[13] Olsson, J. (2004). Forensic Linguistics: An Introduction to Language, Crime and the Law. London: Continuum.
[14] Shuy, R. (2007). Linguistics in the American Courtroom. Language and Linguistics Compass. Blackwell Publishing Ltd.

Website:

[1] Sesum, M. (2009, December 21) Forensic phonetics (video). Retrieved from http://www.youtube.com/watch?v=0A-7AD_ZYys

DATA SECURITY IN THE WI-Fi NETWORK IN BH COMPANIES

Prof. dr. Husnija Bibuljica, email: h_bibuljica@hotmail.com
Mr. sc. Haris Bibuljica

Abstract: *Data security in computer networks are very actual thematic. Accommodation provided by wireless network causes their spiral expansion. In the other hand easy connection to the medium for transmission of data making this networks much exposed to the attacks. Because of that it is necessary to pay much attention about data security in this networks. During the implementation of wireless networks we must decide how to define security policy and as part of this question we must decide what is equipment and data security method best for selection. In this paper as theoretical base are exposed some basic thesis in information theory. There are named often used standards for wireless networks, and standards IEEE 802. 11x. and IEEE 802.16 are detailed presented. There are discussed mechanism for data protection, and in this frame work detailed analyzed weakness and threats for data security. I elaborated the program to change the MAC address of one of the means of network security. Showing systematic measures to improve data security in wireless computer networks and described in more detail some of the technical measures.*

Keywords: *Data security, WLAN, Encryption, Companies*

Introduction

The convenience of the wireless computer network has made it popular, and it is very often used today. For example, in a business environment, universities, in public places, and also in private homes. The security of data transmitted in wireless computing networks is an increasingly frequent issue that users choose. The medium for transmitting information is ether, which means that anyone with the radio and transmitter can receive and send data. This is a threat to the confidentiality of information transmitted in such networks.

At the time WEP was accepted, there were significant limitations in the hardware capabilities of the equipment and the cost of its production, which led to the adoption of such a data protection mechanism. WEP has proven vulnerable to several types of attacks and is now contemplating that it has little value as a mechanism for protecting confidentiality of data. This paper presents how WEP works and several ways to break the protection it provides. In order to improve security, and utilize the existing equipment that was used with the WEP mechanism, the protection was enhanced by the WPA mechanism. It was a transient solution, with still insufficiently effective security. Only WPA2 with AES and the new authentication system finally provides the required level of data security. Current protection systems are a product of human labor, intended for other people. The mistakes in the application of data protection are most often due to the lack of understanding of the concept on which the development of such systems is based. In order to overcome this, new intelligent data protection systems with application of intelligent and intelligent software are developed.

1. Information networks and data security

The information system is an integrated set of components for collecting, recording, storing, processing and transmitting information. Business enterprises, other types of organizations and individuals in modern society depend on information systems for managing their operations and operations, maintaining market competitiveness, offering a variety of services and enhancing their personal abilities and capacities. For example, modern corporations depend on computer information systems to process their financial accounts and business transactions, and manage human resources; municipal administrations depend on information systems for offering basic services to their citizens; Individuals use information systems to improve their knowledge, to purchase, manage bank accounts and transactions, as well as for various financial operations.

The general information system consists of sources of information, encoders of information, communication (portable) channels, decoders and information streams.

Figure 1. General information system view

It is considered that the cryptographic system is weak if it allows the use of bad

keys, if it has flaws in the design or if it can be easily decrypted.

Determining the existence of possible changes to the message during transmission is another essential task of cryptographic systems. Data integrity is provided by adding separate data in the form of a control sum or other redundant data that will be used in the decryption process. Adding the Message Authentication Code (MAC) is the usual way to verify its integrity. MAC is obtained based on the content of the message itself and the key itself. MAC is usually encrypted with the message itself, and it sends it, which adds another layer of integrity check. The recipient also calculates the MAC value in an identical manner and compares its score with the values sent along with the message. Integrity is provided if these two values are the same. It is no longer enough for the tool to be automated and adaptive (in order to overcome user errors). The tool must behave like an intelligent observer, capable of recognizing the "abnormal" behavior of the information flow. It must also be able to make some decisions and be able to completely reconstruct information as it was before unauthorized changes.

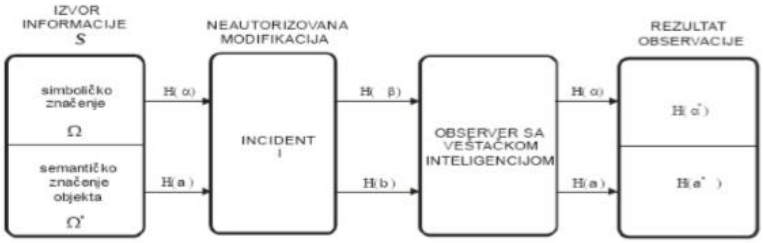


Figure 2. Attacked information system with an intelligent observer

2. Planning a Wi-Fi network

Factors to be considered at the planning stage are required coverage, capacity and costs. As a rule, a large area and a large capacity can only achieve high prices. In other words, less portable power supply, less coverage area. On the other hand, this leads to greater total capacity, by making access points closer to one another. In controlled networks, power settings are generally automatic: power transmission is reduced if access points are located close to each other.

In terms of capacity, the rule is that one access point is located on about 10-15 active users that can serve. Connection limit, i.e. the largest number of users who can connect to the access point at the same time is significantly higher (about 30-50 users, depending on the access point model). Older access point models have less capacity. In principle, coverage coverage can use both 2.4 and 5 GHz bandwidth for planning. In 5 GHz bandwidth, the signal is lost more strongly as a function of distance and as a result of an obstacle than in 2.4 GHz. Area coverage is almost the same, however, a 5 GHz signal allows more power transfer. However, due to the differences between the frequencies, the direction of the antenna need not necessarily work at 5 GHz.

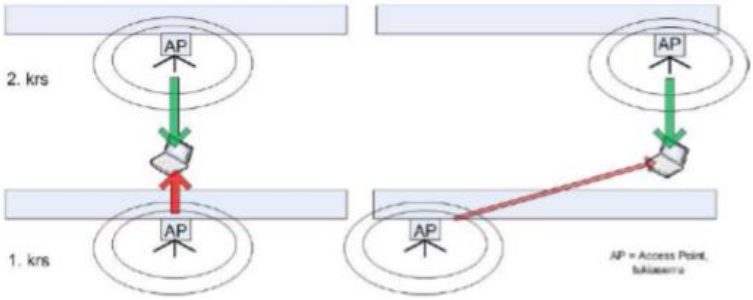
There are at least three ways to carry out the planning of the coverage area: orthodox and methodical, planning based on testing, and planning based on user requirements. However, it should be noted that organizations that are planning their

network are not forced to add access points to sites as a result of users who complain about poor reception of the signal.
To get an idea of area coverage access points, data transfer should be measured in the following locations:

1. In the immediate vicinity of the access point, e.g. directly below it (point A), 2. Near the access point on the same floor, behind the curve in the corridor (point B1) - behind a wall relatively close to the access point (point B2) - behind a wall away from the access point B3) 3. Immediately above the access point on the floor above (point C) or directly below the access point on the floor below (point D).

After WLAN tests it is possible to estimate how often access points should be allocated to cover a large area (given the desired data transfer rate). The desired data transfer speed can be determined independently, giving due attention to the desired total area coverage and budget. However, results below 10 Mbps should not be in the planning phase. However, it should be noted that the actual data ratings can, in the worst case, remain below that. Nothing prevents controller-based access points from it, if the budget permits. In practice, the site of Ethernet and sockets, and in old buildings, the accessibility of the access point also needs to be considered when setting up access points. Where possible, access points should be placed systematically until the entire building is covered. However, the following factors must be considered to ensure the least possible interference between access points: Walls and floors / ceilings prevent access to the area coverage area from being completely spherical.
Figure 3. Interference between access points.

If the access points are placed directly above or below each other, their signals will interrupt each other (left). If access points are located in somewhat different places on



different floors, the jammed signal weakens while traveling through the ceiling, resulting in less disturbance (right). The overall network plan allows the network to be set up, potential problems can be solved after optimization networks.

3. Software tools for wireless network analysis

Kismet is an open source tool.
It is primarily intended for detecting access points and collecting various information about access points. These are information such as network identifier, signal strength, protection used, and even information about clients that are connected to the respective access point. Kismet also stores a lot of data in log files, making it very attractive. Unlike some other tools, Kismet not only detects access points, but records a complete record of all captured packets. Such records can be subsequently used with other tools (Ethereal, Wireshark) for further analysis.
Useful information, which can also be obtained using Kismet, the tool is a list of

clients that are connected to the access point. In the client list view, information about the MAC address of each client is available, and in some cases it is also possible to obtain information about the type of card that the client is using. The number of packages that Kismet captured and the number of packets encrypted is also identified. Kismet also has the ability to identify the IP address of the clients and the strength of their signal.

4. Breaking the protection of wireless networks

Since the time of the famous work on the issue of how to crack the WEP key, there are many works on weaknesses and failures in the WEP mechanism for data protection. As a replacement for WEP, users first accepted VPN and 802.1X. Such a solution allowed the use of existing network equipment while improving data security. Then there was a temporary solution in the form of a WPA mechanism. WPA has eliminated most of the known security vulnerabilities observed with WEP. With the improvement of security, the complexity of the adjustment of the safety mechanisms is growing, which again causes the application to be lower than expected. The final replacement for WEP and WPA is WPA2 (IEEE 802.11i), for which in the enterprise variant there are no reported weaknesses in terms of security so far. Practical examples in this chapter are executed under the Linux operating system due to the limited number of wireless network adapters that have the required functionality. Most of these examples could also be executed under the Windows platform.

5. Measures to improve WLAN security

Control measures for protecting wireless networks

Safety management measures begin with a comprehensive security policy. Security policy is a document on the basis of which the other measures of security, operational and technical are harmonized and implemented. Wireless network security includes the following guidelines:
User's Authorizations and Responsibilities - The policy shows what is involved in it, why it is necessary, and what happens if it breaks. It also defines the responsibility of services and individuals, especially users in general, IT departments and controllers. Protected assets - Security policy can identify or point to sensitive information resources, communication channels and systems that need to be protected in the wireless network. Threats and weaknesses - Security policy can also include a section identifying threats to the wireless network. Analysis of attacks - Security policy can identify the consequences that occur in the event of a violation of wireless network security. Procedures and Responsibilities - Security Policy should identify and define security procedures for the following cases: Planning Security Response Security Operational Measures to Protect Wireless Network Security Physical security is the basic measure to ensure that only authorized users have access to wireless computing equipment. Physical security includes measures such as: Access Control - Identification of passwords, access through identification through card readers, identification by biometric devices are methods that reduce the possibility of

unauthorized access to equipment for the wireless computer network. Personal identification. Multi-level protection - door lock, installation of video surveillance to monitor the space around the objects in which the WLAN is set up. In this way, potential attackers are deterred from access points.

6. Conclusion

Wireless computer networks are a security risk for anyone who uses them. Causes should be sought in the incomplete application of existing protection mechanisms, as well as in the still-valid 802.11a, 802.11b, and 802.11g standards that use WEP as the basis of security.

The first result of this is the adoption of the 802.1X standard, which significantly improves user authentication, thereby increasing overall security. This standard uses EAP as its basis, which allows a large number of different authentication methods for network users. The next step in the evolution of security is the WPA standard that was adopted by the association of network equipment manufacturers for wireless computer networks (Wi-Fi Alliance). WPA has fixed all security vulnerabilities in WEP, and with fewer driver changes, it works on existing hardware. Although the great improvement of WPA is considered only between the 802.11x standard and the latest 802.11i standard that is imposed as the final solution to the security problem of wireless computing networks.

When it comes to protecting the company, we need to pay attention to a few additional things for better wireless security. Companies are potentially more interesting to hackers, because there is always at least one "negligent" employee in the firm whose faults hackers can get confidential information about the company, future projects or bank accounts. Pay attention to the signal itself, it should be limited within the limits of the working environment, this is possible through the software by regulating and directing the antenna, as well as by the physical isolation of the signals at the end walls of that firm. In addition to controlling the access to the local transmitter, the same danger is lurking from "eavesdropping". Namely, by controlling the user who accesses the local transmitter, we did not prevent a third person within the reach of the local transmitter to listen to communication between the transmitter and the receiver (our computer), and in that way potentially obtain sensitive data (e.g., passwords for Internet banking, etc.).

Literature

[1]Discussion forum: http://www.netstumbler.org. 02.2009.
[2] Hall var Helleseth. Data set of WEP encrypted frames. 02 2007.
[3] http://www.sourceforge.net/projects/iperf/
[4] http://www.smallnetbuilder.com/content/view/30224/100/
[5] http://www.kismetwireless.net/
[6] http://www.elitesecurity.org/f24-Cryptography-Encryption
[7] http://www.willhackforsushi.com/Cowpatty.html. 05.06.2009.
[8] http://www.tamos.com/. 05.06.2009.

[9] IEEE list of equipment manufacturers and OUI codes. http://standards.ieee.org/regauth/oui/. 16.02.2009.

[10] Iytisk Martin Scott Fluhrer and Adi Shamir. Weaknesses in the key scheduling algorithm of RC4. http: //www.crypto.com.papers/others/rc4.ksaproc.pdf.

[11] Martin Beck, Erik Tews. Practical attack against WEP and WPA. 2008.

[12] Matthew Gast: 802.11 Wireless Networks: The Definitive Guide, O'Reilly, 2002.eBooks

[13] M. Barbeau. WiMax/802.16 Threat Analysis. ACM Press. str. 8-15, 2005.

[14] Robbie Gill. Security Note on WPA and WPA2 dictionary attacks. 2008.

[15] Ross Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Cambridge, January 2011.

[16] Suzana Stojaković - Čelutska. Building Secure Information Systems, dissertation. Prague. 2000.

[17] Thomas Maufer. Field Guide to Wireless LANs for Administrators and Power Users. Prentice Hall PTR. 2003.

[18] William A. Arbaugh. Real 802.11 Security. 2001.