A Survey on Enterprise Wireless Network Security: Technical Challenges

[1]Hassana Ganame, [2]Lusekelo Kibona, [3]Drissa Kamissoko
[1]Department of Information and Telecommunication, School of engineering of Bamako, Mali
[2]Department of Computer Science, Ruaha catholic University, Tanzania
[3]Department of Information and Telecommunication, School of engineering of Bamako, Mali
[1]ganame_hassana@yahoo.fr, [2]lusekelo2012@gmail.com, [3]idrissakamis@yahoo.fr

Abstract: *Wireless networks offer several assistances in actual world. It has increased popularity as the users need connectivity regardless of their geographic position to achieve their responsibilities. Wireless networks have numerous assistances over the wired networks in terms of mobility, suppleness and cost. Though there are numerous benefits of wireless networks, the security is critical and challenging issue. Many different approaches to overcome the limitation of the security issue have been proposed but attackers still used many methods to bypass the security system of the network. A survey of enterprise wireless network security is to illustrate the keys perception of security, enterprise wireless network and security over enterprise wireless network. Various security systems which helps to protect different types of attacks have been discussed. Finally, the suggestion has been given by considering two virtualization appliances of PSI system interconnected by a trace boxes tool which can detect all the modified packets in the network and packet processing system to establish a language policies in the system.*

Key Words: *Enterprise wireless network, Network security, threats, appliances devices*

1. INTRODUCTION:

Wireless networks and computer systems have become essential tools for business operations. They are now deployed in all sectors professionals: bank, insurance, medicine or the military field [1]. Originally isolated from each other, these networks are now interconnected and the number of access points continues to grow and this remarkable development is naturally accompanied by the increase in the number of users. Wireless networks assist as a transportation mechanism between devices and wired network (enterprise networks and the Internet), and among devices. Wireless networks are various and diverse but are habitually categorized into three groups based on their coverage range: Wireless Wide Area Networks (WWAN), wireless Local Area Network (WLANs), and Wireless Personal Area Networks (WPAN)[2].

Wireless networking presents several advantages as productivity improves because of improved accessibility to information resources [3]. Network deployment is fast, easier and less costly. However the fast evolution of technologies creates a new threats. Due to the replacement of wired network by using radio frequencies "through the air", alters the existing information security risk profile. These users, known or not, are not necessarily full of good intentions to these networks [1]. It is difficult to secure large enterprise networks. Such networks are vulnerable to physical attacks on network components, social engineering attacks where users are forced into revealing sensitive information, and cyber-attacks where malicious attackers realize higher levels of access privilege than should be allowed over network connections[4] also ensuring the confidentiality, integrity, and availability of the modern information technology (IT) enterprise is an immense job. It includes several responsibilities, from strong systems engineering and configuration management (CM) to active cybersecurity or information assurance (IA) policy and comprehensive workforce training. It must also include cybersecurity operations, where a group of people are charged with monitoring and defending the enterprise against all measures of cyber-attack [5].

Despite the efforts that are being made and the very high cost to reduce the menaces in network security. We continue to hear in many ways about catastrophes of existing network security structures, this shows weakness of the traditional network security methods for enterprises including: Perimeter-defences, distributed firewalls [6], Security Information and Occurrence Management systems, and network management between others. Traditional networks do not deal with certain security dimension like isolation, context, agility, visibility (weakness of Middle boxes) and language policies. These dimensions are necessary to improve the security of the enterprise network [6, 7].

Isolation:

A defence system must ensure that security policies must be compatible in order to avoid interferences within the system and also prevent side effects that are also called collateral effects [6, 8].

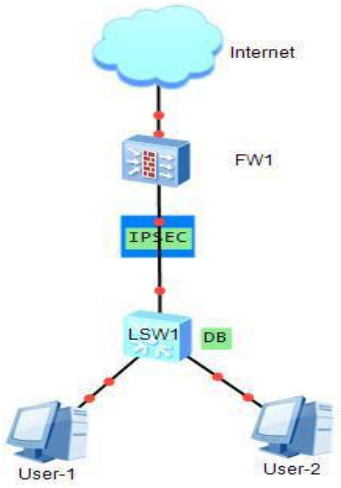

Figure 1: System with lack Isolation

Figure-1 illustrates an example of interference. User-1 and user-2 are connected to the same switch. If the system detects a threat on the user-1 and the system decides to block it by reconfiguring the firewall, by inattention the user-2 who is a normal user can also be affected by this operation. This is called logical interference. A firewall overload can affect the performance of these two users who are not directly connected to the firewall. This is called performance interference. Thus the system defence in lack of isolation induces both logical and performance interference.

Context:

A defence system must have custom processing rules for devices. Knowing the attributes and the state of the devices is crucial for the security of the system.

In the figure-2 we can see that the two HTTP servers are connected to the LAN switch in the same interface even though the system can allow the server-1 to access the database but should denied the server-2 if it's vulnerable[6, 7].

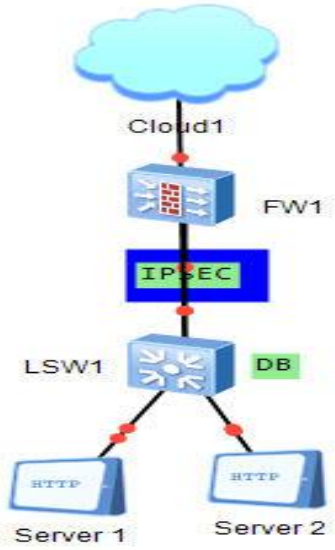

Figure 2: System with lack of context

Agility:

As attackers can dynamically change their strategies, the defence system to detect and face with attackers in their different strategies and must be able to dynamically change the policies security of the network [7].

Weakness of Middle boxes:

A middle box or network appliance is a computer networking device that transforms, inspects, filters, or otherwise manipulates traffic for purposes other than packet forwarding. Middle boxes offer significant security and performance guarantees in networks [7]. Figure-3 shows the different middle boxes used in enterprise networks. The widely deployed middle boxes in enterprise networks to improve network security and performance are: firewalls (FW), which filter unwanted or malicious traffic and Network Address Translators NAT), which modify packets source and destination addresses. Due to dynamic traffic in the network it is hard to manage the network in higher layer protocols, access control and investigation. This also makes it difficult to integrate middle boxes into Software Define Network (SDN)-capable networks and leverage the benefits that SDN can offer.

Figure 3: A middle box world

As we can see in figure 4 ,we have a NAT to dynamically translate private IPs to publics to IPs, a firewall to block the web access (to block the private IP) of H1 and H2 [7, 9]. If at all possible the administrator is wanted to set the policies in the firewall in term of source IP for the network but the private IP cannot be known as the NAT dynamically chooses the public IPs. The risk appear if only H1 and H2 should be directed to the firewall and the rest is allowed to pass through.

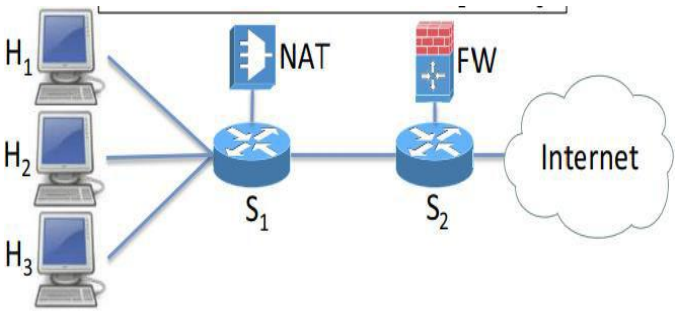

Figure-4: applying a blocking policies[7]

According to the above security problems, the main objective of this research was to identify principle elements related to wireless network security and provide an overview of potential threats, vulnerabilities, and countermeasures (solutions) associated with wireless network security.

Language policies:

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Many enterprises use multiple description security policies to control their data and security system with cause's complex policy to the network. Due to the dispersion of the security policies each one having its own field and model over different environments make the work and the understanding very complex for the network administrator to administer it [10]. The workflow of some application needs to cross many security issues and to satisfy the policy of each one which is also very difficult to achieve.

To overcome the critical security difficulties issues cited above the main goal was to develop a new security system that can detect, prevent, diagnostic and to control the enterprise networks.

2. LITERATURE SURVEY:

A. *General description*

As describe in [10], the lack of standard language to describe diverse middle box functionality and deployment configurations undesirably affects current middle box deployment. In their research paper named "Modelling middle boxes" improved the security of language policies by presenting a simple middle box model to describe the packets processing and demonstrate it by using common middle boxes [11].

[12] Found solution about middle boxes interference in various types of networks as well as enterprise network by implementing the trace box tool which is an extension of the mostly used traceroute. It sends an IP packet with Transfer Control Protocol (TCP) segments and different Time To Live (TTL) values and analyses the packet encapsulated in the returned Internet Control Message Protocol (ICMP) messages. Any modification to the IP packet by upstream middle boxes can be detected in the ICMP message.

In their research in [13] the investigation have been done in the performance of the network by developing a fast and easy-to-use TCP framework that can create lightweight TCP middle boxes to inspect and modify the traffic, as well as inject Packets.

When a devices in the network middle boxes fails it is challenging because the lost state must correctly restore, in the paper [14] titled "Rollback-Recovery for Middle boxes", researcher focus on designing solution to record middle box state in two mechanisms:

- "Ordered logging" which offers lightweight logging of the information needed after recovery.
- "Parallel release" to guarantee that the recovery is always correct.

[15] Investigate in a joint optimization of Middle Box Selection and Routing (MBSR) problem because a high congestions may occur if middle box selection and traffic routing are not well jointly planed in the context of Software-Defined Networking. To solve this problem, they propose a polynomial algorithm by using Markov technique and finally the numerical result shows that it generates near-optimal solution.

In SDN networks the correct and stable information are needed for private and public IPs to decide the packet flow but sometime due to the hidden packet header information by the middle box the process becomes very difficult. Since the middle box change packet header information on their own decision without saying the raison. This may cause a disable load balancing and penetration policies issues. "The paper named "Middle box Driven Security Threats in Software Defined Network" [9] investigate in the packet hidden information, they first list possible middle box-driven security threats.

- Case of using NAT

The figure-5 shows the NAT translate the private IP to public IP, coming to controller the information of the matching private and public is not given by NAT. Due to lack of information it will be very difficult for the controller to identify the source of the packet. The scenario makes controller unable to apply policy to the packet from specific device.

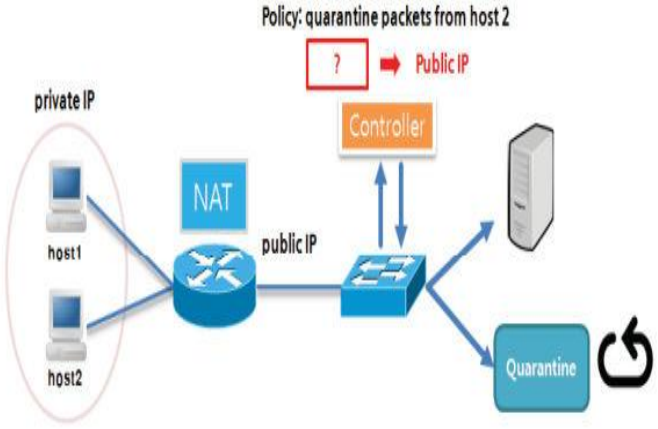

Figure-5: Showing difficulty of getting right information from the packet which has already processed by NAT [9].

- Case of using Proxy:

Proxy is positioned between server and client, it's allows clients indirectly connect to other network services and stores the demanded content in the cache.

In figure-6 shows that the controller wants to apply policies to the incoming packets to go to the firewall for detection and to blocks packets from blacklisted hosts. If the proxy lies between the firewall and host, the host will bypass the firewall to access directly the server. The scenario shows that the proxy can offer attackers a way to bypass security systems.

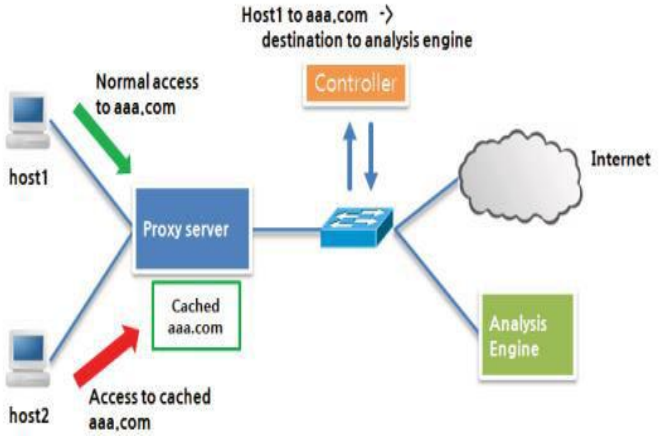

Figure-6: Proxy server's cached data allows abnormal access to blocked path [9].

To solve this problem, they propose to add a vital information to packets and directly control middle boxes by the controller.

Reachability is one of the must offer that the operators can guaranties but the current network reachability is limited because its focus only in a network's subset control plan, in the paper title "Efficient Network Reachability Analysis using a Succinct Control Plane Representation" [16] they first define the control plan as a program that takes determine the behaviour of the data plan and takes the configuration files and the network environment also generate data plan (see figure-7). Data plan is in charge of forwarding packet.

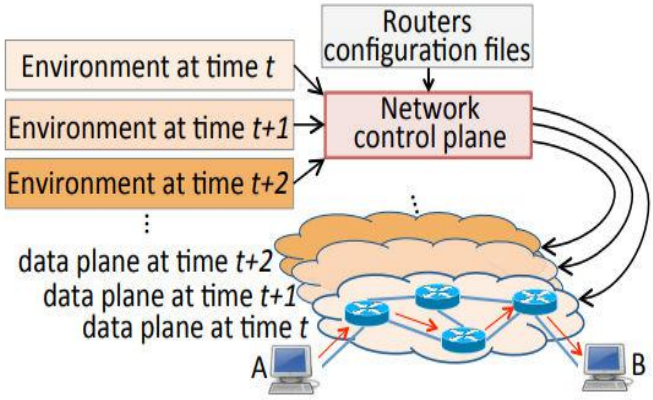

Figure-7: Reachability behaviour of a network (e.g., A can talk to B) is determined by its data plane, which, in turn, is the current incarnation of the control plane [16].

To solve this problem, they proposed a new tool called Efficient Reasoning (ERA) about network reachability. ERA significantly improved the reachability of enterprise network with hundred nodes in few second.

Bring Your Own Device (BYOD) is a technique which provide advantage to enterprise because enterprise employees can access to enterprise network with their own devices. Although it bring many advantages to the enterprise, the challenges is how to guarantee the security of enterprise networks? Existing solution such as Mobile Device Management (MDM) focus their work mostly in the devices control and protection. A new solution is needed for network administrators to control the capabilities of devices and mobiles applications. [17] Provide system for mobile devices management policy administration system on android platform (PBS-DROID) with Programmable BYOD Security (PBS) administrators also benefit from the global network visibility and fine-grained policy programmability.

By exploring four difficult correlation security techniques: namely denial and isolation, degradation and obfuscation, negative information and deception and adversary attribution and counter- operations.

[18] Examine techniques and methods to protect digital information which are widely available online thus access to malicious intent.

B. *Security threats*

[19] Described Border Gateway Protocol (BGP) routers and work on it to improve the security of Internet Service Providers (ISPs).

[20] Gives a general view of different types of attacks in wireless network and briefly describes the precaution for an enterprise to face of those types of attacks.

As peer in the paper named "Policy-driven Network Defence for Software Defined Networks" [21], has largely talked about the identification and resolution of security issues caused by the security issue of applications in the SDN.

Knows very often as dust networks, wireless sensor network is one of the most promising networks of the future, insertion of wireless communication technology also invites several kinds of security threats. [22] Deeply examine in the security problems and the challenges in wireless sensor network. Battery sensing devices are exposed to locations where the environment is often difficult to monitor and supervise. The different security problems that are generally encountered are:

- Passive attacks: The monitoring and listening of the communication channel by illegal attackers are identified as passive attack [22-24]. Most of frequently cases are Monitor, Snooping and Traffic Analysis.
- Active Attacks: The attacker improvements information about the network using passive attack and then launches an active attack. [23]. Most of frequently cases are Routing Attacks in Sensor Networks and Denial of Services [25].

[26] Explained attacker inspiration, vulnerabilities and opportunities currently accessible to hackers. Wireless sensor networks are open to several security threats that can compromise the success of the application. This paper describes that security supports in wireless network is challenging due to the restricted energy, communication bandwidth and computational power. Security problems and currently offered solutions, many types of attacks like - attacks on routing and DoS attack, injecting false packets, attacks on real time requirements, attacks on the network using topological information, attacks on localization.

Security Challenges: due to the architecture of the WSN, it has several limitations.

- Wireless connection

Because of its wireless transmission, it easily allows attackers to catch information, replacing it with corrupted information that is different from the one transmitted by the source. This problem is common to all traditional networks that use wireless transmission.

- Dynamic topology

As known ,we do not have a fixed topology in dynamic topology network such as Ad-Hoc network because the nodes of the networks are self-configured and can move at any time and be replaced by others. Some may fail while moving and this can cause instability in the network. This issue poses a high security challenge so a good dynamic environment must be well implemented.

- Bandwidth

The bandwidth is restricted due to huge number of other events as compare to wired network [27].

Umesh Kumar and Sapna Gambhir [28] widely explain the various types of wireless security attacks like:

- Traffic analysis

The Traffic analysis technique allows hackers to have access to 3 types of important information that are:

Information relating to the identification of activities.

Information about the location of the access point

Information about the Communications Protocol.

- Access Control Attacks (Being stealthy)

When hacker access to the network by bypassing the filters and firewall of the network, he can initiate activities in the network without being noticed or seen by the network defence system. Although it has a mechanism that allows to protect the confidentiality of users such as the VPN (Virtual Private Network) and IPsec [6, 28, 29].

- Denial of Service (DoS):

Attackers use others devices to disable the communication of normal users in the valid wireless networks [28, 30].

- Integrity Attacks:

An integrity attack modifies the data being transmitted. The hacker modifies, deletes or adds additional information to the data that may facilitate other types of attacks.

- Overloading the defence.

Attackers can overload the system defence of the network to reduce the performance of the users [6].

C. *Proposed solution*

Many approaches have been proposed to solve the various problems mentioned above. Among those, the most recent and which takes into account most of the weaknesses that existed in the traditional network is that proposed in [6]. Interference in enterprise network security as well on the logical level and performance, the dynamism of the security and knowing the behaviour of each devices in the networks are key factors to have a more secure network. By using the latest improvements which are:

- In Network Functions Virtualization (NFV) to launch virtualized security functions.
- In Software Define Network (SDN) capabilities to route the traffic to the desired virtual appliances.

[6] Proposed an approach called Precise Security Instrumentation system as shown in Figure-8 that take into the consideration of these mentioned security issues.

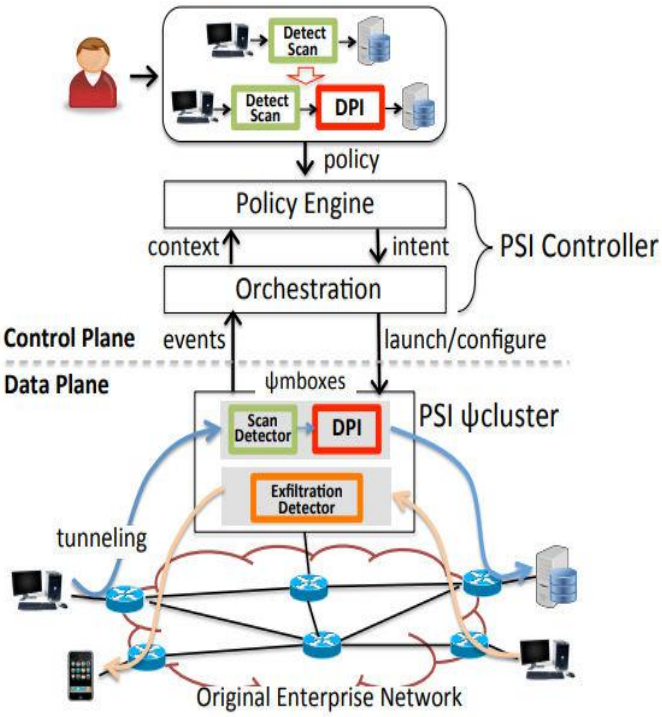

Figure-8: A high-level view of the PSI [6]

In this approach each appliance is connect to each device as next hope, Deep packet inspection (DPI) is generally recognized as a powerful technique which is used for intrusion detection systems for inspecting, deterring and deflecting malicious attacks over the network and packets and recognize contents that match with recognized attacks[31]. NFV technique is used to setup a virtualized appliances called as shown in figure-8 Ψmbox. It has been used to reduce the cost of connecting each appliance to each device and can support up to hundred devices [6]. SDN technique to build a Ψcluster to overcome lack of dynamic invincible appliances. Policy Engine understand the policy concept and calculates the real time security intent updates for each device founded on the existing context. PSI controller's orchestration tools to interpret the high-level intents into a real realization.

3. METHODOLOGY:

The purpose of this survey is to write a literary review of different challenges on enterprise wireless network and the methodology used for this document is:

- To explore on internet the related work to our proposed topic.
- To contract the general idea of each document exploited and referenced while using our own words.

We had also exploited books, papers and short quotations in which ideas converge with ours. It is also important to note that the purpose of modifying some systems is to have consistency in ideas and to make the survey more understandable. To have a wider and more interesting conversation, we consider a model that takes into account of several problems cited in the pass section but which also has shortcomings. Finally, to reach an interesting conclusion and to have a strongest model, we make a comparison in next section between the proposed model described in the previous section and some others models proposed in the related work.

4. DISCUSSION AND COMPARISON:

In this section we are going to compare the different proposed solutions in this survey. As defined in preceding sections, we can characterized the enterprise network attacks in 2 groups: Passive attacks, in this type of attack, attackers will force the network to get information while network is transmitting or receiving. Most of time the detection of these types of attacks is very difficult. Active attacks where attackers will adjust or remove the data in the enterprise network. As we know we have tree mains concepts which needed true security for an enterprise network to do not be vulnerable for attackers. When we compare with the previous progresses, the model suggested by PSI consider the latest enhancement and solved the problem of isolation, context and agility as described in the previous sections.

These efforts significantly improved the enterprise network security but still have weakness at the level of virtualized appliances recommended above. The virtualize appliances can support up to hundred devices, for more security we suggest for example an enterprise in which we have 100 machines to install two virtualize appliances. Both virtualize appliances will be interconnected and separated by a security guard system, doing this will avoid for one being infected to do not automatically infect the second one as shown in the topology of figure-9.

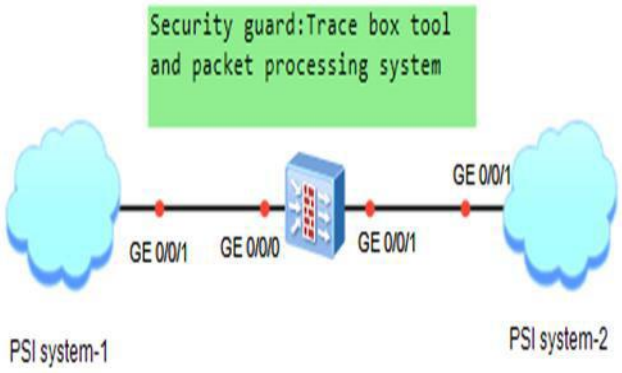

Figure-9: New proposed Enterprise network security system based on PSI system, Trace box tool and packet processing system.

Due to the sensitivity and the difficulty of having a perfect and precise solution of attacker's behaviours, many solutions of middle boxes have been proposed. In the solution of trace box tool which can detect all the modified packets by attackers and the packet processing system allows virtualize appliances and trace box tool to have language policies and to establish and understandable language.

5. CONCLUSION AND RECOMMENDATION:

Even with intense boom in cost, the state of functioning network security is still horrible because hackers and attackers are always in mood to find an appropriate way to detour the different security systems. In this section, the main safety threats for enterprise wireless network which should be considered as a controlling attitude to come up with the challenges to the security matters in enterprise Wireless Network are considered. So we have mentioned a possible approach in detecting and protecting the enterprise network by using two PSI system and secured the two system with a security guard. But the approach seems costed and not to be very sufficient for enterprise wireless networks. Still some strong works are needed especially in the physical transmission connection between devices which can considered as first level security in the system.

REFERENCES :

1. K. Boudaoud, "Détection d'intrusions: Une nouvelle approche par système multiagents," Thèse de doctorat de l'Université de Genève, 2002.
2. T. Karygiannis and L. Owens, "Wireless network security," NIST special publication, vol. 800, p. 48, 2002.
3. M.-k. Choi, R. J. Robles, C.-h. Hong, and T.-h. Kim, "Wireless network security: Vulnerabilities, threats and countermeasures," International Journal of Multimedia and Ubiquitous Engineering, vol. 3, pp. 77-86, 2008.
4. R. P. Lippmann, K. W. Ingols, C. Scott, K. Piwowarski, K. Kratkiewicz, M. Artz, et al., "Evaluating and strengthening enterprise network security using attack graphs," Lexington, Massachusetts October, 2005.
5. C. Zimmerman, "Ten Strategies of a World-Class Cybersecurity Operations Centre. The Mitre Corporation," ed, 2014.
6. T. Yu, S. K. Fayaz, M. Collins, V. Sekar, and S. Seshan, "PSI: Precise Security Instrumentation for Enterprise Networks," in Proc. NDSS, 2017.
7. S. K. Fayazbakhsh, L. Chiang, V. Sekar, M. Yu, and J. C. Mogul, "Enforcing Network-Wide Policies in the Presence of Dynamic Middlebox Actions using FlowTags," in NSDI, 2014, pp. 533-546.
8. J. Mirkovic, M. Robinson, and P. Reiher, "Alliance formation for DDoS defense," in Proceedings of the 2003 workshop on New security paradigms, 2003, pp. 11-18.
9. S. Hwang and K. Kim, "Middlebox driven security threats in software defined network," in Proc. ISITC, 2014, pp. 105-108.
10. C. Ribeiro, A. Zuquete, P. Ferreira, and P. Guedes, "SPL: An Access Control Language for Security Policies and Complex Constraints," in NDSS, 2001.
11. D. Joseph and I. Stoica, "Modeling middleboxes," IEEE network, vol. 22, 2008.
12. G. Detal, B. Hesmans, O. Bonaventure, Y. Vanaubel, and B. Donnet, "Revealing middlebox interference with tracebox," in Proceedings of the 2013 conference on Internet measurement conference, 2013, pp. 1-8.
13. R. Gaillard, "Lightweight Middlebox TCP," 2016.
14. J. Sherry, P. X. Gao, S. Basu, A. Panda, A. Krishnamurthy, C. Maciocco, et al., "Rollback-recovery for middleboxes," in ACM SIGCOMM Computer Communication Review, 2015, pp. 227-240.
15. H. Huang, S. Guo, J. Wu, and J. Li, "Joint middlebox selection and routing for software-defined networking," in Communications (ICC), 2016 IEEE International Conference on, 2016, pp. 1-6.
16. S. K. Fayaz, T. Sharma, A. Fogel, R. Mahajan, T. D. Millstein, V. Sekar, et al., "Efficient Network Reachability Analysis Using a Succinct Control Plane Representation," in OSDI, 2016, pp. 217-232.
17. S. Hong, R. Baykov, L. Xu, S. Nadimpalli, and G. Gu, "Towards SDN-Defined Programmable BYOD (Bring Your Own Device) Security," in NDSS, 2016.
18. M. Almeshekah and E. Spafford, "The case of using negative (deceiving) information in data protection," in International Conference on Cyber Warfare and Security, 2014, p. 237.
19. K. Weitz, D. Woos, E. Torlak, M. D. Ernst, A. Krishnamurthy, and Z. Tatlock, "Bagpipe: Verified BGP configuration checking," in Proc. OOPSLA, 2016.
20. A. Khajuria and R. Srivastava, "Attacks and Challenges in Wireless Networks A Literature survey."
21. W. Han, Policy-driven Network Defense for Software Defined Networks: Arizona State University, 2016.
22. V. Kumar, A. Jain, and P. Barwal, "Wireless sensor networks: security issues, challenges and solutions," International Journal of Information and Computation Technology (IJICT), vol. 4, pp. 859-868, 2014.
23. P. Khare and S. Ali, "Survey of Wireless Sensor Network Vulnerabilities and its Solution," International Journal of Recent Development in Engineering and Technology, vol. 2, 2014.
24. M. Waliullah and D. Gan, "Wireless LAN security threats & vulnerabilities," International Journal of Advanced Computer Science and Applications, vol. 5, 2014.
25. J. G. Ponsam and P. Pradeep, "Secured Intrusion Detection System in Wireless Sensor Network."
26. E. Sabbah, A. Majeed, K.-D. Kang, K. Liu, and N. Abu-Ghazaleh, "An application-driven perspective on wireless sensor network security," in Proceedings of the 2nd ACM international workshop on Quality of service & security for wireless and mobile networks, 2006, pp. 1-8.
27. S. Ughade, R. Kapoor, and A. Pandey, "An Overview on Wormhole Attack in Wireless Sensor Network: Challenges, Impacts, and Detection Approach," International Journal of Recent Development in Engineering and Technology,(ISSN 2347-6435 (Online) Volume 2, Issue 4, 2014.
28. U. Kumar and S. Gambhir, "A literature review of security threats to wireless networks," International Journal of Future Generation Communication and Networking, vol. 7, pp. 25-34, 2014.
29. M. Waliullah, A. Moniruzzaman, and M. S. Rahman, "An Experimental Study Analysis of Security Attacks at IEEE 802. 11 Wireless Local Area Network," International Journal of Future Generation Communication and Networking, vol. 8, pp. 9-18, 2015.
30. S. Gopalakrishnan, "A survey of wireless network security," International Journal of Computer Science and Mobile Computing, vol. 3, pp. 53-68, 2014.
31. T. AbuHmed, A. Mohaisen, and D. Nyang, "A survey on deep packet inspection for intrusion detection systems," arXiv preprint arXiv: 0803.0037, 2008.