Security Analysis for Hybrid Security Architecture

Kamini[1] Rajiv Mahajan[2]
[1]Research Scholar [2]Assistant Professor
[1,2]IK GUJRAL Punjab Technical University, Jalandhar (Punjab), India

Abstract— In this paper WTLS (Wireless transport layer security) and TLS (Transport Layer Security) is discussed and analyze using OPNET Simulation. The WTLS is used for wireless devices security and TLS is used for wired devices security. This review paper shows that how the end to end security takes place between wireless clients to web server using hybrid security.

Key words: Security Analysis for Hybrid Security Architecture, Hybrid Security Architecture

I. INTRODUCTION

The motivation behind this research work is that in current wireless telecommunication networks, all the traffic is in the air is encrypted but end to end security is not provided between the wireless devices and WWW server[1,2]. In existing system double encryption and decryption is used for providing the communication between the mobile devices and a web server. On the other hand when transaction arrives at the gateway Through the WAP the data is encrypted and decrypted for wireless and again it will be Re-encrypted by gateway when the transaction has to pass through the wire[3]. At this time of Re-encryption the data can be hacked by any of the unauthorized user. The use of the Internet and mobile phones may integrate the satellite, radio and audio video communication. The main idea behind this research is to develop a composite security protocol that will provide a single secure channel for end to end communication [4]. The research work aims at providing the new services that will ensure the user privacy, data security and data integrity when transmitted over the mobile channel, using the firewall encryption in order to improve the end to end security in between the hybrid networks [5].Furthermore; this paper examines the security holes in between the wireless client and WAP gateway. The results is used in study is based on OPNET modeler 14.5 which helps to examine and analyze the security related issues for wired and wireless networks [6,7,8].

II. PROBLEM FORMULATION

Sami Jormalainen et al has discussed about the security of the WTLS is analysed. Firstly, the concept of data security is provided for the background information. The common security terms including authentication, privacy, and integrity are explained [9]. Then the most important parts from the specification of the WTLS are presented. The known security threats of WTLS are discussed and their impacts evaluated [10,11]. Finally the analyze is done based on the known facts. The WTLS is, finally, found to be quite a good security solution even with its known security problems. Some improvements for the protocol are necessary, but there is no need for any major changes. If the supported algorithms are combined in an appropriate way it is possible to guarantee a sufficient security level [12l. The null ciphers should not be allowed and the anonymous authentications should be denied [13]. The development work of the WTLS continues and the next version should be released in near future [14,15]. If all known security problems will be fixed then the WTLS provides enough security level.

The trend of mobile computing has many important applications for business, telecommunications, defense, real time control system and in accessing the internet. In future wireless networks will have two widely accepted characteristics [16]. Firstly, those will be based on all IP based network architecture and second those will integrate the heterogeneity in wireless access technologies [17]. The wireless application protocol was developed with an intention to support application programming for the resource constrained devices as mobile phone and the personal digital assistant.

The basic blocks of wireless transport layer security is initialized between the mobile devices and a wireless gateway and a transport layer security is initialized between the WAP gateway and web server [18]. In current wireless telecommunication networks, all the traffic is in the air is encrypted but end to end security is not provided between the wireless devices and WWW server. In existing system double encryption and decryption is used for providing the communication between the mobile devices and a web server. When transaction arrives at the gateway Through the WAP the data is encrypted and decrypted for wireless and again it will be Re-encrypted by gateway when the transaction has to pass through the wire. At this time of Re-encryption the data can be hacked by any of the unauthorized user.

The use of the Internet and mobile phones may integrate the satellite, radio and audio video communication. The main idea behind this research is to develop a compound security protocol that will provide a single secure channel for end to end communication. It aims at providing the new services that will ensure the user privacy, data security and data integrity.

III. RESEARCH METHODOLOGY

Fig. 1: Throughput

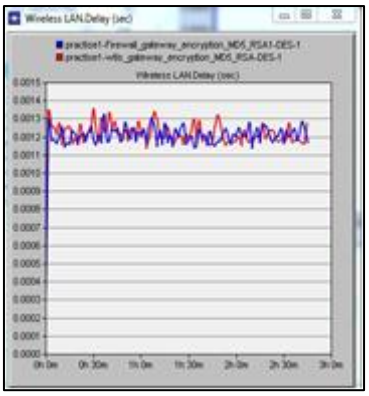

Fig. 2: Delay

Fig. 3: Load in wireless local area network

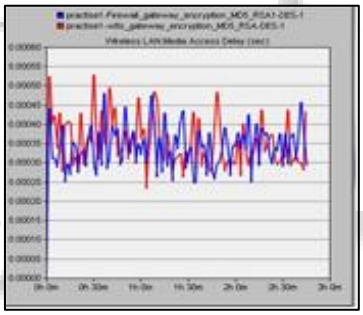

Fig. 4: Wireless LAN Media Access Delay

Fig. 5: DB query traffic received

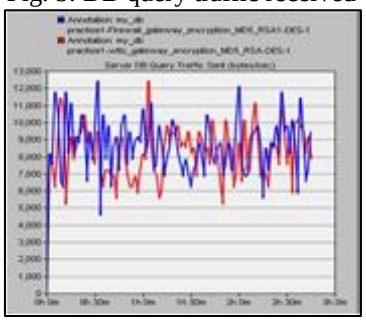

Fig. 6: DB query traffic sent

IV. OBJECTIVES

The objective of research is to improve end to end security between the wired and wireless devices. A new security protocol is introduced at that place in between the gateway called Composite security Protocol.

1) To identify and analyze the security holes in between the wireless client and WAP gateway.
2) To propose an Enhanced Protocol to overcome the security holes.
3) To design and implement the proposed composite security protocol architecture for wired and wireless devices.
4) To compare the performance of Transport layer security and Wireless Transport Layer Security with proposed protocol.
5) To improve the end to end Security in hybrid networks.

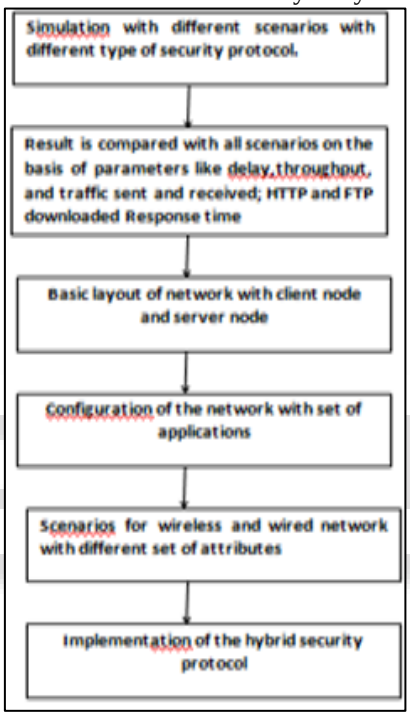

Fig. 7: Flowchart of objectives

V. CONCLUSION

In this research, the main focus on the simulation modeling of wireless devices and wired devices. Today mobile is accessed by most of the person in daily life just because of its features like low bandwidth, small in size and limited power consumption. The WTLS security layer is used for wireless devices and TLS is security layer used for wired devices. During the communication between the wireless devices and the gateway the encryption and decryption are used for WTLS protocol .Again while communicate through the gateway to web server re-encryption is required. This re-encryption leads to the problem of WAP gap. To remove this WAP gap the architecture design for the WTLS and TLS need to be modified. In this research we have analysed the performance of wireless and wired security model with the help of OPNET simulation tool. We the analysed the results of both security protocol on the basis of parameters like delay, throughout, data sent and received etc.

REFERENCES

[1] Rehunathan, D.; Bhatti, S., "Application of virtual mobile networking to real-time patient monitoring," in Telecommunication Networks and Applications Conference (ATNAC), 2010 Australasian, vol., no., pp.124-129, Oct. 31 2010-Nov. 3 2010doi: 10.1109/ ATNAC.2010.5679557
[2] Gustafsson and A. Jonsson, "Always best connected," IEEE Wireless Communications, vol. 10, pp. 49-55, 2003.
[3] Tanenbaum A.S. "Computer Networks," Prentice Hall India (PHI), November 1998.
[4] S. R. Tuladhar, "Inter-Domain Authentication for Seamless Roaming in Heterogeneous Wireless Networks," MSc Thesis, Faculty of Information Sciences, University of Pittsburgh, 2007.
[5] S. Tuladhar, C. Caicedo, and J. Joshi, "Inter-Domain Authentication for Seamless Roaming in Heterogeneous Wireless Networks," in Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'08), Washington, DC, USA, pp. 249-255, 2008.
[6] LAN MAN Standards Committee of the IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standard 802.11, 1999 Edition, 1999.
[7] FON. (2012). Fon Passes 7 Million Hotspots. Available: www.fon.com,Access date: 22/02/2013.
[8] WAP Forum, Wireless Application Protocol Architecture Specification, WAP-210-WAPArch-200100712-a, 12-July- 2001 version, latest version is available athttp://www.wapforum.com.
[9] Inwhee Joe; Jaehyung Lee, "An Enhanced TCP Protocol for Wired/Wireless Networks," in INC, IMS and IDC, 2009. NCM '09. Fifth International Joint Conference on , vol., no., pp.531-533, 25-27 Aug. 2009
[10] Filho, T.A.S.; da Silva, A.C.R.; Grout, I.A.; Rossi, S.R., "Network node with wireless and wired interfaces: Nios II processor and uClinux to development of a NCAP embedded (IEEE 1451.1) with two interfaces, wireless (IEEE 1451.5) and wired (IEEE p1451.2)," in Instrumentation and Measurement Technology Conference (I2MTC), 2011 IEEE , vol., no., pp.1-6, 10-12 May 2011
[11] Cordero Fuertes, J.A.; Philipp, M.; Baccelli, E., "Routing across wired and wireless mesh networks: Experimental compound internetworking with OSPF," in Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International , vol., no., pp.739-745, 27-31 Aug. 2012
[12] Freisleben, B., Jansen, R, (1997) Analysis of Routing Protocols for Ad hoc Networks of Mobile Computers, In: Proceedings of the 15th IASTED International Conference on Applied Informatics, IASTED-ACTA Press, pp. 133-136, Innsbruck, Austria.
[13] Raj Kumar Singh, Dr.A.K.Jain," Research Issues in Wireless Networks" in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2,issue 4,April 2012,ISSN 2277 128X
[14] Sue Webb," Growth in the Deployment and Security of 802.11b Wireless Local Area Networks in Perth, Western Australia" , Bradford Street, Mt Lawley, Western Australia 6050
[15] Dave Singel´ee, Bart Preneel," The Wireless Application Protocol (WAP). COSIC Internal Report, September 2003, Pages 1-5.
[16] Complete WAP Security from Certicom.Available: www.certicom.com pages 5-12.
[17] Website link http://www.tutorialspoint.com/wap/wap_introduction.htm"
[18] Security Issues in WAP and WAP Enabled Devices link http://www.users.cs.umn.edu/~htalkad/files/wap.pdf.Pages 34

