CORONET

White Paper

WPA-Enterprise exposure brief

Executive Summary

Most organizations use the WPA-Enterprise security protocol (also known as WPA-802.1x or WPA-EAP) to manage and protect their Wi-Fi access, allocating individual user credentials to their employees.

The vast majority of organizations implement a solution using WPA-PEAP (or WPA-TTLS) with MS-CHAPv2 authentication in their Wi-Fi network. This is because it employs a simple authentication scheme that doesn't require user-certificate management.

However, because of either device misconfiguration or user ignorance, most mobile devices, such as laptops and smartphones, are exposed to malicious Wi-Fi attacks that grab their Wi-Fi credentials. All an attacker has to do is set up a fake Wi-Fi access point (AP) either at the corporate premises or for example in a nearby food court with the same network name as the legitimate organization and grab the device credential hashes, crack them offline, and then return to the organization to penetrate the network.

Due to the dominance of the Microsoft® Active Directory® name service, many organizations use the same user credentials for both Wi-Fi access and other Active Directory managed services. This enables an attacker to pretend to be an employee, and then access the network and all internal services.

What can you do?

The safest solution is to move to the more robust WPA-TLS authentication protocol. However, this would require significant time and investment in a user-certificate system and related procedures.

You can properly configure Windows® operating system devices to prevent the attack. iOS and OS X® will trigger an alert to the user, so you need to make sure proper user education is in place in your organization. Unfortunately, Android devices are exposed to the attack, do not issue any alert to the user, and cannot be configured to prevent it.

Coronet's wireless protection suite provides protection from the wide range of threats that take advantage of unmanaged wireless networks, including the threat described in this white paper.

The Security Breach

If your organization has more than 100 employees, there's a good chance your Wi-Fi access uses WPA-Enterprise security, and there's more than a 90% chance that your organization uses the WPA-PEAP or WPA-TTLS variants with MS-CHAPv2 authentication. If this is the case, then you should be aware of the major security breach in your wireless access.

MS-CHAPv2 has a well-known vulnerability that allows a brute force attack to expose usernames and passwords of any length and strength. To quote Microsoft, "those credentials could then be re-used to authenticate the attacker to network resources, and the attacker could take any action that the user could take on that network resource". See the full article here.

So, if your employees use the same set of credentials for both Wi-Fi access and intranet services, such as email file server access, then an attacker can gain full access to those services.

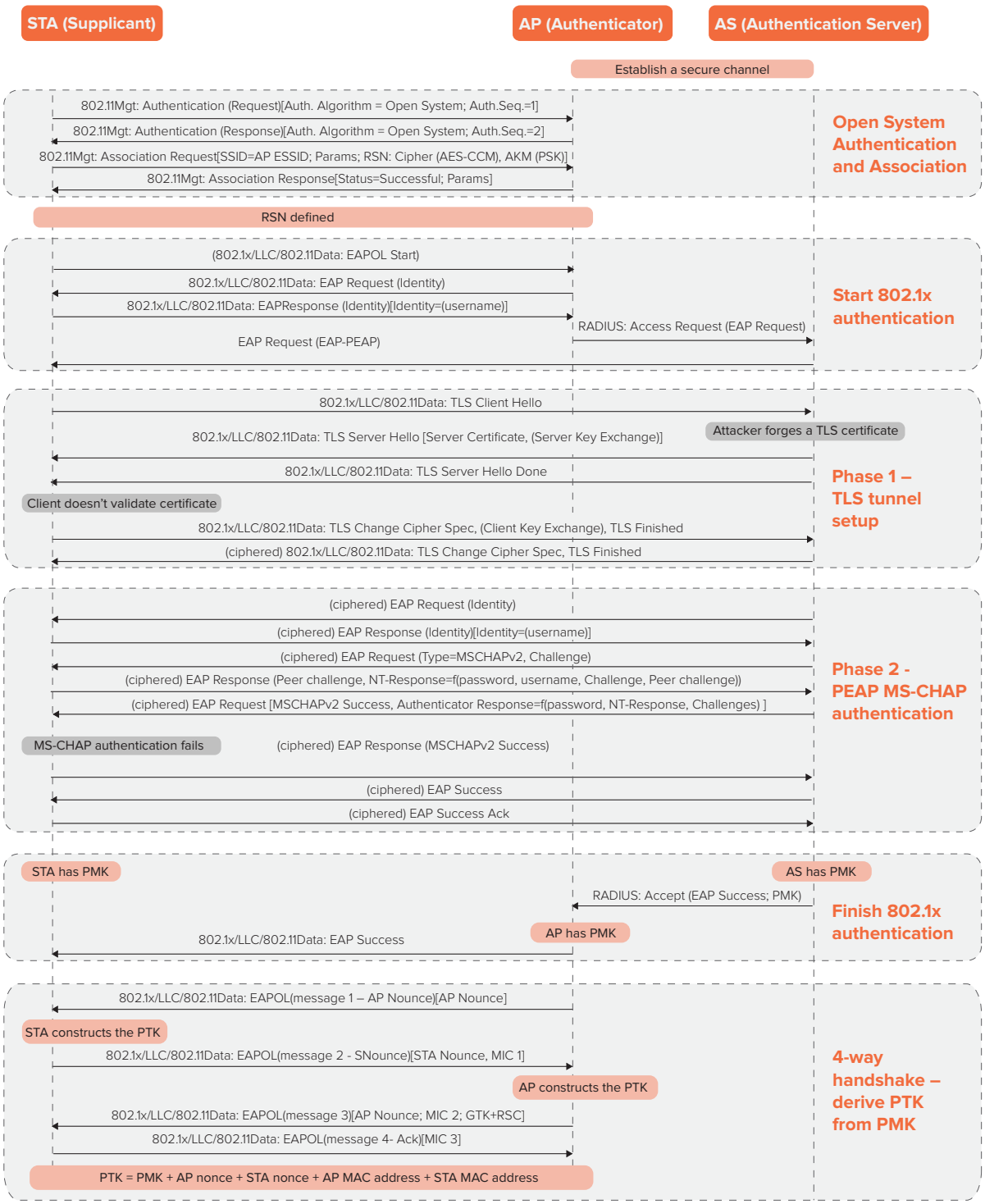
To overcome this vulnerability, PEAP and TTLS tunnel the PEAP protocol within a secure TLS communication session. However, to eliminate the need for cumbersome client-certificate management, both PEAP and TTLS settle with server-side-only certificate validation, so their protection is only as strong as the certificate validation provided by the client application.

Windows gives you the means to enforce certificate validation, causing the attack to fail. With iOS and OS X systems a user is notified about failed validation but they will be allowed to continue the authentication process. Uneducated users might ignore the warning, especially if an attacker creates a fake certificate with the organization's domain name.

The biggest issue arises with Android devices. By default, they ignore server certificates, and don't provide either user notifications or any configuration to force server certificate validation.

Attack Protocol

The figure below shows a WPA-PEAP with MS-CHAPv2 authentication flow and you can see at which point the attacker takes advantage of the system's deficiencies. The same attack protocol works in much the same way for WPA-TTLS with MS-CHAPv2 authentication.



Here's a breakdown of what's happening in the attack:

Set up a fake RADIUS server and forge a fake TLS certificate.

When using WPA-Enterprise, the client authenticates with a RADIUS server. This means that an attacker needs to set up their own fake server and provide it with fake TLS certificates. To make the certificate look more genuine (especially for iOS and OSX users), an attacker would create a counterfeit certificate using the organization's own domain name.

Set up a fake Wi-Fi AP with the organization's SSID.

The attacker can use either a regular Wi-Fi router or set up a soft AP using Kali Linux and a wireless card (e.g. using hostapd daemon). The attacker then provides the new AP with the same name (SSID) as used by the target organization's WPA-Enterprise network. The attacker then links the fake AP to the fake RADIUS server. The attacker can also configure the fake AP to have the same MAC address (BSSID) as one of the organization's legitimate APs, to evade potential wireless intrusion prevention systems (WIPS).

Note: With Kali Linux, the attacker can use the hostapd-wpe daemon to serve as both a fake AP and a fake RADIUS server.

Have the target device connect to the fake AP.

The attacker now needs the target endpoint device to try and connect to its fake AP. Based on the wireless environment, this could involve:

- Transmitting at high-power levels
- De-authenticating the client from a legitimate network
- Taking advantage of the fact that the network's SSID is in the device's PNL (Preferred Network List) and it will try to connect automatically

During the MS-CHAPv2 handshake attempt, the attacker gets all the information they need so they can crack the user's credentials:

1. Username (actually transmitted as clear text).
2. Server Challenge sent by the RADIUS server.
3. Client Challenge.
4. NT-Response (a hashed function of the user name, the two challenges, and the user password) sent by the client.

Note: The connection to the RADIUS server won't succeed since the attacker can't complete the MS-CHAPv2 authentication. This is because at this point, they don't know the user's password and therefore cannot reply with the required Authenticator Response function.

Crack the password.

If the password is simple, a dictionary attack can be used, such as by running the Asleap tool, to extract the user's password. Even complex passwords of any length can be cracked with a brute-force attack within a few hours using an FPGA-based DES cracking platform.

Attack Scenarios

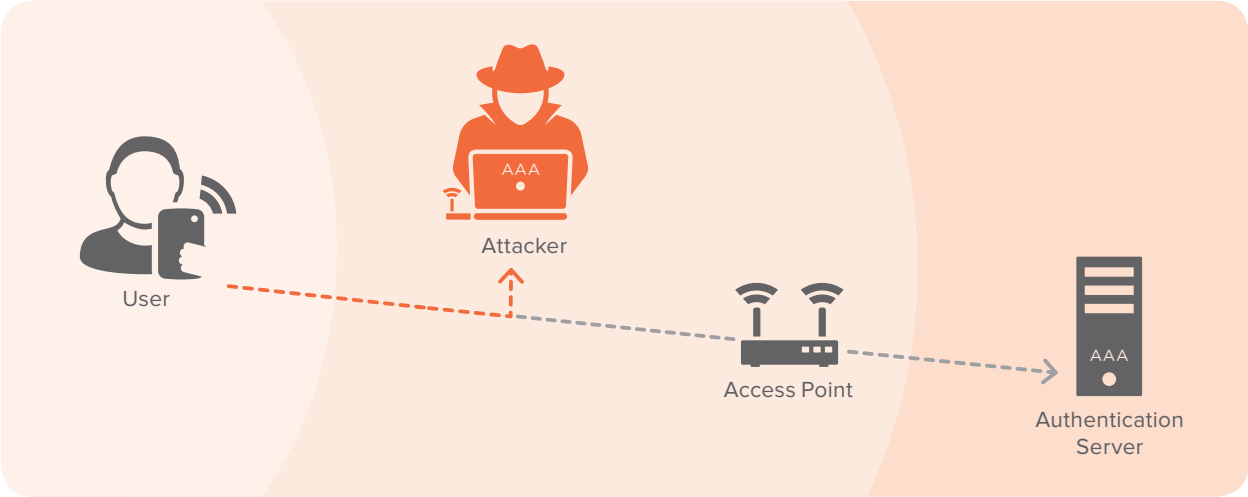
On-premises

The attacker positions themselves either near or actually on the organization's premises. They then set up a fake AP and fake RADIUS server.

An employee's device automatically roams to the fake AP and tries to authenticate with the attacker's fake RADIUS server. Though the authentication attempt will fail almost immediately, it provides enough information to expose the employee's username and password hashes to the attacker.

After collecting one or more user hashes, the attacker can pack up their equipment and move on to the second phase offline. At this point, they'll use either dictionary or brute-force attacks to crack the password. Depending on password complexity and the attacker's cracking capabilities, this could take anywhere from a few minutes to a few days.

Once they crack the password, the attacker can return to the organization premises and with the user credentials infiltrate the no-longer-secure wireless network. If the user's Wi-Fi credentials are the same as their Active Directory credentials, the attacker can connect to all relevant resources, such as email and file servers.



The food court

An attacker positions themselves close to an organization's campus in a nearby food court where corporate employees have their lunch, and away from any potential WIPS systems.

The attacker uses the same fake AP and fake RADIUS server technique described above. However, in this scenario, they take advantage of the fact that employees' devices have the organization's network SSID in their PNL, (Preferred Network List) and will therefore try to connect to the fake network without attracting the employee's attention.

The attacker proceeds to the cracking phase, followed by network penetration, as described in the previous scenario.

What Can You Do?

Move to WPA-TLS

WPA-Enterprise uses EAP (Extensible Authentication Protocol) as its authentication framework. The Wi-Fi Alliance™ has endorsed the following EAP authentication protocols:

- EAP-TLS
- EAP-TTLS/MS-CHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM
- EAP-AKA (and AKA prime)
- EAP-FAST

For no-SIM devices, the most secure protocol is EAP-TLS, which performs mutual authentication, validating both the client and the authentication server and, at least for the time being, is considered to be a relatively secure solution.

The downside of EAP-TLS (and the reason other alternatives have emerged) is that it requires you to manage client-side certificates. This might prove a complex, ongoing public key infrastructure (PKI) operation involving policy management, certificates (issuing, deployment, revocation and update), and managing trusted private and/or public certification authorities (CA).

Configure and educate

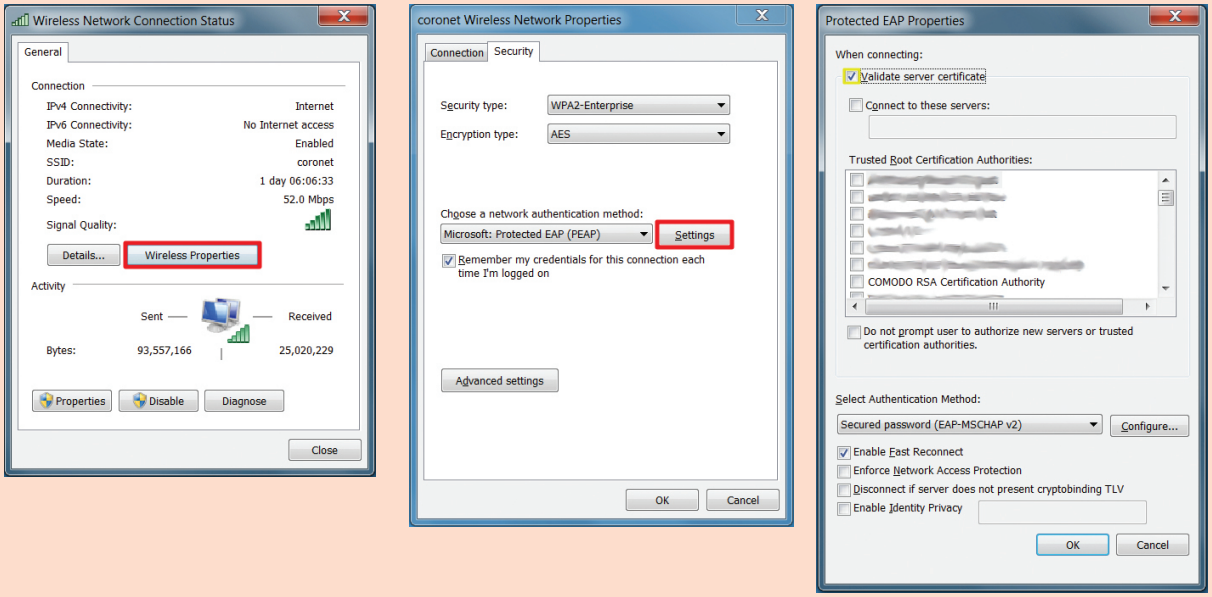
Unfortunately, with the attacks described above, proper configuration may not be enough. If you have Android devices connecting to your Wi-Fi network, they're configured by default not to validate server certificates, and thus are completely exposed to the attack. The user's credentials will be stolen without any warning.

For OS X or iOS devices, the attack will trigger an alert to the user, and so you should educate users not to trust unauthorized certificates. Regrettably, as we all know, not all users follow a security team's recommendations.

Windows is the only system that allows you to configure it in a way that will prevent the attack on the device. The figure below shows the steps you need to follow:

1. Open the **Wireless Settings** dialog box.
2. Go to **Network authentication** method settings.
3. Make sure the **Validate server certificate** checkbox is selected.

Note: If you also select the Do not prompt user to authorize new servers or trusted certification authorities, you'll be opening yourself up to an additional vector of attack where the attacker can issue a certificate from one of the root CAs and thus prevent a warning being issued to the user. Make sure this checkbox is not selected.



Protect Your Devices

Contact Coronet to learn how to protect your mobile workforce from the wide range of threats inflicted via unmanaged wireless networks, including the threat described in this whitepaper.

About Coronet

Coronet is the first company to monitor the global wireless environment for threats, and automatically evaluate the risk associated with connecting to any wireless network anywhere. Coronet arms organizations with real-time visibility to wireless threats on networks around devices, and provides policy-based control on the users' connectivity to networks and on users' access to enterprise resources. Coronet's cloud based solution is easy to deploy, runs on any device and requires no hardware.

For more information, visit: www.coro.net

CORONET

All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from Coronet.
© Coronet 2016