IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

A Survey on Design and Development of Wireless Local Area Network Security and Enhancement Using Wired Equivalent Privacy

Ms. Manju Gopinathan[1], Mr. M. Sengaliappan MCA, M.Phil, ME[2]

M. Phil Scholar, Department of Computer Science, Kovai Kalaimagal College of Arts and Science, Coimbatore, India[1]

Dean, Department of Computer Science, Kovai Kalaimagal College of Arts and Science, Coimbatore, India[2]

Abstract: Wireless LAN deployment improves users' mobility, but it also brings a range of security issues that affect emerging standards and related technologies. WLANs let users access a high-speed connection in areas where physically wired networks can't penetrate or are not cost effective. Many companies use WLANs as add-ons to their main wired networks. The popularity of wireless networks is causing many engineers to analyze weaknesses and vulnerabilities in current wireless protocols. In the 802.11 standard an optional encryption protocol called Wired Equivalency Privacy (WEP) is used to make wireless traffic as secure as wired network traffic. WEP's duty is to encrypt packets and authenticate wireless LAN adapters. WEP is implemented at the data-link layer on all Wi-Fi compliant devices. RC4 is used as the encryption algorithm in WEP, which has been thoroughly analyzed and thought of as secure. In this paper, the various weakness of WEP taken for analyzing. To improve the security of keys used in WEP, 802.11i will most likely use a form of temporal key integrity protocol (TKIP) and CCMP. Although WLANs solve some problems that exist in traditional wired LANs, they also introduce new security issues. Here we identify current and future WLAN security concerns and possible countermeasures, including standards, technologies, management, policies, and service environments. The risks that WLAN services present can only be mitigated rather than completely eliminated.

Keywords: WLAN, LAN, WEP, TKIP, CCMP, OFDM, Wi-Fi, 802.11 Protocol.

I. INTRODUCTION

A wireless local area network (WLAN) links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network. Wireless local area networks (WLANs) are become popular as they are fast, cost effective, flexible and easy to use. There are some challenges of security and for IT administrators the choice of security protocol is a critical issue. To access to the transmitted data is the main difference between wired and wireless networks. Taping the media that is used in network communication is the only possible way in wired networks and in wireless networks communication is done with air media. The radio frequency can access the transmitted data by the equipment that is available for a cheap price in the market readily.

For the development of security needs for the development stages of wireless technology and its security needs, according to the experts the security is the major issue. The traditional wired networks are in here more secure than wireless networks, the transmissions which take place in air with the right equipment can easily intercept those transmissions which are broadcasted in the air. To secure the wireless networks is not a easy task. There are a number of security issues that make securing a WLAN difficult.

II. OBJECTIVE

The main aim of this research work is to detailed study of the various concerns and enhancements of WLAN security. A WLAN's flexibility provides an easy way to install a new network, whether an extension of a wired network or a pure WLAN. The ease and speed with which these networks can be installed is unprecedented: high-speed networks can be installed for a week or a day and then removed once they are no longer needed. The fact that such temporary installations can be created cost-efficiently is a major selling point for WLAN integrations. Although WLANs solve some problems that exist in traditional wired LANs, they also introduce new security issues. In this research, identify current and future WLAN security concerns and possible countermeasures, including standards, technologies, management, policies, and service environments. The risks that WLAN services present can only be mitigated rather than completely eliminated. Although there is no single solution for perfect WLAN security, we believe that WLAN security can be enhanced to an acceptable level by a proper combination of countermeasures. WLANs let users access a high-speed connection in areas where physically wired networks can't penetrate or are not cost effective. Many companies use WLANs as add-ons to their main wired networks. A recent report studied and found that corporations that implemented WLANs increased the availability of their corporate network by 70 minutes per day for the average user, which in turn also enhanced productivity within the

corporation by as much as 22 percent WLANs, also offer much-needed flexibility in a world of high-speed data networks. The various objectives are studied and given below:

- Analyze the weakness and vulnerability of WEP (Wired Equivalent Privacy)
- The major 3 problems of WEP
- Study on shortcomings of WEP
- Analyze the various attacks of WEP
- Analyze the various security concerns and strategies
- Detailed study of Wi-Fi Protected Access (WPA)
- Enhance the TKIP Encryption system for WPA
- Enhance the importance of AES (Advanced Encryption Standard) System

III. SECURITY MECHANISMS, ATTACKS AND SECURITY ENHANCEMENTSFOR

Wired Equivalent Privacy (WEP) protocol was adopted to protect authorized users from unauthorized access and eavesdropping in the IEEE 802.11 wireless LANs. It has been proven that the WEP protocol fails to provide data confidentiality and authentication. This paper first introduces the WEP as well as all kinds of attacks. Then, two approaches to enhance the WEP are proposed to overcome some known vulnerabilities and thus to provide better data confidentiality and authentication. Finally, simulation methodology is presented and simulation results are provided. This research studies show that the proposed enhancements provide better data confidentiality with some degree of computing cost as the trade-off. Data security issues are becoming increasingly important as civilization moves toward a global information age. The migration away from paper work oriented ways of doing things requires the development of digital equivalents for traditional processes such as sealing envelopes, signing letters, and acknowledging receipt of items.

The development of systems with such capabilities is one of the most complex and challenging tasks facing today's engineers. At the same time, the rewards to be reaped from breaking such systems act as an attractive lure for modern criminals. One study estimates that the average traditional bank robber nets$20,000 with a 90% chance of prosecution; the average electronic funds transfer nets $500,000 with a 15% chance of prosecution.

An important sub-problem to that of providing security in general is that of providing secure communications between centers of activity, i.e., network security. This is distinguished from the sub-problem of providing security within a center of activity (e.g., a computer).

It addresses the development of a design methodology for network security based on the International Standards Organization (ISO) 7498 Open Systems Interconnection (OSI) Reference Model and 7498-2 Security Architecture. It should be pointed out, lest one get the impression that all the obstacles are purely technical, that legal and practical problems also stand in the way of a transition to a digital society.

IV. WLAN SECURITY- CURRENT AND FUTURE

WLANs let users access a high-speed connection in areas where physically wired networks can't penetrate or are not cost effective. Many companies use WLANs as add-ons to their main wired networks. WLANs also offer much-needed flexibility in a world of high-speed data networks. Administrators can install them quicker, easier, and more cost-efficiently than traditional wired networks. AWLAN's flexibility provides an easy way to install a new network, whether an extension of a wired network or a pure WLAN. The ease and speed with which these networks can be installed is unprecedented: high-speed networks can be installed for a week or a day and then removed once they are no longer needed. The fact that such temporary installations can be created cost-efficiently is a major selling point for WLAN integrations. Many companies, organizations, and even individuals implement wireless local area networks (WLANs) in various locations such as their offices, conference rooms, homes, and business areas. This type of connection offers users portability because they can move from one location to another while maintaining access to the corporate network, but it does not offer access between locations. Mobility, on the other hand, lets users access the corporate network not only near multiple access locations but also everywhere in between. Wireless local area networks (WLANs) are become popular as they are fast, cost effective, flexible and easy to use. There are some challenges of security and for IT administrators the choice of security protocol is a critical issue. The main motive of their research is to make the non-specialist reader knowledgeable about threats in the wireless security and make them aware about the disadvantages of wireless security protocols. WEP (Wired Equivalent privacy), WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols are defined and examined here.

This security protocols are compared with the common. It is a comparative analysis of WEP, WPA and WPA2. We have tried to perform and check authentication of all 3 protocols by implying the legendary attack vector scripts i.e. Air crack set of tools. The test was conducted on Back Track operating system which is considered as dedicated pretesting operating system. In the test result, we found out that WEP is the weakest, to which WPA was a temporary solution and WPA2 is a very solid and long term solution. It is a mixture of wireless security weaknesses and counter measures to the problems faced until recently. After reading this paper the non-specialist reader will have complete review and awareness about the wireless security and vulnerabilities involved with it.

V. ANALYSIS OF SECURITY PROTOCOLS FOR WIRELESS NETWORKS

Security is a serious concern in wireless networks. In order to eliminate the vulnerabilities in previous Standards, the IEEE 802.11i Standard is designed to provide security enhancements in MAC layer. The authentication process consists of several components, including an 802.1X authentication phase using TLS over EAP, a 4-

WayHandshake to establish a fresh session key, and an optional Group Key Handshake for group communications. The objective of this work is to analyze IEEE 802.11i with respect to data confidentiality, integrity, mutual authentication, and availability. Under or threat model, 802.11i appears to provide effective data confidentiality and integrity when CCMP is used. 802.11i may also provide satisfactory mutual authentication and key management, although there are some potential implementation oversights that may cause severe problems. On the other hand, we identified several Denial of Service attacks. Different solutions are proposed for these vulnerabilities, which result in an improved variant of 802.11i with a more efficient failure recovery mechanism. Some of the resulting improvements have been adopted by the IEEE802.11 TGi in their final deliberation. Here used a finite-state verification tool, called Mur-, to analyze the 4-Way Handshake component. The result shows that finite-state verification is quite effective for analyzing security protocols. Furthermore, we adopted Protocol Composition Logic to conduct a correctness proof of 802.11i, including SSL/TLS as a component. The proof is modular, comprising a separate proof for each protocol component and providing insight into the networking environment in which each component can be reliably used. Finally, we showed that 802.11i can significantly reduce the complexity of designing a secure routing protocol when it is deployed in wireless ad hoc networks.

VI. GIAC SECURITY ESSENTIALS IN WLAN

When the recursive splitting procedure is completed, all insignificant leaves are removed. The remaining leaves are all SDP nodes and together form a pattern set that has the highest possible yield for the chosen item selection criterion. However, such set may very Wireless local area network (WLAN) has been widely used in many sectors. The popularity gained is due to many reasons, such as ease of installation, installation flexibility, mobility, reduced cost-of-ownership, and scalability. However, regardless of the benefits mentioned above, WLAN have some security threats, in which anyone who use it or intend to use it should be aware of. It begins by introducing the concept of WLAN. The introductory section gives brief information on the WLAN components and its architecture. In order to examine the WLAN security threats, this research will look at Denial of Service, Spoofing, and Eavesdropping. The paper will then explain how Wired Equivalent Privacy (WEP) works, which is the IEEE 802.11b/Wi-Fi standard encryption for wireless networking. The discussion of WEP continues by examining its weaknesses, which result in it being much less secured than what was originally intended. This situation leads to further research regarding practical solutions in implementing a more secured WLAN. It will also cover the new standards to improve the security of WLAN such as the IEEE 802.1x standard, which comprises of three separated sections: Point-to-Point Protocol (PPP), Extensible Authentication Protocol (EAP) and 802.1x itself. The 802.1x is actually included in 802.11i, a newly proposed standard for key distribution and encryption that will play a big role in improving the overall security capabilities of current and future WLAN networks. The 802.11i standard provides two improved encryption algorithms to replace WEP, which are Temporal Key Integrity Protocol (TKIP) and CBC-MAC Protocol (CCMP). This paper will also list down several products that will assist users to protect their wireless networks from attacks. Finally, this paper ends with the conclusion of highlighted issues and solutions.

VII. ISSUES IN WIRELESS SECURITY

In their research work, the authors define two concepts. One is key problems with 802.11Wireless LAN Security (WEP), here repeat in key stream which allows easy decryption of data for a moderately sophisticated adversary (Short IV), weak implementation of the RC4 algorithm leads to an efficient attack that allows key recovery and subject to brute force attacks (Short Keys). And also defined about easily compromised keys (Shared keys/No Key management), message modification is possible, no user authentication occurs, subject to Man in the Middle attacks, and organizations are becoming hesitant to deploy 802.11 wireless technology due to weak security. The second aspect is “Wi-Fi Alliance”. The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. In 2001 there were 100 Wi-Fi Certified Products and today there are 500+ Wi-Fi certified products& industry is demanding a more secure wireless environment and can’t wait for the 802.11i standard to be ratified next year. Wi-Fi Protected Access (WPA) is Wi-Fi Alliance’s response to the need for an immediate solution to the WEP problem and recognition that the 802.11i standard is still too far off.

Security WEP is especially dangerous because it establishes a false sense of security that cause people to be more willing to send sensitive data over the network. You still need to use some other encryption method onto of WEP - even at best it gives the privacy of a standard Ethernet AN. Other technologies are under development to improve the state of wireless security, such as the IEEE 802.11 Task Group E, which is trying to develop an authentication scheme suitable for 802.11 wireless networks, or the IEEE 802.1 x protocols which will do similar things at amore generic level. There is no existing good solution to the wireless problem (PPPoE hacks aside).

VIII.CONCLUSION

Here, the security issues in the IEEE802.11 WLANs and proposed two enhancements for the WEP. Furthermore, from the various simulations/ experiment son comparisons of these schemes with the original WEP scheme. The proposed enhancements provide better data confidentiality with some degree of computing cost as the trade-off. The improved schemes overcome the weaknesses resulting from Key Sequence Reuse. They make use of not only the varying IV states, but also varying key states in order to supply a higher seed space resulting in lesser key stream

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

reuse. It is not easy to mount decryption dictionary attacks, since the total number of key streams to be discovered increases largely relative to the WEP and the key streams used change from day today for the same IV.

Key Management is partially solved since the system is not easily compromised despite the secret key remaining unchanged for a longtime. Message Tampering is completely avoided from the use of Keyed Message Authentication mechanism. Security against Message Injection is heightened since discovery of a key stream is useful to the intruder only until the next session key change. If session key is refreshed frequently enough, depending on the network traffic, the vulnerability can be kept under check. Authentication spoofing is made difficult by using Kerberos based authentication. Other schemes may be explored that would improve the randomization factor of key streams. Authentication remains an area to be improved since the proposed authentication mechanism is still vulnerable to replay and man-in-the-middle attacks. In future, may be the strength of the key will be improved from this work. Whenever the improvement is taken for further research for WLAN security, this research work is very useful.

REFERENCES

1. Bandela, C. (2002) 'Improving WEP security in IEEE 802.11wireless networks', Georgia State University, MasterThesis.
2. IEEE 802.11 WG (1999) Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, Standard, IEEE, August.
3. John S.Park & Derrick Decoy, 2003. WLAN Security: Current and Future.
4. Karen Scafone, Derrick Dicoi Matthew Sexton & Cyrus Tibbs July 2008, Guide to Security Legacy IEEE 802.11 Wireless Networks NIST Special Publication 800-48 Revision 1.
5. W. Aiello, S. M. Bellovin, M. Blaze, J. Ioannidis, O. Reingold, R. Canetti, andA. D. Keromytis. Efficient, DoS-resistant, secure key exchange for Internet Protocols. In the 9th ACM conference on Computer and communications security, pages 48–58, 2012.
6. T. Aura and P. Nikander. Stateless connections. In International Conference on Information and Communications Security (ICICS'97), pages 87–97, November2007.
7. M. Burrows, M. Abadi, and R. Needham. A logic of authentication. ACM Transactions on Computer Systems, 8(1):18–36, 2010.
8. N. Cam-Winget, R. Housley, D. Wagner, and J. Walker. Security flaws in802.11 data link Protocols. SPECIAL ISSUE: Wireless networking security, Communications of the ACM, 46(5):35–39, May 2013.
9. A. Datta, A. Derek, J. C. Mitchell, and D. Pavlovic. A derivation system for security Protocols and its logical formalization. In Proceedings of 16th IEEE Computer Security Foundations Workshop, pages 109–125. IEEE, 2003.
10. D. L. Dill, S. Park, and A. G. Now at zyk. Formal specification of abstract memory models. In Symposium on Research on Integrated Systems, pages 38–52, 2013.
11. D. B. Faria and D. R. Cheriton. DoS and authentication in wireless public access networks. In the first ACM Workshop on Wireless Security (WiSe'02), September 2012.
12. S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the key scheduling algorithm of RC4.

DOI 10.17148/IJARCCE.2015.41256