WLAN Information Security

Best Practice Document

Produced by FUNET led working group
on wireless systems and mobility (MobileFunet)
(WLAN security)

Author: Wenche Backman
Contributors: Ville Mattila/CSC – IT Center for Science,
Juha Nisso/Tampere University of Technology,
Mikko Laiho/University of Jyväskylä, Siiri Sipilä/Aalto
University School of Science and Technology,
Matti Saarinen/University of Helsinki, Thomas Backa/Åbo Akademi University,
Tanda Tuovinen/University of Helsinki
June 2010

Document No: GN3-NA3-T4-WLAN-security
Version / date: 08.06.2010
Original language: Finnish
Original title: “WLAN-verkon tietoturva”
Original version / date: 1.0 of 08.06.2010
Contact: wenche.backman (at) csc.fi

FUNET bears responsibility for the content of this document. The work has been carried out by a FUNET led working group on wireless systems and mobility (MobileFunet) as part of a joint-venture project within the HE sector in Finland.

This translated version is based on the Finnish counterpart approved by the Funet annual general meeting on 8 June 2010 after an open consultation period of two weeks.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 238875, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3)'.

Table of Contents

Executive Summary

WLAN information security includes user authentication, encryption as well as rules for handling the user's traffic during the session. Detailed authentication server configuration, WLAN controller and supplicant configuration will be addressed in a later best-practice document, namely the best-practice document on WLAN infrastructure. In this document 802.1X is recommended due to the high-quality security that it provides but web-based authentication is not recommended to be abolished, because of its simplicity. However, security issues related to web-based authentication, including fake login pages, are highlighted. As for encryption, WPA2-AES is recommended both for its security and for the fact that using the same encryption on several campuses eases supplicant configuration for roaming. Furthermore, it is recommended that SMTP connections from Internet to WLAN clients should be denied and SMTP connections from WLAN clients should be allowed only to a few specific SMTP servers. In addition, WLAN clients should not be allowed to communicate directly, without the traffic going through an access point. Unprotected protocols should, if possible, be prohibited if web-based authentication is used. Finally, it is recommended that a separate user password is used for authentication in WLAN.

1 Introduction

WLAN information security consists of user authentication, traffic encryption and the measures used for the management of users' traffic during a session. The underlying rules are usually specified immediately after successful authentication. It is further noted that it would also be advisable to take the recommendations regarding authentication and traffic management into consideration when planning fixed guest networks.

2 Authentication and traffic management

2.1 Authentication

WLANs should be equipped with some form of access control; the most commonly used authentication methods include web authentication and authentication based on the 802.1x standard. Some networks also use a PSK (Pre Shared Key), which involves using the same key for the authentication of all users. The most secure of these methods is 802.1x, which generally requires more advanced and expensive access points. However, high-end access points may also enable the use of various SSIDs (e.g. "guests" and "organisation") with differing security settings (web authentication or 802.1x) as well as user access to various VLANs. In the WLANs of CSC and the University of Jyväskylä, users outside the roaming community are offered a dedicated SSID that uses web authentication. In-house users have a different SSID that uses authentication by 802.1x.

During a conference or course, for example, a web-authenticated network allowing temporary user IDs could be a convenient way of offering network access to guests who do not belong to the roaming community, e.g. eduroam.

Web authentication using a captive portal is a straightforward and popular method for WLAN access control. However, several information security risks are associated with such networks, including:

- The authenticity of the login page cannot be verified. Forging login pages is relatively easy; users might see a login page that appears authentic (including the logo of the organisation, etc.) but would have no way of verifying its authenticity.
- User IDs and passwords can be intercepted and sessions hijacked.

It should further be noted that these types of networks generally lack encryption. A common method for protecting the connection is educating users to use a VPN server for authentication, creating an encrypted tunnel for the user's traffic. However, this method places exacting requirements on the VPN server, resulting in a lack of scalability.

In terms of information security, the administrator should pay consideration to the contents of the user database during network planning and implementation. For example, does the database contain a shared user ID whose password is known by all staff members? Roaming access using such IDs should be blocked. The administrator should also consider the possible impact of the user ID and password falling into the wrong hands. Potential attackers can cause considerable damage if the same ID can be used to access critical services. WLAN password interception is rare, however. Internet-based information security threats are far more common and have severe consequences. Attacks on WLANs are generally targeted at specific users; even large universities have not experienced any cases of WLAN password interception.

In some cases WLAN support for 802.1x may be a requirement for membership in a roaming access community. For example, eduroam requires 802.1x support, but networks that use only web authentication can be included in Funet roaming. In networks complying with the 802.1x standard the user's identity is protected in connection with authentication, and the authenticity of the organisation's authentication server may be verified using a certificate. No other traffic apart from authentication messages is relayed on the network until successful authentication has taken place.

2.2 Traffic Management

Network administrators should pay attention to the networks to which the user is granted access after authentication. Several Funet members have configured their WLANs to allow access only to the external network; the internal network can only be accessed from wired network sockets. If possible, it would be considerate to give visiting WLAN users access to resources such as specified printers and journal databases, depending on the applicable licence agreement. After successful authentication, users could well be directed to a dedicated VLAN. However, the points of use of that VLAN should be taken into consideration to prevent users from accidentally accessing networks or machines that need to be protected.

Especially on networks using web authentication, but also to an extent on 802.1x networks, information security and stability can be improved by using MAC address blacklisting. Although it is relatively easy to falsify MAC addresses, blacklisting effectively eliminates unintentional misuse. MAC address falsification is rare. Blacklisting can be used to prevent access for the following reasons, for example:

- The user frequently requests the web authentication page, e.g. 100 times per minute. The reason behind this may be a script attempting to gain access to a certain service, such as a social media site, without realising that user authentication is required.
- The user's device is performing unauthorised actions, for example, spreading a worm or constantly reserving new IP addresses.
- Notice of copyright violation from a motion picture company, for example.

The user should be notified of the device being blacklisted and advised to contact IT support in order to resolve the issue.

With regard to e-mail, the SMTP servers accessible from the network should be checked. The restriction of connections can make it significantly more difficult for infected devices to send out spam. Only connections to the organisation's own SMTP servers should be allowed from WLANs; SMTP connections from the Internet should be blocked completely.

To ensure WLAN information security, users' devices should also be blocked from acting as DHCP servers, and traffic between devices connected to the WLAN without message relaying by access points should be prevented.

2.3 Recommendations and comments

With regard to authentication, it is recommended that:

- Users should be convinced, through counselling and education on the weaknesses of unencrypted networks, of the need to switch to 802.1x. Because of the method's ease of use and reliability, web authentication must not be abandoned, but the users should be informed of the weaknesses involved.
- Different passwords should be used for WLAN authentication than for other systems.
- Users should be granted access to VPN without web authentication.
- If possible in practice, use of unencrypted protocols on web-authenticated networks should be blocked.
- SMTP connections from the Internet to WLAN users should be blocked completely, and SMTP connections from WLAN users should be limited to connections to the organisation's own SMTP servers.
- Users' devices connected to the WLAN should be blocked from acting as DHCP servers, and direct messaging between devices connected to the WLAN should be prevented. All traffic must be relayed by an access point.

The following comments are given with regard to authentication:

- The misuse of open networks is a reality; contacts by Sony Entertainment and other motion picture companies regarding copyright infringement should be expected.
- MAC address blacklisting is a convenient method for improving both network information security and stability.

3 Encryption

3.1 Overview

In addition to user authentication, WLANs often involve the need to encrypt users' network traffic. On networks using web authentication, traffic is not generally encrypted on the radio air interface, but information security is offered to users at a higher level, such as the network level using VPN technology. 802.1x networks use WPA or WPA2 encryption on the radio air interface. WEP encryption is an outdated technology that is not recommended because it can be broken in a matter of minutes. Its only benefit is in preventing the accidental use of the network.

The development of WLAN encryption is depicted in Figure 1. The 802.11i standard was developed following the discovery of weaknesses in WEP encryption. WPA encryption, which is based on the third draft of the standard, was introduced before the completion of the standard. WPA2 encryption is based on the final standard. The 802.11i standard makes use of two new information security protocols: TKIP and CCMP. TKIP includes the following improvements over WEP: regular key rotation, per-frame key mixing, a frame sequence counter to protect against replay attacks, and an improved message integrity check algorithm. CCMP utilises the AES algorithm and is consequently often called AES-CCMP. CCMP offers superior protection compared to TKIP, with per-frame key management and integrity checks being handled by a single component. The AES encryption used provides an excellent level of information security, and is recommended for use in all wireless networks.

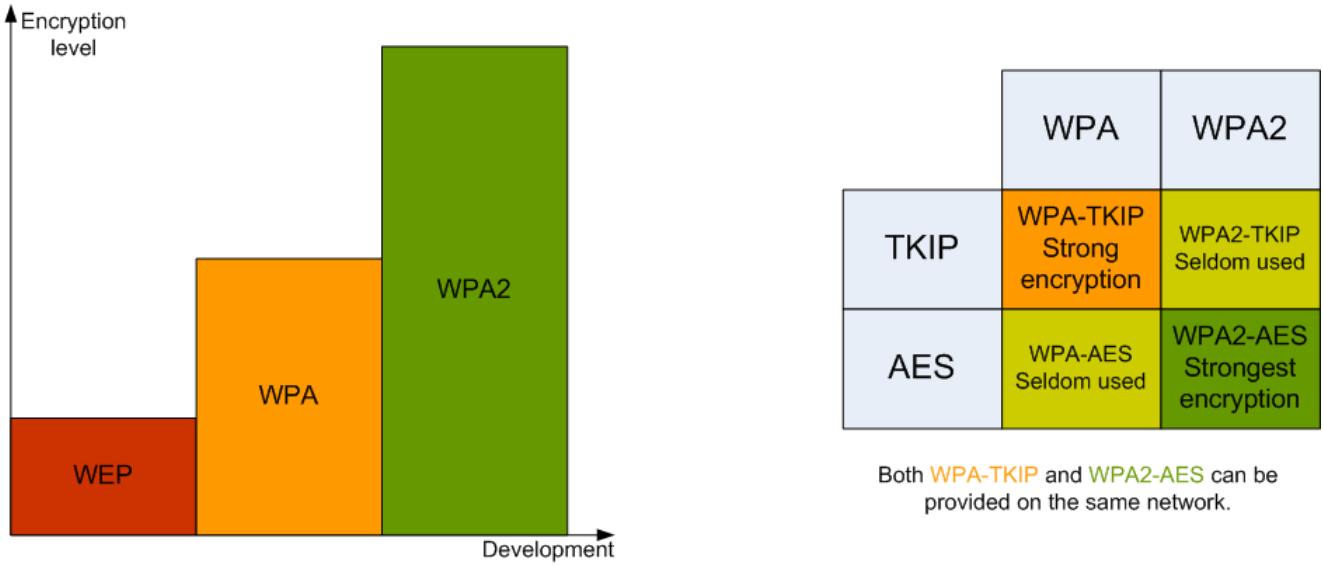

Figure 1. WLAN encryption development.

The master key used by the encryption methods (TKIP and AES) must be known by both the access point and the terminal. The master key is either created from a password or using a server. WPA-PSK, also known as WPA Personal, uses passwords for network access. This method is intended for use by households and small offices that do not have an 802.1x-compatible server. WPA Enterprise requires an authentication server, such as a RADIUS server, combined with a user database. The master keys used are created using the server. The RADIUS server is also used for user authentication, with one of the specified EAP methods employed in the authentication process. More information on EAP methods will be available in subsequent Best Practice Documents.

The safest of the encryption methods is WPA2-AES, but both WPA2-AES and WPA-TKIP are much more secure than web authentication. However, WPA2-AES is slightly more secure than WPA-TKIP; the changes to network infrastructure and terminals required by the introduction of WPA2-AES only are not as significant as those required when abandoning web authentication.

The interim versions WPA-AES and WPA2-TKIP do not carry any additional benefits, and may even cause confusion for users. For example, when connecting to a network such as eduroam, users may need to select the encryption method used, depending on the supplicant. The widely used Windows inbuilt supplicant requires that the encryption method used is known. When configuring WLAN controllers, it is not uncommon to leave all four methods enabled (WPA2-AES, WPA-TKIP, WPA-AES and WPA2-TKIP). It is recommended that only WPA2-AES and WPA-TKIP be used on all networks until switching over to use WPA2-AES only.
By way of illustration, let us examine a user who has used WPA-AES in the wireless network of his or her home organisation without any problems, who then visits an organisation supporting WPA2-AES and WPA-TKIP only. If the user connects to the network using the Windows inbuilt supplicant, he or she will need to change the encryption method used. This problem could have been avoided if both networks had used WPA2-AES only. This is why WPA-AES and WPA2-TKIP should be disabled immediately on all networks. WPA-TKIP may be supported until the end of 2010 to allow for the modernisation of hardware. It should also be noted that hardware lacking support for WPA2-AES may even be outdated to the extent of causing information security risks.

Network-level security using VPN is applicable to both unencrypted and 802.1x networks. VPN also protects the connection outside the air interface. However, only the use of 802.1x ensures improved mobility (the VPN connection is lost if the IP address changes) and support for IP multicast. When using network-level protection the lowest layers, such as the data transfer layer, should be protected using a firewall, for example.

3.2 Recommendations

With regard to encryption, it is recommended that:

- Only encryption methods WPA2-AES and WPA-TKIP should be used. WPA-AES and WPA2-TKIP should not be used at all.
- Encrypted networks should switch over by the end of 2010 to WPA2-AES only.
- The use of PSKs should be abandoned and each user should be given a personal user ID and password.

3.3 TKIP vulnerability

A weakness discovered in TKIP encryption at the end of 2008 makes WLANs using WPA-TKIP or WPA2-TKIP encryption vulnerable to, for example, false ARP messages, see [1]. This is another reason why it is advisable to introduce WPA2-AES encryption on WLANs.

The TKIP vulnerability has had an impact on the policy of eduroam, the world-wide roaming access service. New eduroam providers should provide WPA2-AES encryption only on their networks. Organisations already

using WPA-TKIP on their WLANs may continue as before. It should be noted, however, that the international eduroam policy is likely to change in the near future to allow only WPA2-AES encryption. The configuration of WPA-TKIP networks can be changed to provide more security, but the countermeasures are not without side effects (for more information, see [2]).

A new method for cracking TKIP was introduced in September 2009, based on the above-mentioned vulnerability. The new method, [3], enables the forging of short encrypted packets (e.g. ARP packets) in a considerably shorter time than before (approximately 1 minute compared to 12-15 minutes), increasing the likelihood of a session being hijacked.

References

[1] http://dl.aircrack-ng.org/breakingwepandwpa.pdf

[2] http://www.eduroam.org/downloads/docs/advisory/eduroamOT-admin-advisory-003.pdf

[3] http://jwis2009.nsysu.edu.tw/location/paper/A%20Practical%20Message%20Falsification%20Attack%20on%20WPA.pdf

Glossary

AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CSC	CSC - IT Center for Science Ltd.
DHCP	Dynamic Host Configuration Protocol
Funet	Finnish University and Research Network
IP	Internet Protocol
MAC	Medium Access Control
MobileFunet	a working group on wireless systems and mobility led by Funet
PSK	Pre Shared Key
RADIUS	Remote Authenticated Dail-In User Service
SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identification
TKIP	Temporal Key Integrity Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA and WPA2	Wi-Fi Protected Access