IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 4, April 2016

Comparing Wireless LAN Standards and a Model Proposal for University Wireless Network Security with 802.1x

Mehmet Kösem[1], Ali Güneş[2]

Fatih Sultan Mehmet University, İstanbul[1]

İstanbul Aydın University, İstanbul[2]

Abstract: With the increasing use of wireless devices, information sharing, use of systems and many different applications were taken into account over Wireless Network. One of the biggest problems of Wireless network is that it might lead to many security gaps. When Universities, naturally considering academic staff, managers and student population the number of users in Wireless Network are many, therefore Universities are firms that need to be careful about security due to the different applications. In this research, the Security Methods and Standards were generally discussed, after comparing them, secure wireless network architecture has been designed for Universities and the design has been applied in Fatih Sultan Mehmet University.

Keywords: wireless networks, network security, 802.1x, campus network architecture.

1. WIRELESS LAN STANDARDS

With the development of technology day by day, and easy use of technology, improvements of Wireless LAN Standards and especially users' choice on mobile devices increased the interest in wireless networks. With the increasing use of wireless devices, information sharing, use of systems and many different applications were taken into account over Wireless Network. But wireless networks are the systems of realization of communication between air broadcasting devices and the devices that get that broadcast[1], during the exchange of data, there may be many people who can follow this broadcast and Users from different authorization levels who are included in that broadcast can reach the data within the network. Such situations may result in security vulnerabilities in many networks. There are many standards in wireless networks. These standards can be classified according to their security structures that are used in local networks and wireless networks. The characteristics of local wireless network standard are given in Table-1.

Table-1Comparison of Wireless LAN Standards

Standard	Release Date	Frequency Band	Data SPEED	Distance (Indoor)	Distance(Outdoor)
802.11	1997	2.4 GHz	1-2 Mpbs	10M	75M
802.11a	1999	5 Ghz	54 Mpbs	13M	100M
802.11b	1999	2.4 GHz	11 Mpbs	35M	110M
802.11g	2003	2.4 GHz	19 Mpbs	35M	150 M
802.11h	2003	5 Ghz	54 Mpbs	30M	100M
802.11n	2008	2.4 GHz-5 Ghz	248Mpbs	70M	250M
802.11y	2008	3.7 Ghz	54 Mpbs	500M	5000M
802.11ac	2013	5 Ghz	433 Mpbs		

As it was seen on the Table1, there is a big increase on historical development of Wireless LAN Standards, data speed and wireless coverage areas and the opportunity of users to reach the data faster and to benefit from the larger wireless network systems has increased the use of these systems. Naturally, several vulnerabilities have appeared in currently heavily used wireless network systems and security needs began to emerge in the wireless network

2. SECURITY WIRELESS NETWORKS AND USES METHODS

The ISO / IEC 27001 security, the confidentiality of information assets of an organization (unauthorized information, institution or to be available to process or disclosure to be provided to property), integrity (removal of the guarantee feature of the accuracy of the existence and completeness) and usability (the feature is not available at the request of a competent authority) protection, the right technology, knowledge by using the right purpose and the right way in any medium, preventing the acquisition by undesirable persons, persons and institutions threats they may encounter when using this technology and making the analysis of the hazard is defined as taking the prerequisite measures .

Equivalent Privacy (WEP Wired)

Wired Equivalent Privacy (WEP), 1999 Wi-Fi security

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 4, April 2016

when the standard is set as 64-bit encryption using the development process has increased to 128-bit encryption and security for up to 256 bits, but has been widely used 128-bit. Despite the development process used by many security vulnerabilities due to be officially since 2004, it has been proposed.

Wi-Fi-Protected Access (WPA)

Wi-Fi-Protected Access began to use in 2003 is a Wi-Fi Standard which is developed to completely eliminate the WPA,WEP openings. WPA-PSK(Pre-shared Key) gained a great advantage against WEP by using 256 bit switching technology also monitored the traffic between user and client by adding a key to each transmitted packet with Temporal Key Integrity Protocol. Despite these progresses, since WEP used RC4 Algorithm, in a short time, Security vulnerabilities and Security Weakness have appeared.

Wi-Fi-Protect Access II(WPA2)

Wi-Fi Protected Access 2 has been used as of 2006. Using the AES algorithm and CCMP (conter cipher mode with block chaining message authentication code protocol) is used instead of TKIP. It is much more powerful encryption method than CCMP TKIP. WPA2 is the most important standard recommended to use but an opening was found in WPA2 and the way to take advantage of this vulnerability, you must be connected to the network.

Media Access Control (MAC)

MAC (Media Access Control-Media Access Control) address is defined as Unique MAC Address defining itself with letters between A-F and numbers between 0-9 of a hardware device that wants to connect to system in wired and wireless network system. Thanks to MAC Address, MAC Addresses and credentials of users are added to Access Point Controller Device, Access Point. With the Help of The MAC Address Authorization, Uses can access Network System if MAC Address is true or attached in the system. MAC Address Authorization was a very important authorization method in the pastbut nowadays it is generally preferred in non-continuously variable Institution which has low user number. In large organizations updating, controlling and managing MAC Addresses is difficult. In addition, by listening to network, obtaining or changing the MAC Addresses of Involved users in system makes it difficult to identify this process and causes system vulnerabilities.

Service Set Identifier(SSID)

A service set identifier, is the name of the wireless network broadcast. The name of the broadcast service set identifier with the feature of wireless network card can be perceived by the client. Once user selected this broadcast, they can get into system with password, involved users can communicate and share the data between the other users and hardware in the same broadcast. Hardware that broadcast SSID broadcasts to a specific area, Different users in the concerned area can see the name of the SSID to reach the system. Therefore SSID hardware chooses the option that disables the name of the broadcast for safety. In this way, security can be provided on a wireless network.

802.1x Authentication

802.1x Authentication is a port-based authentication standard to help improve security of wired and wireless networks. 802.1x uses an authentication to verify users and to provide them a network access. In wireless network 802.1x can work with WPA,WPA2 and WEP keys.This type of authentication is typically used when connecting to the work area network[3].

In 802.1x wireless network system gets included in control of identity by A client requesting connection on Access Point (AP) Extensible Authentication Protocol (EAP) sends a start message, if successful it reaches the system ,if fails it cannot reach the system because the port that it will use to get in is closed[4].

Extensible Authentication Protocol (EAP)

With EAP a random authentication mechanism authenticates a remote access connection. The exact authentication scheme is determined by the consensus between remote access client or the Remote Authentication Dial-In User Service [RADIUS] server. EAP allows for an open-ended conversation between the remote access client and the authenticator. Interview consists of the information which is requested by the authenticator and responses of the remote client. When all questions have been answered successfully, it passed the remote access client authentication. A specific EAP authentication scheme is termed an EAP type. EAP authentication methods such as MD5, TLS, TTLS, PEAP, LEAP are used [5].

Table-2 Comparison of EAPType

	MD5	**TLS**	**TTLS**	**PEAP**	**LEAP**
Standard	Open	Open	Open	Open	Company
Client Certificate	x	✓	X	x	x
Service Certificate	x	□	✓	✓	x
Security	x	Strong	Strong	Strong	Weak
User DATABASE	Open Text Password	Active directory	Token systems, SQL,LDAP	Active Directory, NT Domain	Active Directory, NT Domain
Dynamic Key Exchange	x	□	□	□	□
Mutual Authentication	x	□	□	□	□

As it was seen on the Table-2 comparison of Eap,802.1x standard EAP authentication methods have been examined and the method of EAP-PEAP, and in addition, have been proposed for use with EAP-MSCHAPV2.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 4, April 2016

3. UNIVERSITY WIRELESS SECURITY METHOD

Wireless Network Security methods were examined, due to the security weakness in used network safety methods, resistance against the attacks which were made, encryption methods and its importance in today's technology, 802.1x was proposed for Universities. In addition to the standard, to be raised to a higher level of wireless network security enhanced by virtual network architecture and design examples for use in university design method has been created and has been implemented in the Fatih Sultan Mehmet Foundation University. Due to faculties, institutes, departments located in the University and professors, administrative staff, number of students, the most appropriate authentication and network security standard IEEE 802.1x was adopted. In addition to this standard by introducing the virtual network architecture because of differences in user, created separate virtual networks for different user groups and virtual networks to communicate between each other restrictions are implemented.

An additional security system was created on the virtual network architecture and the network, packet take-give, bandwidth; broadcast control has become more manageable by making network traffic more flexible. Below, one can see the methods for Universities and basic features and concepts of network which is designed for FSMVU.

3.1Virtual LocalArea Network

Virtual local area network (LAN) is connected to the network on a wired or wireless network system.

University Virtual Local Area Network Design

Analyses were performed according to security level of user groups in the wireless network architecture and as a result of these analyses the proposed virtual network design was given in the Table-3.

Table-0 VLAN Sample Design Table

VLAN Name	Tag Id	Ip Address	Net mask	Default Gateway	DHCP Server
Student_vlan	2000	10.10.0.2	255.255.255.0	10.10.0.1	10.10.0.1
Academy_vlan	2001	10.10.1.2	255.255.255.0	10.10.1.1	10.10.1.1
Bim_vlan	2002	10.10.2.2	255.255.255.0	10.10.2.1	10.10.2.1
Administrative_vlan	2003	10.10.3.2	255.255.255.0	10.10.3.1	10.10.3.1
Server_vlan	2004	10.10.4.2	255.255.255.0	10.10.4.1	10.10.4.1

3.2 Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol is a directory service standard. The information contained in the directory access protocol and structure of the database is called nominal. Directory access protocol information in the database is described as a list that contains data about each of the objects and has an ordering logic. Openldap, Sun directory server and directory services such as Microsoft Active Directory can be used for LDAP [7].

Active Directory (A.D)

The directory service network is a network management system that we can edit permission and authorization of users who can reach any kind of data, shared resources, and hardware devices on the network system. Another important feature of the directory service is the definition of user and group users can access the directory service after a certain authentication. Different policies can be taken for users and groups according to the authentication.

Table-4 The Directory Service (AD) University Design Sample

Organization Unit	Groups	Users
Administrative	Information Technology .D Student Affairs .D	ITD.User1 SAD.User1
Academic staff	Faculty of Engineering Institu of Fine Arts	FE.User1 IFA.User1
Student	Faculty of Arts Vocational School	FA.stuUser1 VS.stuUser1
Server		S.User1
Guest		GUser1

The directory service design model for universities are given in the Table-4

The directory service certification service

Directory certificate service is a service used in software security systems and makes use of public key technology with public key infrastructure (PKI Public Key Infrastructure).

3.3 Authentication and Authorization server (RADIUS Server)

RADIUS (Remote Authentication Dial-in User Service) makes the process for users who connect remotely server user name-password authentication reporting/ access time accounting and authorization

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 4, April 2016

Radius can be used as server for free radius and like Microsoft network policy server[8].

Network Policy Server (NPS)

In the draft for University, Microsoft NPS service was used for RADIUS because of simplicity of management, high level of security and the ability to configure it in a few easy steps. By NPS, Network access policies were created in the entire university for authorization procedures, connect request authorization, client health. For wireless connections EAP methods -as we can see the data in the Table-2 in 802.1x standard can be enlarged protectively due to the high level of safety. Protected Extensible Authentication Protocol (PEAP), and in addition to PEAP for secure password authentication is used with MS-CHAP v2 together.

3.4 Access Point Controller

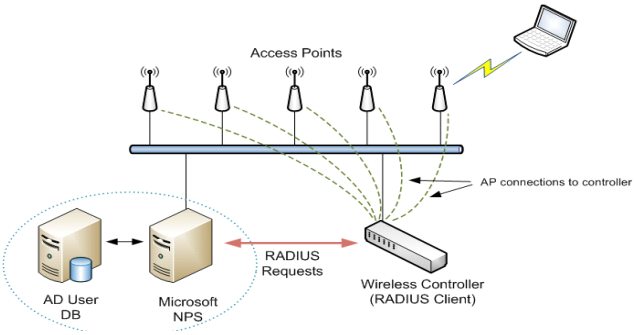

Figure-1 Access Point Controller

In Figure-1 Communication between the access point and radius server is managed by the access point controller. Access Point (AP) is a hardware device in the wireless network system that SSID was broadcasted and connection re-question of users over the broadcasted SSID. AP is a device that controls, reports and manages all AP Devices and when connection request was transmitted to AP devices, it tells us by which configuration 802.1x will be affected. The access point controller designed on virtual networks, it is necessary configurations to communicate with the Network Policy Server.

3.5 Switch

It constitutes an important part of the network switch and routing data communications in a wireless network system. Even if the wireless network broadcast was made on the air, we must create the configuration on switch key. Because devices such as AP devices, access point, firewall and network policy server communicate via Ethernet port or Fiber connection.

3.6 Firewall

The firewall is a hardware and software system that is developed to protect the resources on the network system against the attacks on the internal network system or another network system. Generally it can be inferred as network solution that controls traffic between the external and internal network according to the rules of institution. Thus, On that draft , it needs to be defined that on which virtual network number it will connect the internet by creating zones and Interfaces and also IP address needs to be defined by forming DHCP to identify the traffic on the virtual networks and for user to get an IP address according to the rules we made .

4. TESTING THE STRUCTURE OF THE DESIGNED NETWORK

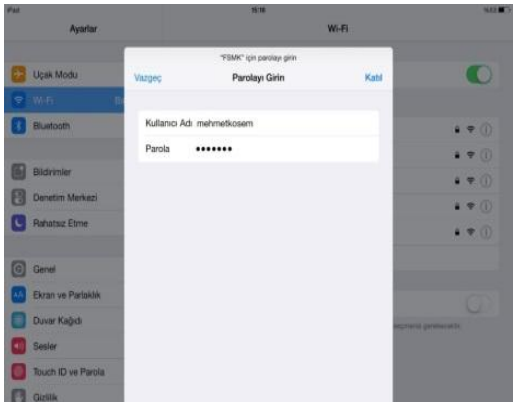

Figure-2 Username and Password Screen

Figure-3 Certification

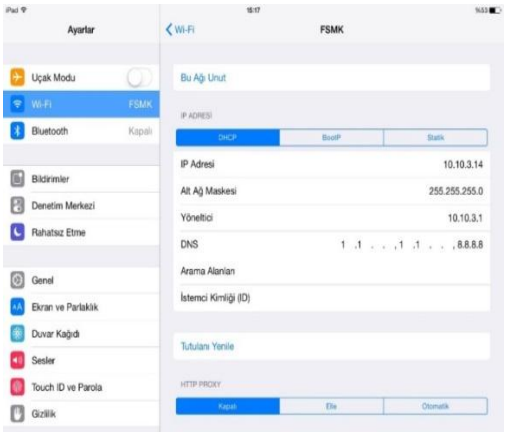

Figure-0 Wireless Network Information

In Figure-4, after entry and certification (Figure-2 and Figure-4),user Mehmet Kosem, in the 802.1x standard test, His identity was approved Firewall transferred the user according to virtual network number of user to administrative _test virtual network and assigned the user

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 4, April 2016

IP Address as 10.10.3.14,default gateway 10.10.3.1and User could reach IOS operating system.

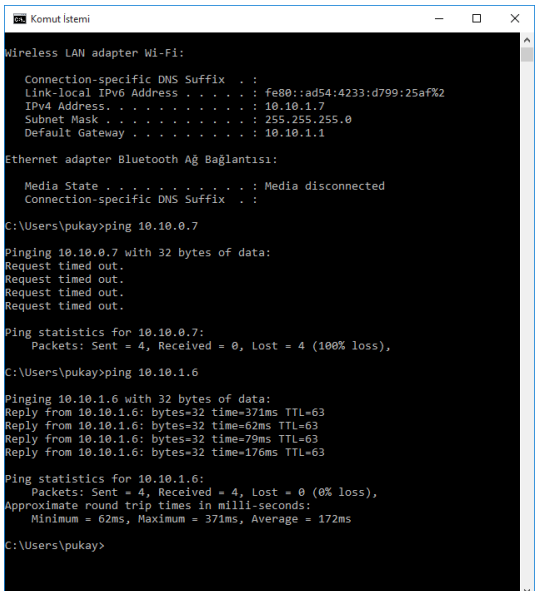

Figure-5 IP Address Configuration and Ping Information

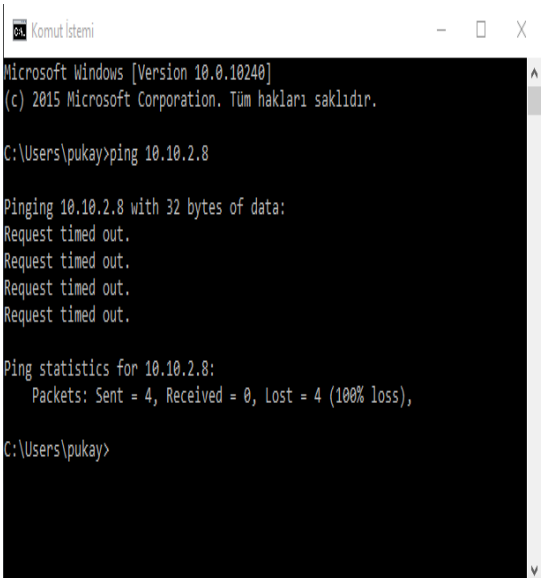

Figure-6 Ping Information

After his identity was approved in 802.1x standard, the user Yocal reached the system on academic virtual network and he received the 10.10.1.7. But he couldn't send data to (As seen in Figure-5) 10.10.0.7 and (As seen in Figure-6)10.10.2.8 IP addresses. Although he could communicate with the academic network since he was in the network, he couldn't communicate with the Student and Administrative Networks. Thus Communication security between virtual networks was increased

5. CONCLUSIONS AND RECOMMENDATIONS

The use of a wireless network with the development of technology is increasing every day. With the increase in the utilization rate of authentication and many studies are performed on wireless network security. In this study, wireless network security methods have been worked out and the 802.1x standard for wireless network authentication and access control systems have been proposed. In this study, as a result of the applications of 802.1x standard in University wireless network Security, Designs that has hardware and software-free material have been proposed and It is claimed that use of 802.1x standard after identity approval on wireless network must be together with virtual network to increase the security of Network System. Also 802.1x standards was examined with Eap (PEAP) and since still cannot be revealed the results of encryption and listening to the data when used with EAP MSCHAPV2, using them together has been suggested.

In this study, wireless network security authentication server, certificate server, directory service server, Access Point controller, network switching equipment, test environment of firewall devices have been created and the configuration process for 802.1x standards at the university were carried out. After the test, results have been reported and methods have been proposed for the university.

REFERENCES

1. ERKINAY M,Wireless Networks and Wireless Network Security, YuzuncuYilUniversity,Unpublished Master Thesis, Istanbul, 2006,
2. CALDER, A., "Nine Steps to Success: An ISO 27001 Implementation Overview", IT GovernenceInstitute Conference, (2006)
3. http://windows.microsoft.com/tr-tr/windows/what-are-wireless-network-security-methods#1TC=windows-7
4. tr.wikipedia.org/wiki/IEEE_802.1X
5. http://csirt.ulakbim.gov.tr/dokumanlar/Ag_Kimlik_Denetimi.pdf
6. http://Ulakbim.gov.tr
7. http://docs.comu.edu.tr/howto/ldap-howto-intro.html
8. yunus.hacettepe.edu.tr/~b0145561/bilg_aglar.html
9. http://www.chip.com.tr/haber/merakli-komsulara-son-wi-fi-korumali-erisim_41190_2.html