GLOBECOM) (pp. 1-7). IEEE.

[17] Airehrour, D., Gutierrez, J., & Ray, S. K. (2017, November). A testbed implementation of a trust-aware RPL routing protocol. In 2017 27th International Telecommunication Networks and Applications Conference (ITNAC) (pp. 1-6). IEEE.

[18] Airehrour, D., Gutierrez, J., & Ray, S. K. (2017). A trust-aware RPL routing protocol to detect blackhole and selective forwarding attacks. Journal of Telecommunications and the Digital Economy, 5(1), 50-69.

SYSTEM END-USER ACTIONS AS A THREAT TO INFORMATION SYSTEM SECURITY

Paulus Kautwima, Titus Haiduwa, Kundai Sai, Valerianus Hashiyana and Nalina Suresh

Department of Computing, Mathematical and Statistical Sciences, University of Namibia, Windhoek, Namibia

ABSTRACT

As universities migrate online due to the advent of Covid-19, there is a need for enhanced security in information systems in the institution of higher learning. Many opted to invest in technological approaches to mitigate cybersecurity threats; however, the most common types of cybersecurity breaches happen due to the human factor, well known as end-user error or actions. Thus, this study aimed to identify and explore possible end-user errors in academia and the resulting vulnerabilities and threats that could affect the integrity of the university's information system. The study further presented state-of-the-art human-oriented security threats countermeasures to compliment universities' cybersecurity plans. Countermeasures include well-tailored ICT policies, incident response procedures, and education to protect themselves from security events (disruption, distortion, and exploitation). Adopted is a mixed-method research approach with a qualitative research design to guide the study. An open-ended questionnaire and semi-structured interviews were used as data collection tools. Findings showed that system end-user errors remain the biggest security threat to information systems security in institutions of higher learning. Indeed errors make information systems vulnerable to certain cybersecurity attacks and, when exploited, put legitimate users, institutional network, and its computers at risk of contracting viruses, worms, Trojan, and expose it to spam, phishing, e-mail fraud, and other modern security attacks such as DDoS, session hijacking, replay attack and many more. Understanding that technology has failed to fully protect systems, specific recommendations are provided for the institution of higher education to consider improving employee actions and minimizing security incidents in their eLearning platforms, post Covid-19.

KEYWORDS

Information Systems, Security Threats, End-user errors, Human Factors, DDoS, Virus, Worms, Trojan.

For More Details : **https://aircconline.com/ijnsa/V13N6/13621ijnsa06.pdf**

Volume Link : **https://airccse.org/journal/jnsa21_current.html**

REFERENCES

[1] N.Uushona. "University Of Namibia ICT Policy". 2016. Available: http://unamintranet.unam.na/documents/ict-policy.pdf. (2016)

[2] J. M. Pizza. "Guide to Computer Network Security". (4th Ed.). Chattanooga: Springer International Publishing Ag. 2017.

[3] W. Stallings. Network Security Essentials: Applications and Standards. 4th Ed. 2011. ISBN-10:013608059. Prentice-Hall.

[4] L. Neely. "Threat Landscape Survey: Users on the Front Line". 2017. California: Sans Institute. Available: https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910

[5] O. Safianu, F. Twum & J. B. Hayfron-Acquah. "Information System Security Threats and Vulnerabilities". International Journal of Computer Applications 143(5), 8-14, 2016. Available: https://www.ijcaonline.org/archives/volume143/number5/25071-2016910160

[6] M. Pill. "Top Ten Database Attacks", 2016. Available: https://www.bcs.org/content-hub/top-ten-database-attacks.

[7] P. Silver. Vulnerability Assessment with Application Security. Washington DC: F5 Networks, Inc., 2013.

[8] A. Lamar. Types of Threats to Database Security. 2012. Available: http://ir.knust.edu.gh/bitstream/123456789/10083/1/omar%20safianu.pdf, (accessed June 2020).

[9] Kizza, J. M. (2017). Guide to Computer Network Security (4th Ed.). Chattanooga: Springer International Publishing AG.

[10] S. Kamara, Fahmy, E. Schultz, F. Kerschbaum, & M. Frantzen. "Analysis of vulnerabilities in internet firewalls". 2010. Available: https://www.cs.purdue.edu/homes/fahmy/papers/firewall-analysis.pdf (accessed July 31, 2019).

[11] I.M. Kassiri, & A. Shahidinijad. "A survey of security issues in the firewall: a new approach for classifying firewall vulnerabilities". International Journal of Engineering Research and Applications (IJERA), 3(2), 585-591, 2013

[12] A. W. Soomro, A. Nizamudin, U. Iqbal, & A. Noorul. "Secured Symmetric Key Cryptographic Algorithm For Small Amount of Data". 3rd International Conference on Computer and Emerging Technologies (ICCET), 2013.

[13] Kaspersky Lab. "Software Vulnerabilities", 2013. Available: http://www.securelist.com/en/threats/vulnerabilities?chapter=35.

[14] Marc van Zadelhoff. The Biggest Cybersecurity Threats Are Inside Your Company. Harvard Business Review, 2016.

[15] P. Kearney. Security: The Human Factor. 2010. Cambridge Shire: IT Governance Publishing.

[16] M. Evans, L. A Maglaras, Y. He, & H. Janicke. Human Behavior as an Aspect of Cybersecurity Assurance. Security and Communication Networks, 9(17), 4667-4679, 2016.

[17] L. Hadlington. "Human Factors in Cybersecurity: Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours". (Vol. 3). London: Heliyon, 2017.

[18] H. Lee. "The Human Factor in Cybersecurity: Exploring the Accidental Insider". UK: IGI Global, 2018.

[19] B. A. Gyunka, & A. O. Christiana. "Analysis of Human Factors in Cyber Security: A Case Study of

[20] J. W. Creswell. Research Design (4th ed., Vol. 4).2014. SAGE Publications. https://www.amazon.com/Research-Design-Qualitative-Quantitative-Approch

[21] B. Davis. What is the target population in research methods? 2021. from https://www.mvorganizing.org/what-is-target-population-in-research-methods/

[22] K. S. Muhammad. Basic Guidelines for Research. Research design, 1(1), 111–169. 2016. from https://www.researchgate.net/publication/325847047_research_design

[23] C. Tilley. Qualitative research: What is it and why should you use it.2019. https://www.onepoll.com/qualitative-research-what-is-it-and-why-should-you-use-it/#:%7E:text=In%20short%2C%20in%20comparison%20to,new%20concepts%2C%20theories%20and%20products.

[24] S. Shantikumar. Methods of sampling from a population. 2018. https://www.healthknowledge.org.uk/public-health-textbook/research-methods/1a-epidemiology/methods-of-sampling-population

[25] M. Saunders, P. Lewis, & A. Thornhill. Research Methods for Business Students. 2012. New York: Pearsons Education Limited.

[26] A. Liaropoulos. A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia. Journal of Information Warfare. Vol. 14, pp. 15-24, 2015. Peregrine Technical Solutions. From https://www.jstor.org/stable/26487503

[27] K, Renaud & S, Flowerday. Human-centred Cyber security. Journal of Information Security and Applications. 2017. 34. 10.1016/j.jisa.2017.05.007.

[28] M, Grobler, R, Gaire & S, Nepal. User, Usage, and Usability: Redefining Human Centric Cyber Security. 2021. Front. Big Data 4:583723. DOI: 10.3389/fdata.2021.583723.

[29] C, Barbara. How to Adopt a Human-Centric Approach to Security. 2018. from https://www.csoonline.com/article/3245741/how-to-adopt-a-human-centric-approach-to-security.html

AUTHORS

Paulus Kautwima is currently a Lecturer in the School of Computing, Department of Computer Science, University of Namibia. His area of research is Networking and Security, Online Child Protection, eLearning, IOT, Cloud Computing and Security, AI, Robotics, egovernment, and educational technologies.
Tel:+264814131922, pkautwima@unam.com; pkautwima@gmail.com

Kundai Sai is currently a Ph.D. candidate at University of KwaZulu-Natal, SA. He holds a BSC Degree in Physics and Computer Science from Great Zimbabwe University, a Master of Science Degree in Information Systems Management from Midlands State University.
Tel: +264814515699, ksai@unam.na

Titus Haiduwa is currently a Lecturer in the Department of Information Technology, School of Computing, University of Namibia. He currently holds a Diploma and a Bachelors' Degree in Information Technology from Namibia University of Science & Technology, as well as a Master Degree in Engineering with specialization in Software Engineering from Wuhan University.
Tel: +264812001246, thaiduwa@unam.na

Nalina Suresh is currently a Senior Lecturer in the School of Computing, Department of Information technology University of Namibia. Her area of research is Networking and Security, Computational Theory and modelling, Automation, IOT, Cloud Computing and Security, AI, Robotics, ML, DSP, educational technologies.
Tel: +264812229533, nsuresh@unam.com; nalina.kss@gmail.com

Valerianus Hashiyana is currently a Senior Lecturer at School of Computing and Head of Department: Computer Science, University of Namibia. His area of research are Cybersecurity, Networking, IOT, e-health, Next generation computing.
Tel: +264812830277, vhashiyana@unam.na; vhashiyana@gmail.com

USE OF MARKOV CHAIN FOR EARLY DETECTING DDOS ATTACKS

Chin-Ling Chen[1] and Jian-Ming Chen[2]

[1]Department of Information Management, National Pingtung University, Pingtung, Taiwan 900
[2]Genesis Technology, Inc., HsinChu, Taiwan 300

ABSTRACT

DDoS has a variety of types of mixed attacks. Botnet attackers can chain different types of DDoS attacks to confuse cybersecurity defenders. In this article, the attack type can be represented as the state of the model. Considering the attack type, we use this model to calculate the final attack probability. The final attack probability is then converted into one prediction vector, and the incoming attacks can be detected early before IDS issues an alert. The experiment results have shown that the prediction model that can make multi-vector DDoS detection and analysis easier.

KEYWORDS

DDoS, attack detection, Markov chain, TCP SYN flood, ICMP flood, HTTP flood, LAND, UDP flood.

For More Details : **https://aircconline.com/ijnsa/V13N4/13421ijnsa01.pdf**

Volume Link : **https://airccse.org/journal/jnsa21_current.html**

REFERENCES

[1] Karras, D. A. &Zorkadis,V. C. (2008) "On efficient security modelling of complex interconnected communication systems based on Markov Processes," 2008 New Technologies, Mobility and Security, pp1-7.

[2] Zhai, J., Liu, G.& Dai, Y. (2010) "A covert channel detection algorithm based on TCP Markov model," 2010 International Conference on Multimedia Information Networking and Security, pp893-897.

[3] Abdulmunem, A.-S. M. Q.&Kharchenko, V. S. (2016) "Availability and security assessment of smart building automation systems: combining of attack tree analysis and Markov models," 2016 Third International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), pp302-307.

[4] Kolisnyk, M.,Kharchenko, V.&Iryna, P. (2019) "IoTserver availability consideringDDoS-attacks: analysis of prevention methods and Markov model," 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT).

[5] Shing, M. -L.&Shing, C. -C. (2010) "Information security risk assessment using Markov models," 2010 Third International Symposium on Electronic Commerce and Security, pp403-406.

[6] Cao,L. -C. (2007) "A high-efficiency intrusion prediction technology based on Markov Chain," 2007 International Conference on Computational Intelligence and Security Workshops (CISW 2007), pp518-521.

[7] Le,N. T.& Hoang,D. B. (2018) "Security threat probability computation using Markov Chain and common vulnerability scoring system," 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), pp1-6.

[8] Wang, C., Shi, C., Wang, C.& Fu,Y. (2016) "An analyzing method for computer network security based on Markov game model," 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), pp454-458.

[9] Miehling, E., Rasouli, M.&Teneketzis, D. (2017) "A dependency graph formalism for the dynamic defense of cyber networks," 2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP), pp511-512.

[10] Zheng, J.&Namin,A. S. (2018) "Defending SDN-based IoTnetworks againstDDoSattacks using Markov Decision Process," 2018 IEEE International Conference on Big Data (Big Data), pp4589-4592.

[11] Kuang, G. C., Wang, X. F.& Yin, L. R. (2012) "A fuzzy forecast method for network security situation based on Markov," 2012 International Conference on Computer Science and Information Processing (CSIP), pp785-789.

[12] Sun, S. (2015) “The research of the network security situation prediction mechanism based on the complex network,” 2015 International Conference on Computational Intelligence and Communication Networks (CICN), pp1183-1187.

[13] C. Zhou, S. Huang, N. Xiong, S. -H. Yang, H. Li, Y. Qin & X. Li, (2015) “Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2015, Vol.45, No.10, pp1345-1360.

[14] Teoh, T. T., Nguwi, Y. Y., Elovici, Y., Cheung, N. M.& Ng, W. L. (2017) “Analyst intuition based Hidden Markov Model on high speed, temporal cyber security big data,” 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), pp2080-2083.

[15] Holgado, P., Villagrá, V. A.& Vázquez, L. (2020) “Real-time multistep attack prediction based on Hidden Markov Models,” IEEE Transactions on Dependable and Secure Computing, 2020, Vol.17, No.1.

AUTHORS

Chin-Ling Chen received the BS degree from National Taiwan University in 1988, the Master degree in Management Information System from the University of Wisconsin, Milwaukee, in 1992, and the Ph.D. degree in Information Management from National Taiwan University of Science and Technology, 1999. Since the spring of 1999, he has joined the faculty of the Department of Information Management at National Pingtung University, Taiwan. His research interests include Internet QoS, network technology, and network security. He is a member of IEICE.

Jian-Ming Chen received his master's degree in Information Management from National Pingtung University, 2019. Currently, he is a software engineer of Genesis Technology, Inc, Hsinchu, Taiwan.

EFFECT MAN-IN THE MIDDLE ON THE NETWORK PERFORMANCE IN VARIOUS ATTACK STRATEGIES

Iyas Alodat

Department of Computer and Information System, Jerash University, Jerash, Jordan

ABSTRACT

In this paper, we examined the effect on network performance of the various strategies an attacker could adopt to launch Man-In The Middle (MITM) attacks on the wireless network, such as fleet or random strategies. In particular, we're focusing on some of those goals for MITM attackers - message delay, message dropping. According to simulation data, these attacks have a significant effect on legitimate nodes in the network, causing vast amounts of infected packets, end-to-end delays, and significant packet loss.

KEYWORDS

Wireless Network, Mobile Network, security; Man-In-The-Middle Attack; smart cities; simulation; Intelligent Transportation System; Internet-of-Things.

For More Details : **http://aircconline.com/ijnsa/V13N3/13321ijnsa02.pdf**

Volume Link : **http://airccse.org/journal/jnsa21_current.html**

REFERENCES

[1] Burchfiel, J., Tomlinson, R., & Beeler, M. (1975, May). Functions and structure of a packet radio station. In Proceedings of the May 19-22, 1975, national computer conference and exposition (pp. 245-251).

[2] Toor, Y., Muhlethaler, P., Laouiti, A., & De La Fortelle, A. (2008). Vehicle ad hoc networks: Applications and related technical issues. IEEE communications surveys & tutorials, 10(3), 74-88.

[3] Bauwens, J., Jooris, B., Giannoulis, S., Jabandžić, I., Moerman, I., & De Poorter, E. (2019). Portability, compatibility and reuse of MAC protocols across different IoT radio platforms. Ad Hoc Networks, 86, 144-153.

[4] Chaqfeh, M.; Lakas, A. A Novel Approach for Scalable Multi-hop Data Dissemination in Vehicular Ad Hoc Networks. Ad Hoc Netw. 2016, 37, 228–239

[5] Shi, Y., Ross, A., & Biswas, S. (2018). Source identification of encrypted video traffic in the presence of heterogeneous network traffic. Computer Communications, 129, 101-110.

[6] Williams, R., Samtani, S., Patton, M., & Chen, H. (2018, November). Incremental hacker forum exploit collection and classification for proactive cyber threat intelligence: An exploratory study. In 2018 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 94-99). IEEE.

[7] Wang, J., Juarez, N., Kohm, E., Liu, Y., Yuan, J., & Song, H. (2019, April). Integration of SDR and UAS for malicious Wi-Fi hotspots detection. In 2019 Integrated Communications, Navigation and Surveillance Conference (ICNS) (pp. 1-8). IEEE.

[8] Phung, C. V., Dizdarevic, J., Carpio, F., & Jukan, A. (2019, May). Enhancing rest http with random linear network coding in dynamic edge computing environments. In 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 435-440). IEEE.

[9] AMIR, A. Z. B. (2018). A study on Rogue Wireless Devices with Detection of Mousejack Attacks and Vulnerabilities.

[10] Vanhoef, M., Bhandaru, N., Derham, T., Ouzieli, I., & Piessens, F. (2018, June). Operating channel validation: preventing Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks. In Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (pp. 34-39).

[11] Chittamuru, S. V. R., Thakkar, I. G., Pasricha, S., Vatsavai, S. S., & Bhat, V. (2020). Exploiting Process Variations to Secure Photonic NoC Architectures from Snooping Attacks. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.

[12] Rupprecht, D., Kohls, K., Holz, T., & Pöpper, C. (2019, May). Breaking LTE on layer two. In 2019 IEEE Symposium on Security and Privacy (SP) (pp. 1121-1136). IEEE.

[13] Ullas, S. U., & Sandeep, J. (2019). Reliable Monitoring Security System to Prevent MAC Spoofing in Ubiquitous Wireless Network. In Advances in Big Data and Cloud Computing (pp. 141-153). Springer, Singapore.

[14] Maithili, K., Vinothkumar, V., & Latha, P. (2018). Analyzing the security mechanisms to prevent unauthorized access in cloud and network security. Journal of Computational and Theoretical Nanoscience, 15(6-7), 2059-2063.

[15] Tochner, S., Zohar, A., & Schmid, S. (2020, October). Route Hijacking and DoS in Off-Chain Networks. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (pp. 228-240).

[16] Alharthi, D. N., Hammad, M. M., & Regan, A. C. (2020, March). A taxonomy of social engineering defense mechanisms. In Future of Information and Communication Conference (pp. 27-41). Springer, Cham.

[17] Metz, L. A. E. P. (2020). An evaluation of unity ML-Agents toolkit for learning boss strategies (Doctoral dissertation).

[18] Shringarputale, S., McDaniel, P., Butler, K., & La Porta, T. (2020, November). Co-residency Attacks on Containers are Real. In Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop (pp. 53-66).

[19] Xia, W., Cong, W., Wei, Y., & Li, C. (2020). Critical angle of attack and the corresponding impact cavity for non-circuitous trajectory of water entry of circular cylinder. Applied Ocean Research, 103, 102322.

[20] Huang, Y., Kuo, H. K., Thomas, S., Kons, Z., Audhkhasi, K., Kingsbury, B., ... & Picheny, M. (2020, May). Leveraging unpaired text data for training end-to-end speech-to-intent systems. In ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 7984-7988). IEEE.

[21] Verma, S., Hamieh, A., Huh, J. H., Holm, H., Rajagopalan, S. R., Korczynski, M., & Fefferman, N. (2016, August). Stopping amplified dns ddos attacks through distributed query rate sharing. In 2016 11th International Conference on Availability, Reliability and Security (ARES) (pp. 69-78). IEEE.

[22] A. Guruswamy, R. S. Blum, S. Kishore and M. Bordogna, “On the Optimum Design of L-Estimators for Phase Offset Estimation in IEEE 1588,” IEEE Transactions on Communications, Vol. 63 , No. 9, pp. 5101 – 5115, Dec. 2015.

[23] Karthik, A. K., & Blum, R. S. (2016). Estimation theory based robust phase offset estimation in the presence of delay attacks. arXiv preprint arXiv:1611.05117.

[24] Tsigkari, D., & Spyropoulos, T. (2020). An approximation algorithm for joint caching and recommendations in cache networks. arXiv preprint arXiv:2006.08421.

[25] Stricot-Tarboton, S.; Chaisiri, S.; Ko, R.K.L. Taxonomy of Man-in-the-Middle Attacks on HTTPS. In Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016; pp. 527–534. [CrossRef]

[26] Chen, Z.; Guo, S.; Duan, R.; Wang, S. Security Analysis on Mutual Authentication against Man-in-the-Middle Attack. In Proceedings of the First International Conference on Information Science and Engineering, Nanjing, China, 26–28 December 2009; pp. 1855–1858. [CrossRef]

[27] Conti, M.; Dragoni, N.; Lesyk, V. A Survey of Man In The Middle Attacks. IEEE Commun. Surv. Tutor. 2016, 18, 2027–2051. [CrossRef]

[28] Glass, S.M.; Muthukkumarasamy, V.; Portmann, M. Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks. In Proceedings of the International Conference on Advanced Information Networking and Applications, Bradford, UK, 26–29 May 2009; pp. 530–538.

[29] Kaplanis, C. Detection and Prevention of Man in the Middle Attacks in Wi-Fi Technology. Master's Thesis, Aalborg University, Aalborg, Denmark, 2015.

PHISHING MITIGATION TECHNIQUES: A LITERATURE SURVEY

Wosah Peace Nmachi and Thomas Win

School of Computing & Engineering University of Gloucestershire, Park Campus, Cheltenham GL50 2RH United Kingdom

ABSTRACT

Email is a channel of communication which is considered to be a confidential medium of communication for exchange of information among individuals and organisations. The confidentiality consideration about e-mail is no longer the case as attackers send malicious emails to users to deceive them into disclosing their private personal information such as username, password, and bank card details, etc. In search of a solution to combat phishing cybercrime attacks, different approaches have been developed. However, the traditional exiting solutions have been limited in assisting email users to identify phishing emails from legitimate ones. This paper reveals the different email and website phishing solutions in phishing attack detection. It first provides a literature analysis of different existing phishing mitigation approaches. It then provides a discussion on the limitations of the techniques, before concluding with an explorationin to how phishing detection can be improved.

KEYWORDS

Cyber-security, Phishing Email Attack, Deep Learning, Stylometric Analysis, Cyber Human Behaviour

For More Details : **https://aircconline.com/ijnsa/V13N2/13221ijnsa05.pdf**

Volume Link : **http://airccse.org/journal/jnsa21_current.html**

REFERENCES

[1] Leite C., Gondim J. J. C., Barreto P. S., and Alchieri E. A., (2019). Waste flooding: A phishing retaliation tool

[2] Xiujuan W., Chenxi Z., Kangfeng Z., Haoyang T., &Yuanrui T.(2019)detecting spear-phishing emails based on authentication

[3] Duman S, Kalkan-Cakmakci K, Egele M. (2016)EmailProfiler: Spear phishing filtering with header and stylometric features of emails.

[4] Calix K., Connors M., Levy D., Manzar H., McCabe G., & Westcott S. (2008). Stylometry for E-mail author identification and authentication

[5] Gupta B. B., Arachchilage N A.G., &Psannis K. E. (2018).Defending against phishing attacks: taxonomy of methods, current issues and future direction

[6] Dewan P, Kashyap A, &Kumaraguru P. (2014). Analysingsocial and stylometric features to identify spear phishing emails

[7] AbahussainO. &Harrath Y. (2019). Detection of malicious emails through regular expressions and databases

[8] Helmi R. A. A., Ren C. S.&Jamal A. (2019). Email anti-phishing detection application

[9] Asanka N. G.A.,Steve L.&Beznosov K. (2016) Phishing threat avoidance behaviour: An empirical investigation

[10] Mohammad R., Thabtah F. & McCluskey L. (2015): Tutorial and critical analysis of phishing websites methods

[11] Heartfield Ryan& George Loukas, (2018) Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework

[12] Baniya T., Gautam D.& Kim Y. (2015). Safeguarding web surfing with URL blacklisting

[13] Canova G., Volkamer M., Bergmann C., &Borza R. (2014). NoPhish: An anti-phishing education app

[14] Bottazzi G., Casalicchio E., Marturana F., &Piu M. (2015). MP-shield: A framework for phishing detection in mobile devices.

[15] Li, J., Li, J., Chen, X., Jia, C., & Lou, W. (2015) Identity-based encryption without sourced revocation incloud computing

[16] Qabajeh I.,Thabtah F.,&Chiclana F. (2018) A recent review of conventional vs. automated cybersecurity anti-phishing techniques

[17] Lötter Andrés.&Futcher Lynn, (2015) A framework to Assist Email Users in the Identification of Phishing Attacks

[18] Gascon H., Ullrich S., Stritter B. &Rieck K. (2018) Reading between the lines: content-agnostic detection of spear-phishing emails

[19] Smadi S., Aslam N., & Zhang L. (2018). Detection of online phishing email using dynamic evolving neural network based on reinforcement learning

[20] Chandrasekaran M., Narayanan K., andUpadhayayaS. (2006) Phishing e-mail detection based on structural properties.

[21] Ghafir I., Saleem J., Hammoudeh M., Faour H., Prenosil V., Jaf S., Jabbar S. & Baker T. (2018). Security threats to critical infrastructure: the human factor

[22] Khonji M, Iraqi Y& Jones A. (2011). Mitigation of spear phishing attacks: A Content-based Authorship Identification framework

[23] Iqbal F, BinsalleehH&Fung B C M. (2010). Mining writeprints from anonymous e-mails for forensic investigation

[24] Lyon, J.& Wong M. (2006). Sender ID: authenticating e-mail," RFC 4406.

[25] KunjuM.V., Esther D., Anthony H. C. &BhelwaS. (2019) Evaluation of phishing techniques based on machine learning

[26] Peng T., Harris I., &Sawa Y. (2018).Detecting phishing attacks using natural language processing and machine learning

[27] SahingozO.K.,Buber E., Demir O., &Diri B. (2019). Machine learning based phishing detection from URLs

[28] Zhang, Y., Hong, J. I., &Cranor, L. F.(2007). Cantina: A content based approach to detecting phishing web sites.

[29] Suganya V. (2016): A review on phishing attacks and various anti-phishing techniques

[30] Abdelhamid N., Ayesh A. &Thabtah F. (2014) Phishing detection based associative classification data mining

[31] SternfeldUri&Striem-Amit Yonatan. (2019) Prevention of rendezvous generation algorithm (RGA) and domain generation algorithm (DGA) malware over exiting internet services.

[32] Akarsh S., Sriram S., &Poornachandran P.(2019) Deep learning framework for domain generation algorithms prediction using long short-term memory.

[33] Bagui S., Nandi D.,Subhash B. & White J.R (2019) Classifying phishing email using machine learning and deep learning

[34] Jain Kumar Ankit. & Gupta B.B. (2018). A machine learning based approach for phishing detection using hyperlinks information

[35] Vinayakumar R., Soman K. P., Poornachandran P., Akarsh S. &Elhoseny M. (2019) Deep learning framework for cyber threat situational awareness based on email and url data analysis.

[36] Park Gilchan and Rayz Julia (2018).Ontological detection of phishing emails

[37] Surbhi G., Abhishek S.&Akanksha K. (2016). A literature survey on social engineering attacks: phishing attack

[38] Jamil A., Asif K.& Ghulam Z. (2018) MPMPA: A mitigation and prevention model for social engineering based phishing attacks on facebook

[39] Platsis George, (2018) Thehuman factor: Cyber security's greatest challenge

[40] NaimBaftiu. (2017).Cyber security in Kosovo

[41] Abdelhamid N., Thabtah F. & Abdel-jaber H. (2017) Phishing detection: A recent intelligent machine learning comparison based on models content and features

[42] Alsharnouby M., Alaca F., Chiasson S. (2015)Why phishing still works: User strategies for combating phishing attacks

[43] Chou N., Ledesma R., Teraguchi Y., Boneh D., and Mitchell J. C. (2004) “Client-side defence against web-based identity theft”.

[44] Prakash P., Kumar M., Rao R. K. and Gupta M. (2010) PhishNet: Predictive blacklisting to detect phishing attacks

[45] Delany Mark, (2007) Domain-based email authentication using public keys advertised in the DNS (Domain Keys).

[46] Saidani N., Adi K. and AlliliM. S. (2020)A semantic-based classification approach for an enhanced spam detection.

[47] Bhowmick A. and Hazarika S.M. (2016) Machine learning for e-mail spam filtering: review techniques and trends.

PROOF-OF-REPUTATION: AN ALTERNATIVE CONSENSUS MECHANISM FOR BLOCKCHAIN SYSTEMS

Oladotun Aluko[1] and Anton Kolonin[2]

[1]Novosibirsk State University, Novosibirsk, Russia
[2]Aigents Group, Novosibirsk, Russia

ABSTRACT

Blockchains combine other technologies, such as cryptography, networking, and incentive mechanisms, to enable the creation, validation, and recording of transactions between participating nodes. A consensus algorithm is used in a blockchain system to determine the shared state among distributed nodes. An important component underlying any blockchain-based system is its consensus mechanism, which principally determines the performance and security of the overall system. As the nature of peer-to-peer(P2P) networks is open and dynamic, the security risk within that environment is greatly increased mostly because nodes can join and leave the network at will. Thus, it is important to have a system that can check against malicious behaviour. In this work, we propose a reputation-based consensus mechanism for blockchain-based systems, Proof-of-Reputation(PoR) where the nodes with the highest reputation values eventually become part of a consensus group that determines the state of the blockchain.

KEYWORDS

Consensus Mechanism, Distributed Ledger Technology, Blockchain, Reputation System, Social Computing.

For More Details : **https://aircconline.com/ijnsa/V13N4/13421ijnsa03.pdf**

Volume Link : **http://airccse.org/journal/jnsa21_current.html**

REFERENCES

[1] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman. (2016) Blockchain technology: Beyond bitcoin. [Online]. Available: https://j2-capital.com/wp-content/uploads/2017/11/AIR- 2016-Blockchain.pdf?forcedefault=true.

[2] A. Baliga, "Understanding blockchain consensus models," 2017.

[3] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," J. Inf. Process. Syst., vol. 14, pp. 101–128, 2018.

[4] Quantaloop.io. (2020) Types of consensus algorithms in blockchain. [Online]. Available: https://quantaloop.io/proof-of-work-vs-proof-of-stake-101.

[5] F. Hendrikx, K. Bubendorfer, and R. Chard, "Reputation systems: A survey and taxonomy," Journal of Parallel and Distributed Computing, vol. 75, pp. 184–197, 2015.

[6] V. Gramoli, "From blockchain consensus back to byzantine consensus," Future Generation Computer Systems, vol. 107, pp. 760–769, 2020.

[7] S. Azouvi, P. McCorry, and S. Meiklejohn, "Betting on blockchain consensus with fantomette," arXiv preprint arXiv:1805.06786, 2018.

[8] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensuses algorithms: A survey," arXiv preprint arXiv:2001.07091, 2020.

[9] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2018, pp. 1545–1550.

[10] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1432–1465, 2020.

[11] A. Gervais, G. O. Karame, K. Wu¨st, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, 2016, pp. 3–16.

[12] A. Josang and R. Ismail, "The beta reputation system," in Proceedings of the 15th bled electronic commerce conference, vol. 5, 2002, pp. 2502– 2511.

[13] J. Weng, Z. Shen, C. Miao, A. Goh, and C. Leung, "Credibility: How agents can handle unfair third-party testimonies in computational trust models," IEEE Transactions on Knowledge and Data Engineering, vol. 22, no. 9, pp. 1286–1298, 2009.

[14] S. Song, K. Hwang, R. Zhou, and Y.-K. Kwok,"Trusted p2p transactions with fuzzy reputation aggregation," IEEE Internet computing, vol. 9, no. 6, pp. 24–34, 2005.

[15] K.K.Bharadwaj and M.Y.H.Al-Shamri,"Fuzzy computational models for trust and reputation systems," Electronic commerce research and applications, vol. 8, no. 1, pp. 37–47, 2009.

[16] W. L. Teacy, M. Luck, A. Rogers, and N. R. Jennings, "An efficient and versatile approach to trust and reputation using hierarchical bayesian modelling," Artificial Intelligence, vol. 193, pp. 149–185, 2012.

[17] M. Tavakolifard and S. J. Knapskog, "A probabilistic reputation algorithm for decentralized multi-agent environments," Electronic Notes in Theoretical Computer Science, vol. 244, pp. 139–149, 2009.

[18] A. Whitby, A. Jøsang, and J. Indulska, "Filtering out unfair ratings in bayesian reputation systems," in Proc. 7th Int. Workshop on Trust in Agent Societies, vol. 6. Citeseer, 2004, pp. 106–117.

[19] A. Jøsang, Subjective logic. Springer, 2016.

[20] A. Jøsang and T. Bhuiyan, "Optimal trust network analysis with subjective logic," in 2008 Second International Conference on Emerging Security Information, Systems and Technologies. IEEE, 2008, pp. 179– 184.

[21] L. C. Freeman, "Centrality in social networks conceptual clarification," Social networks, vol. 1, no. 3, pp. 215–239, 1978.

[22] L. Kleinrock, R. Ostrovsky, and V. Zikas, "Proof-of-reputation blockchain with nakamoto fallback," in International Conference on Cryptology in India. Springer, 2020, pp. 16–38.

[23] J. Horton and J. Golden,"Reputation Inflation An Online Marketplace," New York I, vol. 1, 2015.

[24] G. Swamynathan, K. C. Almeroth, and B. Y. Zhao, "The design of a reliable reputation system," Electronic Commerce Research, vol. 10, no. 3, pp. 239–270, 2010.

[25] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Computing Surveys (CSUR), vol. 42, no. 1, pp. 1–31, 2009.

[26] M. Gupta, P. Judge, and M. Ammar, "A reputation system for peer-to-peer networks," in Proceedings of the 13th international workshop on Network and operating systems support for digital audio and video, 2003, pp. 144–152.

[27] F. Gai, B. Wang, W. Deng, and W. Peng, "Proof of reputation: A reputation-based consensus protocol for peer-to-peer network," in International Conference on Database Systems for Advanced Applications. Springer, 2018, pp. 666–681.

[28] J. Yu, D. Kozhaya, J. Decouchant, and P. Esteves-Verissimo,"Repucoin: Your reputation is your power," IEEE Transactions on Computers, vol. 68, no. 8, pp. 1225–1237, 2019.

[29] M. T. de Oliveira, L. H. Reis, D. S. Medeiros, R. C. Carrano, S. D. Olabarriaga, and D. M. Mattos, “Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications,” Computer Networks, vol. 179, p. 107367, 2020.

[30] C. Dwork, N. Lynch, and L. Stockmeyer, “Consensus in the presence of partial synchrony,” Journal of the ACM (JACM), vol. 35, no. 2, pp. 288–323, 1988.

[31] G. Chalkiadakis, E. Elkind, and M. Wooldridge, “Computational aspects of cooperative game theory,” Synthesis Lectures on Artificial Intelligence and Machine Learning, vol. 5, no. 6, pp. 1–168, 2011.

[32] P. Berman, J. A. Garay, K. J. Perry et al., “Towards optimal distributed consensus,” in FOCS, vol. 89. Citeseer, 1989, pp. 410–415.

[33] L. Xiong and L. Liu, “Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities,” IEEE transactions on Knowledge and Data Engineering, vol. 16, no. 7, pp. 843–857, 2004.

[34] A. Kolonin and S. SingularityNET, “Reputation systems for human-computer environments,” Complexity, Informatics and Cybernetics, 2019.

[35] A. Kolonin, B. Goertzel, D. Duong, and M. Ikle, “A reputation system for artificial societies,” arXiv preprint arXiv:1806.07342, 2018.

[36] I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” in International conference on financial cryptography and data security. Springer, 2014, pp. 436–454.

[37] C. Grunspan and R. Perez-Marco, “On profitability of selfish mining,” arXiv preprint arXiv:1805.08281, 2018.

[38] K. A. Negy, P. R. Rizun, and E. G. Sirer, “Selfish mining re-examined,” in International Conference on Financial Cryptography and Data Security. Springer, 2020, pp. 61–78.

[39] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse attacks on bitcoin’s peer-to-peer network,” in 24th {USENIX} Security Symposium ({USENIX} Security 15), 2015, pp. 129–144.

[40] J. Bonneau, "Why Buy When You Can Rent?" in International Conference on Financial Cryptography and Data Security. Springer, 2016, pp. 19–26.

AUTHORS

Oladotun Aluko received his BSc (2017) in Computer Science and Engineering from Obafemi Awolowo University, Nigeria. He is currently working on his MSc in Big Data Analytics and Artificial Intelligence at Novosibirsk State University, Novosibirsk, Russia. His research interests are in Distributed Computing, Blockchain Technology, Machine Learning and Cloud Databases.

Anton Kolonin received his PhD in 1998 after he independently developed a software-algorithmic complex for processing geophysical data, introduced into production in many CIS countries. He has also participated as a leader or lead architect in many projects to develop algorithms and software, including those related to the use of AI, including the recognition of static text, moving objects, music, extracting information from texts and identifying events on financial markets – in Russian and foreign companies. Since 2017, he has also been a software architect for AI and blockchain in the Singularity NET project, leading projects on unsupervised language learning and reputation systems.

SECURE BLOCKCHAIN DECENTRALIZED VOTING FOR VERIFIED USERS

Piotr Pospiech, Aleksander Marianski and Michal Kedziora

Department of Computer Science and Management, Wroclaw University of Science and Technology, Wroclaw, Poland

ABSTRACT

The paper focuses on introducing a decentralized e-voting scheme that uses blockchain to achieve security and anonymity. A blockchain network based on Ethereum was applied, to provide a decentralized and distributed database based on the Peer-to-Peer architecture. During the implementation, smart contracts were used. Thanks to this, it is possible to code the terms of the contract required to perform the transaction. The proof-of-concept implementation uses the blind signature protocol and encryption with the RSA algorithm. Presented in this paper scheme for blockchain decentralized voting is fully implemented and potential issues are analyzed and discussed.

KEYWORDS

Blockchain, e-voting, Ethereum

For More Details : **https://aircconline.com/ijnsa/V13N5/13521ijnsa02.pdf**

Volume Link : **https://airccse.org/journal/jnsa21_current.html**

REFERENCES

[1] Li Y. Alvarez R., Levin I. Fraud, convenience, ande-voting: howvotingexperience shapes opinions about voting technology, May 2018.

[2] Chaum D. Blind signatures for untraceable payments, 1983.

[3] Maaten E. Towards remote e-voting: Estonian case, January 2004.

[4] Akram R. Markantonakis K. Hardwick F., Gioulis A. E-votingwithblockchain: Ane-voting protocol with decentralization and voter privacy, July 2018.

[5] Chowdhury M. Jabed M. Comparison of e-voting schemes: Estonian and Norwegian solutions,September 2013.

[6] Wang Q. Liu Y. An e-voting protocol based on blockchain, 2017.

[7] Embele K. Ndu A. Awodola O. Mawutor J., Enofe A. Fraud and performance of deposit money banks, May 2019.

[8] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system, October 2008.

[9] Chen M. Jia C. Liu C. Wang Z. Shao W., Li H. Identifying bitcoin users using deep neural network,December 2018.

[10] KSHETRI, Nir; VOAS, Jeffrey. Blockchain-enabled e-voting. IEEE Software, 2018, 35.4: 95-99.

[11] Specter, Michael A., James Koppel, and Daniel Weitzner. "The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in our federal elections." 29th {USENIX} Security Symposium ({USENIX} Security 20). 2020.

[12] Park, Sunoo, et al. "Going from bad to worse: from internet voting to blockchain voting." Journal of Cybersecurity 7.1 (2021):

[13] Kedziora, Michal, and Wojciech Wojtysiak. "Practical Analysis of Traceability Problem in Monero's Blockchain." ENASE. 2020.

[14] Yang, Xuechao, et al. "Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities." Future Generation Computer Systems 112 (2020): 859-874.

[15] Trojanowska, Natalia, et al. "Secure Decentralized Application Development of Blockchain-based Games." 2020 IEEE 39th International Performance Computing and Communications Conference (IPCCC). IEEE, 2020.

[16] Lam, Peter. "From Helios to Voatz: Blockchain Voting and the Vulnerabilities It Opens For The Future.", 2017

[17] Jing H. Zheng Z. Zhang Q., Xu B. Ques-chain: an ethereum based e-voting system, May 2019

[18] Kedziora, Michal, et al. "Anti-Cheat tool for detecting unauthorized user interference in the unity engine using Blockchain." Data-Centric Business and Applications. Springer, Cham, 2020. 191-209.

[19] Kedziora, Michal, Patryk Kozlowski, and Piotr Jozwiak. "Security of Blockchain Distributed Ledger Consensus Mechanism in Context of the Sybil Attack." International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems. Springer, Cham, 2020.

[20] Dimitriou, Tassos. "Efficient, coercion-free and universally verifiable blockchain-based voting." Computer Networks 174 (2020): 107234

[21] Pospiech, Piotr, Aleksander Marianski, and Michal Kedziora. "Blockchain Decentralized Voting for Verified Users with a Focus on Anonymity." CS & IT Conference Proceedings. Vol. 11. No. 8. CS & IT Conference Proceedings, 2021.

CONSTRUCTING THE 2-ELEMENT AGDS PROTOCOL BASED ON THE DISCRETE LOGARITHM PROBLEM

Tuan Nguyen Kim[1], Duy Ho Ngoc[2] and Nikolay A. Moldovyan[3]

[1]Faculty of Information Technology - Duy Tan University, Da Nang 550000, Vietnam
[2]Department of Information Technology, Ha Noi, Vietnam
[3]St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, St. Petersburg, Russia

ABSTRACT

It is considered a group signature scheme in frame of which different sets of signers sign electronic documents with hidden signatures and the head of the signing group generates a group signature of fixed size. A new mechanism for imbedding the information about signers into a group signature is proposed. The method provides possibilities for reducing the signature size and to construct collective signature protocols for signing groups. New group signature and collective signature protocols based on the computational difficulty of discrete logarithm are proposed.

KEYWORDS

Groupdigital signature, Collective digital signature, difficult computational problems, Signing group.

For More Details : **https://aircconline.com/ijnsa/V13N4/13421ijnsa02.pdf**

Volume Link : **http://airccse.org/journal/jnsa21_current.html**

REFERENCES

[1] Shah F., Patel H.,"A Survey of Digital and Group Signature", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.6, P. 274-278, (2016).

[2] Camenisch J.L., Piveteau J.M., Stadler M.A.,"Blind Signatures Based on the Discrete Logarithm Problem", Advances in Crypology – EUROCRYPT'94 Proc, Lecture Notes in Computer Science. Springer Verlang, Vol. 950,P. 428–432, (1995).

[3] Moldovyan A.A., Moldovyan N.A.,"Blind Collective Signature Protocol Based on Discrete Logarithm Problem",Int. Journal of Network Security, Vol. 11, No. 2, P. 106–113, (2010).

[4] Qi Su, Wen-Min Li, "Improved Group Signature Scheme Based on Quantum Teleportation", International Journal of Theoretical Physics, Vol. 53, No. 4, P. 1208, (2016).

[5] Alamélou Q, Blazy O, Cauchie S., Gaborit Ph.,"A code-based group signature scheme", Designs, Codes and Cryptography, Vol. 82, No 1-2, P. 469–493, (2017).

[6] San Ling, Khoa Nguyen, Huaxiong Wang, "Group signature from lattices: simpler, tighter, shorter, ring-based", Proc. of 18th IACR International Conference on Practice and Theory in Public-Key Cryptography,P.427-449, (2015).

[7] Moldovyan N.A,"Blind Signature Protocols from Digital Signature Standards", Int. Journal of Network Security, Vol. 13, No. 1, P. 22–30, (2011).

[8] Duy H.N., Binh D.V., Minh N.H., Moldovyan N.A. "240-bit collective signature protocol in a non-cyclic finite group", 2014 International conference on Advanced Technologies for Communications (ATC),Hanoi, P. 467 – 470, (2014). (DOI 10.1109/ATC.2014.7043433)

[9] Moldovyan A.A., Moldovyan N.A., "Group signature protocol based on masking public keys", Quasigroups and related systems, Vol. 22, P. 133-140, (2014).

[10] Moldovyan N.A., Nguyen Hieu Minh, Dao Tuan Hung, Tran Xuan Kien,"Group Signature Protocol Based on Collective Signature Protocol and Masking Public Keys Mechanism", International Journal of Emerging Technology and Advanced Engineering, Vol. 6, Issue. 6, P. 1-5, (2016).

[11] Phong Q. Nguyen, Jiang Zhang, Zhenfeng Zhang, "Simpler efficient group signature from lattices", Proc. of 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, P.401-426, (2015).

[12] Berezin A. N., Moldovyan N. A., Shcherbakov V. A.,"Cryptoschemes Based on Difficulty of Simultaneous Solving Two Different Difficult Problems", Computer Science Journal of Moldova, Vol. 21,No.2(62), P. 280-290, (2013).

AUTHORS

Tuan Nguyen Kim was born in 1969, received B.E, and M.E from Hue University of Sciences in 1994, and Hanoi University of Technology in 1998. He has been a lecturer at Hue University since 1996. From 2011 to the present (2021) he is a lecturer at School of Computer Science, Duy Tan University, Da Nang, Vietnam. His main research interests include Computer Network Technology and Information Security.

Duy Ho Ngoc was born in 1982. He received his Ph.D. in Cybersecurity in 2007 from LETI University, St. Petersburg, Russia Federation. He has authored more than 45 scientific articles in cybersecurity.

Nikolay A. Moldovyan is an honored inventor of Russian Federation (2002), a laboratory head at St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, and a Professor with the St. Petersburg State Electrotechnical University. His research interests include computer security and cryptography. He has authored or co-authored more than 60 inventions and 220 scientific articles, books, and reports. He received his Ph. D. from the Academy of Sciences of Moldova (1981).