

The Evil Twin problem with WPA2-Enterprise

Ludwig Nussel <ludwig.nussel@suse.de>
SUSE Linux Products GmbH

Version 1.1
April 19, 2010

Contents

1	Introduction	1
2	WPA2 Enterprise	2
2.1	Overview	2
2.2	Authentication with the RADIUS Server	3
2.3	Verifying the identity of the RADIUS server	3
3	The Evil Twin	4
4	Conclusion	5
A	Deployment Scenarios	7
A.1	Setup without CA	7
A.2	Setup with public CA	7
A.3	Setup with custom CA	8
B	Credits	8

1 Introduction

The Evil Twin problem for wireless networks is known and documented for several years[1]. To perform the attack, a rouge access point broadcasts an SSID that the victim's system wants to connect to. Usually clients are configured to automatically connect to known networks when they come in range. So by having a better signal strength or by placing the access point at a location where the original network is not reachable clients would try to associate with the rogue access point. That poses a problem especially on public hot spots that do not use encryption as the client can't distinguish the real from the rogue access point. Also the user won't notice any difference after connecting if the attacker provides Internet access too. So the common advice is to always use WPA2 encryption[2][3]. When using a shared key a link with a rogue access point won't succeed as the access point can't decrypt packets from the client and vice versa. However, little information is available about how this affects WPA2 Enterprise. A publication in February 2008 about the dangers of misconfigurations went mostly unnoticed[6]. This document aims to emphasize the need for administrators to review their WPA2 Enterprise deployments and shake up software developers to improve their client software implementations.

2 WPA2 Enterprise

2.1 Overview

In environments with a large number of users, such as corporations or universities, WPA2 Personal with shared key for all participants in the wireless network is not feasible. For example, it wouldn't be possible to track which users are connected and it would be impossible to revoke access to the network for individuals without changing the key for everyone. Therefore WPA2 Enterprise authenticates users against a user database (RADIUS). Two common methods to do that are WPA2-EAP-TTLS and WPA2-PEAP. The procedure is outlined in figure 1.

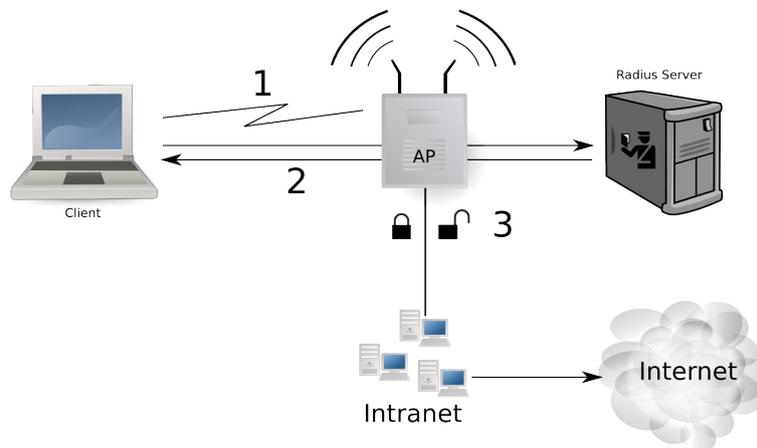


Figure 1: Overview[4][5]

- 1 the client establishes an 'anonymous' WiFi link with the access point. At this point the access point does not grant access to the Network.
- 2 the client talks to the RADIUS server for authentication. Since communication at IP level is not permitted for the client at this point, the access point acts as proxy between client and RADIUS server.
- 3 after successful authentication the RADIUS server allows the access point to unlock the client so it can communicate with the Network, for example a Company's Intranet

2.2 Authentication with the RADIUS Server

To prevent third parties from sniffing sensitive data the client establishes an SSL/TLS tunnel with the RADIUS server. Inside that tunnel an authentication protocol is used to supply user name and password to the RADIUS server. Such protocols are typically designed to authenticate the client against the server only and can't be used to also verify the server against the client. EAP-TTLS for example supports PAP as known from good old dial-up lines. PAP sends user names and passwords in plain text to the server.

Therefore the authentication procedure relies on the security of the TLS link. Both, for encrypting the communication as well as for authenticating the server against the client.

2.3 Verifying the identity of the RADIUS server

SSL/TLS use public key cryptography. In order to verify the identity of the peer, either the peer's public key must be known beforehand or a mediator trusted by both sides must testify that the public key indeed belongs to it's alleged owner. That's similar to identifying persons in the real world. Either one knows the subject in question personally or one has to verify the subject's passport. Verifying a passport means:



- one has to trust the agency that issued the passport
- one has to verify that the passport photo actually matches the person

In the SSL/TLS case X.509 certificates serve the role of passports. Certificates are containers with additional information for the public keys. By signing an X.509 certificate, a Certificate Authority (CA) attests the identity of the certificate's subject.

So in order to verify the identity of the RADIUS server the client has to:

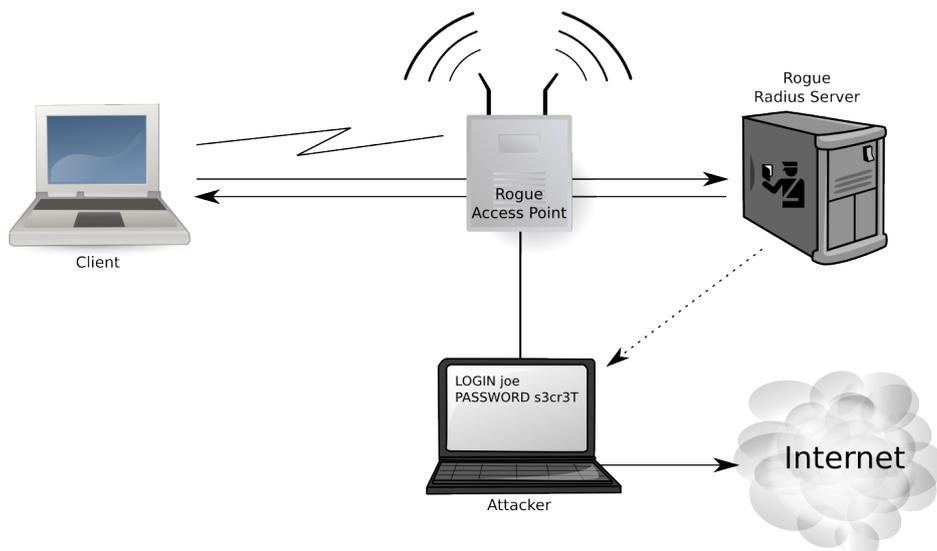
- verify that the server certificate is issued by a CA the client trusts
- verify that the identity of the server matches the identity the certificate was issued for

At first glance this sounds similar to what browsers do when connecting to SSL enabled sites on the Internet. On the Internet host names or IP addresses are used as identity. So when connecting to for example `bugzilla.novell.com` a browser can - or rather must - use that host name to verify that the certificate presented by the server actually is issued for `bugzilla.novell.com`.

The browser trusts the CA that it verified that the host is actually owned by Novell.

However, communication with the RADIUS server isn't at IP level therefore host names or IP addresses don't exist. The only user visible identity information about a wireless LAN is its SSID. The SSID can be freely chosen though. So there's no registry that ensures an SSID is unique and has a canonical owner. Therefore the Certificate Authorities trusted to attest identities on the Internet cannot be used to attest the identity of a wireless network nor it's RADIUS server. If such a public CA is used nevertheless the relation between the RADIUS server's identity to the wireless network has to be established manually somehow.

3 The Evil Twin



Setting up an Evil Twin for WPA2-Enterprise means the adversary has to run an access point that broadcasts the same SSID as the network he wants to impersonate. Clients typically just connect to the access point with the best signal strength. There is no way to determine whether an access point is legitimate or not.

After connecting to the access point a client will try to authenticate with a RADIUS server. Therefore the adversary needs to set up a RADIUS server that supports the same authentication method as configured on the victim's client. That's quite simple with e.g. FreeRADIUS[8] as included in any

RADIUS server.

Administrators should therefore make sure that:

- Client software used to access the wireless network actually can be configured in a secure way. It has to be kept in mind that nowadays WPA2 Enterprise implementations are not only available on traditional computers or laptops but also for mobile equipment such as phones. MAC address filtering could be used to hinder users in connecting with such devices.
- Passwords used to authenticate for access to the wireless network are not used for other services as well. Passwords of insufficiently configured clients are rather easy to steal by launching an Evil Twin attack. Therefore not using the same credentials also for e.g. computer logins, VPN or mail access reduces the value of stolen passwords for attackers.

Users cannot be held responsible for using an insecure configuration if the client side software makes it hard or even impossible to use a secure setup. Developers of wireless network client software should therefore:

- Design the user interface in a way that makes it hard for users to get it wrong. For example, offering an optional blank text entry field for entering the Subject or Common Name of the server certificate will certainly expect too much technical knowledge from users. It would only misguide them to leave the field blank or ignore it.
- Have the software autodetect and pre-set server identity and authentication settings. Assuming that users typically configure the client by choosing the wireless network's SSID from a list of scan results while inside the companies grounds, smart software can probe the settings and certificate offered by the RADIUS server.
- Pay attention to the error case when connecting to a network. For example, offering dialogs that allow the user to simply accept changed certificates would defeat all efforts to only permit secure configurations. Also, software should not automatically proceed if a RADIUS server suddenly changes the requested authentication method from e.g. MD5-Challenge to a plain text method like PAP.

A Deployment Scenarios

If WPA2-EAP-TTLS or WPA2-PEAP have to be used for wireless LAN authentication it's crucial that clients are configured to correctly verify the identity of the RADIUS server before sending credentials. The settings on the client required to achieve a secure setup depends on the kind of certificate used on the RADIUS server.

A.1 Setup without CA

The RADIUS server uses a self-signed certificate or the CA certificate is not available to clients.

The client software must compare the certificate offered by the RADIUS server with a reference certificate stored on the client. That means, the client software has to have an option to import a certificate from e.g. a USB stick.

Alternatively the client software may, when connecting to the network for the first time, display the certificate and offer to store it for future reference. The user has to verify the fingerprint of the certificate in this case.

Administrator notes

- make sure the validity period of the certificate is sufficient. Clients will refuse to connect if the certificate expires and need to be reconfigured.

A.2 Setup with public CA

The certificate of the RADIUS server is signed by a public CA as used on the Internet.

In case of public certificate authorities the host name of a system is typically used as identity information. It's either stored as "Subject Alternative Name" (subjAltName) or "Common Name" in the certificate. That means client software needs to allow entering the value of at least the Common Name field or one of the subjAltName fields.

Administrator notes

- client software often allows to select a system CA for the connection but does not require to enter identity information too. Such a configuration is insecure (see Section 2.3).

A.3 Setup with custom CA

The certificate of the RADIUS server is signed by a company internal CA that is only used for servers in the wireless LAN.

The client software needs to offer an option to import that CA certificate and associate it with the connection. Identity information is not strictly required if the CA doesn't issue certificates for other purposes.

Administrator notes

- If not entering identity information don't use the same CA to also sign user certificates. A stolen certificate could be used to install an Evil Twin then.

B Credits

Vojtech Pavlik brought the issue of deficiencies in WPA2-Enterprise client configurations to the document author's attention and inspired the document.

References

- [1] ISS Wireless LAN Security
http://www.iss.net/documents/whitepapers/wireless_LAN_security.pdf
- [2] Defeating Evil Twin attacks
http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1167674,00.html
- [3] Evil Twins FAQ
http://www.wi-fi.org/files/kc_4_Preventing%20Evil%20Twins-Wiphishing%20QandA.pdf
- [4] IEEE Std 802.11
8.4.8 RSNA key management in an ESS
<http://standards.ieee.org/getieee802/download/802.11-2007.pdf>
- [5] IEEE Std 802.1X
8. Port Access Control Protocol
<http://standards.ieee.org/getieee802/download/802.1X-2004.pdf>

- [6] Josh Wright, Brad Antoniewicz, PEAP: Pwned Extensible Authentication Protocol
http://www.willhackforsushi.com/presentations/PEAP_Shmocon2008_Wright_Antoniewicz.pdf
- [7] Jochen Eisinger, Exploiting known security holes in Microsoft's PPTP Authentication Extensions (MS-CHAPv2)
http://penguin-breeder.org/pptp/download/pptp_mschapv2.pdf
- [8] FreeRADIUS
<http://freeradius.org/>
- [9] FreeRADIUS Wireless Pwnage Edition
<http://willhackforsushi.com/FreeRADIUS-WPE.html>
- [10] SSLSNIFF
<http://www.thoughtcrime.org/software/sslsniff/>
- [11] SSLSTRIP
<http://www.thoughtcrime.org/software/sslstrip/>
- [12] Moxie Marlinspike, Null Prefix Attacks Against SSL Certificates
<http://www.thoughtcrime.org/papers/null-prefix-attacks.pdf>
- [13] Cliparts courtesy of openclipart.org, German passport sample courtesy of the [Bundesdruckerei](http://www.bundesdruckerei.de)