Analytical Study of Security Threats of Wireless Networks

K.P Singh
Assistant Professor, Dept. of IT
Institute of Technology and
Science, Ghaziabad,

Gaurav Kumar
Assistant Professor, Dept. of IT
Institute of Technology and
Science, Ghaziabad,

Abhay N. Tripathi
Assistant Professor, Dept. of IT
Institute of Technology and
Science, Ghaziabad,

ABSTRACT

The Wireless Technology has become indispensible and integral part of our lives. Lots of services are provided using various applications available through wireless network. Due to its characteristics and nature the wireless network is more vulnerable in terms of security threats. The wireless network is heterogeneous and widespread by interconnecting different types of networks services, information, persons, and transactions. For intruder it can be easily targeted for security breach. In this paper we are putting in our efforts to analyze various security threats available for wireless network and its level of severity based on damage done to either user or infrastructure.

Keywords

Wireless Networks, Security Threats, CIAAS Pentagon, Attack Severity Scale, Types of Security Attacks, Confidentiality, Authentication, Integrity, Secrecy, Availability.

1. INTRODUCTION

Wireless Network has the advantage of ubiquity, mobility & collaborations [17], lower cost of ownership, installation simplicity [16], speed and so on, but it is inherently less secure and easy target for security threats

There are various types of security threats which can breach the security of wireless networks. On the basis of its types and strength the security threats can be categorized in three levels in terms of harm and damage could be made to either users of wireless network or infrastructure of wireless networks. These categories of security threats can be termed as low level, medium level and high level. In this paper, we are enlightening the security threats and categorizing them. We have considered five critical components of wireless network such as Confidentiality, Integrity, Authentication, Availability and Secrecy. We have proposed a score level on scale of severity of a threat based on damage done by it. The scale of severity is termed as Attack Severity Scale that is evaluated based on total score which is calculated through proposed equation

$$\boxed{\text{Attack Severity Scale} = \sum_{i=1}^{5} \mathrm{CWi},}$$

Where CWi is consigned weight value of component of wireless network which is affected by any particular security attack. The CWi can vary from 1 to 5 where larger value defines more importance any particular component of wireless network.

2. TAXONOMY OF SECURITY THREATS

Wireless Networks security attacks are typically divided into passive and active attacks. These two categories are divided into some further categories [7]:

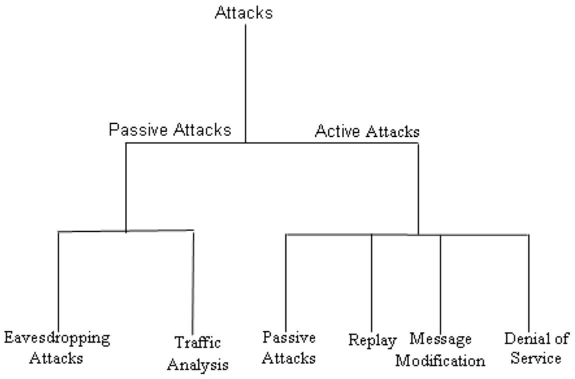

Figure 1. *Taxonomy of Security Attacks*

2.1Passive Attack

A Passive attack is a type of attack where intruder prime objective is gain the access on informational contents in an unauthorized manner. but modification is not the part of passive attack. In general approach following are the two subcategories under this approach of attack, eavesdropping or traffic analysis (analysis of flow of traffic). The briefings of the two subcategories are explained as below.

(i) Eavesdropping: The Intruders being vigilant for transmission for the content of message for example a person tapping into the transmissions on a LAN between two clients (node stations) otherwise tuning into transmissions between a wireless handset and a base station.

(ii) **Traffic analysis:** The intruder tries to analyze the pattern of communication between sender and receiver. One can have unauthorized access to large information content by viewing such type of data.

2.2 Active Attack

The prime objective in this type of attack is to change the contents of the message, data stream or file. The detection of such types of attack is possible but cannot be totally restricted. Categorically we can have following types under this type of intrusion.

(i) Masquerading: Impersonation of an authorized information user is deliberately considered to gain an unauthorized access to the vital information resources.
(ii) Replay: Retransmission of information is done by the attacker to the intended destination after capturing it in between the transmission.
(iii) Message Modification: The contents of the information deliberately modified (deleted, changed or rearranged).
(iv) Denial-of-service: The communication management or its use is prevented or prohibited by the attacker to the intended authorized users.

3. CIAAS PENTAGON

The security threats of wireless networks can impair it in terms of disturbance to a set of five critical components of wireless network that are liable to reliability and robustness of not wireless network but all kinds of computer networks also. We can refer it CIAAS Pentagon, where CIAAS is expanded as Confidentiality, Integrity, Authentication, Availability, and Secrecy which is shown in Fig. 2 [3].

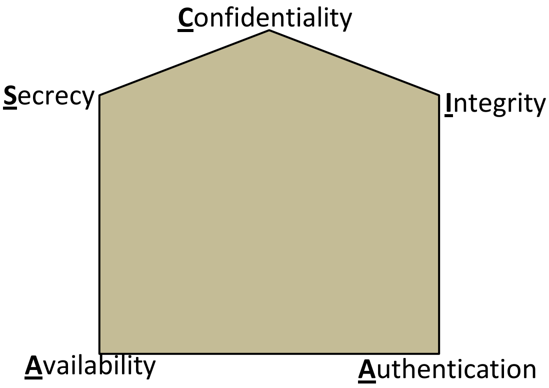

Figure 2. Outline of CIAAS *Pentagon*

3.1 Confidentiality

Confidentiality is referred to protecting the information from disclosure to unauthorized user by making computer network secure.
In today's era users generally access very critical information on wireless network such as banking details, credit card numbers, personal information, online transactions, trade secrets, government documents and so on. The loss or hacking of such information may lead to financial, social or personal mischief.

3.2 Integrity

Integrity of information refers to protecting information from being tampered by unauthorized users. For instance any transaction of $100 is tampered to $10,000 it can become very harmful for user.

3.3 Authentication

It is at the authentication stage that you prove that you are indeed the person or the system you claim to be. The network systems may incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and was sent by someone possessing the proper signing key.

3.4 Availability

Availability of network may lead to misuse of wireless two ways. Firstly the network can be accessed by outside users who are not actually authorized to do for example the network of Wi-Fi can be accessed by outsiders it is not made secure. Secondly the accessibility of network can be protected from access of authorized users if it is controlled by wrong users.

3.5 Secrecy

Secrecy of wireless network attempts applies cryptographic approach to hide information that can be gleaned by intruders and can be misused.

4. ANALYSIS FOR IMPORTANCE OF COMPONENTS OF CIAAS PENTAGON

Based on damage done by security attacks to wireless networks, we can consign the weightage, CW_i to each component of CIAAS Pentagon by considering financial, social, personal, infrastructure loss [2].

In CW_i i can vary from one to five as per importance of component. As per our analytical study of all five components the weight value of each component can be assigned as below [2]:

CW_1 = Confidentiality = 5

CW_2 = Integrity = 4

CW_3 = Authentication =3

CW_4 = Secrecy = 2

CW_5 = Availability = 1

Figure 3. *Weight value of each component of CIAAS Pentagon*

For instance if any attack affects all of the five components of CIAAS Pentagon then severity scale of that particular attack become 1+2+3+4+5 =15.

The above study derives an **Attack Severity Scale** as:

$$\text{Attack Severity Scale} = \sum_{i=1}^{5} CWi \qquad \text{……………(1)}$$

5. PROPOSED CATEGORIZATION OF SECURITY THREATS BASED ON ATTACK SEVERITY SCALE

There are so many types of security attacks done on computer networks. The number and types of attacks is comparatively more in case wireless network due its nature and characteristics. Though the importance and weightage of components of CIAAS Pentagon may vary as per case to case like for military networks confidentiality becomes more delightful where as for banking operations integrity becomes more important. We have consigned the importance of components of CIAAS Pentagon on an average[1].

In this paper we have put our efforts to analyze the severity of security threats for wireless network that is based on level of damage in terms of financial, social, personal etc. Based on our analytical study of various security threats of wireless networks these are scaled up as per value of 'Attack Severity Scale' [Equation 1].

The range of value of 'Attack Security Scale' can vary in the range from 0 to 15. This range has been divided into three levels[8].

Low Level → From 1 to 5

Medium Level → From 6 to 10 and

High Level → From 11 to 15

The below tables 1, 2 and 3 show the different categories of security threats[1], [2], [9]-[15] based on above given range of scale.

5.1 Low, Medium, High Level Security Threats

Table 1. Low Level Security Threats

S.No.	Security Threat	Affected Components of CIAAS Pentagon	Attack Severity Scale
1	Rogue access points	Authentication, Availability	5
2	Misconfiguration	Authentication, Availability	5
3	The evil twin	Confidentiality	5
4	The promiscuous client	Authentication, Availability	5
5	Viruses in devices	Integrity	4
6	Viruses in Network	Integrity	4
7	Endpoint Attacks	Authentication	3
8	802.1X EAP Downgrade	Authentication	3
9	AP Theft	Availability	1
10	Queensland DoS	Availability	1
11	802.11 Beacon Flood	Availability	1
12	802.11 Associate / Authenticate Flood	Availability	1
13	802.11 TKIP MIC Exploit	Availability	1
14	802.11 Deauthenticate Flood	Availability	1
15	802.1X EAP-Start Flood	Availability	1
16	802.1X EAP-Failure	Availability	1
17	802.1X EAP-of-Death	Availability	1
18	802.1X EAP Length Attacks	Availability	1

Table 2. Medium Level Security Threats

S.No.	Security Threat	Affected Components of CIAAS Pentagon	Attack Severity Scale
1	Denial of Service Attack	Availability, Integrity, Authentication	8
2	Eavesdropping	Confidentiality	5
3	Bluesnarfing and Bluejacking	Authentication, Availability, Secrecy	10
4	Network injection	Authentication, Availability, Confidentiality	10
5	Bluetooth Attacks	Authentication, Secrecy, Availability	6
6	PEAP and TTLS Configuration Weaknesses	Authentication, Confidentiality	8
7	Wireless Phishing	Confidentiality, Secrecy	7
8	Man in Middle Attack	Confidentiality, Authentication	8
9	WEP Key Cracking	Secrecy , Confidentiality	7
10	Shared Key Guessing	Authentication, Integrity,	7
11	PSK Cracking	Secrecy , Authentication, Availability	6
12	Application Login Theft	Authentication, Secrecy, Availability	6
13	VPN Login Cracking	Authentication, Secrecy, Availability	6
14	802.1X Identity Theft	Authentication, Secrecy, Availability	6
15	802.1X Password Guessing	Authentication, Secrecy, Availability	6
16	802.1X LEAP Cracking	Authentication, Secrecy, Availability	6
17	Misbehaving Clients	Authentication, Integrity	7

Table 3. High Level Security Threats

S.No.	Security Threat	Affected Components of CIAAS Pentagon	Attack Severity Scale
1	War Drivers	Confidentiality, Integrity, Availability, Authentication	13
2	Domain Login Cracking	Authentication, Confidentiality, Secrecy, Availability	11
3	802.11 Frame Injection	Integrity, Confidentiality, Secrecy, Availability	12
4	802.11 Data Replay	Integrity, Confidentiality, Secrecy, Availability	12
5	802.1X EAP Replay	Integrity, Confidentiality, Secrecy, Availability	12
6	802.1X RADIUS Replay	Integrity, Confidentiality, Secrecy, Availability	12
7	Caffe Latte attack	Confidentiality, Integrity, Availability, Authentication	13

6. CONCLUSION

Wireless Network is one of the revolutions in the field of Information Technology which is growing day by day. Due to its features and applications, it has become essential part of our day to day lives. There are so many advantages of use of wireless network such as saving of time, its ubiquity, mobility & collaborations [17], Lower Cost of Ownership, Installation Simplicity [16], speed and so on[18]. Along with all these benefits and features of wireless networks it also becomes more vulnerable and an easy target for security threats due to its nature and characteristics like mobility, accessibility, availability. In this paper we have put our efforts to not only list out most of the security threats of wireless networks but also done analytical study of these. We have constructed a scale to categorize the security threats based on the possible severity of damage done by any particular security attack. The attack severity scale is formed based on some critical components of wireless network. Our future efforts would be focusing on study of medium and high level security threats in depth then we would focus on analytical study of wireless security protocols followed by scope of enhancement of security measures of wireless network.

7. REFERENCES

[1] Network Security Fundamentals, By Gert DeLaet, Gert Schauwers, Published Sep 8, 2004 by Cisco Press. [2] Security Threats and Risk Mitigation in a Retail Network Environment, Columbitech White Paper February 2008.

[3] Swati Sukhija, Shilpi Gupta, " Wireless Network Security Protocols A Comparative Study, International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 1, January 2012.

[4] A Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[4] Arockiam .L. and Vani .B, ―A Survey of Denial of Service Attacks and its Countermeasures on Wireless Network, International Journal on Computer Science and Engineering, Vol.02, No. 05, pp. 1563-1571, 2010.

[5] Arunesh Mishra, William, A. Arbaugh, ―An Initial Security Analysis of The IEEE 802.1X Standard‖, University of Maryland, Department of Computer Science and University of Maryland Institute for Advanced Computer Studies Technical Report CS-T R-4328 and UMIACS-TR-2002-10 6 February 2002.

[6]Microsoft Technet Library, How 802.11 Wireless Works, Technical Reference, Available: http://technet.microsoft.com/en-us/library/cc757419(WS.10).aspx.

[7]Tom Karygiannis, Les Owens, "Wireless Network Security 802.11, Bluetooth and Handheld Devices, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Special Publication 800-48. [8]Gast, Matthew. *802.11 Wireless Networks: The Definitive Guide, Second Edition.* Sebastapol, CA: O'Reilly & Associates, Inc., 2005.

[9]Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, "Wireless Network Security: Vulnerabilities, Threats and Countermeasures", International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008.

[10]http://en.wikipedia.org/wiki/Wireless_security.

[11]http://www.sans.edu/research/security-laboratory/article/wireless-security1/.

[12]http://www.ciscopress.com/articles/article.asp?p=177383&seqNum=5.

[13]http://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks.

[14]http://www.esecurityplanet.com/views/article.php/3869221/Top-Ten-WiFi-SecurityThreats.htm.

[15] http://www.posdata.com/article-wireless-services.html.

[16]http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/work_from_anywhere/why_go_wireless/index.html

[17] http://kbserver.netgear.com/kb_web_files/N100688.asp.