INTENDANCE AND MAINTAING OF WIRELESS NETWORKING

Eva DANKOVÁ, Martin CHOVANEC, Peter FANFARA
Department of Computers and Informatics, Faculty of Electrical Engineering and Informatics,
Technical University of Košice, Letná 9, 042 00 Košice, Slovak Republic,
e-mail: eva.dankova@tuke.sk, martin.chovanec@tuke.sk, peter.fanfara@tuke.sk

ABSTRACT

Wireless network is more and more exploited technologies, because of its availability and connectivity from any place in the range of its access point, without restrictions on cable. Very important area in wireless networks is the managing of the wireless network. The paper describes proposed secure wireless network with a system for managing to evaluate the real conditions in the network. The study is intended on analysis of various securities, because priority of each system is the security of the system. First part of the article handles with software technologies, which are used to design web applications. Based on this analysis the proposed system was implemented by Zend Framework, due to limpidity and use of the PHP language.

Keywords: *wireless, managing, monitoring, zend framework, secure system*

1. INTRODUCTION

Wireless technology is the fastest growing communications technology of recent decades in many areas, as business or the education system, while it incorporates the most important features as the flexibility and mobility.

The most widespread and most discussed topic of wireless networks remains a question of security and confidentiality of data. Many publications are devoted to the study and description of security and it seems that this question is exhaustless. It is not only the security and different security algorithms being developed, but rather the mechanisms to break these algorithms. The paper will focus on the description of the various security standards to provide maximum security for data transmission, but also to protect users. The primary intention is to create a secure wireless network design and implementation of a system for managing such a network. The next section will be therefore devoted to a comparison of software technologies and a description of a quite new framework technology, Zend Framework. Zend Framework has become the leading technology for the creation of different software projects, mostly web applications using PHP. It uses a model for implementation, known as MVC (Model-View-Controller) model, which results to separating application logic from the graphic design while the code becomes simple and transparent.

Studies of wireless networks and security issues, the technology of Zend Framework, are the subjects of this paper. De facto, all studies mentioned in the following sections are sufficient and contribute for creating a wireless network and a simple management using Zend Framework.

2. THE TECHNOLOGY OF WIRELESS NETWORK

During couple of years a mass of improvements were introduced. The strategy of development is still focused on standards and protocols from the last century as far as they can be concerned.

2.1. IEEE 802.11 and the OSI reference model

One of the most important standard is 802.11 developed by IEEE. 802.11 is a member of IEEE 802 family, which is a series of specifications and technologies of Local Area Networks (LAN). IEEE 802 specifications are focused on the two lower layers of the OSI reference model, as they include components of physical and link layers (Fig. 1). [1], [2]

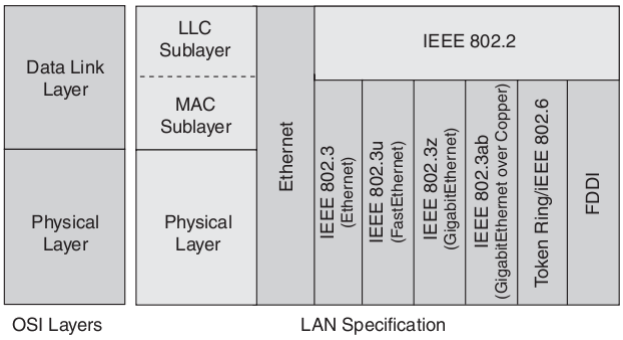

Fig. 1 IEEE 802.11 and the OSI reference model

All network components 802 include MAC and PHY. MAC is a set of rules by which it determines access to medium and send data. Transmission and reception is left to the physical component of the PHY. [3]

802.11 belong to link layer using 802.2/LLC encapsulation. 802.11 specifications are based on:

- 802.11 MAC layer
- PHY layer:
  - frequency-hopping spread-spectrum FHSS
  - direct-sequence spread-spectrum DSSS

Later, newer revisions of 802.11 were added and additional specifications of physical layer were created. 802.11b specifies a layer with higher bit rate as the original DSSS transmission. It refers to high-rate direct sequence (HR/DSSS). 802.11a describes the physical layer based on orthogonal frequency division multiplexing (OFDM). 802.11g uses OFDM transmission at higher bit rates. It is backwards compatible with 802.11b. However,

the use of 802.11b and 802.11g networks will reduce the maximum speed for 802.11 network users. [2], [3]

2.2. Security in wireless networks

Wireless Local Area Network (WLAN) is not a trustworthy network unless it complies with standards and security specified for wireless networks. Unsecured networks are easily accessible to unauthorized users and provide space for carrying out various attacks, e.g. a permanent communications interception, falsification of MAC addresses or IP address of any authorized user, or launch Denial of Service (DoS) attacks.

Nowadays, there are mechanisms and rules which are sufficient to cover security in wireless networks and provide strong protection against attackers. However, providing full network security is not so trivial. Securing a WLAN is running over all levels of the OSI model, from the lowest layer - the physical and link layers, to the higher layers - presentation and application layers. [3]

Generally it can be assumed that each layer of the OSI model can provide some form of security. Depending on services and requirements of different applications, security is mostly applied only to certain layers of the OSI model. In addition, certain security services are better defined on specific layers (e.g. message verification). In the next section security and safety of services and applications at different layers of the OSI model will be described.

Physical layer is focused on a hardware connection and includes signal modulation, noise and interference solutions, and determining the link between distance and throughput. Therefore, security at this layer defines the following criteria:

- Define and limit the spread of the signal area - to minimize signal overlap with construction materials, isolation, or coatings, and to limit the use of other wireless technologies.
- Locate the antennas - antennas wireless routing plays an important role in maintaining and improving safety, recommends the use of directional antennas and the limited use of omni-directional antenna, thus restricting access to unauthorized users.
- Hidden system identifier - network identifier, the SSID (or ESSID), differentiates logical networks in the same physical space. Without this ID, the client cannot connect to WLAN, it is recommended not to dispose, but preferably hide the SSID.

Data-Link layer implements data transmission over physical medium. Data-Link layer contains a sub layer called MAC (Media Access Control), which provides access control to media. Details of the transfer itself are secured on the physical layer PHY, which is the physical interface between network devices. Data-Link layer provides functions such as establish and complete logical connection between two computers, send and receive frames and their acknowledgement, identify and recover from errors, check the integrity of received frames, create and recognize borders between the frames. For mentioned functions some safety and security steps can be taken:

Filter MAC addresses - MAC address is a unique identifier of network cards that can be used for clarification of permitted and prohibited WLAN clients. Access Control List (ACL) based on MAC addresses defines the network access for each client (enabled or disabled access).

- Filter protocols – traffic can be filtered when using more network protocols in the WLAN (e.g. disable IPX, AppleTalk).
- Access authentication - verifying the identity of the client can run in different ways: open (not verified), using shared WEP key, or using EAP (IEEE 802.1X) with an authentication server (typically RADIUS).
- Encryption - encryption of communication using mechanisms specified by WEP, 3DES (64-bit keys) or AES (128-bit keys).

Network layer allows creating connection and routing between two stations along with network conditions. According to that the network layer provides functions: transmission of the frames into the router, split frames into smaller frames if necessary by a router, conversion of the logical address to physical network card address (MAC). The functions of network layer specify the security at this level:

- Filter IP addresses - access control on this level is done by ACL based on logical - IP addresses, similarly as ACL based on physical addresses.
- Use firewall - a firewall is often part of a wireless router that blocks traffic, typically from the Internet into WLAN.
- Use VPN - IP VPN (Virtual Private Network) is built through the mechanisms of the lowest three layers, e.g. encryption with IPSec (IP Security Protocol) and L2TP (Layer 2 Tunneling Protocol).

Transport layer ensures reliable communication - correct sequence of messages, dealing with losses and duplicated data. Depending on whether the network using reliable or unreliable connection, the transport layer need not/must ensure shifting frames, confirmation messages, detect or recover from errors. The transport layer functions include: receiving messages from higher layers, and their division into several frames, as well as reliable delivery confirmation messages.

Session layer provides a logical connection between two points – creates a session. Session layer functions are: initialization, tracking and ending of virtual circuits between two processes which are identified by their unique process address, determining the beginning and the end of administration support functions to enable two-way communication process through the network, such as verification of users and provide access to individual facilities.

Presentation layer has already made meaningful high - the application layer. Presentation layer provides functions such as: the translation of character codes (e.g. ASCII code to EBCDIC code), conversion and data compression or data encryption for security reasons (e.g. encryption, passwords). [4]

3. MANAGEMENT OF WIRELESS NETWORKS

The rapid evolution and development of wireless technologies impact the robustness and the problems associated with managing such a network. Currently, it is necessary to deploy a centralized management of wireless networks.

3.1. Technical aspects for managing wireless networks

Early wireless networks were based on independent access points (so-called "fat" APs) with an autonomous approach. Autonomous AP does not rely on central control facility. Such devices are accepted as long as problems do not occur with scalability, configuration consistency, monitoring the status of each AP, poor coverage, etc. The best solution is then a centralized system for monitoring and managing of wireless network.

One of the major systems is centrally managed unified wireless network from Cisco - Cisco Unified Wireless Network (CUWN), (Fig. 2b). In CUWN is needed to use lightweight AP (Lightweight Access Point - LWAP) in the network instead of the autonomous AP, which involves a controller.

Eventually, the environment changes, the network grows or shrinks, or even is being moved, and each change has an impact on wireless coverage. Using LWAP allows the configuration to be easily obtained from controller, that means the changes are made directly on a controller and dynamically updating all LWAP associated with it. Using CWUN LWAP enables sharing the configuration and thus improves the consistency of wireless networks and eliminates inconsistencies in the AP configuration.

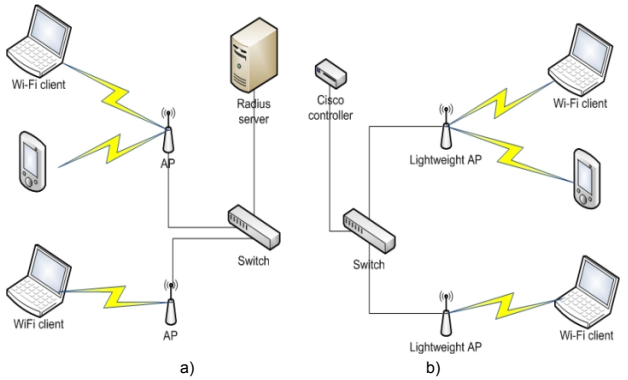

Fig. 2 Network architecture: a) Autonomous wireless network, b) Centralized wireless network with Cisco devices

Although a centralized system is more effective and less time-consuming, it cumbers the company financially. In this work, therefore I will propose a wireless network using the autonomous system associated with a central authentication server using database for user management, (Fig. 2a).

3.2. Development of management system using software technologies

For a graphical interpretation of network management different software and applications are being used with various programming languages. When creating web applications often languages such as Java, PHP, C++ or Python, Perl and Ruby are used.

In Tab. 1 are compared some popular softwares used to develop web applications. The comparison is relied on programming language and on use of MVC model in development. According to some criteria, as easy testing and deployment with PHP programming language and database migration, Zend Framework can be considered as the best project for web application development.

Table 1 Overview of projects for web application development

Project	ASP.NET	OpenXava	Eclipse	Zend Framework	CakePHP	Ruby on Rails	Pyjamas
Language	ASP.NET	JAVA	JAVA	PHP	PHP	Ruby	Python
MVC	yes	yes	-	yes	yes	yes	yes

Zend Framework (ZF) is an open source framework for developing Web services and applications with object-oriented PHP5 code. The structure of ZF components is unique [5] - each component is designed with few dependencies on other components. Although loosely bound architecture allows developers to use components individually, the combination of components in a standard ZF library creates a powerful and extensible web application framework.

4. WIRELESS NETWORK AND SYSTEM MANAGEMENT PROPOSAL

The intention of this work was to propose a wireless network solution for an existing LAN topology. The architecture of the proposed wireless network, given in (Fig. 3), has been prepared in accordance with some facts and objectives.

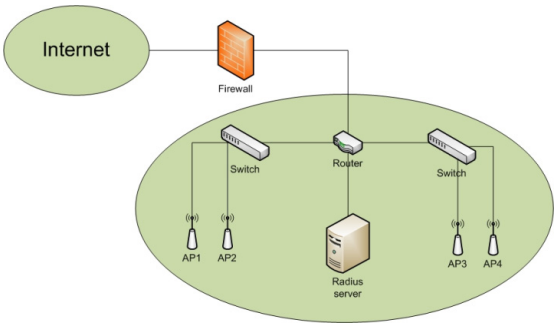

Fig. 3 Wireless network topology proposal

4.1. Wireless network deployment

There is an importance of reducing the costs and expenses in the implementation stage of the wireless network by using open source software and reducing the number of used servers. Afterwards, it was necessary to create a secured wireless network with limited access using specific authentication process and simple user-friendly authentication method. We defined the solution for the user authentication using a central RADIUS authentication server with proper database for authenticated users. [6]

The security in the created wireless network INTRAK is defined as WPA2-Enterprise, using AES (Advanced Encryption Standard) block ciphering. This ciphering

algorithm refers to WPA/AES and is called as Counter-mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). The network authentication method is Protected EAP (Extensible Authentication Protocol) authenticating against authentication server – RADIUS; whereas credentials are being sent throw a created tunnel. The RADIUS server is connected with mySQL database, where credentials - login and password, are being stored.

4.2. System management deployment

To simplify the administration of users, we can often encounter a web application where users can register individually or can be registered by an administrator. The web application we suggested has to serve as a database of registered user allowed to use the wireless network. The administration system should be accessible for defined administrators of the wireless network and end users within the created intranet. Requirements for a system to manage the wireless network were to securely log on or off from the system, add, edit and delete groups according to specified rights within the system, add, edit and delete users.

In the web application, we distinguished two different interfaces – admin and user interface. Admin interface is intended for the administrator who is authorized to add users to the database based on specified identifiers. User interface is available only for specific user after logging in successfully. Users wishing to use the wireless network must first be registered with a web application by entering the identifiers specified in the database. After successful registration of user receives a login and password that can be used to connect to the wireless network and log in the administration system. The application is implemented using the Zend Framework which is primarily designed for creating web applications in PHP. The developed system is accessible via web browser. Zend Framework uses the MVC model, and a specific directory structure is maintained – the view and the functionality are separated. In MVC model, Controller works with View, collects and delivers data from/to Model and View have access to data from Model, but cannot modify the data. Following this manner, we can learn that Model is used for creating application, View represents the graphical interface of web application and Controller adds functionality and implementation of actions.

5. CONCLUSION

The implemented wireless network provides a simple way to connect to the Internet using wireless technology. The simplicity results from prompting user's name and password, while the security is on high level using an encryption protocol. In the future, the wireless network can be extended by applying a centralized management with a controller, using Active Directory or LDAP for authentication. Extension options remain unlimited.

The created web application meets all the requirements for managing and monitoring users of the wireless network. Using Zend Framework for the implementation of the administration system confirmed the expectations and supported theoretical knowledge of Zend Framework background. The environment is understandable, the source code easily readable and without problems editable in the future. It is appropriate to add additional features in the future to the system for user management, such as monitoring and logging user access to a wireless network, creating a module for statistical purposes, etc.

ACKNOWLEDGMENTS

Supported by a grant from Iceland, Liechtenstein and Norway through the EEA Financial Mechanism and the Norwegian Financial Mechanism. This project is also co-financed from the state budget of the Slovak Republic.

REFERENCES

[1] VOKOROKOS, L.: Digital Computers Principles, Budapest, pp. 232, Typotex 2004, ISBN 9639548 09.

[2] GAST, M.: 802.11 wireless networks: the definitive guide, O'Reilly Media, Inc., 2. edition, 2005.

[3] ROSHAN, P. – LEARY, J.: 802.11 Wireless LAN fundamentals, Cisco Press, 2004.

[4] Planet3 Wireless, "Certified Wireless Network Administrator official study guide", McGraw-Hill Professional, 3. Edition, 2005.

[5] POTTER, B. – FLECK, B.: Securing Wireless Networks, O'Reilly Media, Inc., 2003.

[6] ALLEN, R. – LO, N. – BROWN, S.: Zend Framework in Action, Manning Publication, 1. edition, 2008.

[7] McCULLOUGH, A.: Designing a Wireless Network, Syngress, 2001.

Received August 22, 2010, accepted November 16, 2010

BIOGRAPHIES

Eva Danková (Ing.) was born on 6.2.1985 in Poprad. In 2009 graduated at the Department of Computers and Informatics of the Faculty of Electrical Engineering and Informatics at the Technical University of Košice. She is currently studying her PhD.

Martin Chovanec (Ing., PhD.) was born in Lučenec, Slovakia, on 11.1.1982. He received the engineering degree in Informatics in 2005 from Faculty of Electrical Engineering and Informatics, Technical University of Košice. 2008 he received PhD. degree at the Department of Computers and Informatics of the FEE&I TU of Košice and his scientific research was focused on network security and encryption algorithms. Currently he is a director of UVT at the Technical University of Košice.

Peter Fanfara (Ing.) was born on 8.11.1986 in Rožňava. In 2010 graduated at the Department of Computers and Informatics of the Faculty of Electrical Engineering and Informatics at the Technical University of Košice. He is currently studying heis PhD.