

Wireless Network at TUCN – Case Study

Sándor Rózsa, Adrian Mircea Roiban, Emil Cebuc, Zoltán Majó

Abstract — Wireless networks have the potential to be applied in educational and research environment. Deploying wireless networks on an organizational level poses many challenges such as security problems, signal propagation and mobility.

We present the design of an educational wireless network which handles security based on 802.1X standard.

Keywords — Wireless networks, security, mobility, WIFI, RADIUS, EduRoam

I. INTRODUCTION

Nowadays mobility is an additional requirement for computer networks. New mobile technologies are emerging and getting widely accepted. Ten years ago the main goal of telecommunication companies was making audio-based communication widespread. This tendency is changing – internet based communication is the main trend.

There are many types of mobile networks. Long range mobile networks are built on traditional cellular phone networks (GSM, 3G, and 4G). Short range mobile networks are mainly used to connect peripheral devices. These technologies include Bluetooth (802.15) and infrared. Computer wireless networks include WLAN (802.11, WiFi [1], HIPERLAN) and WMAN (LMDS, WiMax, HIPERMAN) technologies.

Our paper presents the design and implementation of a secure university-wide wireless network, which also offers mobility to its users.

In the first sections (II, III, IV, V) we present the security solutions used in our network, such as

S. Rózsa is system engineer at the Data Communication Center “Pusztai Kálmán”, Technical University of Cluj-Napoca, RoEdu Branch Cluj-Napoca, Romania, Str Barițiu, Nr: 26-28, Room 29 (phone: +40/264/401247; fax: +40/264/594684; e-mail: sandor@cluj.roedu.net, web: <http://cc.utcluj.ro>).

A. M. Roiban was system engineer at the Data Communication Center “Pusztai Kálmán”. He is now with Fortech SRL, Cluj-Napoca, Romania (phone: +40/745/314052; e-mail: adi@roiban.ro).

E. Cebuc, PhD, is deputy manager at the Data Communication Center “Pusztai Kálmán”, Technical University of Cluj-Napoca, RoEdu Branch Cluj-Napoca, Romania, Str Barițiu, Nr: 26-28, Room 28 (phone: +40/264/401246; fax: +40/264/594684; e-mail: Emil.Cebuc@cs.utcluj.ro, web: <http://users.utcluj.ro/~cemil>).

Z. Majó is system engineer at the Data Communication Center “Pusztai Kálmán”, Technical University of Cluj-Napoca, RoEdu Branch Cluj-Napoca, Romania, Str Barițiu, Nr: 26-28, Room 29 (phone: +40/264/401247; fax: +40/264/594684; e-mail: majoz@cluj.roedu.net; web: <http://cc.utcluj.ro>).

authentication, tunneling and the 802.1X standard. In Section VI we describe the hierarchical architecture of our system. Section VII is about our approach for the authentication, user management, mobility and monitoring problems. In Section VIII, EduRoam, the solution for the WiFi mobility between universities is presented.

II. SECURITY IN WIRELESS NETWORKS

To ensure the security of computer networks there are three attributes that have to be maintained. *Integrity* refers to maintaining data identically during transfer. This attribute is violated if data is modified by unauthorized users. *Confidentiality* is achieved if only those being authorized have access to the information transferred on the network. The last criterion of network security is *availability*. In order to be able to use information, it has to be available all the time.

In the past, wireless LAN technology proved to fail in all three areas. Most notable failures were targeted towards confidentiality aspects, both in terms of the fundamental flaws in early encryption protocols (RC4 IV flaw) and the lack of strong user authentication (WEP key management).

These problems were solved in newer protocols, however we still have a fundamental flaw regarding availability of wireless network due to its shared transmission medium and the physical properties of radio waves, problem for which no solution is seen in the near future[5] [6].

III. AUTHENTICATION PROTOCOLS

Authentication protocols are used in the process of authenticating the user to the network. One of the first protocols widely used for authentication was PAP (Password Authentication Protocol) and it is the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. The Basic Authentication feature built into the HTTP protocol uses PAP. The main weakness of PAP is that it make a gullible assumption of a safe physical link layer and both the username and password are transmitted "in clear" or unencrypted form.

To overcome PAP problems a new protocol was produced: CHAP. Short for Challenge Handshake Authentication Protocol, CHAP is a type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. Both the sender and peer share a predefined secret. The peer concatenates the random value, the ID and the secret and calculates a one-way hash using MD5. The hash value is sent to the authenticator, which in turn builds that same string on its side, calculates the MD5 sum itself and compares the result with the value received from the peer. If the values match, the peer is authenticated. By transmitting only the hash, the

secret can't be reverse-engineered. The ID value is increased with each CHAP dialogue to protect against replay attacks. A modified version of CHAP MS-CHAP version 2 provides mutual authentication between peers by piggybacking a peer challenge on the Response packet and an authenticator response on the Success packet in this way a cryptographic key pair could be established.

IV. SECURE NETWORK TRANSPORT

During the communication process sometimes there is a need to guarantee the identity of both involved parties and also provide communication privacy. On the application layer of the ISO/OSI model there are protocols that satisfy these requirements, such as the *Transport Layer Security (TLS)* protocol.

When a TLS connection is established, authentication of both parties is provided through certificate exchange. In order to connect with a server the client must send a certificate that is verified by the server. On the other hand the server must authenticate itself to the client by sending a certificate that can be validated against a list of trusted certificate authorities. By this the client is sure that credentials weren't sent to a third party or server who appears in the role of the valid server. After the initialization phase when authentication is done communication takes places using symmetric cipher encryption.

The only problem with TLS is that clients must have certificates. These certificates have to be generated and distributed among clients. Managing the distribution of user certificates is a major challenge for the organization.

To face this issue other protocols like *TTLS (Tunnelled TLS)* have been created. In the first phase of the process a TLS tunnel is established between the client and the server. Digital certificates exist on the servers so that the identity of the server can be verified. After the TLS tunnel is established encryption is provided and the identity of the client can be verified. For validating the client's identity other methods than digital certificates are used, for example username-password pairs. As a conclusion TTLS is much simpler to deploy in organizations where some kind of database with user credentials exists, but there is no existing public key infrastructure.

V. 802.1X

The IEEE 802.1X protocol which implements port-based network access control. The advantage of the IEEE 802.1X protocol is that it doesn't bind a client to a named port. Instead, it is enough for a client to have a set of credentials (username, password and/or certificates). Based on these credentials access is given to the client no matter on what port he or she plugs in.

Technically speaking the IEEE 802.1X standard involves three parties. An 802.1X *supplicant*: a client that connects to a port of the switch and is able to communicate according to the standard. An 802.1X *authenticator*: a port on a switch, through which network services are accessible suppose that the supplicant has successfully authenticated himself. Before authentication no traffic is allowed on the port, except EAP (Extensible Authentication Protocol) data units. When a supplicant plugs in to a port on which

authentication is enabled, the authenticator sends an EAP-PDU requesting credentials. The 802.1X *authentication server*: the supplicant sends its credentials to the authenticator, which forwards them to a RADIUS server. The server verifies the credentials, and if they are valid, tells the authenticator to grant access to the requested port.

RADIUS (Remote Authentication Dial In User Service) is an AAA (authentication, authorization, accounting) protocol designed for applications such as network access or IP mobility. It is intended to work in both local and roaming situations. One of the failures of this design is that it authenticates the hardware people use rather than the users themselves. Luckily RADIUS design could be easily extended in order to provide authentication of the user.

RADIUS is a client/server protocol. The RADIUS client is typically a NAS and the RADIUS server is usually a daemon process running on a UNIX or Windows NT machine. The client passes user information to designated RADIUS servers and acts on the response that is returned. RADIUS servers receive user connection requests, authenticate the user, and then return the configuration information necessary for the client to deliver service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers [3] [4].

EAP (Extensible Authentication Protocol) is a transport protocol which is designed for authentication. EAP supports many authentications methods like EAP-TLS, EAP-TTLS, and PEAP. The contents of an EAP packet will vary depending on the method chosen.

EAP-TLS is well-supported among wireless vendors. It offers a good deal of security, since TLS is considered the successor of the SSL standard. It uses PKI to secure communication to the RADIUS authentication server, and this fact may make it seem like a daunting task to set up. So even though EAP-TLS provides excellent security, the overhead of client-side certificates may be its Achilles heel and this is the main reason why an EAP-TTLS method is preferred [2].

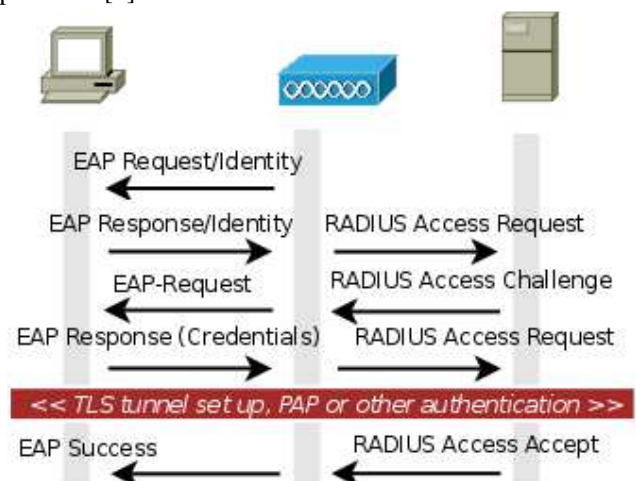


Figure 1: The authentication method in detail

EAP-Tunnelled Transport Layer Security, or EAP-TTLS, is widely supported across platforms, and offers very good security, using PKI certificates only on the authentication server. It relies on EAP-TLS and inside the tunnel any authentication method secure or non-secure can

be used. The most common method used inside the TTLS is PAP; using CHAP inside the tunnel unnecessarily increase the method complexity as security is already provided by TLS. EAP-TTLS is not supported by Microsoft Windows system and this fact made this method not so popular. Figure 1 shows the authentication process using EAP-TTLS-PAP in detail.

VI. THE SYSTEM ARCHITECTURE

Our goal at the design time was to obtain a system with a hierarchical structure. At the highest layer we have the enterprise authentication servers (protected with firewalls from the other parts of the network). For a 7/24 availability this servers must be replicated. The users' data are checked using the RADIUS authentication protocol [3] [4].

At the middle layer we have the data transmission systems (Cisco Catalyst switches). This layer makes the connection between the access points, the authentication centers and the Internet. The mobility is also solved at this layer: all the clients in successive cells are placed in the same broadcast domain[10].

The access points are placed at the lowest layer. When a user is connecting to the wireless network the user id and the password is sent to the highest layer's servers via a TTLS tunnel. If the authentication database contains the user id associated with the password, the system permits the connection to the network.

VII. CHALLENGES AND SOLUTIONS

One of our main goals was to “reuse” an existing database for the user authentication. We chose the LDAP databases of the mail servers. The RADIUS authentication server is connected to the mail server’s users' database (Figure 2.). If there is an authentication request on the

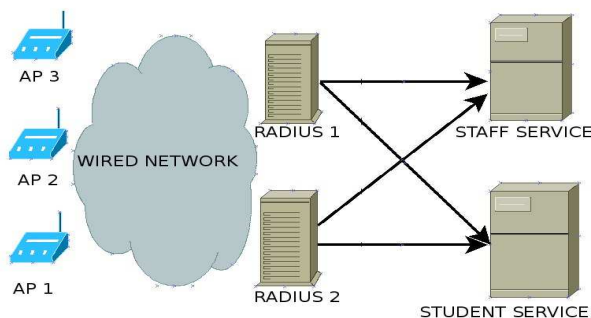


Figure 2: The wireless system

RADIUS server, this server sends a query to the LDAP [7] [8] server, to verify if the user exists or not in the database. If the user exists and the password is correct, the RADIUS permits the network connection. Both of the RADIUS servers are connected to two different LDAP database servers, one for the university staff and one for the students. We use two RADIUS servers for redundancy. On access points we specify the address of each RADIUS servers. If the first authentication center is not available,

the access point will try the authentication on the other RADIUS server.

Due to the vulnerability of the wireless networks we had to isolate the wireless network from the other parts of the network. For this reason virtual LANS (VLAN) were created. All the clients are connected to the same VLAN. Using this approach we are able to monitor and filter the traffic from the wireless network to the Internet and from the Internet to the wireless network. The clients' IP addresses are distributed via DHCP. Thanks to the virtual network the IP addresses are valid in the whole wireless network. When a client moves in another wireless cell there is no need for a DHCP address request (only authentication). Using this method we solve the problem of the mobility in the wireless network.

We use access points complying with 802.11 B and G standards (Linsksys brand). At configuration time the WPA-Enterprise option is selected as authentication method.

To find a proper physical layout for the wireless access points was a challenge for itself. In order to achieve maximum coverage and roaming we have selected several locations. After some trial and error we have selected the most appropriate and secure places. For the time being we have placed 30 access points in 7 different areas of the university campus.

Monitoring the wireless network is also a major task. The first step in the monitoring process is the availability checking of the wireless access points. We tried out multiple solutions such as: SmokePing [11] and Nagios [12]. In the second step we analyze the bandwidth usage with the MRTG [13] system. The malicious attempts are discovered analyzing the RADIUS logs. There is on going work in automating the RADIUS log processing system.



Figure 3: Authentication on Windows systems

VIII. EDUROAM

The presented wireless network respects the EduRoam specifications [14]. The benefit of being part of EduRoam is that users visiting an other EduRoam connected institution are able to log on to the visited WLAN using the same credentials (username and password) the user

would use if he or she were at their home institution.

On Windows systems users have to install the program named SecureW2 [15], an open source EAP-TTLS client (Figure 3).

To support EAP-TTLS security method wpa_supplicant [16] utility must be installed. On Debian and Ubuntu the wpa_supplicant installation is possible via “apt-get”. Figure 4 presents the configuration for wpa_supplicant.

```
network={
  ssid="eduroam"
  scan_ssid=1

  key_mgmt=WPA-EAP
  eap=TTLS
  phase2="auth=PAP"

  identity="      @student.utcluj.ro"
  password="      "
  ca_cert="/etc/wpa_supplicant/ca.utcluj.ro.cer"
}
```

Figure 4: Authentication on Linux systems using wpa_supplicant

CONCLUSIONS

In this work we provide a complete solution of an educational wireless network. The modularity of this system should enable progressive development of the network. The future work of the authors will involve the monitoring of the wireless networks, discovering in real time the malicious attempts.

REFERENCES

- [1] *** IEEE Standard 802.11g, Available: <http://standards.ieee.org/getieee802/download/802.11g-2003.pdf>
- [2] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowitz: *RFC 2784, Extensible Authentication Network (EAP)*, Available: <http://tools.ietf.org/html/rfc3748>
- [3] C. Rigney, S. Willens, A. Rubbens, W. Simpson: *RFC 2865, Remote Authentication Dial In User Service (RADIUS)*, Available: <http://tools.ietf.org/html/rfc2865>
- [4] C. Rigney: *RFC 2866, RADIUS Accounting*, Available: <http://tools.ietf.org/html/rfc2866>
- [5] B. Potter: *802.11 Security*, O’ Reilly, 2005
- [6] M. Gast: *802.11 Wireless Networks: The Definitive Guide*, Second Edition, O’ Reilly, 2005
- [7] J. Semersheim: *RFC 4611, Lightweight Directory Access Protocol (LDAP): The protocol*, Available: <http://tools.ietf.org/html/rfc4511>
- [8] R. Harrison: *RFC 4513, Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms*, Available: <http://tools.ietf.org/html/rfc4513>
- [9] John R. Vacca: *Guide To Wireless Network Security*, 2005, Springer
- [10] *** Cisco *Secure Wireless Design Guide*, Available http://www.cisco.com/application/pdf/en/us/guest/nets/ol/ns386/c649/ccmigration_09186a0080871da5.pdf
- [11] *** *Smokeping*, Available: <http://oss.oetiker.ch/smokeping/>
- [12] *** *Nagios*, Available: www.nagios.org
- [13] *** *MRTG*, Available: <http://oss.oetiker.ch/mrtg/>
- [14] *** *EduRoam*, Available: <http://www.eduroam.org/>
- [15] *** *SecureW2*, Available: <http://www.securew2.com/>
- [16] *** *WPA Supplicant*, Available: http://hostap.epitest.fi/wpa_supplicant/