International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 5, October 2019, pp. 3862~3871
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i5.pp3862-3871

Reviewing effectivity in security approaches towards strengthening internet architecture

Vidya M.S[1], Mala C Patil[2]
[1]Department of Computer Science and Engineering, BMS Institute of Technology and Management (BMSIT & M), India
[2]Department of Computer Science, COHB, University of Horticultural Sciences, India

Article Info

Article history:

Received Jun 22, 2018
Revised Apr 1, 2019
Accepted Apr 10, 2019

Keywords:

Future internet architecture
Intrusion
Online threats
Security
Vulnerability
Web 2.0

ABSTRACT

The usage of existing Internet architecture is shrouded by various security loopholes and hence is highly ineffective towards resisting potential threats over internet. Hence, it is claimed that future internet architecture has been evolved as a solution to address this security gaps of existing internet architecture. Therefore, this paper initiates its discussion by reviewing the existing practices of web security in conventional internet architecture and has also discussed about some recent solutions towards mitigating potentially reported threats e.g. cross-site scripting, SQL inject, and distributed denial-of-service. The paper has also discussed some of the recent research contribution towards security solution considering future internet architecture. The proposed manuscripts contributes to showcase the true effectiveness of existing approaches with respect to advantages and limitation of existing approaches along with explicit highlights of existing research problems that requires immediate attention.

Corresponding Author:

Vidya M. S,
Department of Computer Science & Engineering,
BMS Institute of Technology and Management (BMSIT & M),
Bengaluru, India.
Email: research2015ns@gmail.com

1. INTRODUCTION

There are various applications running on current internet architecture that offers wide range of communication and data exchange at present times. Although, millions of users and their adopted applications run over existing internet architecture, it is never safe from all the potential threats arising every day [1]. The existing version of internet architecture has been serving since 40 years for all communication needs and has also contributed to many successful implementation of communication protocols. The security system of existing internet architecture tremendously suffers from various critical challenges with consistent changes in the internet technology. At the same time, mobile networks as well as cloud computing has also boosted the need of an efficient security system over the web-based services as well as application [1]. Majority of the application of present times are supported by mobile technologies where tremendous amount of data is generated, stored, as well as queried. There are also various studies that has emphasized on the cloud security [2-4]; however, challenges are yet to be resolved. Majority of the reported and studied attacks over the existing interne architecture are related to financial factors or privacy factors [5-9]. However such forms of security issues are arising from different forms of infinite list of web-based attacks that keeps on evolving almost all days. Existing researchers have also evolved up with certain level of solutions towards such problems in existing internet architecture. Some of the newly evolving solutions are network virtualization [10], software defined network [11], named data networking [12], etc.

However, the above mentioned techniques are just in nascent stage of research that requires more level of investigation with the rising demands of distributed network system as they are no more potential

especially with respect to security factor. There are various reasons behind this viz. i) they use IP network that is host centric and cannot cater up any form of distributed communication system, which is the need of present age, ii) the policy of IP address is encountering exhaustion with the exponential rise of users, iii) no inclusion of security attributes (except IPv6 that offers distinct and unique IP addresses to promote security), iv) highly non-flexible posing difficult to incorporate new operation [13]. Therefore, web security has become one of the essential concerns among the network communities [14-16] and this leads to the formation of Future Internet Architecture (FIA) [17]. One of the essential parts of FIA is its security inclusion. Funded by National Science Foundation (NSF) in United States, FIA project has been initiated that has transformed the existing host centric web design to content centric architecture [18] with more capability to perform an effective traffic management. Some of the reputed projects of FIA are Mobility First [19], XIA [20], SCION [21], COAST [22], etc. However, work carried out by Ding et al. [23] has reported significant level of problems associated with almost all the evolved projects of NSF. This leads to a conclusion that there is a need to investigate the security demands of FIA right from gauging strength of existing web security approaches.

Therefore, this paper reviews the existing system of web security practiced over present state of internet architecture and then discusses about some of the recent research approaches towards securing future internet architecture followed by investigation of unexplored problems in this domain of research. The organization of the paper is as following: Section-2 discusses about the security problems associated with the Web followed by discussion of different approaches to ensure web security in Section-3. Discussion of approaches towards securing future internet architecture is carried out in Section 4 followed by discussion of unsolved research problems in Section 5.Finally, Section 6 summarizes the findings of the paper.

Security threat evolves in web in various shape and forms with different intensities of attack. There are diversified forms of security threatsreported in existing internet architecture of Web 2.0 and till date there is no full proof solution against mitigating such threat. Figure 1 highlights that there existing research work classifies security tools to resists threat into various forms, where majority are attack specific.

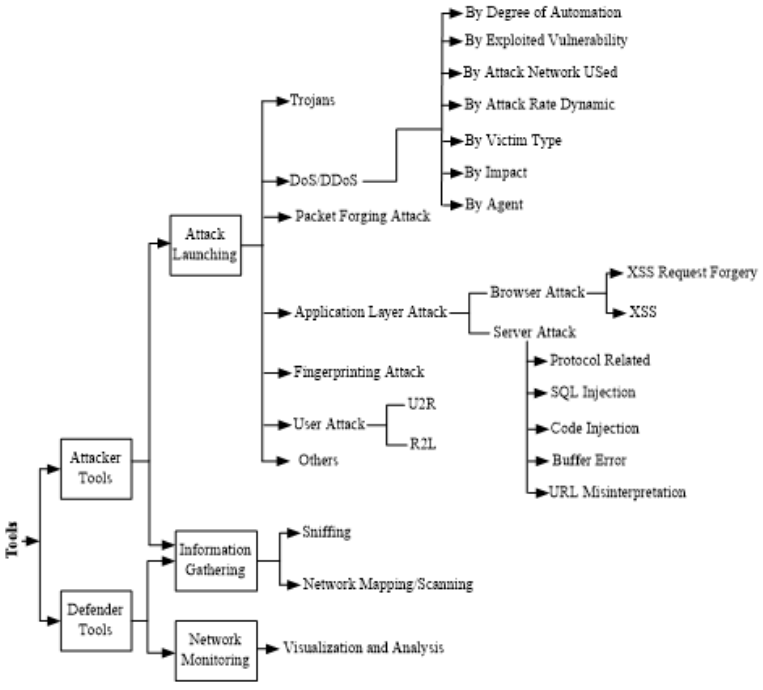

Figure 1. Classification of web-based attacks

All the attacks highlighted above are also anticipated to continue to lead in its enhanced version of internet architecture in future too. The most frequently found internet-based attacks are malware, phishing, SQL injection attack, cross-site scripting, Denial-of-Service, Session Hijacking, Man-in-Middle attack, Credential reuse, etc. In existing system, there are two forms of tools where one is used for attack and another is used for defender. The tools used by attackers are mainly used for launching malicious programs e.g. Trojans, Denial-of-Service, packet forging attack, fingerprinting attack, application layer attack, user attack.

The initiation of Denial-of-Service is carried out by degree of automation, by exploited vulnerability, by attack network used, by attack rate dynamics, by victim type, by impact, and by agent. The application layer attack is again classified into types i.e. browser attack and server attack. The browser attack is again initiated using XSS request while server attack is initiated by protocols, SQL injection, code injection, buffer error, URL misinterpretation. Thetools used by defender mainly user network monitoring tools e.g. visualization and analysis. Interestingly, there is a common tool usage found between attacker and defender i.e. information gathering tool. This tool is used for sniffing and network mapping operation where the intention of attacker is to look for suitable environment of launching attack while intention of defender is to capture the presence of abnormal or vulnerable network condition to report a problem. There is no doubt maximum information is circulated through the web and it becomes the hub of all the attackers too. Unfortunately, existing internet architectures lacks robustness as well as capabilities to identify and prevent all the lethal forms of attacks irrespective of usage of expensive firewall system. There are various researchers e.g. [24] who have already stated the challenges associated with existing cyber security that possible immense threat to existing web users. This leads to evolution of FIA, however, it is still unknown how much existing web security is prepared to be customized for shaping itself to offer maximum security when used with FIA. The next section discusses about existing web security approaches.

Apart from the above mentioned discussion of threats, there exists different other forms of attacks, refer Figure 2. Out of different other forms of attacks Cross Site Scripting (XSS) is considered to the most lethal threats when it comes to attacking web-based applications. However, there are other forms of attack also that is nearly similar to XSS i.e. Local File inclusion, File Upload, SQL injection, general bypass, etc.

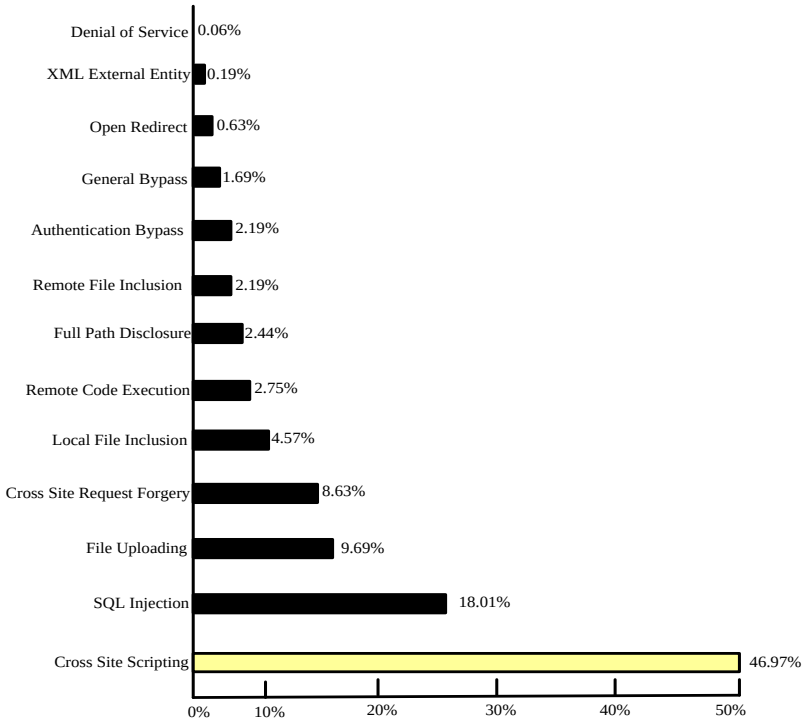

Figure 2 Statistics of web-based attacks

2. APPROACHES ON WEB SECURITY

This section discusses about various approaches reported in the existing literatures towards securing web-based services. Web services as well as its corresponding application is frequently used and accessed by millions of users worldwide. With increasing incorporation of securing the web, it is equally important to enhance the user's experience too. According to Stritter et al. [25], Web 2.0 is highly prone to different forms of intrusion over its cross-site scripting while adversely affecting Domain Name System. Usage of public key infrastructures for securing Web 2.0 is also claimed to be unjustified. Study towards identification of attacks on web-application is carried out by Kozik et al. [26] by introducing a joint implementation of machine

learning and clustering approaches. A very unique prototype has been introduced by Tsalaportas et al. [27] that uses cross-platform environment. The complete prototype is designed by making it independent from any server side and is purely self-contained. This is a lightweight concept of security but lacks consideration of identification of any specific security indicators. The work carried out by Tatli and Urgun [28] have evolved up with a benchmarked tool with capability of investigating intrusion while searching the web using Java scripts. According to the mechanism, the system performs an initial configuration of their crawling process, which is then followed by forwarding all forms of HTTPP request. A robust tool to capture phishing event was discussed by Mao et al. [29].

The authors have used certain feature that are not possible to be corrupted by attackers and has emphasized more on script security. The features were formed from whitelisted database, target page, and suspicious page which when subjected to similarity comparison detects phishing. The analysis of the study is carried out considering dataset if phishing event whereas the outcome is assessed considering accuracy parameters e.f. recall, precision, etc. Study towards resisting phishing has been carried out by Marchal et al. [30] where the approach is to identify different constraint encountered by attacker to construct forged page. Literature has also witnessed certain hybridized technique for securing web application. Goldsteen et al. [31] have hybridized network layer and presentation layer to introduce a secure masking policy to safeguard sensitive information.

The authors have also discussed about the certain masking rules that should be adhered upon while working on such security policies. However, the loophole of this work is that it doesn't support securing any contents generated by multiple parties on web. This problem is reported to be addressed by Phung et al. [32] where security of JavaScript and mixed flash contents are subjected to security. However, the work doesn't safeguard many other forms of attacks e.g. denial-of-Service (DoS) attack. Therefore, it is essential to study the internal knowledge about the attack strategy and mining approach is most suitable for this task. Adoption of mining approach was seen in work of Medieros et al. [33] where policy for attack detection was formulated and then it was used to capture diverse attacks. However, owing to inclusion of iterative rules, it could offer computational complexity that has not been assessed. Similar direction of research was also carried out by Antunes and Viera [34] considering benchmarking approach for SQL injection and work of Gillman et al. [35] who discussed about delivering contents securely.

From the above existing approaches towards securing threats over web, it can be visualized from above table that researchers have offered solution towards phishing problems, DoS attack, identification of attack problems etc. Apart from this generic research work, there are some exclusive research work towards identifying and preventing some lethal threats as below:

2.1. Studies towards resisting cross-site scripting attack (XSS)

Basically, this is the most frequently reported attacks on web application that let the adversary inject malicious code in the web-pages for invoking attacks. Existing literature has reported towards promoting identification process of XSS attack. The work carried out by Das et al [36] have presented an unique method of identifying only legal set of actions executed by normal user as well as adversary considering multiple attack examples.

However, the isolation process recommended by the authors has not been checked for its mitigation quality. Research towards evolving up with an effective mitigation policy has been carried out by Yusof and Pathan [37] where the authors have emphasized more on constructing security policy for sensitive web contents. The researcher has constructed a prototype web-based application in order to testify their algorithms over various browsers. Study towards resisting similar attack has also been presented by Shar and Tan [38]. However, they have spoken theoretically the strength of various tools and practices. Similar theoretical study of security loopholes of Web 2.0 and existing web application is also discussed by Saiedian [39]. According to author, domain-based XSS attacks are quite hard to mitigate.Salas and Martins [40] have presented a black-box based mechanism to resist attacks on web-services. However, the study lacks any discussion of possible overheads. Work carried out by Faghani and Nguyen [41] have discussed about a security mechanism using social network and clustering concept to formulate a strategy for resisting spread of XSS attacks. An analytical modeling has been carried out using graph theory to implement this concept where the outcome is assessed using number of compromised users as well as different forms of clustering metrics of social networks. Shar et al. [42] have adopted machine learning-based approach for forecasting the attack events for web applications. The technique uses validation inputs as well as code patterns for carrying out the computation using semi-supervised learning approach. Shar and Tan [43] have presented a study towards auditing the defensive charecteristics of XSS. An interesting part of this study is that it offers a comprehensive assessment of the defense measures adopted to restrict XSS attacks. The technique adopted by this author is quite unique and adheres to the security requirements discussed by Halderman [44]. Hence, research work towards resisting XSS based attacks are quite new and less number of

standard research work exists at present. Majority of the existing researchers have made theoretical discussion towards XSS attacks while less number of work are carried out towards implementing robust solution. However, apart from XSS, there are other lethal attacks on web applications too that are discussed next.

2.2. Studies towards resisting SQL injection

SQL injection is a kind of attack technique where an attacker inserts their own code into a pre-existing database in order to steal data-information by targeting web-based applications. It can be mitigated by ensuring that a system has powerful security system. This section discusses the existing Web security approaches to avoid the SQL injection attacks.The work carried out by Appelt et al. [45] have considered the failure of web security system in presence of SQL injection attacks and formulated this issue as optimization problem. The authors have used machine learning approach and genetic algorithm to fix the vulnerability of security system. The experimental implementation demonstrates that the presented approach efficiently blocks the attacks. Khoury et al. [46] have investigated effectiveness the existing security scanner that used to detect stored attacks.

The author have performed custom test-bed scenario that show that existing security scanner is not much effective in detecting stored SQL injection vulnerabilities. Li et al. [47] have presented a new dynamic model based on Hidden Markov Model to detect attacks and to analyze the behavior of attacker and the legal user. The experimental performance of proposed model reveals that it achieves higher accuracy rate compared to *K*-means technique in terms of detecting malicious user and attacks. Ping et al. [48] have developed prototype architecture to prevent the attacks in the Web applications. The authors have used Randomization technique that randomizes the SQL queries which result in to detect SQL injected attacker. Experimental effects display that proposed architecture obtains good performances to preventing attacks with the low-cost rate. Xiao et al. [49] have investigated existing approaches to attacks detection and found that these methods have some defects which do not meet full requirements of the detection system.

The outcomes of this study show that the presented approach overcomes the issues of existing approach with higher accuracy. Yassin et al. [50] have presented intrusion detection framework for cloud service provider to detected attacks. The proposed framework provides interrelationship between the HTTP request and the SQL queries which helps to identify the attacks without modifying source code of cloud application. The author have also proposed that the presented framework is integrated in Amazon Web Services which allows a cloud provider to reduce its infrastructure costs by pooling many computing resources to provide multiple clients or applications.Majority of the research work is not benchmarked and yet the problem is open-end.

2.3. Studies towards resisting DDoS attacks

At present, the usage of internet or web services becoming very essential for everyone such as organizations, governments, as well as in the education sector. Unfortunately, with the growth of the number of hosts, the number of attacks on the internet is also incredibly increasing fast. Thus, there are different kinds of attacks, out of them DDoS attack is the most common and significant threat. To prevent such kind of attacks, several researchers introduced the different approaches, are briefly discussing in this section.

In [51], Luo et al. have proposed prevention mechanism against DDoS attacks, i.e., identifier or locator separation method which shows that how can prevent & defend the web services from DDoS attacks. Also introduced the mapping approach of identifier onto locator and demonstrated how this mechanism makes it difficult for the attackers to manage botnets. But proposed “Identifier or locator” separation mechanism has its features which are mainly intended to solve the routing problems in the internetworking. Shea et al. [52], have presented an experimental study on modern virtualization machines under networked DoS attacks. In this study, have examined the performance of virtualization techniques beneath standard TCP based DDoS attacks.

For the result analysis, have compared the same DDoS on non-virtualization servers. Shiaeles and Papadaki [53], proposed an enhanced multi-layer IP-Spoof detection method, was named as a hybrid IP spoofing detection method for internet DDoS attacks. The proposed mechanism based on fuzzy empirical policies which can identify the IP offensive as well as mitigate the traffic offending. The experimental results showed that hybrid spoofing approach analyzed ten thousand packets, and precisely identified 99.9% of traffic within 5 sec. The primary limitation of this approach is, there is the need for geographical information, so that has to maintain a database with appropriate TTL values forms the IPs with the country.

Tang et al. [54] have investigated the impact of low rate DoS attack on feedback control system. Also proposed a methodology to compute the effect of low rate Daniel of service attack on feedback control system which identifies the different attack scenarios and calculates the impact of all attack scenarios. The simulation results demonstrated the tradeoff between the effect of DoS attack and its revenue, which

represents the existence of optimal DoS attack. Zhou et al. [55] have introduced a lightweight method to filter the DoS attacks on SIP (i.e., Session Initiation Protocol) and defeat the DoS attacks by blocking SIP packets. The empirical calculation showed that proposed history based IP filtering method reaches the useful improvement in CPU utilization beneath denial of service attacks.

Yoon [56], proposed a DDoS attack mitigation mechanism for critical web services. The study noticed that critical web services can continue their business if significant users can access their services. The primary aim was to design a white listing i.e. very important IP addresses. Finally, the experimental analysis showed that the proposed white listing scheme efficiently mitigate the DDoS attacks and provides a new defense mechanism for complex web services. But major drawback was that there should be strong binding among the application level ID & Login IPs.Hong et.al [57], have proposed a novel of network based DDoS attack defense scheme, which was assisted by SDN which can identifies and mitigates the HTTP distributed DoS attack in the internet. The simulation outcomes showed that proposed DDoS defense scheme efficiently protects the internet severs against Distributed DoS attacks.

3. STUDIES TOWARDS SECURING FUTURE INTERNET

Basically, Future Internet Architecture (FIA) is meant for overcoming the pitfalls of conventional architecture of current version of internet. The discussion of Pan et al. [58] has elaborated about different scale of contributions towards future internet architecture. However, projects carried out in FIA still have open scope of security incorporation. A good initiative towards investigating security over FIA (called as CoLoR) was carried out by Chen et al. [59] where the authors have carried out comparative strength analysis of various threat levels. According to authors, designing FIA considering service location and inter-domain routing could offer better resource management as well as its packet forwarding strategy is highly resistive against reflection attacks, poisoning of DNS cache, prefix hijacking, bandwidth depletion, falsification of routing path, etc. However, the study doesn't consider any form of enhancing task for network security.

This problem was further investigated by Chen et al. [60] where it was discussed that path identifiers plays a critical role in securing communication in FIA. It was discussed that if the path identifiers were changed dynamically that it could significantly escalate network security. The findings of Malyuk and Miloslavskaya [61] show that a highly structured form of data security is demanded in FIA. Just like IoT, Reconfigurable Computing is also claimed to be used extensively in FIA. The discussion of Mesquita and Rosa [62] shows that there is an ongoing research towards securing incorporation of such concepts in FIA. As cloud and virtualization environment is highly required for secure hosting of applications on FIA so Network virtualization becomes highly essential to be considered. Chances to intrude network virtualization is more owing to vulnerability of virtual machines irrespective of various existing studies towards securing virtual machines over cloud [63, 64]. There are certain desperate research attempts towards securing FIA.

A unique test-bed of security has been formulated by Ozcelik et al. [65] that deals with data security mainly. The work carried out by Rebahi et al. [66] has investigated about the security strength of network technologies of autonomic type. The authors have discussed about Generic Autonomic Network Architecture (GANA) as a reference model and discusses about various hypothetical means to elevate the security strength of GANA. Samad et al. [67] have discussed about different strategies that could protect IoT from different risk factors. The authors have developed a technique that performs assessment of risk using contextual attributes.There are also work being carried out towards resisting specific forms of attacks in cloud environment as well as cyber-physical system owing to increase of complexity in design.

Work of Ge et al. [68] have presented architecture with double loop system for leveraging the optimal security system. The problem of pollution attack was addressed by Guo et al. [69] using simulation-based approach that uses diversity factor of path in point-of-presence network. The authors have used bloom filter for incorporating security. IoT and adhoc networks are some of the prominent backbone of FIA which requires higher degree of security. From these existing contribution it is found to be resilient against certain set of lethal attacks. However, problems continue to exist as these solutions has their own scope and own limitations that couldn't encapsulate all the security problems associated with FIA.

4. OPEN RESEARCH ISSUES

From the prior section, it is evident that there is various research works being carried out towards web security as well as towards securing future internet architecture. These section further briefs of the open research issues explored as follows:

- Solution Highly Focus on Attack: Majority of the existing security solutions towards FIA is developed on the basis of specific attacks e.g. pollution attacks, table overflow attack, suppression attack, collusion

attack, etc. There are few studies to emphasize the effectiveness of such attack-specific solution to be functional if the adversary changes.

- Less Emphasis on Component: FIA is considered as a wholesome architecture of communication that is constructed on multiple components. Since, last decade, there have been various changes in every projects of FIA with evolution of new characteristics. However, none of the projects on FIA (e.g. NEBULA, Mobility First, etc) have been found to emphasize on the changing trend of robust components for developing potential FIA e.g. Content Centric Network (CCN), Internet-of-Things, and Software Defined Network. There is no doubt that there exists massive literature talking about problems associated with above mentioned components but none of them are actually correlated with FIA or there was no visualization about its usage in FIA. This leads to avenue of more set of problems in these component inclusion with respect to security as:
- Gap between Web Security and FIA security: A closer look into existing literatures shows that there are quantitatively more research papers for web security as compared to FIA security. However, neither research towards web security has no consideration of FIA standards and vice-versa. Hence, applicability of both on each other remains undisclosed at present. Moreover, very few research work is found to be benchmarked as the concept of FIA security is quite novel.
- Security Threats in CCN: There are various studies that has claimed that content centric network is one of the most effective and secure data delivery system for FIA owing to verifiable integrity, absence of address, resistance against DoS, and name resolution. However, they also present some of the potential challenges towards privacy e.g. conversation cloning, timing attack, etc.
- Security Threat in SDN: SDN offers a suitable network management for IoT operations in FIA but is vulnerable to various forms of attacks. The existing interface design of SDN is never meant for controlling its controller system completely and securely. This rests in poor access control system when existing SDN system is used in FIA.
- Security Threat in IoT: The concept of IoT in FIA is very vast and hence is also vulnerable to attacks on different layers of protocol stack. Although, there exists some novel security solution in IoT, but it is yet unknown that which one of them could be possible used for a given scenario of resisting threats. Rather than resisting threat, IoT requires a universal framework that could offer true picture of threat specifically.

5. CONCLUSION

This paper has discussed about the existing techniques of security-based approaches used both in existing system as well as in FIA. After reviewing the existing approaches, it is realized now that there is a long way to go for customizing the existing web security approaches. The essential findings of the proposed review work are: i) Existing internet architecture cannot be modified or changed as it is not flexible and hence a completely novel approach is required for enhanced web security, ii) existing approaches of web security as well as some of the novel research attempts towards securing FIA are quite experimental and less practical as they were never being jointly studied. There could be fair possibilities that some of the existing web security approaches could be designed considering FIA in mind, but there was no such research attempt. iii) even the security solutions considering FIA has not considered some of the essential components e.g. IoT, SDN, CCN, and many more. Without such consideration, the claimed system may offer security but they may be less functional as compared to the claimed enhanced functionality of FIA. Hence, a serious research gap existed between existing approaches and what is actually demanded. Therefore, our future work will be in direction of addressing such research gap. We will like to investigate by inclusion of SDN, CCN, and IoT very specifically using mathematical modeling to evolve up with more secure solution in FIA with more practical assumption. Our future work will also involve performing optimization of the existing approaches to check for viable security results.

REFERENCES

[1] Dennis Sheppard, “Beginning Progressive Web App Development: Creating a Native App Experience on the Web,” *Apress*, 2017

[2] Esther Omolara Abiodun, Aman Jantan, Humaira Arshad, Oludare Isaac Abiodun, "A Novel Encryption Algorithm for Securing Files in the Cloud using Phony Documents", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 9, No. 3, pp. 1871-1878, 2019

[3] N. Chandrakala, B.Thirumala Rao, "Migration of Virtual Machine to improve the Security inCloud Computing", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 9, No. 1, pp. 210-219, 2019

[4] Sugandh Bhatia, Jyoteesh Malhotra, "CSPCR: Cloud Security, Privacy and Compliance Readiness -A Trustworthy Framework", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol.8, No.5, pp. 3756-3766, October 2018
[5] M. A. Aman and E. K. Cetinkaya, "Towards Cloud Security Improvement with Encryption Intensity Selection," *DRCN 2017 - Design of Reliable Communication Networks; 13th International Conference*, Munich, Germany, pp. 1-7, 2017.
[6] W. Chung and J. Paynter, "Privacy issues on the Internet," *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, pp. 9, 2002.
[7] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri and G. Baldini, "Security and privacy issues for an IoT based smart home," *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, pp. 1292-1297, 2017.
[8] M. Al-Zyoud, T. Atkison and J. Carver, "An Overview of Emerging Privacy Issues in the Internet of Things," 2016 *International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, pp. 212-217, 2016.
[9] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," in *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250-1258, Oct. 2017.
[10] Ashalatha R., J. Agarkhed and S. Patil, "Network virtualization system for security in cloud computing," *2017 11th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, 2017, pp. 346-350, 2017.
[11] Paul Goransson, Chuck Black, Timothy Culver, "Software Defined Networks: A Comprehensive Approach, Morgan Kaufmann", 2016.
[12] S. H. Bouk, S. H. Ahmed, D. Kim and H. Song, "Named-Data-Networking-Based ITS for Smart Cities," in *IEEE Communications Magazine*, vol. 55, no. 1, pp. 105-111, January 2017.
[13] Ke Xu, Min Zhu, Guang Wu, "Towards evolvable Internet architecture-design constraints and models analysis", *Springer-Science China Information Sciences*, vol.57, Iss.11, pp.1-24, 2014
[14] B. Zhou, Q. Shi and P. Yang, "A Survey on Quantitative Evaluation of Web Service Security," *2016 IEEE Trustcom/BigDataSE/ISPA*, Tianjin, pp. 715-721, 2016.
[15] H. C. Huang, Z. K. Zhang, H. W. Cheng and S. W. Shieh, "Web Application Security: Threats, Countermeasures, and Pitfalls," in *Computer*, vol. 50, no. 6, pp. 81-85, 2017.
[16] W. J. Buchanan, S. Helme and A. Woodward, "Analysis of the adoption of security headers in HTTP," in *IET Information Security*, vol. 12, no. 2, pp. 118-126, 2018.
[17] M. Ambrosin, A. Compagno, M. Conti, C. Ghali and G. Tsudik, "Security and Privacy Analysis of National Science Foundation Future Internet Architectures," in *IEEE Communications Surveys & Tutorials*. doi: 10.1109/COMST.2018.2798280, 2018.
[18] Z. Su, Y. Hui and Q. Yang, "The Next Generation Vehicular Networks: A Content-Centric Framework," in *IEEE Wireless Communications*, vol. 24, no. 1, pp. 60-66, February 2017.
[19] A. Venkataramani, J. Kurose, D. Raychaudhuri, K. Nagaraja, M. Mao, and S. Banerjee, ``MobilityFirst: A mobility-centric and trustworthy Internet architecture," *ACM SIGCOMM Comput. Commun. Rev*., vol. 44, no. 3, pp. 74-80, 2014.
[20] D. Naylor et al., ``XIA: Architecting a more trustworthy and evolvable Internet," *ACM SIGMOBILE Comput. Commun. Rev*., vol. 44, no. 3, pp. 50-57, 2014.
[21] D. Barrera, R. M. Reischuk, P. Szalachowski, and A. Perrig. ``SCION _ve years later: Revisiting scalability, control, and isolation on next-generation networks." [Online]. Available:http://arxiv.org/abs/1508.01651, 2015.
[22] COAST: Content Aware Searching Retrieval and sTreaming, accessed on Nov. 9, 2015. [Online]. Available: http://www.synelixis.com/coast/, November 2015.
[23] W. Ding, Z. Yan and R. H. Deng, "A Survey on Future Internet Security Architectures," in *IEEE Access*, vol. 4, pp. 4374-4393, 2016.
[24] L. Kotut and L. A. Wahsheh, "Survey of Cyber Security Challenges and Solutions in Smart Grids," *2016 Cybersecurity Symposium (CYBERSEC)*, Coeur d'Alene, ID, pp. 32-37, 2016.
[25] B. Stritter et al., "Cleaning up Web 2.0's Security Mess-at Least Partly," *in IEEE Security & Privacy*, vol. 14, no. 2, pp. 48-57, Mar.-Apr. 2016.
[26] R. Kozik, M. Choraś and W. Hołubowicz, "Packets tokenization methods for web layer cyber security," in *Logic Journal of the IGPL*, vol. 25, no. 1, pp. 103-113, Feb. 2017.
[27] P. G. Tsalaportas, V. M. Kapinas and G. K. Karagiannidis, "Solar Lab Notebook (SLN): An Ultra-Portable Web-Based System for Heliophysics and High-Security Labs," in *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 8, no. 8, pp. 4141-4150, Aug. 2015.
[28] E. İ. Tatli and B. Urgun, "WIVET—Benchmarking Coverage Qualities of Web Crawlers," in *The Computer Journal*, vol. 60, no. 4, pp. 555-572, March 2017
[29] J. Mao, W. Tian, P. Li, T. Wei and Z. Liang, "Phishing-Alarm: Robust and Efficient Phishing Detection via Page Component Similarity," in *IEEE Access*, vol. 5, pp. 17020-17030, 2017.
[30] S. Marchal, G. Armano, T. Gröndahl, K. Saari, N. Singh and N. Asokan, "Off-the-Hook: An Efficient and Usable Client-Side Phishing Prevention Application," in *IEEE Transactions on Computers*, vol. 66, no. 10, pp. 1717-1733, Oct. 1 2017.
[31] A. Goldsteen, K. Kveler, T. Domany, I. Gokhman, B. Rozenberg and A. Farkash, "Application-Screen Masking: A Hybrid Approach," in *IEEE Software*, vol. 32, no. 4, pp. 40-45, July-Aug. 2015.

[32] P. H. Phung, M. Monshizadeh, M. Sridhar, K. W. Hamlen and V. N. “. Venkatakrishnan, "Between Worlds: Securing Mixed JavaScript/ActionScript Multi-Party Web Content," in *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 443-457, July-Aug. 1 2015.
[33] I. Medeiros, N. Neves and M. Correia, "Detecting and Removing Web Application Vulnerabilities with Static Analysis and Data Mining," in *IEEE Transactions on Reliability*, vol. 65, no. 1, pp. 54-69, March 2016.
[34] N. Antunes and M. Vieira, "Assessing and Comparing Vulnerability Detection Tools for Web Services: Benchmarking Approach and Examples," in *IEEE Transactions on Services Computing*, vol. 8, no. 2, pp. 269-283, March-April 2015.
[35] D. Gillman, Y. Lin, B. Maggs and R. K. Sitaraman, "Protecting Websites from Attack with Secure Delivery Networks," in *Computer*, vol. 48, no. 4, pp. 26-34, Apr. 2015.
[36] D. Das, U. Sharma and D. K. Bhattacharyya, "Detection of Cross-Site Scripting Attack under Multiple Scenarios," in *The Computer Journal*, vol. 58, no. 4, pp. 808-822, April 2015.
[37] I. Yusof and A. S. K. Pathan, "Mitigating Cross-Site Scripting Attacks with a Content Security Policy," in *Computer*, vol. 49, no. 3, pp. 56-63, Mar. 2016.
[38] L. K. Shar and H. B. K. Tan, "Defending against Cross-Site Scripting Attacks," in *Computer*, vol. 45, no. 3, pp. 55-62, March 2012.
[39] H. Saiedian and D. Broyle, "Security Vulnerabilities in the Same-Origin Policy: Implications and Alternatives," in *Computer*, vol. 44, no. 9, pp. 29-36, Sept. 2011.
[40] M. I. Palma Salas and E. Martins, "A Black-Box Approach to Detect Vulnerabilities in Web Services Using Penetration Testing," in *IEEE Latin America Transactions*, vol. 13, no. 3, pp. 707-712, March 2015
[41] M. R. Faghani and U. T. Nguyen, "A Study of XSS Worm Propagation and Detection Mechanisms in Online Social Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1815-1826, Nov. 2013.
[42] L. K. Shar, L. C. Briand and H. B. K. Tan, "Web Application Vulnerability Prediction Using Hybrid Program Analysis and Machine Learning," in *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 6, pp. 688-707, Nov.-Dec. 1 2015.
[43] L. K. Shar and H. B. K. Tan, "Auditing the XSS defence features implemented in web application programs," in *IET Software*, vol. 6, no. 4, pp. 377-390, August 2012.
[44] J. A. Halderman, "To Strengthen Security, Change Developers' Incentives," in *IEEE Security & Privacy*, vol. 8, no. 2, pp. 79-82, March-April 2010.
[45] D. Appelt, A. Panichella and L. Briand, "Automatically Repairing Web Application Firewalls Based on Successful SQL Injection Attacks," *2017 IEEE 28th International Symposium on Software Reliability Engineering (ISSRE)*, Toulouse, pp. 339-350, 2017.
[46] N. Khoury, P. Zavarsky, D. Lindskog and R. Ruhl, "An Analysis of Black-Box Web Application Security Scanners against Stored SQL Injection," *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and IEEE Third International Conference on Social Computing*, Boston, MA, 2011, pp. 1095-1101, 2011.
[47] P. Li *et al.*, "Application of Hidden Markov Model in SQL Injection Detection," *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, Turin, pp. 578-583, 2017.
[48] Chen Ping, Wang Jinshuang, Pan Lin and Yu Han, "Research and implementation of SQL injection prevention method based on ISR," *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, Chengdu, pp. 1153-1156, 2016.
[49] Z. Xiao, Z. Zhou, W. Yang and C. Deng, "An approach for SQL injection detection based on behavior and response analysis," *2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN)*, Guangzhou, pp. 1437-1442, 2017.
[50] M. Yassin, H. Ould-Slimane, C. Talhi and H. Boucheneb, "SQLIIDaaS: A SQL Injection Intrusion Detection Framework as a Service for SaaS Providers," *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, New York, NY, 2017, pp. 163-170, 2017.
[51] H. Luo, Y. Lin, H. Zhang and M. Zukerman, "Preventing DDoS attacks by identifier/locator separation," in *IEEE Network*, vol. 27, no. 6, pp. 60-65, November-December 2013.
[52] R. Shea and J. Liu, "Performance of Virtual Machines under Networked Denial of Service Attacks: Experiments and Analysis," in *IEEE Systems Journal*, vol. 7, no. 2, pp. 335-345, June 2013.
[53] S. N. Shiaeles and M. Papadaki, "FHSD: An Improved IP Spoof Detection Method for Web DDoS Attacks," in *the Computer Journal*, vol. 58, no. 4, pp. 892-903, April 2015.
[54] Y. Tang, X. Luo, Q. Hui and R. K. C. Chang, "Modeling the Vulnerability of Feedback-Control Based Internet Services to Low-Rate DoS Attacks," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 339-353, March 2014.
[55] C. V. Zhou, C. Leckie and K. Ramamohanarao, "Protecting SIP server from CPU-based DoS attacks using history-based IP filtering," in *IEEE Communications Letters*, vol. 13, no. 10, pp. 800-802, October 2009.
[56] M. Yoon, "Using whitelisting to mitigate DDoS attacks on critical Internet sites," in *IEEE Communications Magazine*, vol. 48, no. 7, pp. 110-115, July 2010.
[57] K. Hong, Y. Kim, H. Choi and J. Park, "SDN-Assisted Slow HTTP DDoS Attack Defense Method," in *IEEE Communications Letters*, vol. 22, no. 4, pp. 688-691, April 2018
[58] J. Pan, S. Paul and R. Jain, "A survey of the research on future internet architectures," in *IEEE Communications Magazine*, vol. 49, no. 7, pp. 26-36, July 2011.
[59] Z. Chen, H. Luo, Jianbo Cui and M. Jin, "Security analysis of a future Internet architecture," *2013 21st IEEE International Conference on Network Protocols (ICNP)*, Goettingen, pp. 1-6, 2013.

[60] Z. Chen, H. Luo, M. Zhang and J. Li, "Improving Network Security by Dynamically Changing Path Identifiers in Future Internet," *2015 IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, 2015, pp. 1-7
[61] A. Malyuk and N. Miloslavskaya, "Information Security Theory for the Future Internet," *2015 3rd International Conference on Future Internet of Things and Cloud*, Rome, pp. 150-157, 2015.
[62] D. Gomes Mesquita and P. Frosi Rosa, "Reconfigurable Computing and Future Internet: Considerations on Flexibility and Security," in *IEEE Latin America Transactions*, vol. 15, no. 7, pp. 1326-1334, 2017.
[63] M. Aslam, C. Gehrmann and M. Björkman, "Security and Trust Preserving VM Migrations in Public Clouds," *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Liverpool, pp. 869-876, 2012.
[64] Yaqiang Mao, Xujian Chen and Yuan Luo, "HVSM: An In-Out-VM security monitoring architecture in IAAS cloud," *ICINS 2014 - 2014 International Conference on Information and Network Security*, Beijing, pp. 185-192, 2014.
[65] I. Ozcelik, I. Ozcelik and S. Akleylek, "TRCyberLab: An infrastructure for future internet and security studies," *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Antalya, Turkey, pp. 1-5, 2018.
[66] Y. Rebahi, N. Tcholtchev, R. Chaparadza and V. N. Merekoulias, "Addressing security issues in the autonomic Future Internet," *2011 IEEE Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, pp. 517-518, 2011.
[67] J. Samad, K. Reed and S. W. Loke, "A risk aware development and deployment methodology for cloud enabled Internet-of-Things," *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, Singapore, pp. 433-438, 2018.
[68] H. Ge and Z. Zhao, "Security Analysis of Energy Internet with Robust Control Approaches and Defense Design," in *IEEE Access*, vol. 6, pp. 11203-11214, 2018.
[69] H. Guo, X. Wang, K. Chang and Y. Tian, "Exploiting Path Diversity for Thwarting Pollution Attacks in Named Data Networking," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2077-2090, Sept. 2016.

BIOGRAPHIES OF AUTHORS

Vidya M. S. completed B.E from Gulbarga University, M. Tech from VTU and pursuing PhD under VTU. Her area of Research is Network Security, and has teaching experience of 14 years. Published papers in National and International journals.

Mala C. Patil completed B.E from Karnataka University, Dharwad, M.S from bits Pilani and PhD from Anna University. She has teaching experience of 25 years. Her area of research is Software Engineering. She has Published papers in various national and international journals.