3rd International Conference on Advanced Research in Biology, Engineering, Science and Technology (ICARBEST'16)
Organized by
International Journal of Advanced Research in Biology, Engineering, Science and Technology (IJARBEST)
19th March 2016

MAGIC COOKIE AND MAC ADDRESS VALIDATION FOR PREVENTING SESSION HIJACKING

K.Pon Muthu Bharathi[1],S.Suganthi[2],P.Venisula Mary[3],C.BalaMurugan[4]

[1], [2],[3]-CSE Final Year,V V College Of Engineering

[4]-Asst.Prof.CSE Department,V V College Of Engineering

***Abstract*-Wireless communication networks square measure pervasive each fact of our lives attributable to their quick easy and cheap preparation. Square measure becoming present and are wide used to transfer essential information like banking accounts, credits card,e-mail and social networks credentials. The further pervasive the wireless technology goes to be, the extra necessary it's security issue area unit planning to be wherever because the gift security protocols for wireless networks have self-addressed the privacy and confidentiality issues, there unit of measurement unaddressed vulnerabilities threatening their convenience and integrity(e.g. denial of service, session hijacking and hijacking and waterproof addressed spoofing attacks).. In this paper we describe the about the cookie based attack prevention method and MAC address Validation. Session hijacking attack will take place when the user session is start. When the access time exceeds the valid duration and the session expires,the clients of the web applications must send requests and data all over again from the beginning, at this time the attacker use sniffer to capture the user details. This type of attack is called as session hijacking. To prevent this type of session hijacking we use the magic cookie and MAC address.**

***Key Words*- Wireless networks, Session, Prevention, magic cookie, Mac Address, Validation**

I.INTRODUCTION

Recent advances in wireless technology have created it the foremost wide used communication medium, both in home and enterprise networks. the most blessings of wireless networks versus wired networks s

square measure their quality , flexibility and cheap readying and maintenance cost , particularly in places that wiring is troublesome. With the exponential growth within the readying of wireless native space Networks (WLAN), the protection issue of those networks has some become a significant concern for each users and suppliers. The first wireless local area network commonplace, IEEE 802.11 has been ratified in 1997 [1]. Since then, totally different revisions have been conducted to enhance the bottom common place [2]. Although most of the revisions have centred on the performance, the IEEE 802.11i [3] commonplace was dedicated to security amendments. Despite IEEE 802.11i has provided sensible mechanisms to improve privacy and confidentiality, it still will not offer enough protection for availableness and integrity (e.g. Denial of service, session hijacking and Macintosh address spoofing attacks) [4]. The failure of current wireless networks extremely necessary. The Intrusion Detection Systems (IDSs) can offer safer networks by observance the behaviour of the protocol to notice any abnormal events differed by wireless attacks. Although completely different intrusion detection system are out there for wired networks are performing on completely different intrusion detection systems are out there for wires networks, they can't be applied on to wireless networks. Whereas\ the intrusion detection system in wired networks are performing on completely different layers of the network, in wireless networks to cannot simply

access the content of the highest layers that are usually encrypted. Therefore, unlike the wired networks, most of the wireless intrusion detection systems operate at the 2 lower layers (Physical and Data Link). We can categories the offered wireless Intrusion Detection Systems (WIDS) consistent with the reference knowledge or the analysis techniques. Consistent with the reference knowledge we will group the Wireless IDS into 3 clusters: those that focus on the physical layer knowledge [5]-[7], those that use the information link layer (MAC layer) knowledge [8]-[10] and also the ones that mix the information from each layer [11]. According to the analysis technique, IDSs square measure classified into two categories: Misuse Detection and Anomaly Detection [12].In misuse Detection Technique, the system uses a group of rules and signatures to model the malicious activities and attacks. Associate alarm is generated whenever those rules square measure detected. The misuse detection technique is one in all the primary steered intrusion detection techniques, and there are several industrial merchandise supported this approach [13]-[15]. The misuse detection systems have low false positive alarms, however on the opposite hand, they suffer from low detection rate for new attacks especially those of zero day attacks. The other disadvantages of misuse detection system is that the need to be manually updated with new attack signatures. From low detection rate for brand spanking new attacks particularly those of zero day attacks. the opposite disadvantage of misuse detection systems is that they have to be manually updated with new attack signatures. In this paper we present a Magic Cookie and MAC Address. If the user login into the website with user-id and password ,Normally the browser create the cookie with the encrypted user information. This cookie will passed through the network as packet. This may be stealed by the attacker. To prevent this we use Magic cookie and MAC Address. Magic cookie will have the summary of the original cookie information. This will not provide the necessary user information's to the attacker, So they will not able to hack the user information's. For our more security purpose we use the MAC Address Validation in our proposed system. The remaining section of this paper organized as follows: In Section II, we discuss the related works. In section III the general behaviour of the Magic cookie and MAC Address validation procedures. In Section IV we present the experimental results and evaluation of our work. The summary of the research presented and planned future work is given in section V.

II.RELATED WORKS

As it was mentioned wireless intrusion Detection System can be classified supported the reference knowledge and therefore analysis technique of the mackintosh layer frames. Based on reference knowledge, we will reason the IEEE 802.11 Intrusion Detection systems (IDS) into three groups: Tthose that target the physical layer data[5],[6],[16],[18],[25], those that use the info link layer knowledge [8],[20],[21],[23], and therefore the ones that mix the information from each layers [11]. Most of the physical layer IDS systems check the wireless signal specification so as to notice the physical layer attacks like ECM [5],[18]. The common ECM detection approaches square measure supported signal strength and placement consistency [5],[7]. What is more , there are another waterproof layer attacks [6],[16],[25].for instance, sheng et al used signal strength to notice the waterproof address spoofing attack [6].the mackintosh layer based mostly systems use the data within the header of the IEEE 802.11 frames for intrusion detection. There is plenty of data within the IEEE 802.11 frames switch are often used. As an example, some approaches use the available sequence number in IEEE 802.11 header to detect the MAC address spoofing [8],[20],[21]. These methods are based on the fact that even if the MAC address an be easily spoofed frames compared with the original frames are almost unavoidable by the attackers [22]. They use information mining and pattern matching techniques to detect these anomalies gill et al. Proposed a specification based approach to model the state machine of IEEE 802.11 an then monitored the MAC layer frames transferred between each station and access-point in order to generate a state transition model. During testing, any state transition violation is considered as an abnormal activity. Torres et al. [22] combined the sequence number tracking with state machine model to develop a more powerful system. In addition, there are some other approaches which use the combination of physical and MAC layer information to detect the wireless attacks. Fayssal

et al. Combined the physical and MAC layer information to obtain a richer feature set for their wireless IDS [11]. Powerful system. In addition, there area unit another approaches which use the micture of physical and waterproof layer information to sight the wireless attacks. Fayssal et al. Combined the physical and waterproof layer info to get a richer feature set for his or her wireless IDS [11]. Although there square measure totally {different|completely different} options from different layer which will be used for intrusion detection, adding a lot of features from totally different layers don't essentially improve the performance. EL-Khatib has applied totally different features selection techniques to pick the foremost economical feature set from IEEE 802.11 header fields [19]. Hid final feature set includes only eight options out of thirty eight potential fields.

The use of cookies ad session authentication has raised security issues since theric adoption in the mid-90's. Many surveys [24, 27] have incontestable the multiple issues with net authentication mechanisms, together with vulnerability to session hijacking attacks. As a result security researchers have proposed changes to boost the strength of authentication cookies. Park et al. [32] and Fu et al. [24] suggested by mistreatment well-known science techniques. Additionally, these authors projected the employment of cookie expiration times to reduce the impact of session hijacking attacks. However several applications use long expiration times to avoid affecting user expertise, reducing the intercourse effectiveness of this approach. Juels et al. [29] proposed the utilization of cache cookies, different styles of persistent state within the browser (e.g., browser history, temporary net files), as an alternate to cookies for storing user and session identifiers. Whereas proof against pharming attacks, cache cookies still want HTTPS protection to forestall active attacks. Bortsz et al. [30] demonstrated a brand new category of attacks to steal cookies, related-domain attacks, wherever cookies keep by one website will be changed by another if the 2 sites happen to share a sufficiently long suffix. To prevent this type of attacks the authors planned origin cookies, associate extension to plain cookies that need minimal implementation prices. However, because the previous solutions, origin cookies are still prone to session hijacking. Other planned various to authentication cookies is that the use of hidden type fields to store authentication tokens. for instance, the ASP.NET View State [26] practicality uses this method. However, the sole difference between cookies and View State values ar the place wherever they're keep in the browser; each are static tokens. Hence, View State is additionally prone to session hijacking.

III.BEHAVIOUR ANALYSIS

3.1 OVERVIEW

3.1.1 PROPOSED SYSTEM

Session cookies allow users to be recognized within a website so any page changes or item or data selection you do is remembered from page to page. The most common example of this functionality is the shopping cart feature of any e-commerce site. When you visit one page of a catalog and select some items, the session cookie remembers your selection so your shopping cart will have the items you selected when you are ready to check out. Without session cookies, if you click CHECKOUT, the new page does not recognize your past activities on prior pages and your shopping cart will always be empty.

Without cookies, websites and their servers have no memory. A cookie, like a key, enables swift passage from one place to the next. Without a cookie every time you open a new web page the server where that page is stored will treat you like a completely new visitor. In our project we use two main concepts to avoid session hijacking. They are magic cookie and MAC address. A magic cookie, or just cookie for short, is a token or short packet of data passed between communicating programs, where the data is typically not meaningful to the recipient program. The contents are opaque and not usually interpreted until the recipient passes the cookie data back to the sender.

To prevent session hijacking, a special technique is proposed under which, using magic Cookie to prevent this Session hijacking

attack. Magic cookie is not like a normal cookie which produces the message digest by using some digest algorithm. And this message digest is changed randomly. So the attacker can't able to guess the original cookie information.Simultaneously the server gets the mac address of the particular system and validates it. If the current mac address is not matched with the initial mac address, then the server rejects the request from the client and produces the login page.

Proposed System Advantage:

1.Using a MAGIC cookie will prevent this session hijacking attack by encrypting the Cookie with MAC address so that attacker cannot any type of session hijacking.

2. This cookie/Session will be changing frequently so that attacker will not all be guess Session details even this can prevent Session brute forcing attack also.

3.2. METHODOLOGY

3.2.1 DATAFLOW DIAGRAM

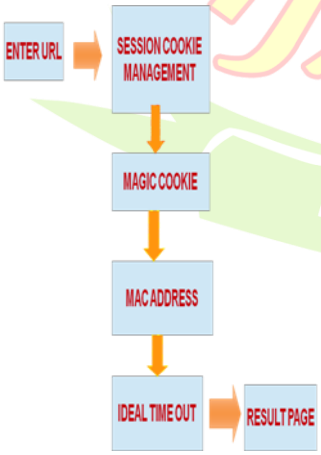

Figure 3.1 session hijacking modules

Our project includes three main modules, they are shown in the figure 3.1.

3.2.2. SESSION HIJACKING MODULES:

1. Cookie Management
2. Magic cookie
3. Idle Timeout

MODULE DISCRIPTION:

COOKIE MANAGEMENT:-

Many web sites use SSL encryption for login pages to prevent attackers from seeing the password, but do not use encryption for the rest of the site once authenticated. This allows attackers that can read the network traffic to intercept all the data that is submitted to the server or web pages viewed by the client. Since this data includes the session cookie, it allows him to impersonate the victim, even if the password itself is not compromised. Unsecured Wi-Fi hotspots are particularly vulnerable, as anyone sharing the network will generally be able to read most of the web traffic between other nodes and the access point.

MAGIC COOKIE:

A magic cookie, or just cookie for short, is a token or short packet of data passed between communicating programs, where the data is typically not meaningful to the recipient program. The contents are opaque and not usually interpreted until the recipient passes the cookie data back to the sender or perhaps another program at a later time. The cookie is often used like a ticket – to identify a particular event or transaction

IDLE TIMEOUT:

The other type of session attack is session fixation. Here, instead of stealing/hijacking the victim's session, the attacker fixes the user's session ID before the user even logs into the target server (that is, before authentication), thereby eliminating the need to obtain the user's session ID afterwards. Before going into detail of session fixation attacks, we must classify two types of sessions managed on Web servers:

1. Permissive sessions allow the client's browser to propose any session ID, and create a new session with that ID if one does not exist. After that, the server continues to authenticate the client with the given ID.
2. Strict sessions allow only server-side-generated session ID values.

A successful session fixation attack is generally carried out in three phases:
Phase I or session set-up: In this phase, the attackers set up a legitimate session with the Web application, and obtain their session ID. However, in some cases the established trap session needs to be maintained (kept alive) by repeatedly sending requests referencing it, to avoid idle session time-out.

Phase II or fixation phase: Here, attackers need to introduce their session ID to the victim's browser, thereby fixing the session.

Phase III or entrance phase: Finally, the attacker waits until the victim logs into the Web server, using the previous session ID.

3.2.3 BLOCK DIAGRAM

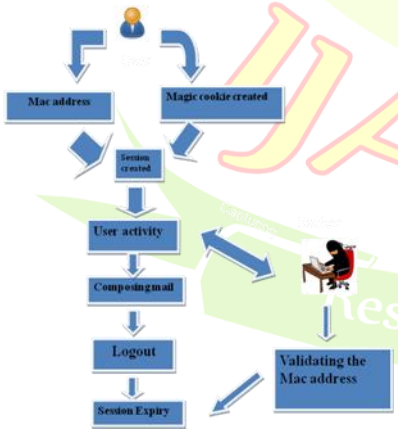

Figure 3.2 Processing steps of session hijacking

- At first, the user gives the username and password to login to the page.
- Then the browser creates a magic cookie ,simultaneously it gets the MAC address of the machine.
- Magic cookie value is changed randomly. Any attacker or intruder may steal the cookie/session as like normally but in this case even when attacker steal the cookie/session he/she not able to access the webpage without user credential.
- And the mac address of the machine is validated on the server. If the initial mac address and the current mac address of the machine are not same, then the server gives only the login page to the user.

3.3 ALGORITHM

In our project we use SHA-1 algorithm for producing message digest.

3.3.1 SHA-1

A cryptographic hash function developed by the NSA (National Security Agency). SHA-1 produces a 160-bit (20-byte) hash value known as a message digest of an input data sequence (the message) of any length.

SHA-1 algorithm is used to produce the message digest of the cookie information and this message digest value is not reversible. So the attacker is can't able to calculate the original cookie information.

Step 1: Append Padding Bit

Message is "padded" with a 1 and as many 0's as necessary to bring the message length to 64 bits less than an even multiple of 512.

Step 2: Append Length

64 bits are appended to the end of the padded message. These bits hold the binary format of 64 bits indicating the length of the original message.

Step 3: Prepare Processing Functions

SHA1 requires 80 processing functions defined as:

1.f(t;B,C,D) = (B AND C) OR ((NOT B) AND D) (0 <= t <= 19)

2.f(t;B,C,D) = B XOR C XOR D
(20 <= t <= 39)

f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 <= t <=59)

f(t;B,C,D) = B XOR C XOR D (60 <= t <= 79)

Step 4: Prepare Processing Constants

SHA1 requires 80 processing constant words defined as:

K(t) = 0x5A827999 (0 <= t <= 19)

K(t) = 0x6ED9EBA1 (20 <= t <= 39)

K(t) = 0x8F1BBCDC (40 <= t <= 59)

K(t) = 0xCA62C1D6 (60 <= t <= 79)

Initialize Buffers

SHA1 requires 160 bits or 5 buffers of words (32 bits):

H0 = 0x67452301

H1 = 0xEFCDAB89

H2 = 0x98BADCFE

H3 = 0x10325476

H4 = 0xC3D2E1F0

Step 6: Processing Message in 512-bit blocks (L blocks in total message)

This is the main task of SHA1 algorithm which loops through the padded and appended message in 512-bit blocks.

Input and predefined functions:

3.M[1, 2, ..., L]: Blocks of the padded and appended message f(0;B,C,D), f(1,B,C,D), ..., f(79,B,C,D): 80 Processing Functions K(0), K(1), ..., K(79): 80 Processing Constant Words

4.H0, H1, H2, H3, H4, H5: 5 Word buffers with initial values

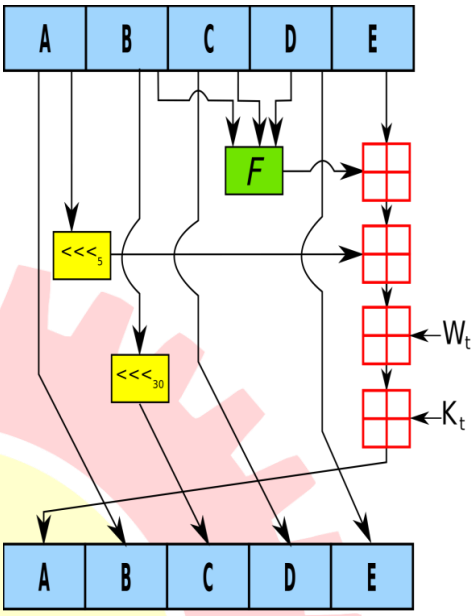

Figure 3.3 SHA-1 processing functions

Step 7: Pseudo Code

For loop on k = 1 to L

(W(0),W(1),...,W(15)) = M[k] */* *Divide M[k] into 16 words* */*

For t = 16 to 79 do:

W(t) = (W(t-3) XOR W(t-8) XOR W(t-14) XOR W(t-16)) <<< 1

A = H0, B = H1, C = H2, D = H3, E = H4

For t = 0 to 79 do:

TEMP = A<<<5 + f(t;B,C,D) + E + W(t) + K(t) E = D, D = C,

C = B<<<30, B = A, A = TEMP

End of for loop

H0 = H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D, H4 = H4 + E

End of for loop

IV. IMPLEMENTATION AND RESULT

4.1 SCREEN SHOTS

4.1.1 SESSION HIJACKING WITHOUT PREVENTION:

To understand the problem first we discuss about session hijacking without prevention. At first the user gives the username and password to login to the page. When the login button is click, it go to the user profile page. Profile page contains the information about the user personal details, education details and contact details. At this time the cookie will be created by browser. This cookie is send from client to server. Here, the attacker steals the cookie information. Normally cookies contains the information about what we do. For that we use the information in the URL. In without prevention, the attacker steal the cookie and he/she can able to view the user's information.

4.1.2 SESSION HIJACKING WITH PREVENTION:

Here we discuss about the session hijacking with prevention .At first the user gives the username and password to login to the page. When the login button is click, it go to the user profile page. User's profile page contains the information about the personal details, education details and contact details. Now magic cookie is created .For our understandings purpose we just show the MAC address and the magic cookie information on the top of the page. This magic cookie information is changed periodically. Here, the attacker steals the cookie and try to get the unauthorized access to the page.z Here, the server checks the attacker's MAC address (i.e) current MAC address with the initial mac address. If they are not same then the server gives only login page to the attacker.

V.CONCLUSION

In this paper we reviewed the IEEE 802.11 security issues and briefly reviewed the MAGIC cookie and MAC Address validation procedures and methodologies. It can detect different types of attacks with high detection rate. After going through all the aspects of session hijacking, it can be concluded that it is successful because of unawareness in users about their security. Systems are compromised as of insecure handling, weak session IDs and mostly no account lockout. All in order to prevent this must apply the countermeasures in their daily routine of internet access. To prevent session hijacking attack against attacker by implementing the software like RSA ID generator that helps communication between server and client machine will be safe attacker not able to perform any sort of attack.

REFERENCES

[1] IEEE Standard for Information Technology—Telecommunicatio and Information Exchange Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEEStandard.11-1997, 1997. [Online]. Available:http://dx.doi.org/10.1109/IEEESTD.1997.85951

[3] Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Standard 802.11i-2004, Jul. 2004.

[4] C. He and J. C. Mitchell, "Security analysis and improvements for IEEE 802.11i," in Proc. 12th Annu. Netw. Distrib. Syst. Security Symp. (NDSS), San Diego, CA, USA, Feb. 2005, pp. 90–110.

[5] A. Sheth, C. Doerr, D. Grunwald, R. Han, and D. Sicker, "MOJO: A distributed physical layer anomaly detection system for 802.11 WLANs," in Proc. 4th Int. Conf. Mobile Syst., Appl. Services, Uppsala,Sweden, Jun. 2006, pp. 191–204.

[6] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11MAC layer spoofing using received signal strength," in Proc. IEEE 27th Annu. Conf. Comput. Commun. (INFOCOM), Apr. 2008, pp. 13–18.

[7] W. M. Suski, II, M. A. Temple, M. J. Mendenhall, and R. F. Mills,"Using spectral fingerprints to improve wireless network security," inProc. IEEE Global Commun. Conf. (GLOBECOM), Nov./Dec. 2008, pp. 1–5.

[8] Q. Li and W. Trappe, "Detecting spoofing and anomalous traffic inwireless networks via forge-resistant relationships," IEEE Trans. Inf.

Forensics Security, vol. 2, no. 4, pp. 793–808, Dec. 2007.

[9] M. Raya, J.-P. Hubaux, and I. Aad, "DOMINO: A system to detect greedy behavior in IEEE 802.11 hotspots," in Proc. 2nd Int. Conf. Mobile Syst., Appl., Services (MobiSys), 2004, pp. 84–97.

[10] S. Radosavac, G. Moustakides, J. S. Baras, and I. Koutsopoulos, "Ananalytic framework for modeling and detecting access layer misbehaviorin wireless networks," ACM Trans. Inf. Syst. Security, vol. 11, no. 4, Jul. 2008, Art. ID 19.

[11] S. Fayssal, S. Hariri, and Y. Al-Nashif, "Anomaly-based behavior analysis of wireless network security," in Proc. 4th Annu. Int. Conf. Mobile Ubiquitous Syst., Netw. Services (MobiQuitous), Aug. 2007, pp. 1–8.

[12] P. Helman, G. Liepins, and W. Richards, "Foundations of intrusion detection [computer security]," in Proc. Comput. Security Found. Workshop,Jun. 1992, pp. 114–120.

[13] Snort-Wireless. [Online]. Available: http://snort-wireless.org/, accessed Sep. 5, 2013

[14] AirMagnet. [Online]. Available: http://www.airmagnet.com/, accessed Sep. 5, 2013.

[15] Airdefence. [Online]. Available: http://www.airdefense.net, accessed Sep. 5, 2013.

[16] D. Madory, "New methods of spoof detection in 802.11b wireless networking," M.S. thesis, Thayer School Eng., Dartmouth College,Hanover, NH, USA, Jun. 2006.

[17] K. Bicakci and B. Tavli, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks," Comput. Standards Interf., vol. 31,no. 5, pp. 931–941, Sep. 2009.

[18] A. G. Fragkiadakis, V. A. Siris, and A. P. Traganitis, "Effective and robust detection of jamming attacks," in Proc. Future Netw. Mobile Summit, Jun. 2010, pp. 1–8.

[19] K. El-Khatib, "Impact of feature reduction on the efficiency of wireless intrusion detection systems," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 8, pp. 1143–1149, Aug. 2010.

[20] D. Dasgupta, J. Gomez, F. Gonzalez, K. Yallapu, R. Yarramsettii, andM. Kaniganti, "MMDS: Multilevel monitoring and detection system," in Proc. 15th Annu. Comput. Security Incident Handling Conf., Ottawa, ON, Canada, 2003, pp. 22–27.

[21] F. Guo and T. Chiueh, "Sequence number-based MAC addressspoof detection," in Proc. 8th Int. Symp. Recent Adv. Intrusion Detection (RAID), Seattle, WA, USA, 2005, pp. 309–329.

[22] L. M. Torres, E. Magana, M. Izal, D. Morato, and G. Santafe, "Ananomaly-based intrusion detection system for IEEE 802.11 networks," in Proc. IFIP Wireless Days (WD), Oct. 2010, pp. 1–6.

[23] R. Gill, J. Smith, and A. Clark, "Specification-based intrusion detectionin WLANs," in Proc. 22nd Annu. Comput. Security Appl.Conf. (ACSAC), Dec. 2006, pp. 141–152.

[24] K. Fu, E. Sit, K. Smith, and N. Feamster. Dos and don'ts of client authentication on the web. USENIx Security Symposium, 2001 .

[25] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," IEEE Trans Parallel Distrib. Syst., vol. 24, Jan. 2013

[26] S. Mitchell. Understanding ASP.NET View State. http://msdn.microsoft.com/en-us/library/ ms972976.aspx, 2004.

[27 C. Visaggio. Session Management Vulnerabilities in Today's Web. IEEE Security and Privacy, 2010

[28] H. Alipour, "An anomaly behavior analysis methodology for networkcentric systems, Ph.D. dissertation, Dept. Elect. Comput. Eng., Univ. Arizona, Tucson, AZ, USA, 2013.

[29] J. S. Park and R. Sandhu. Secure Cookies on the Web. IEEE Internet Computing, 2000.

[30 J. Grossman. Cross-Site Tracing (XST).http://www.cgisecurity.com/whitehatmirror/WhitePaper screen.pdf, 2003

[31] H. Alipour, Y. B. Al-Nashif, and S. Hariri, "IEEE 802.11 anomaly-based behavior analysis," in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Jan. 2013, pp. 369–373.

[32] C. Jackson and A. Barth. Forcehttps: protecting high-security web sites from network Attacks. I Proceeding of the ACM international conference on World Wide Web (WWW), 2008

[33] Jehiah. XSS - Stealing Cookies 101. http://jehiah.cz/a/xss-stealing-cookies-101, 2006.

[34] A. Juels, M. Jakobsson, and T. Jagatic. Cache cookies for browser authentication (Extended.Abstract) In IEEE Symposium on Security and Privacy, 2006.

[35]A.Koch.DroidSheep. http://droidsheep.de/, 2011.

.