IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10343

Preventing Cyber Attacks: A Multi-Layered Approach

Swapnil B. Kolambakar[1], Dr. Praveen Kumar[2]

Research Scholar, School of Science & Technology, The Glocal University, Saharanpur (U.P) [1]

Associate Professor, School of Science & Technology, The Glocal University, Saharanpur (U.P) [2]

Abstract: Cybersecurity threats have become increasingly prevalent in recent years, causing significant damage to businesses, individuals, and governments. As a result, preventing cyber attacks has become an important issue. This paper examines different ways to prevent cyber attacks and the importance of a multi-layered approach. It highlights the need for education, software updates, secure configurations, network segmentation, access controls, and incident response plans as key components of a comprehensive prevention strategy. This paper also discusses emerging technologies that can help in the fight against cybercrime, such as artificial intelligence and blockchain.

INTRODUCTION

Cyber attacks have been increasing in frequency and complexity over the years. Hackers are finding new and creative ways to breach security measures and gain access to sensitive information.

These attacks can cause significant financial losses, damage to reputation, and legal liabilities for businesses and individuals. Governments are also at risk, with critical infrastructure and sensitive data under constant threat. It is, therefore, crucial to implement measures to prevent cyber attacks. In this paper, we examine the different approaches to preventing cyber attacks and the importance of a multi-layered strategy.

Education:

Education is an essential component of preventing cyber attacks. It is essential to train employees and individuals on safe browsing practices, email safety, and social engineering attacks. Most cyber attacks occur due to human error, making education a vital first step in preventing them. Training should include password hygiene, recognizing phishing emails, and avoiding public Wi-Fi networks. Organizations should also establish policies that promote secure online behavior.

Software Updates:

Software vulnerabilities are a significant avenue for cybercriminals to exploit. Hackers can use unpatched software to gain access to sensitive data or install malware. Organizations should, therefore, ensure that they apply software updates promptly. Software developers regularly release patches to fix vulnerabilities, and organizations should have an automated update mechanism in place to ensure that they are applied promptly.

Secure Configurations:

Configuring software and systems securely is another essential step in preventing cyber attacks. Organizations should ensure that software and systems are configured securely from the outset. For example, disabling unused ports and protocols, implementing two-factor authentication, and disabling remote access to critical systems.

Network Segmentation:

Network segmentation is the process of dividing a network into smaller subnetworks, each with its security measures. This strategy limits the impact of a cyber attack by preventing the attacker from moving laterally through the network. It also makes it easier to identify and contain an attack. Network segmentation is an essential component of a comprehensive cybersecurity strategy.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10343

Access Controls:

Access controls are critical in preventing unauthorized access to sensitive data. Organizations should implement strong access controls, including limiting user privileges to the minimum required to perform their job functions. Organizations should also implement role-based access controls, which allow access based on the user's job function.
Incident Response Plan:

An incident response plan is a set of procedures for responding to a cyber attack. It should include procedures for identifying and containing the attack, restoring systems and data, and communicating with stakeholders. Organizations should test their incident response plan regularly to ensure that it is effective and up-to-date.

Emerging Technologies:

Emerging technologies such as artificial intelligence (AI) and blockchain are showing promise in the fight against cybercrime. AI can be used to detect and respond to cyber attacks in real-time, allowing organizations to respond quickly. Blockchain can help secure critical infrastructure and sensitive data by providing an immutable and tamper-proof record of transactions.

Parameters used in SecureAuthKey Key agreement algorithm is mentioned below

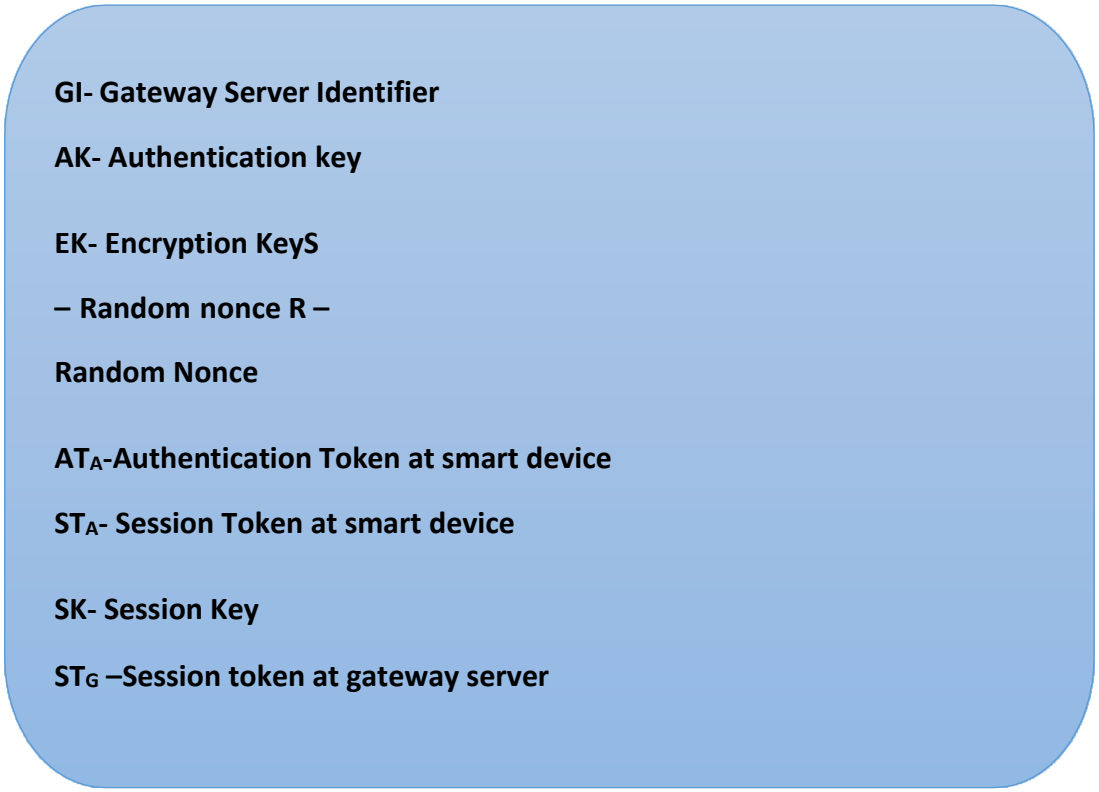

Figure 1 : Parameters in SecureAuthKey Key agreement Algorithm

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10343

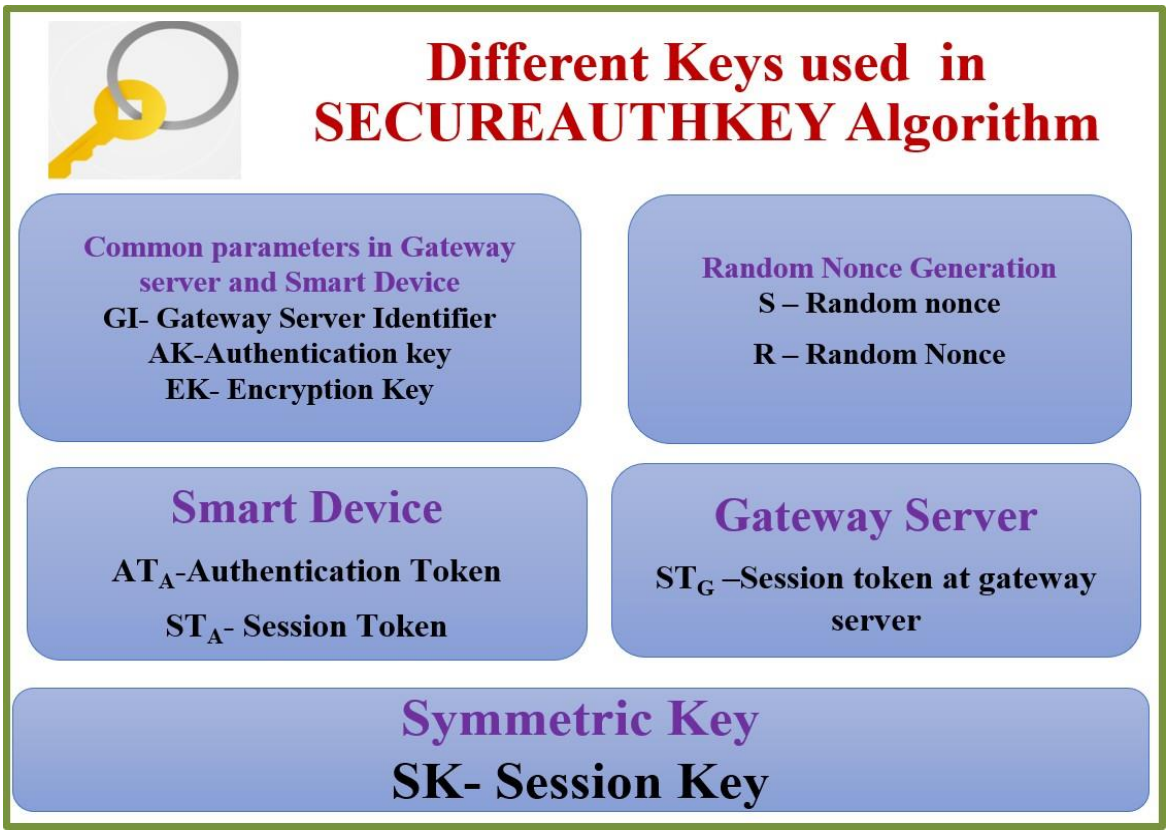

Figure 2 : Keys used in SecureAuthKey Algorithm

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10343

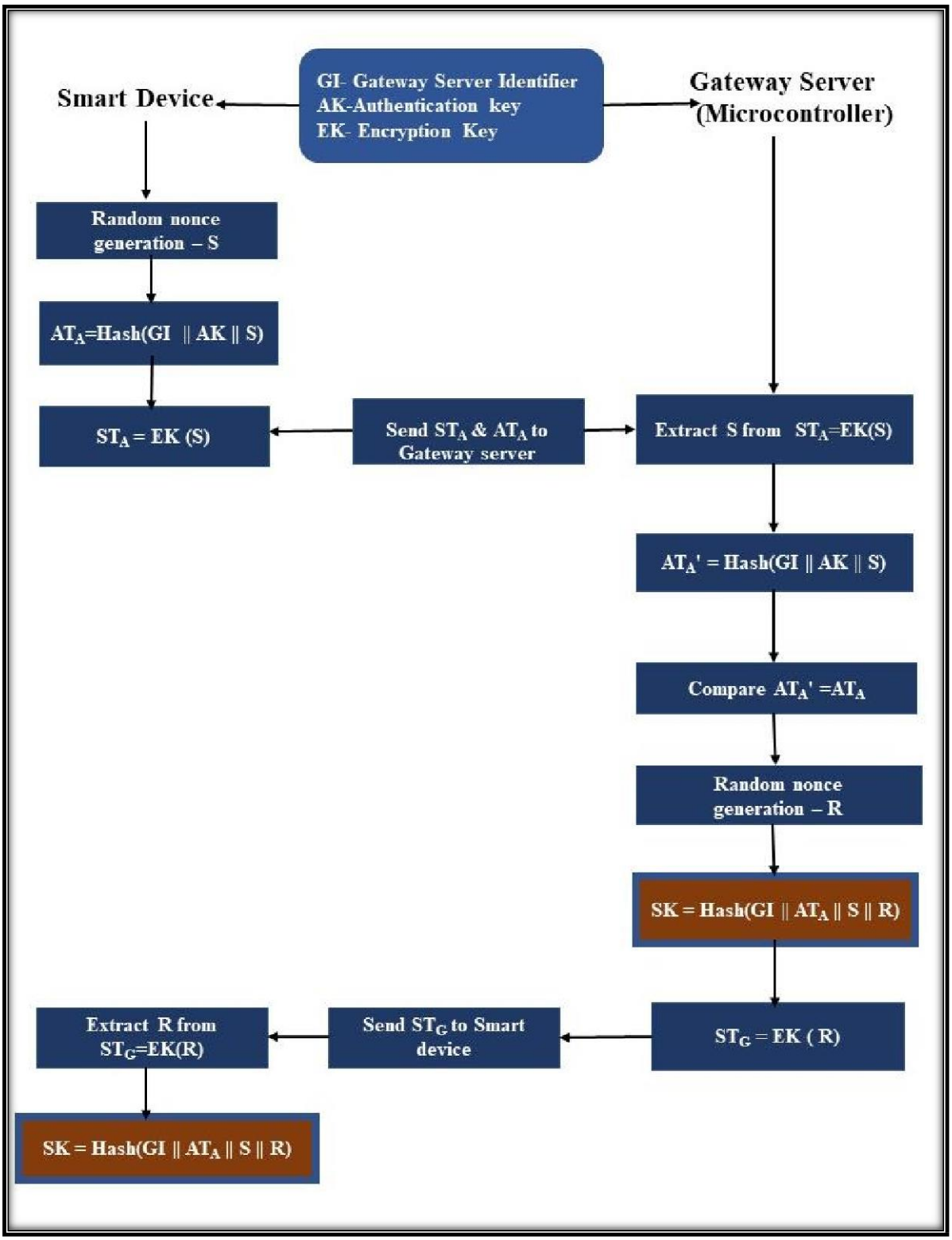

Figure 3: SecureAuthKey : A Session Key generation Algorithm

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10343

CONCLUSION

Preventing cyber attacks requires a multi-layered approach that includes education, software updates, secure configurations, network segmentation, access controls, and incident response plans. Emerging technologies such as AI and blockchain are showing promise in the fight against cybercrime. Organizations should take a proactive approach to cybersecurity and implement these measures to reduce the risk of a cyber attacks.

REFERENCES

[1] Akhgar, S., Yates, B., 2013. Strategic Intelligence Management, 1st Edition, Butterworth-Heinemann, 9780124071919, 56-255. Axa Corporate Solutions official web-site, description available at http://www.axa-corporatesolutions.com (website visited on July 15, 2014).

[2] Cenzic, 2014 Cenzic, Application Vulnerability Trends Report: 2014, description available at: www.cenzic.com (website visited on January 03, 2015). CISCO, 2014. CISCO 2014 Annual Security Report, description available at: www.cisco.com (website visited on January 04, 2015). CISCO, 2013. CISCO 2013 Annual Security Report, description available at: www.cisco.com (website visited on January 04, 2015). CISCO, 2012.

[3] CISCO 2012 Annual Security Report, description available at: www.cisco.com (website visited on January 04, 2015). Google Project Zero blog, description available at: http://googleprojectzero.blogspot.co.uk/2014/07/announcing-project-zero.html (website visited on January 10, 2015).

[4] Federal Bureau of Investigation, 2013. 2013 Internet Crime Report, description available at: http://www.fbi.gov/stats-services/publications (website visited on January 04, 2015).

[5] Federal Bureau of Investigation, 2012. 2012 Internet Crime Report, description available at: http://www.fbi.gov/stats-services/publications (website visited on January 04, 2015).

[6] Federal Bureau of Investigation, 2011. 2011 Internet Crime Report, description available at: http://www.fbi.gov/stats-services/publications (website visited on January 04, 2015). FireEye company, 2012.

[7] Li, C., Ge, J., Li, Z., Huang, L., Yang, H., Luo, B.: Monitoring interactions across multi business processes with token carried data. IEEE Trans. Serv. Comput. 1 (2018)

[8] Liu, L., De Vel, O., Han, Q., Zhang, J., Xiang, Y.: Detecting and preventing cyber insider threats: a survey. IEEE Commun. Surv. Tutorials **20**(2), 1397–1417 (2018)

[9] Macak, M., Kruzelova, D., Chren, S., Buhnova, B.: Using process mining for git log analysis of projects in a software development course. Educ. Inf. Technol. 1–31 (2021)

[10] Macak, M., Kruzikova, A., Daubner, L., Buhnova, B.: Simulation games platform for unintentional perpetrator attack vector identification. In: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, pp. 222–229 (2020)

[11] Macak, M., Vanat, I., Merjavy, M., Jevocin, T., Buhnova, B.: Towards process mining utilization in insider threat detection from audit logs. In: 7th International Conference on Social Networks Analysis, Management and Security, pp. 1–6 (2020)

[12] Mardani, S., Shahriari, H.R.: A new method for occupational fraud detection in process aware information systems. In: 10th International ISC Conference on Information Security and Cryptology, pp. 1–5 (2013)

[13] Myers, D., Radke, K., Suriadi, S., Foo, E.: Process discovery for industrial control system cyber attack detection. In: ICT Systems Security and Privacy Protection, pp. 61–75. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-58469-0_5

[14] Myers, D., Suriadi, S., Radke, K., Foo, E.: Anomaly detection for industrial control systems using process mining. Comput. Secur. **78**, 103–125 (2018)

[15] Reinkemeyer, L.: Process Mining in Action: Principles. Use Cases and Outlook, Springer Nature (2020)

[16] Rojas, E., Munoz-Gama, J., Sepulveda, M., Capurro, D.: Process mining in healthcare: a literature review. J. Biomed. Inform. **61**, 224–236 (2016)

[17] Rosa, N.S., Campos, G.M., Cavalcanti, D.J.: Lightweight formalisation of adaptive middleware. J. Syst. Archit. **97**, 54–64 (2019)

[18] Rozinat, A., van der Aalst, W.M.: Conformance checking of processes based on monitoring real behavior. Inf. Syst. **33**(1), 64–95 (2008)

[19] Sahlabadi, M., Muniyandi, R., Shukur, Z.: Detecting abnormal behavior in social network websites by using a process mining technique. J. Comput. Sci. **10**, 393–402 (2014)

[20] Salnitri, M., Alizadeh, M., Giovanella, D., Zannone, N., Giorgini, P.: From security-by-design to the identification of security-critical deviations in process executions. In: International Conference on Advanced Information Systems Engineering, pp. 218–234. Springer (2018). https://doi.org/10.1007/978-3-319-92901-9_19

[21] dos Santos Garcia, C., Meincheim, A., Junior, E.R.F., Dallagassa, M.R., Sato, D.M.V., Carvalho, D.R., et al.: Process mining techniques and applications - a systematic mapping study. Expert Syst. Appl. **133**, 260–295 (2019)

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10343

[22] Senator, T.E., Goldberg, H.G., Memory, A., Young, W.T., Rees, B., Pierce, R., et al.: Detecting insider threats in a real corporate database of computer usage activity. In: Proceedings of the 19th ACM/SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 1393–1401 (2013)
[23] Talamo, M., Povilionis, A., Arcieri, F., Schunck, C.H.: Providing online operational support for distributed, security sensitive electronic business processes. In: International Carnahan Conference on Security Technology, pp. 49–54 (2015)
[24] Viticchié, A., Regano, L., Basile, C., Torchiano, M., Ceccato, M., Tonella, P.: Empirical assessment of the effort needed to attack programs protected with client/server code splitting. Empirical Softw. Eng. **25**(1), 1–48 (2020)
[25] Williams, R., Rojas, E., Peek, N., Johnson, O.A.: Process mining in primary care: a literature review. Stud. Health Technol. Inform. **247**, 376–380 (2018)
[26] Yen, T.F., et al.: Beehive: large-scale log analysis for detecting suspicious activity in enterprise networks. In: Proceedings of the 29th Annual Computer Security Applications Conference, pp. 199–208. ACM (2013)
[27] Young, W.T., Goldberg, H.G., Memory, A., Sartain, J.F., Senator, T.E.: Use of domain knowledge to detect insider threats in computer activities. In: 2013 IEEE Security and Privacy Workshops, pp. 60–67 (2013)
[28] van Zelst, S.J., van Dongen, B.F., van der Aalst, W.M.: Event stream-based process discovery using abstract representations. Knowl. Inf. Syst. **54**(2), 407–435 (2018)
[29] Zerbino, P., Aloini, D., Dulmin, R., Mininno, V.: Process-mining-enabled audit of information systems: methodology and an application. Expert Syst. Appl. **110**, 80–92 (2018)
[30] Zhou, X., Jin, Y., Zhang, H., Li, S., Huang, X.: A map of threats to validity of systematic literature reviews in software engineering. In: 23rd Asia-Pacific Software Engineering Conference, pp. 153–160 (2016)