WPA Security: An Overview

How Elektron Keeps Your Wi-Fi Network Safe

Wi-Fi networks have created productivity improvements in organizations, providing greater mobility to users by untethering them from the corporate network. This ease of access has also created new security headaches for network administrators: the same roaming access available to legitimate users is also available to potential attackers.

The requirements for Wi-Fi network security can be broken down into two primary components: authentication and privacy. Authentication ensures that only users who have been granted access to the Wi-Fi network are able to access the network, and privacy ensures that data transmitted on the Wi-Fi network is unavailable to unauthorized users. This paper will discuss the issues involved in securing your Wi-Fi network and how Elektron helps solve the security problems associated with Wi-Fi networking.

Authentication

A critical element of Wi-Fi security is keeping unauthorized users off the network. Authentication is used to confirm the actual identity of a user or machine on a Wi-Fi network. Once a user's identity has been verified, the decision whether or not to allow access to the network can be made (in a process called authorization). Without performing strict identity checking on a network, attackers could access protected resources on your network, either by pretending to be an authorized user and accessing the corporate network directly or by spoofing the corporate network and convincing legitimate users to login to the attacker's own false network.

In the context of Wi-Fi network security, there are two authentications being formed: the server that protects network access (e.g., Elektron) must authenticate the identity of the user attempting to access the network, and the user accessing the network must confirm the identity of the server.

User Authentication

The task of user authentication is performed by your Elektron server. In a typical Wi-Fi network login, a user will identify herself to the Elektron server by providing a username and password. Elektron will then verify that the username exists, and if so, that the password provided matches the password associated with the username in Elektron's database. If both conditions are met, the user is granted access to the network.

A risk in using password-based authentication is that during the login process the user must send to the server their username and password before the secure wireless channel has been established. This would leave the login prone to passive eavesdropping by an attacker. Secure Wi-Fi logins avoid this problem by establishing a encrypted channel that is used only for the login process prior to sending usernames and passwords. Once the user's identity has been established and access to the Wi-Fi network has been granted, the encrypted login channel is torn down and all wireless communications between the access point and the client are encrypted using a dynamic encryption key separate from that used during the login.

Standards bodies have defined a number of different methods of password-based user authentication. Many of these do not send the password in plaintext form, but rather as a cryptographic digest, in an attempt to mask the password from potential attackers. Some of these methods are also designed to provide mutual authentication (i.e., the server can authenticate the client and the client can authenticate the server). However, none of the methods provide protection against man-in-the-middle attacks, nor do they protect the username in anyway. In order to protect against these and other attacks, Elektron encrypts all password-based logins (with the exception of LEAP, which we recommend against using if your client software supports either PEAP or TTLS).

Server Authentication

While Elektron is responsible for verifying the identity of users attempting to login to your Wi-Fi network, users have the responsibility to verify the identity of the Elektron server. This is an important and sometimes overlooked aspect of network security. It is arguably the more difficult of the two authentications performed for Wi-Fi network access, as it requires configuration of each client machine that will be accessing the network.

Unlike users, which typically identify themselves using a username and password, Elektron proves its identity using a digital certificate. Validating the server's digital certificate can happen automatically within the user's wireless networking client software, provided the client software has been pre-configured to recognize the certificate authority that issued the server's certificate. Elektron makes it easy to configure client certificate verification, creating double-clickable installers for both the Mac OS X and Windows XP platforms.

In order to verify the server's identity, users must perform digital certificate chain validation. If the digital certificate validation fails, then the Elektron server's identity could not be verified and the Wi-Fi network access attempt should be terminated by the user. Such a failure can be indicative of a attacker attempting to lure a legitimate user into logging into fake network, thus fooling the user into giving up their username and password. Once armed with the user's credentials, the attacker can then use them to login to the legitimate corporate network.

Privacy

In addition to authentication, a secure wireless network requires privacy. A traditional wired network can rely on its physical security to remain protected. So long as an attacker cannot physically connect to the wired network, the attacker cannot access data flowing across the network. A wireless network does not respect an organization's physical boundaries, so an attacker need only be in proximity to a wireless network to compromise it.

While authentication can prevent an attacker from actively joining a wireless network, encryption can prevent passive eavesdropping of user data. An attacker with a packet sniffer sees only scrambled bits. This keeps sensitive business information such as email and files private as users access corporate servers via the wireless network.

Wi-Fi Protected Access

The first attempt at keeping wireless networks private was a protocol known was Wired Equivalent Privacy (WEP). It was designed to be easy to deploy, and as its name suggests, to provide a level of security equal to that of a wired network. For a time it was the only means of security available in wireless hardware.

WEP clients and access points encrypt their communications using a key shared amongst all users. This makes for easy configuration: simply enter the key into each piece of wireless hardware that will be on the network. However, while having shared keys makes system administration easier, it is also WEP's Achilles' heel. Cryptographic flaws in WEP's design and the network administration headaches associated with a single shared key contributed to WEP's demise.

As wireless networking gained in popularity, its security shortcomings became increasingly apparent. In response, the IEEE began work on a new standard designed to address these shortcomings. This new standard, dubbed 802.11i, began to work its way through the lengthy IEEE review and approval process. In the meantime, the Wi-Fi Alliance, an industry trade group, created an interim standard called Wi-Fi Protected Access (WPA).

The primary new feature of WPA is the appearance of the Temporal Key Integrity Protocol (TKIP) in place of WEP's basic RC4 encryption. TKIP continues to use RC4, but in a more secure way than WEP. The initialization vector in TKIP is increased from 24 bits to 48 bits, per-packet key mixing is added to increase the difficulty in divining a network key, and a Message Integrity Check (MIC) is added to confirm that a packet has not been tampered with.

WPA is available in most Wi-Fi hardware produced today. In order to be considered "Wi-Fi Certified" by the Wi-Fi Alliance, access points and client hardware must support WPA.

WPA comes in two flavors: WPA Personal and WPA Enterprise. As the names suggest, the former was intended for small office/home office use, while latter was targeted toward large organizations. Elektron enables the use of WPA Enterprise for organizations of any size.

WPA Personal

In an effort to simplify WPA deployment for small networks, the Wi-Fi Alliance defined the WPA Personal mode. This mode is also known as WPA-PSK (Pre-Shared Key). Like WEP, it uses a single master key for all participants in the network. Thus, like WEP, it suffers from the security issues associated with using a single key for all users.

WPA Personal has its shortcomings, but is far better than no security at all. With WPA Personal enabled on their network, administrators can limit network access to users that have been provided the WPA key, while also encrypting data transmitted on the network.

WPA Enterprise

The WPA Enterprise mode is the most secure method available for locking down Wi-Fi networks, enhancing both authentication and privacy. WPA Enterprise provides for a separate username and password for each network user. It also generates dynamic keys that are unique to each user and that are changed frequently.

WPA Enterprise utilizes the 802.1X/EAP protocol to authenticate users, and thus requires a server to provide this authentication. This is the role filled by Elektron.

There are a number of advantages to using Elektron to provide WPA Enterprise services to your network over using WPA Personal:

User Management Each network user gets her own login, meaning that when if a user leaves your organization and will no longer have access to the network, only that user's credentials are affected. Under WPA Personal, all systems must be reconfigured to use a new master key.

Authentication Elektron can maintain its own database of users, or use operating system services to check logins. On Windows, this means that the Active Directory or SAM database can be used, and on Mac OS X Open Directory can be used. This means that only one user database must be maintained, so changes such as adding or removing users need only happen once.

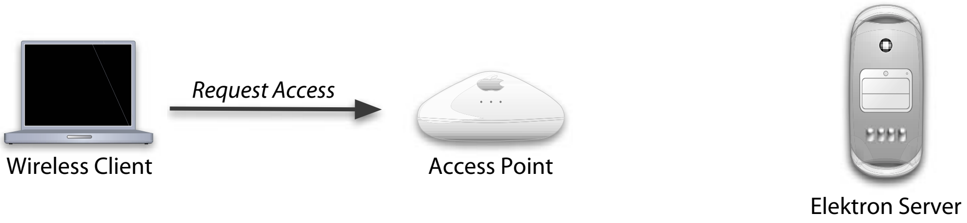
Auditing Because each user has her own username, it is easy to keep track of who is logging into your network, and when.

Encryption Dynamic encryption keys are generated for each user at each login, and then changed frequently. This means that attackers should be unable to determine any user keys. What's more, because each user's key is unique, no user will be able to decrypt another user's network transmissions.

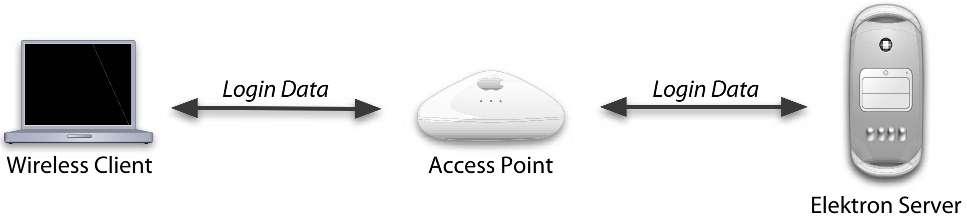
A WPA Enterprise Walk-Through

In order to connect to a WPA Enterprise protected network, a wireless client must go through several steps:

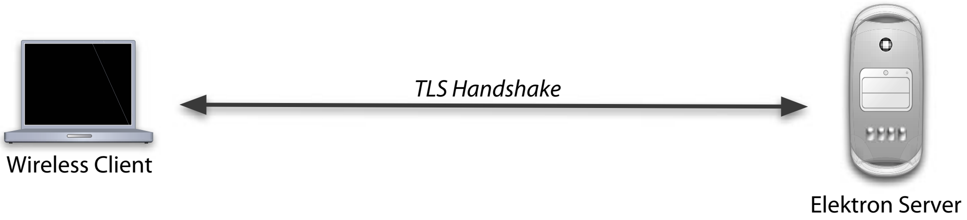
Step 1 First, upon initial connection to the wireless access point, the wireless client will be informed that WPA Enterprise authentication is required. At this point, the client is not allowed to forward any non-authentication related data packets to the wireless network.



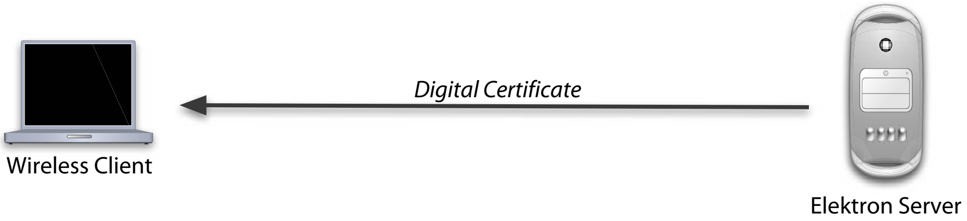
Step 2 The wireless client initiates a WPA Enterprise login. Once the login process begins, the access point begins forwarding data received from the client to the Elektron server, and vice versa. It is Elektron's responsibility to manage the client login; the access point merely forwards packets back and forth between the client and server. While in this state, the access point will continue to disallow any non-login related data packets from the client.



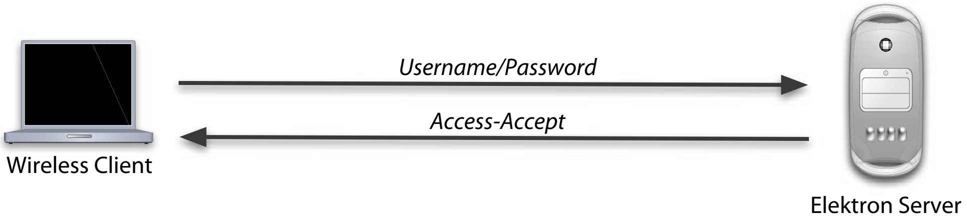
Step 3 The client creates a TLS connection to the Elektron server. This will establish the server's identity and protect further communications from eavesdropping.



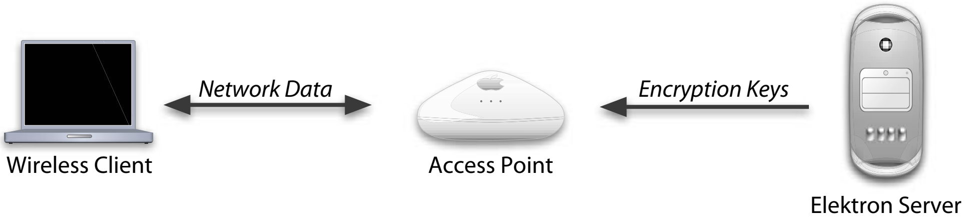
Step 4 While establishing the TLS connection, Elektron sends to the client its digital certificate. The client must verify the certificate's authenticity in order to continue with the connection. If the server's certificate cannot be authenticated, the client should terminate the login. Doing so can help prevent the client from inadvertently sending their login information to an attacker.



Step 5 After the TLS connection is established and the server's identity is confirmed, the client sends her username and password. Elektron validates the username and password, sending either an "access-accept" or "access-reject" message to the client.



Step 6 If the result is "access-accept", Elektron sends to the access point the dynamic keys to be used for encrypting the wireless session. The client computes these keys itself, and the secure wireless session begins.



The wireless login process is transparent to the user, with all of the details handled by Elektron and the client software.

Login Protocols

There are a number of competing protocols defined for use during the WPA Enterprise login process. While the overview above applies to the two most common of these protocols (PEAP and TTLS), there are some technical differences in their implementation. Elektron supports three different login protocols:

PEAP The Protected Extensible Authentication Protocol was jointly developed by Microsoft and Cisco. It consists of any Extensible Authentication Protocol (EAP) method wrapped inside of a TLS channel. It is the most widely deployed form of WPA Enterprise authentication thanks to its appearance as a component of Windows XP. Some examples of of EAP methods used in conjunction with PEAP are EAP-MS-CHAP-V2 (used by Microsoft) and EAP-GTC (used by Cisco).

While PEAP was created by Microsoft and Cisco for the purpose of interoperability between their respective product lines, each company went off and created incompatible implementations. Elektron is capable of handling both the Microsoft and the Cisco dialects of PEAP.

PEAP also suffers from version creep: as of this writing, there are no fewer than three different, incompatible version of PEAP defined in various IETF internet drafts.

TTLS The Tunneled Transport Layer Security protocol is similar to PEAP in that it tunnels user authentication data inside a TLS channel. The difference is that TTLS can handle any authentication method, not just EAP methods. TTLS also does not suffer the incompatibility problems of PEAP, and has just one well-defined specification.

LEAP The Lightweight Extensible Authentication Protocol was defined by Cisco prior to the appearance of either PEAP or TTLS. It does not use a TLS channel to protect a user's login information. LEAP is a derivative of Mircosoft's MS-CHAP-V2 login protocol, and has some well-known security vulnerabilities. Its use should be limited to clients that do not support PEAP or TTLS and is included in Elektron only for backwards compatibility.

The Future of WPA

As described above, WPA is an interim specification designed to bridge the gap between WEP and the adoption of IEEE 802.11i. The intent was to get stronger security into the hands of users as quickly as possible. WPA provides a subset of 802.11i that can be implemented by hardware manufacturers and software developers without having to require replacement of existing equipment. In fact, most Wi-Fi equipment sold today is either WPA capable out of the box or is firmware-upgradeable to support WPA. The Wi-Fi Alliance requires that all "Wi-Fi Certified" equipment support WPA.

The future of WPA is the adoption of the full 802.11i specification rather than the subset supported now. Some of the new features of 802.11i are:

AES Encryption The option to use the federal Advanced Encryption Standard as the algorithm used to encrypt data packets in place of the Temporal Key Integrity Protocol (TKIP). Some Wi-Fi equipment makers are shipping AES with their products today.

Secure Fast Handoff This allows roaming between access points without requiring clients to fully re-authenticate to every access point. Re-authentication can slow roaming, disrupting real-time networking applications like multimedia or VoIP.

Secure IBSS Independent Basic Service Set (IBSS) wireless topologies, sometimes called ad-hoc networks, receive new security features in 802.11i.

Because 802.11i does not mandate any changes to the 802.1X protocol as implemented by Elektron, meaning that deploying Elektron today will protect your network now and in the future.