InteropNet Labs

7 in a Series

# Security: Which Layer?

by Matthew Gast

Where should you apply security to a wireless LAN? With the hype surrounding wireless security vulnerabilities, many network administrators are left wondering what measures are necessary to secure wireless LANs. Have Layer 2 protocols overcome their historical weakness? Is IPSec too stringent and complex, and can it address layer 2 concerns? Deciding at which layer to apply security is a key decision that will dictate network architecture and many of your purchasing decisions. This paper discusses the differences between layer 2 and layer 3 security to help you find the right middle ground for your network. Of course, there are other security options, such as using application layer encryption or web-based authentication. This paper focuses on the two most comparable methods used on IP networks.

## *Compound Authentication Methods and the Binding Problem*

Most traditional methods of user authentication are not secure. While the resistance of authentication protocols to attack is increasing, older, widely-deployed methods of authentication will be used for many years to come because users want to protect their investment in them. But the downside to that investment protection is that these protocols face new threats that are outside the original design.

One common tactic to protect older authentication protocols from prying eyes is to encrypt them inside strong tunnels using technologies such as the Transport Layer Security (TLS) and the IP Security protocols (IPSec). Using a strong tunnel to protect a much weaker legacy method is often called a *compound authentication method* because a set of protocols is used to accomplish the authentication goal. Any method that uses a series of authentication methods, possibly with different credentials at different stages, is a compound authentication method. The most notable examples are the TLS tunneling methods used on wireless networks (TTLS and PEAP, which are described more fully in the iLabs white paper titled "TTLS and PEAP Comparison"), as well as the eXtended Authentication (XAUTH) commonly used with IPSec.

Compound authentication methods are often used to extend legacy authentication methods into new realms by providing necessary security enhancements. Older authentication methods were originally designed for less demanding environments, and usually do not protect user identification information, authentication credentials, or validate the integrity of protocol messages. Adding these functions to legacy protocols can be either by adding security to the older protocols directly, or combining the older protocol with a second protocol that can provide the required cryptographic safeguards. Designing cryptographically secure protocols is extremely demanding work, and it is easier and safer to use a widely deployed and analyzed protocol such as TLS or IPSec to provide the necessary cryptographic components.

In October 2002, researchers found that the common design shared by most compound authentication methods is insufficient to prevent certain types of man-in-the-middle (MITM) attacks. In the case of tunneled compound methods, one of the major problems is that the tunneled "inner" authentication method is not strongly associated with the "outer" protective tunnel. Before exchanging the sensitive "inner" authentication data inside the tunnel, the protocols do not provide for a check that the authentication is occurring with the endpoint of the "outer" tunnel. The resulting compound binding problem does not occur because of weaknesses within the tunnel protocols or inner methods, but rather in the way they are combined. Fixing the problem requires that each step of the compound authentication method depends on the previous step and demonstrates that the endpoints have participated in all of the prior authentication exchanges.

## *Layer 3 Security: IPSec*

If the objective of deploying IPSec is to protect against vulnerabilities in the wireless LAN security protocols, you *must* deploy certificate-based authentication, or use an authentication method which tightly binds the inner and outer authentications. IPSec tunnels can be secure against compound binding problems, although this is difficult to do using tunneled legacy authentication based on XAUTH---the most common implementation. XAUTH suffers from the same basic compound binding problem as the TLS-based authentication methods in wireless LANs, and has other security problems which make it a poor choice for wireless environments.

The strength of IPSec is that it is a trusted, proven cryptographic system that has been extensively tested in the crucible of the Internet and has no known design flaws. IPSec's strength allows it to be compliant with the Federal Information Processing Standards (FIPS) required for use on some U.S. government networks. Additionally, IPSec is the only protocol suitable for end-to-end protection. Remote users who use wireless networks in "hot spots" must use IPSec to secure the connection back to the home network, just as they would secure any IP connection across the Internet. IPSec has some limitations with respect to wireless LAN security, however. Even with both static addresses and digital certificates, an IPSec implementation requires that the network be run completely open to any potential station. In such an environment, attackers can obtain IP addresses and launch attacks against other wireless network users or denial-of-service attacks against the VPN components.

## *Layer 2 Security: 802.1X*

802.1X acts as a gatekeeper for basic network access. By denying access to the network before authentication is successful, 802.1X can prevent many attacks against network infrastructure that depend on having basic IP connectivity. With the right deployment architecture, 802.1X can even enhance IPSec. Because IPSec security associations are established between IP addresses,any change of address will interrupt communications and require re-establishment of the VPN tunnel. Many 802.1X-capable products are capable of dynamically attaching clients to the network depending on the result of authentication. By enabling users to stay attached to the same IP subnet, IPSec will function smoothly. 802.1X is also a framework that provides significant cryptographic enhancements in Layer 2 encryption. Encryption keys will be derived in part from the authentication exchange, and can be changed at short intervals to protect against all known attacks against WEP. Significant improvements in Layer 2 encryption are expected later this year when the Wi-Fi Alliance requires that all Wi-Fi certified products incorporate Wireless Protected Access (WPA).

While the compound binding problem is a theoretical risk for 802.1X, its practical drawback can be reduced by simple configuration changes. Exploiting the compound binding weakness requires successfully completing the first phase of a tunneled authentication protocol, and then attracting a victim to steal the inner credentials. For a successful attack, the victim's client must be submit inner credentials to the attacker. Clients do not submit weak inner authentication protocols directly, so the main avenue of attack is to steal EAP-TLS credentials and use it as the inner protocol for a PEAP/EAP-TLS or TTLS/EAP-TLS attack. Configuring authentication servers not to accept EAP-TLS as an inner protocol eliminates much of the risk of the compound binding problem. As an alternative, using EAP-TLS with client certificates provides strong mutual authentication in one step and also bypasses the vulnerabilities associated with compound binding. Reducing compound binding risks is an active area of research and development, and further protocol enhancements should further mitigate risks. As a practical consideration, exploiting compound binding weaknesses requires that attackers install equipment in the target network and make numerous active radio transmissions.

## *Recommendations*

802.1X and IPSec are used at different layers of the protocol stack, and are not mutually exclusive. Your choice of Layer 2 security, Layer 3 security, or both will depend on your goals and requirements. By understanding the different security properties of each protocol, you can select the best one for your environment. Both 802.1X and IPSec provide encryption to protect messages from eavesdroppers. Both can provide strong user authentication, though most IPSec implementations require the use of certificates, while 802.1X implementations can build strong authentication based on existing authentication servers. 802.1X protects against many attacks from unauthorized users by denying network access before authentication completes. 802.1X used in conjunction with improved Layer 2 encryption is likely to meet the security needs of most organizations.

In simple terms, the security of an IPSec tunnel is greater than a WEP “session,” even one re-keyed frequently using 802.1X protection. Whether that additional protection is necessary depends on your requirements. (The most notable example is that some organizations have policy requirements to use only FIPS-certified cryptographic systems.) When 802.11i is fully implemented using AES encryption, the goal is for 802.11i wireless sessions to have near equivalent security levels to IPSec security associations. However, the authentication of 802.1X is better thought-out than IPSec remote access methods such as XAUTH, giving 802.1X the security edge on the authentication side.