ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

A Literature Review on Cyber Security Automation for Controlling Distributed Data

Ujjwala D. Deore[1], Vijaya Waghmare[2]

M. E. Student, Dept. of Computer Engineering, Saraswati College of Engineering, Kharghar, Navi Mumbai, Maharashtra, India

Professor, Dept. of Computer Engineering, Saraswati College of Engineering, Kharghar, Navi Mumbai, Maharashtra, India

ABSTRACT: In the today computer engineering era data protection and cyber security are becoming challenge for scientist. Cyber security is the activity of protection of information and information systems like network, computers, data base, data centre and application. Most of the government and private organizations are trying to protect our data and information from cyber terrorist or hackers. Cybersecurity plays important role in information system as well as data sharing. For the protection of important information and data most of the software was developed by many organization using different techniques. In this paper we are collecting literature data regarding cyber security as well as different automation software for securing our data. For developing software many techniques are used like one time password, event log analysis, malicious attack detection, and virtualization.

KEYWORDS: Cyber security, event log analysis, malicious attack, one time password.

I. INTRODUCTION

In information technology data protection or information security is one of the great challenges for the world. In IT industries data security is one of the serous issue. But in whole world internet is one of the important and faster growing things for business development as well as in different private and government organization [1]. Because of the internet use in different areas like banking, government department, ecommerce, communications, national defense, entertainment, finance firm, private organization for various functions. Because of the most use of internet for all above functions in our life chances of the attack from attacker on our information are higher [2]. For protection of our data we are developing different techniques in the area of cyber security term. Cyber security is one of the most important term in computer and information technology. Protection of our data or critical information is very essential for everyone. This is technology age, everybody wants technology in its hand to solve his problem, simplify work or increase efficiency of work. But because of the tremendous use of internet in every field the protection and privacy also get affected. For the protection of our privacy and data from attacker and hacker we are developing different techniques and software. From year 2006 the privacy and personal data protection level increases to public concern [3]. In information technology data protection is challenge today in the world. Data base goes through the different attacks [4] like direct attack or indirect attack. These attacks also classified into active attack and passive attack [5]. In this are attacker or hacker are plays there role to attack or hack the information. Some times they attack on network as well as hack all information or our sites.

Data sharing is also challenge for government as private organization. Most of the information was hacked at the time of sharing personal or government or official information. Different techniques are developed and used by scientist for the protection of information from attacker. In this technique attack detection, one time password, cryptographic techniques are used. We are searching different papers for the new idea development. In cyber security data protection is very important on this idea we think to develop new automation technique or software for our data security. For that purpose we are using base paper [6] in which virtual machine concept used distributed cyber security automation frame work. The malicious injection attack [7] against smart grid detected by using event log analysis in cyber security. We are listed some techniques for developing new software like user virtualization, Event log analysis

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

one time password and malicious attack detection. In this paper we discussed most of the literature who work automation and cyber security for data protection.

We also reports some literature related to privacy protection. T. Manirathnam [8] reported frame work for the protection of personalized web search. In this paper they also reported two new greedy algorithms GreedyDP and GreedyIL. Lidan Shou etl. [9] described about the supporting privacy protection in personalized web search. In this paper they explained the above two algorithm how increased the search efficiency and support for privacy protection. N. Dewangan [10] explained hierarchical user profiles for privacy protection. A. Ukande1, etl. [11] described implementation of new algorithm String Similarity Match Algorithm (SSM Algorithm) for improving the better search quality results. This was help for securing users profiles.

II. LITERATURE REVIEW

In this paper we disclosed or summarized various articles or journals regarding the cyber security and privacy protection of data or information. For the purpose of security we divided the references topic wise. First we discuss regarding attack, attacker and hackers. In second point we discuss regarding One Time Password which helps secure our account as well as our data or information. The third section explained about different techniques for attack detection and thoroughly about malicious attack detection. Section four described the user virtualization can help day to day life and save our efforts regarding space and efficient working.

2.1 Attacker

Attacker means a person get control of other system or network and destroy. Examples like hacker, adversary in terms of computer security and algorithm. In literature different types of attacks reported as active and passive as well as insider and outsider attack. For the preventation of attack various methods or techniques developed by researcher. S. Shrivastava [12] described about rushing attack and its preventation techniques for reducing harmful effect on network. N. Nigam etl. [13] explained various different techniques using threads, prevent from wormhole attack.

2.2 One time password

For all online shopping or transaction one time password is important part for the security. Same thing for data protection or information protection we can use one time password system for account authentification or file opening. In this area most of the researcher was work, we are listed below. E. Kalaikavitha etl. [14] reported the encrypted OTP system how helps in our routine life as well as how it work from user to mobile and authentification system. They are also explained different methods for OTP generation as well as mathematical formulae for the generation of OTP. A. Shesashaayee [15] explained regarding encrypted OTP in mobile system how we ca n protected our data. Generated OTP was send by SMS to the user on mobile for the authentification of his account. For mobile banking or internet banking it is very important. In this paper they also described different threats occur in OTP generation and transaction as well as different techniques for securing OTP.

T. Saini [16] described the generation of OTP system. Every time of transaction a new password generation for the transaction by using genetic algorithm with elliptic curve cryptography. It is very important when we lost our old password we need not to worry. We can get new password every time which increase the security of our system or operation. P. Ahlawat [17] described in his paper different techniques for secure our OTP from hackers. Also solve the synchronization issues when access OTP. In other literature regarding OTP like Y. Huang [18] described new method for the OTP generation by changing calculation method. K. W. Hussein [19] explained the OTP based on the unique factor and biometric in which novel authentification scheme used. The generated OTP has unique no and biometric authentification which increase the security of our data or operation. Some literature M.H. Khan [20] explained OTP generation using SHA algorithm which help generate new OTP every time. B.K. Kushwaha [21] gives new approach to OTP authentification which gives extra security to our OTP. In this paper studied graphical password and shoulder suffering problem also explained.

2.3. Malicious Attack Detection

Various attacks are observed in internet or information as well as on network system. They are detected and identified by different methods. Different techniques or methods or systems are developed for protection from all these

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

attack. Malicious attack is one of the attacks listed here which detected and prevented by different method. In this paper we are collected some literature regarding malicious attack detection by different techniques listed as below.

F. N. Abdesselam [22] described an efficient method for detect and avoid wormhole attacks in the OLSR protocol. The detection mechanism of wormhole explained in this paper. The solution given in this paper has very good advantage against previous methods. S. Jain [23] also explains different methods for identify and isolating wormhole without using any cryptographic method. In this paper Y. Chun Hu [24] explained a general mechanism, for the detection and protection from wormhole which is called as packet lashes. Implementation of this system also described in this paper. Saranya, T. etl. [25] explained new system for the protection of mobile by using new malicious attack detection method. This method developed for android system using algorithm. J. Puthenkovilakam [26] described the malicious attack detection using real time operating system environment.

Some of the researcher C. Danai [27] explained different program from vulnerabilities and attacks. Z. Xin [28] described Ack-based adversary identification (AAI) detection mechanism in his paper which involves to define which data packets to acknowledge, and which intermediate nodes should respond to the ack request sent by the source.

2.4 User Virtualization

In this internet and computer world virtualization is very important. Virtualization has done by different methods and technologies. In 1960 first virtual machine prepared by IBM and in 1998 first virtualization done of x86 by VMware. In virtualization different types are observed like Emulation, Full/Native virtualization and same hardware CPU. We are listed some literature which explained about user virtualization.

R. P. Goldberg [29] proposed different literature about the virtual machine. In this paper author explained how made virtual machine and different techniques for the preparation of virtual machine. G. J. Popek [30] described requirements for the third generation virtual machine architectures. M. Rosenblum [31] explained how we can monitor the virtual machines in day to day working. Z. J. Estrada [32] described how we can check performance comparison and tuning of virtual machine for sequence alignment software. In some survey by Susanta Nanda and Tzi-cker Chiueh also explain all architecture and working about virtualization technologies. O. Agesen etl. [33] described different software techniques to avoid virtualization exist. B. D. Payne etl. [34] explained regarding the security of virtual machine in which they make one architecture for monitoring virtual machine.

III. CONCLUSIONS

In the cyber security are many scientist are developed various techniques and software. The developed techniques by researcher they used different algorithms for the privacy protection of our data and information. In this paper we summarized the literature for protection for our data and information as well as protection of our privacy. We also described attacker's literature and different types of attack. In another section we are introducing one time password protection (OTP) and user virtualization. In another section we discuss malicious attack detection. All above literature summery help for researcher to design new technique and software's

REFERENCES

1. Ravi Sharma, 'Study of Latest Emerging Trends on Cyber Security and its challenges to Society', International Journal of Scientific & Engineering Research, Vol. 3, Issue 6, 2012.
2. A. D. Sofaer, David Clark, and W. Diffie, 'Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy', http://www.nap.edu/catalog/12997.html, 'Cyber Security and International Agreements, Internet Corporation for Assigned Names and Numbers', pp.185-205.
3. T. Rajaretnam , ' The Society of Digital Information and Wireless Communications (SDIWC),International Journal of Cyber-Security and Digital Forensics', Vol.1, Issue 3, pp. 232-240, 2012.
4. Emil Burtescu, 'Database Security-attack and control method's', Journal of Applied Quantitative Methods, Vol. 4, no. 4, 2009.
5. S. Kulkarni, S. Urolagin, 'Review of Attacks on Databases and Database Security Techniques', International Journal of Emerging Technology and Advanced Engineering, Vol. 2, Issue 11, 2012.
6. G. Rush, Daniel R. Tauritz, 'DCAFE: A Distributed Cyber Security Automation Framework for Experiments', 2014 IEEE 38th Annual International Computers, Software and Applications Conference Workshops.
7. Jinping Hao, Robert J. Piechocki, Dritan Kaleshi, Woon Hau Chin and Zhong Fan, 'Optimal malicious attack construction and robust detection in Smart Grid cyber security analysis', 2014 IEEE International Conference on Smart Grid Communications, pp. 836-841, 2014.
8. T. Manirathnam, R. Devi, Dr. A. Muthukumaravel, 'Supporting privacy protection in personalized web search', International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 6, pp 326-330, 2014.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

9. Lidan Shou, He Bai, Ke Chen, and Gang Chen, 'Supporting Privacy Protection in Personalized Web Search', IEEE transactions on knowledge and data engineering, Vol.26, no.2, 2014.
10. Neha Dewangan, Rugraj, 'Supporting privacy protection in personlized web search-A review', International Journal of Computer Engineering and Applications, Vol. VIII, Issue II, pp76-82. 2014.
11. Archana Ukande1, Nitin Shivale, 'Supporting privacy protection in personalized web search with secured user profile', International Journal of Science and Research, Vol. 3 Issue 12, pp. 2179-2182, 2014.
12. S. Shrivastava, 'Rushing Attack and its Prevention Techniques' International journal of Application and innovation in engineering and management, Vo. 2, Issue 4, pp. 453-456, 2013.
13. Nidhi Nigam, Vishal Sharma, 'A comprehension on Wormhole Attack prevention technique using THREADS in MANET', International Journal of Computer Science & Communication Networks, Vol. 2, Issue 4, pp. 531-535, 2014.
14. E. Kalaikavitha, J Gnanselvi, 'Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology', Research Inventy: International Journal of Engineering and Science, Vol. 2, Issue 10, pp. 14-17, 2013.
15. D. A. Shesashaayee, D. Sumathy, 'OTP Encryption Techniques in Mobiles for Authentication and Transaction Security', International Journal of Innovative Research in Computer and communication engineering, Vol. 2, Issue 10, 2014.
16. T. Saini, 'One Time Password Generator System', International Journal of advanced research in computer science and software Engineering, Vol. 4, Issue 3, 2014.
17. P. Ahlawat, R. Nandlal, 'A Survey: Novel Approach Secure Authentication Technique by One Time Password using Mobile SMS', International Journal of Enhanced Research in Science Technology & Engineering, Vol. 4, Issue 6, pp. 145-148, 2015.
18. Y. Huang, Z. Huang, H. Zhao, X. Lai, 'A new One-time Password Method', IERI Procedia 4, pp. 32-37, 2014.
19. K. W. Hussein, N. F. Mohd. Sani, R. Mahmod, Mohd. T. Abdullah, 'Active Authentication by one Time Password Based on Unique Factor and Behavioral Biometric', International Journal of Computer Networks and Security, Vol. 23, Issue 2, pp. 1138-1141, 2015.
20. M.H. Khan, 'OTP Generation using SHA', International Journal on Recent and Innovation Trends in Computing and Communication, Vol. 3, Issue 4, pp. 2244-2245.
21. A. K. Kushwaha, 'A Survey: Novel Approach Secure Authentication Technique by One Time Password using Mobile SMS', Journal of Global Research in Computer Science, Vol. 3, No. 11, 2012.
22. F. N. Abdesselam, 'LITEWORP: Detection and Isolation of the Wormhole Attack in Static Multi hope Wireless Networks', The International Journal of Computer and Telecommunications Networking, Vol. 51, Issue 12, pp 3750-3772, 2007
23. S. Jain, 'Mitigation of Control and data traffic attacks in wireless ad-hoc and sensor networks' IEEE, Vol. 6, Issue 3, pp. 344-362.
24. Y. Chun Hu, 'WAP: Wormhole Attack Preventation Algorithm in Mobile Ad Hoc Networks', IEEE International conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, SUTC' 08. pp. 343-348, 2008.
25. Saranya, T., Shalini, A., Kanchana, A., International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3, pp. 3577-3584, 2014.
26. J. Puthenkovilakam, ' Malicious attack detection and prevention in ad hoc network based on real time operating system environment', International Journal of Research in Engineering and Technology Vol. 02, Issue 06, pp. 1043-1046, 2013.
27. C., Danai, W., Qiang, W., Tilam. 'Attack on network infrastructure', In proceeding of Twentieth IEEE International Conferences on Computer communications and Networks (ICCCN), 2011.
28. Z. Xin, P., Adrin. Packet-dropping adversary identification for data plane security. In Proceeding of the 2008 ACM CoNEXT Conference (New York, NY, USA, 2008), CoNEXT'08, ACM, pp.24.1-24.12, 2008.
29. R. P. Goldberg, 'Survey of virtual machine research', Computer, vol. 7, no. 6, pp. 34-45, 1974.
30. G. J. Popek and R. P. Goldberg, 'Formal requirements for virtualizable third generation architectures', pp. 121-128, 1973.
31. M. Rosenblum and T. Garfinkel, 'Virtual machine monitors: Current technology and future trends', Computer, vol. 38, no. 5, pp. 39-47, 2005.
32. Z. J. Estrada, F. Deng, Z. Stephens, C. Pham, Z. Kalbarczyk, and R. Iyer, 'Performance comparison and tuning of virtual machines for sequence alignment software', Scalable Computing: Practice and Experience, vol. 16, no. 1, 2015.
33. O. Agesen, J. Mattson, R. Rugina, and J. Sheldon, 'Software techniques for avoiding hardware virtualization exits', in USENIX Annual Technical Conference, pp. 373-385, 2012.
34. A. D. Payne, M. Carbone, M. Sharif, and W. Lee, 'Lares: An architecture for secure active monitoring using virtualization', In Security and Privacy, SP 2008. IEEE Symposium on. IEEE, 2008, pp. 233-247, 2008.