USING IEEE 802.1x STANDARD IN SECURITY OF ELECTRONIC HEALTH RECORDS

Meriç ÇETİN

Department of Computer Engineering, University
Pamukkale, Kinikli Kampusu, 20017 Denizli,
Turkey
e-mail: mcetin@pau.edu.tr

Murat AYDOS

TUBITAK, The Scientific and Technological
Research Council of TURKEY,
Tunus Caddesi No: 80, 06100, Kavaklıdere,
Ankara, Turkey
e-mail: murat.aydos@tubitak.gov.tr

Abstract— **In this study; the solution of some security problems encountered in the protection of the data security, the methods of automatic VLAN configuration and use of IEEE 802.1x Standard for the procedures of identity authentication of all users to access the network have been applied. With the use of IEEE 802.1x Standard in securing of Electronic Health Record (EHR), the protection of hospital data has been aimed. Those data should be protected against the attacks from both inside and outside of the Hospital, and were allowed for access only by the authorized users that only with the permissions granted to them. Together with the automatic VLAN organization; the accuracy and the confidentiality of the data, prevention of lose, protection in the units grouped according to authorizations, and prevention of unauthorized access have been implemented.**

Keywords: EHR, IEEE 802.1x, Automatic VLAN, Security.

1. INTRODUCTION

The importance of the communication systems has increased rapidly and computers become indispensable in our daily lives as a result of the prevalence of technological systems and the Internet. During this rapid development, some of the standards in information systems have not been matured properly but put into application, so the control and management of networks have become more difficult and also some security problems in networking have been occurred. Therefore, implementation of some features such as confidentiality, originality and integrity of data in information systems are very important [1, 2].

It is necessary to protect private data processed and used in electronics environments according to rules of the most governmental health organizations. If the private data do not keep safe, security of the personal data, privacy and integrity faces to a risk. To overcome such risks in Hospital Information System (HIS), the confidentiality must be ensured by means of applications of identity authentication, role based access control and cryptographic methods. Also, it is required that the clinical data of the patients as well as the doctor's, prevention of economic loss and the protection of the reputation of the institution should be secured.

As a case study, in the related circulars of Health Ministry of Turkey, the subjects of EHR security, patient privacy and patients' rights are dealt with. To this effect;

- In order to become sure of the doctor and the patient, authentication in electronic environment should be performed.
- Role based access control should be ensured in the electronic environment for patient privacy.
- Patients' data should be confidentially transferred in the electronic environment.

Due to the variety of the types of services and roles in the public institutions that offer health services, access to the required information requires quite a hard and a complicated process. Therefore, the methods for producing and accessing the information should be designed very well. As the subjects such as producing and sharing data and information, reliability, saving time and resources make the foundation of the HIS. Hospital networks should have information systems that can reply to the requests and the needs of the system on 7 days 24 hours bases.

The fact that the data in electronic environment can be accessed by vast amount of people has increased the rate of risks about these data. Prevalence of the application of information systems in hospital networks has introduced some problems in terms of data and information security. The confidentiality and the privacy of patients and the records of diseases in particular are important. Another aspect of the security is the authorization levels in medical records. Therefore, it is important that the data should be protected and different persons should have different access rights to these data [1, 2].

The subjects of the “Security of Health Records” and “Privacy of the Personal Records” are the subjects which are independent from each other, however, the collection and the storage of these health records should be performed in line with the security criteria in all circumstances. After ensuring these conditions, the issue “who will access these data with which rights?” should be determined. After this stage, there comes the privacy of the personal health records and the level of access rights determines the limits of the privacy. Therefore, access to these data including the personal health records should be restricted and the authorizations should be ranked. Some of the security elements that cause danger for hospital networks can be listed as follows:

- Possible mistakes that could be made in the organization of the static VLAN.
- Failure to control and audit the access to the network via personal computers.
- Encountering problems in deploying the updates from a single point and in a short period of time to the computers that are not members of the domain.
- The fact that anyone in the hospital can access personal computers and the servers over the allowed ports over the firewall.
- Failure to proposed restrictions changing with time.
- Failure to prevent locally access of the user-non-grata.

2. THE PROPOSED AUTOMATIC VLAN AND IEEE 802.1X AUTHENTICATION MECHANISMS

For solution of the mentioned these types of security problems that could be encountered in vital EHR security, the method of automatic VLAN organization and having the users who will access the network of the hospital perform the authentication procedures with IEEE 802.1x Standard both in cable and wireless networks of the hospital have been preferred. These mechanisms are explained in section 2.1 and section 2.2.

2.1 IEEE 802.1x Authentication Mechanism

IEEE 802.1x Standard is used for allowing authenticated network access to cable and wireless networks and performing port based access control [3, 4]. Although this standard means a framework for authentications and authorizations, it is very eligible for IEEE 802 based local area network and it is very sensitive against the security attacks. IEEE 802.11i Standard uses 802.1x authentications based with Extensible Authentication Protocol (EAP) for mutual authentication. EAP is an authentication environment supporting multi-authentication methods and the connection to the LAN is performed by this protocol [5].

Use of an authentication server (Remote Authentication Dial in User Service-RADIUS) between the client and the access point, IEEE 802.1x Standard allows authentication and port based access control. As shown in Figure 1, this standard is composed of three parts which are Supplicant, Authentication Server and Authenticator.

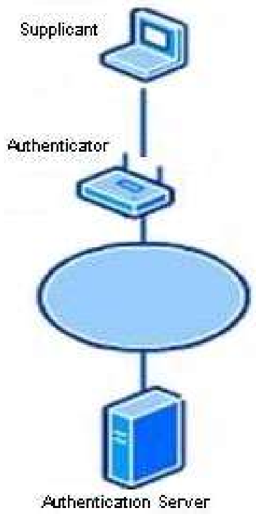


Fig.1 IEEE 802.1x Authentication Components

Supplicant; after making request for authentication, it sends the user name/password to the Authenticator and it uses EAP for this communication [4]. Authentication Server; is a server that performs authentication process like RADIUS. It verifies the username/password information that comes from Supplicant and determines whether it has authorization for access or not. Authenticator is an access point between Supplicant and Authentication Server, ensuring 802.1x port security and checking access to the network. It gets username/password information from the user, passes it to RADIUS and performs the required filtration or allows the action based on the results coming from the RADIUS [3, 6, 7]. The operation principle among different components of IEEE 802.1x Standard and these components are shown in Figure 2.

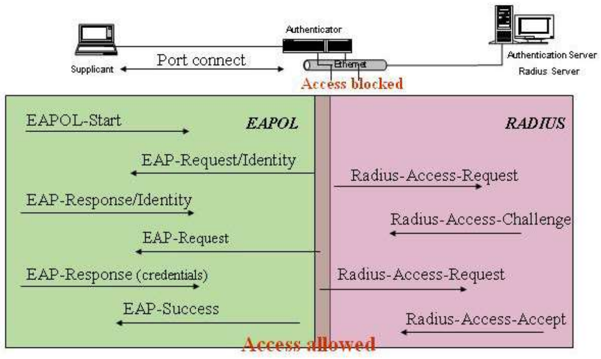


Fig.2 IEEE 802.1x Authentication Process and Message Exchange

- Firstly, Authenticator filters all external traffic of input/output created by Supplicant, except for those required for authentication.
- Then, it starts to communicate with Supplicant by means of EAP over LAN (EAPoL) protocol.
- Supplicant requests connection from Authenticator.

- When Authenticator receives the connection request, it keeps all ports closed and opens a port only itself between the Supplicant.
- After the Authenticator asks for the identification from the Supplicant, the Supplicant sends its identity (username/password). The Authenticator sends this identity information to a RADIUS server.
- RADIUS server matches the identity that was enquired by Supplicant with the information that was kept in the database. When identification procedure is performed, the Server sends the "Accept" message to the Authenticator.
- The Authenticator, after these procedures, makes the port of Supplicant into the authorized port. So, the access of Supplicant is guaranteed [3].

2.2 Automatic VLAN Mechanism

Recognized, today, as one of the most important network organization techniques are Virtual Local Area Networks (VLANs). These networks are created by logical grouping of the ports on a switch that makes switching processes, using source and target Media Access Control (MAC) addresses. Although they seem like a single network physically, virtual networks are created with VLAN application and these virtual networks carry most of the features of non-virtual networks. Generally, VLANs are arranged according to the settlement of the users, their function, department or the application protocol that is being used.

The created VLAN is assigned to switch ports dynamically or statically. While creating a static VLAN, network administrator includes certain ports of the switch into VLAN. Until the ports have been changed by the network administrator, they remain as members of this VLAN. In dynamic VLAN creation, network administrator uses MAC based or user based 802.1x authorization methods during the set up stage and performs VLAN membership [4].

In MAC based 802.1x authorization; MAC addresses of all devices on the network are taken into a database and VLAN membership of the addresses on the network is completed. When the place of a user on the network is changed, the switch in the new place where the user has started finds from the MAC database which VLAN the user were a member of, and makes that port a member of that VLAN. So, the changes are easily made over network management terminal without having to re-organizing the physical connection. This feature improves the network performance and it eases network management and security. Because broadcast traffic is imprisoned into VLAN, the visible bandwidth of the system increases and data flow at higher speeds are ensured.

User based 802.1x authorization; is made with IEEE 802.1x port authentication. When the user has somehow successfully introduced itself to the network by using this authentication, it has automatically been placed into its own VLAN. For this, the user firstly sends 802.1x information to Internet Authentication Service (IAS) server with RADIUS protocol [8]. Remote access policies written in IAS server are used to decide whether or not the user is a member of a special VLAN. If the user account is a part of a VLAN group and if the authentication has successfully been completed, the user information which is associated with the VLAN group is sent back to the Authenticator by using RADIUS feature. When the user port over the Authenticator matches dynamically with VLAN information, it is assigned to the VLAN, and it becomes a member of the user port based VLAN [4]. An example of this mechanism is shown in Figure 3.

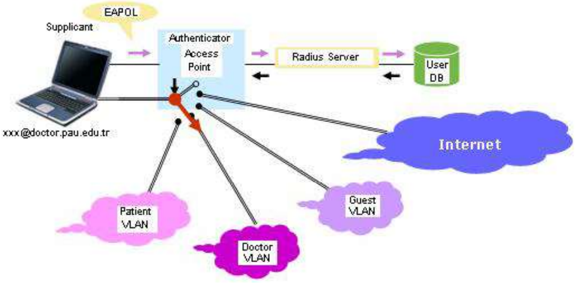


Fig.3 A Sample of Automatic VLAN and The IEEE 802.1x Authentication Mechanisms

3. A CASE STUDY OF THE PROPOSED MECHANISMS

The steps for 802.1x authentication process for users and automatic VLAN configuration are listed in seven titles below.

3.1 Active Directory Configuration

Within the proposed solution;

- It is suggested that in order to open user sessions in their domains, authentication should be performed in a De-Militarized Zone (DMZ) separate from HIS server DMZ.
- The authorization rules for the users and computers in Active Directory Domain are defined with the group policies.
- Various group policies can be applied within the whole hospital networks by dividing it in to different functional sections.
- In order to manage the workstations and the users in the system from a single point, Active Directory Domains are established, various sections are defined on the basis of department or task, and then the users and the computers are located in to these departments.

As shown in Figure 4, domain trees are built within a single forest structure by establishing sub domains for each location of Hospital Networks. By defining unique group policies using the benefits of Active

Directory Domain structure, section-based rights and rules are written.

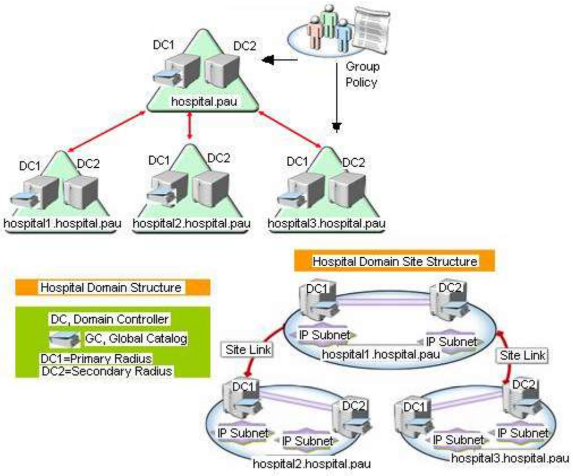


Fig.4 The Structure of a Hospital Active Directory Domain

By adding users, computers and sources located at different floors of the hospital in to the same Windows group, it can be made possible that all these elements would be in the same VLAN therefore in the same network group. Users should be divided in to separate groups in order to control the access to the network in the hospital. In the last step of configuration the Active Directory concept, the remote access permissions for the users in the domain are set.

3.2 IAS Configuration

Each domain contains its own IAS server within its domain, and for each domain authentication and accounting processes are being performed on these IAS servers [8]. This structure prevents additional RADIUS traffic between remote nodes in separate domains. As shown in Figure 5, while building IAS servers in domain, in each domain RADIUS server pairs are located as primary and secondary servers.

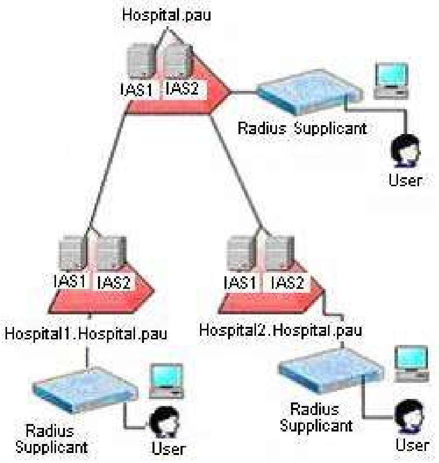
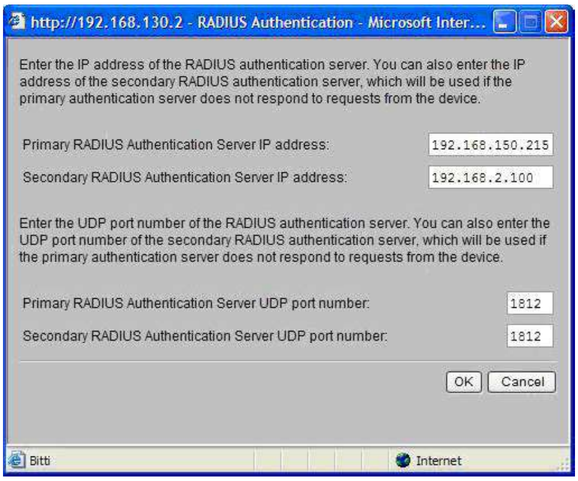


Fig.5 The Configuration of IAS Servers

This prevents a single failure point in authentication, authorization and accounting processes of single IAS server. With the use of backed up servers; the excessive authentication and accounting demands can be balanced. These servers and the port numbers should be adjusted for IAS structure. Furthermore, the main floor switches should be presented to IAS as RADIUS clients.

3.3 Configuring The Edge Switches As An Authentication Switch

Processes such as authentication, accounting and security settings on the edge switches are completed on RADIUS authentication menu. Port settings of primary and secondary RADIUS servers are being entered using this authentication menu. All the security settings on all the ports of the switch are set to provide Access for authorized users. These settings are shown in Figure 6.


http://192.168.130.2 - RADIUS Authentication - Microsoft Inter...

Enter the IP address of the RADIUS authentication server. You can also enter the IP address of the secondary RADIUS authentication server, which will be used if the primary authentication server does not respond to requests from the device.

Primary RADIUS Authentication Server IP address: 192.168.150.215

Secondary RADIUS Authentication Server IP address: 192.168.2.100

Enter the UDP port number of the RADIUS authentication server. You can also enter the UDP port number of the secondary RADIUS authentication server, which will be used if the primary authentication server does not respond to requests from the device.

Primary RADIUS Authentication Server UDP port number: 1812

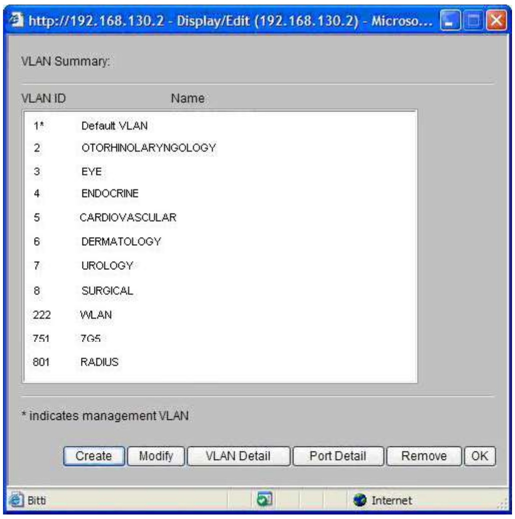
Secondary RADIUS Authentication Server UDP port number: 1812

Fig.6 Determination of Primary and Secondary RADIUS Servers over Edge Switches

3.4 The Configuration of Backbone and Edge Switches for Automatic VLAN

For automatic VLAN configuration the following actions are performed:

- As shown in Figure 7, all the VLANs are defined on the backbone switch, interfaces are created, and IP addresses are assigned to these interfaces.
- The link type of all the ports to which floor level switches are connected is defined as *Trunk* [4]. This enables multiple VLANs on that port be defined.
- There might be some cases in which users might desire to access to the main network from any single room in the hospital. In order to provide this type of access, all the defined VLANs on the network should also be defined on the edge switches.


http://192.168.130.2 - Display/Edit (192.168.130.2) - Microso...

VLAN Summary:

VLAN ID	Name
1*	Default VLAN
2	OTORHINOLARYNGOLOGY
3	EYE
4	ENDOCRINE
5	CARDIOVASCULAR
6	DERMATOLOGY
7	UROLOGY
8	SURGICAL
222	WLAN
751	7G5
801	RADIUS

* indicates management VLAN

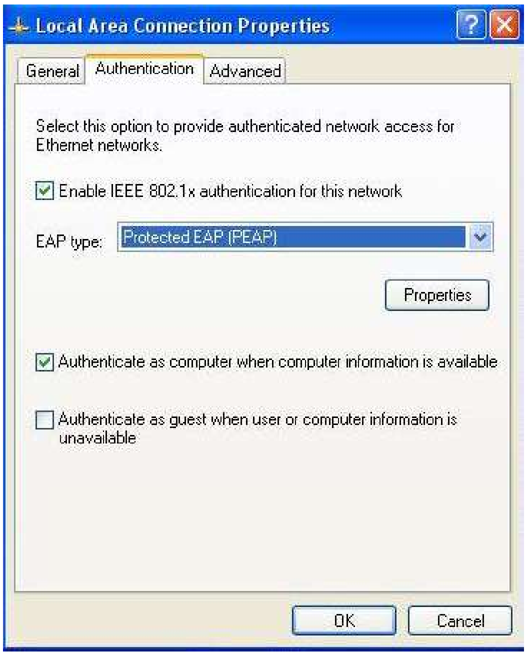
Fig.7 Entering All of VLANs over the Edge Switches

A simple example for this type of configuration is given below:

[SW7700] vlan 2
[SW7700] vlan 3
[SW7700] interface vlan-interface 2
[SW7700] interface vlan-interface 3
[SW7700-vlan-interface2] ip address 192.168.2.1 255.255.255.0

3.5 Configuration of User Computers for PEAP MS-CHAPv2

Windows XP SP2, Windows XP SP1 or Windows 2000 SP4 must be installed on computers in order to activate PEAP MS-CHAPv2, and then the settings shown in Figure 8 should be realized.


Local Area Connection Properties

Select this option to provide authenticated network access for Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

☑ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

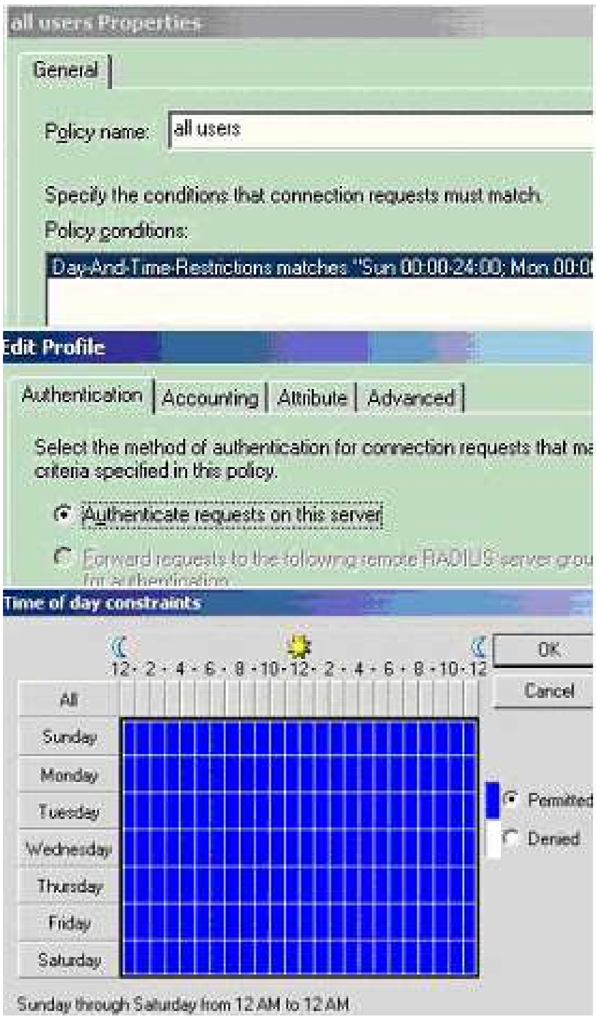
Fig..8 Setting of the IEEE 802.1x Authentication on User Computers

3.6 Configuration of The Certification Server

In the case of PEAP MS-CHAPv2 type of authentication; computer certificates on the IAS server and computer certificates on the client side should be distributed. To do this, root certificates are needed. Additionally, IAS and certificate server needs to be implemented on the network domain controller. Furthermore, group policies should be written for automatic registering computer certificates in the domain.

3.7 Determination of Remote Access Policy

Authentication and authorization steps are being performed according to the remote access policies configured on the IAS and user account features on the Active Directory. For each remote access policy the followings are defined: Whether to grant access to users granted that several expectations met, given the fact that the access permissions are granted what type of profile and features will be there for the access; such as on which VLAN this access will sit, duration of session. As shown in Figure 9.


all users Properties

Policy name: all users

Specify the conditions that connection requests must match.

Policy conditions:

Day-And-Time-Restrictions matches "Sun 00:00-24:00; Mon 00:0

Edit Profile

Select the method of authentication for connection requests that m criteria specified in this policy.

● Authenticate requests on this server

○ Forward requests to the following remote RADIUS server grou for authentication

Time of day constraints

● Permitted
○ Denied

Sunday through Saturday from 12 AM to 12 AM

Fig.9 Setting Access Policy Conditions

4. CONCLUSION

In this work, in order to solve some security threats against EHRs, automatic VLAN setup has been performed in both wired and wireless hospital networks. To support this, the authentication for all users accessing to the networks should be done with the use of IEEE 802.1x Standard according to the proposed method. With the use of the proposed method, it has been provided that the hospital networks can be managed automatically from a single point, the automation system is able to run continuously with maximum performance and also many applications are able to run in synch with the use of the features of the software and the hardware. All these advances proposed in our method are able to provide the access control to network resources, prevent unauthorized access to the network both from internally and externally, and provide access to important information only to authorized users with certain level of permission. With the very first use (on the networks of all Turkish Hospitals) of this solution proposal the following benefits are expected [9, 10];

On the security side

- Protecting the hospital networks against attacks by use of some limitations and restrictions on IP and port level
- Providing security between separate VLANs that are not connected to the firewall
- Preventing attacks from wide area networks to the center of the hospital networks
- Presenting security by giving access to HIS and Laboratory Information System (LIS) servers only from predetermined ports such as SQL and ORACLE
- Increasing performance and controlling data flow on the system by the use of the role based authorization.

On the Authentication Phase

- Determining and defining the access hours to Internet or hospital automation by the users
- Preventing unauthorized user access to electronic services
- Keeping the internal electronic office documents in a secure place in the center and providing access to only authorized users to these documents
- Performing authentication process for domestic hospital users/computers and foreign mobile devices in use connecting internal networks
- Maintaining access control for HIS and LIS systems

On the side of wireless network

- Providing secure access to mobile devices having no access rights to internet for security reasons over the wireless network
- Performing patient related HIS procedures while accompanying patients with the use of Tablet PCs and PDAs over the wireless network.

Keeping the size of the hospital Networks structure in mind, we aim to design a Smart Network. There are some bottlenecks to overcome. These are limited number of personnel, the excessive number of devices which are necessary to monitored and detecting daily attacks to the network. The Smart network should be able to shut down the user ports by the use of software for access rules and these processes should be done automatically by the Smart Network [11].

ACKNOWLEDGEMENT

This study is supported by The Commission of Pamukkale University Scientific Research Projects (PAUBAP).

REFERENCES

[1] Privacy Rights Clearing House.

[2] http://www.privacyrights.org/medical.htm

[3] [Electronic Privacy Information Center.

[4] http://www.epic.org/privacy/medical/

[5] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Standard 802.1x-2001, June 2001

[6] IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks, IEEE Standard 802.1q, Dec.1998

[7] Blunk, L. and Vollbrecht, J., PPP Extensible Authentication Protocol (EAP), RFC 2284, 1998.

[8] Rigney, C., Willens, S., Rubens, A. and Simpson, W., "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[9] Aboba, B., and Calhoun. P., "RADIUS Support for Extensible Authentication Protokol (EAP)", RFC 3579, 2003.

[10] Microsoft "Internet Authentication Service for Windows 2000", 154s. http://download.microsoft.com/download/b/6/4/b64bcb2e-867c-4458-aee8-589d750e68a8/IAS.doc

[11] Çetin, M. ve Aydos, M., "The Effects of Using IEEE 802.1x Standard in Automatic VLAN Structures on System Performance" The Second National Symposium of Communication Technologies, p.211-214, Nov. 2005, The University of Çukurova, Adana, Turkey (in Turkish)

[12] Çetin, M., "Automatic VLAN Designs and Quality of Service Analysis on Campus Networks", The University of Pamukkale, Master Thesis, June 2006, Denizli, Turkey (in Turkish)

[13] The University of Texas Health Science Center at Houston Prescribes TippingPoint for a Healthy

[14] Network.http://www.tippingpoint.com/pdf/resources/casestudies/505324-001_UTHealthCaseStudy.pdf