Technology for a Secure Mobile Wireless LAN Environment: Evolution, Requirements, Options

Introduction

Wireless LANs are now in use in essentially every application amenable to implementation on a local area network. With the advent of the 11 Mbps IEEE 802.11b (and, soon, the 54 Mbps IEEE 802.11a), wireless LANs (WLANs) have found a home in five key application areas, providing networking functionality essentially identical to that on wire, but without the need to be tethered to the wall:

- Vertical applications – these continue to remain an important area of use for WLANs, typically involving data collection, bar codes, and industrial automation solutions.

- The enterprise – the major growth area for WLANs over the past few years, microcellular-based WLANs allow roaming across a floor, building, campus, and even between facilities.

- Small business – smaller firms without dedicated network management and operations staff can benefit from the simplicity and ease-of-use inherent in wireless LANs.

- The residence/home office – homes are often much more difficult to wire than businesses, so wireless LANs in the home are rapidly growing in popularity - and the mobility especially appeals to anyone who brings a notebook computer home from the office.

- Public spaces – one of the hot growth areas for WLANs over the next few years will be their deployment in "hot spots" within high-traffic public spaces - airports, hotels, convention centers, and even coffee shops.

And while all of these venues benefit from the location-independence and freedom of movement inherent in wireless, they also all have the same core challenge – security.

The Security Imperative

Security is one of the most significant, but also least understood and appreciated, elements of data communications and information technology. While everyone can agree it's important, if not vital, to keep sensitive information confidential and prevent unauthorized access to networks and the information resources they connect, the mechanisms for accomplishing these goals can be complex. A good security solution, therefore, stresses *simplicity* and *ease of implementation* with *no* compromise in mission or effectiveness.

Looking at the issue in a little more depth, there are two key components to any security solution:

_ *Encryption* – The most basic form of security is in the encryption of any user data moving over the network. There are now many forms of encryption available, and the designers of the IEEE 802.11 standard had the forethought to include encryption in their original standard as released in 1997.

Unfortunately, the so-called "Wired Equivalent Privacy" (or "WEP") capability included in 802.11 has a number of critical weaknesses. Perhaps, most notably, the key length in 802.11 is only 40 bits. This limit was included to meet export restrictions in place at the time 802.11 was ratified. A 40-bit key is known to be quite weak given the inexpensive computer power available today to break encryption schemes.

As a consequence, most vendors have implemented 128-bit (or greater) keys providing some added security.

Corporate Headquarters
PO Box 1209
Mt. Gilead, NC 27306

Compsee

International Sales Office
2500 Port Malabar Blvd.
Palm Bay, FL 32905

While the 40-bit limitation in the standard will be removed in an update to 802.11 (currently under development by 802.11 "Task Group i", or "TGi"), other problems remain. These include the lack of key distribution, key management (both must be done manually), key rotation (an added security technique which changes security keys on a regular or irregular basis), and the fact that WEP only encrypts data over the air, between the access point and the client. A more end-to-end approach is required, ensuring that data appears in the clear only on authorized clients and servers. WEP also shares security keys among users, creating a big opportunity for keys (and thus the entire network) to be compromised.

Finally, in a highly-publicized recent series of technical papers and articles, it has been demonstrated that WEP (which is based on the well-known and widely-implemented RSA RC4 algorithm) can be broken in close to real time, and can no longer be relied upon when subject to a dedicated attack (and, of course, it can be very difficult to determine if such an attack is underway in a wireless environment). Thus, WEP cannot be relied upon for complete security, and therefore network managers need to consider alternatives.

➢ *Authentication* – Authentication ensures that only authorized users are allowed on the network. Again, there are rudimentary authorization techniques included in 802.11, such as an "SSID" which all clients must know in order to gain access to the network, and in some cases the ability to specifically include or exclude a given wireless client from participation (via an "Access Control List"). Note, however, that the specific wireless network interface card (NIC) and not the human user is actually being authenticated via this mechanism, creating a major security hole if a given card is stolen or misplaced. It's clear that more-sophisticated authorization is required to ensure both network and data integrity. Dedicated hackers know and understand the 802.11 protocols; greater defensive measures beyond what's in the standard are required here as well.

So it's easy to see that a more end-to-end approach is required in any wireless network, using, oddly enough, techniques that are not that different from what's available on wired networks. A wireless LAN is, after all, a LAN. A single set of unified security techniques to manage both wired and wireless LANs under a single umbrella is most desirable. The key to a great security solution for a wireless LAN is meeting this requirement while supporting the key benefits of wireless, most notably the ability for users to roam while remaining connected to the network.

WLAN Security System Requirements

From the above discussion, a number of key elements for security in WLAN implementations become apparent:

- *Mutual authentication* – both the client and server must authenticate with each other. This of course guarantees that only authorized users are allowed on the network, but it also helps to guard against rogue access points and other wireless devices not specifically allowed on a given network.

- *End-to-end encryption* – user data must never be allowed to appear in the clear on the network except at authorized end points.

- *Per-client keys* – keys must be unique for each authorized user. This prevents the compromising of security keys due to theft or otherwise unauthorized access.

- *Key distribution* – a technique for the central management of security keys is essential. Manual processes are both error-prone and subject to compromise.

- *Full support for mobility* – Finally, any security implementation must take into account the fundamental nature of wireless LANs – that users can move from access point to access point as they roam throughout a given facility, and even between facilities.

Corporate Headquarters
PO Box 1209
Mt. Gilead, NC 27306

Compsee

International Sales Office
2500 Port Malabar Blvd.
Palm Bay, FL 32905

(800) 628-3888 ● (321) 724-4321 – V ● (321) 723-2895 – F ● sales@compsee.com ● www.compsee.com

A wide variety of options for meeting the above exist. One of the most obvious is services, which operate at layer 3 (the network or IP layer) or above. One popular technique is the use of a virtual private network (VPN), an approach based on "tunneling" encrypted traffic through a network. This has a number of benefits. Among these are centralized management, uniformity across media, and suitability to both in-building use and remote access. However, VPNs have not been standardized and may have implementation dependencies that can make them complex in operation.

The Remote Authentication Dial-In User Service (RADIUS) approach is also popular, and it can be effective for authentication of client and server. When used in WLAN applications, the problem with RADIUS is that its heritage as a dial-up remote access product is visible – there is currently no support for mobility, no key distribution or support for key exchange, no inherent security features, and fundamental issues with latency that can interfere with roaming.

Finally, a variety of fundamentally proprietary techniques have been implemented, even by major vendors. The core issues are extensibility and compatibility with future WLAN products and standards – while these approaches can be quite secure, their use can mandate significant costs as new products are introduced into existing networks. Clearly, an open, standards-based approach is best.

Kerberos

The Kerberos network authentication protocol was originally developed at MIT as part of the legendary Project Athena in the 1980s. Named after the Greek mythical threeheaded guard dog that provided maximum security and protection for the underworld, Kerberos (also known as Cerberus) provides all the tools for maximum security and protection of your network. Now in version 5, Kerberos is operating system and application independent, and has been applied in operating environments as diverse as Windows 2000, the Internet, and versions of UNIX. Kerberos provides a mutual authentication between a client and a server, and between servers before a network connection is opened.

The Kerberos protocol assumes that initial transactions take place on an open network where clients and servers may not be physically secure and packets traveling on the network can be monitored and even possibly modified at will. The assumed environment is much like the Internet today. Note that Kerberos is independent of the security features defined in 802.11. This is particularly important since, as we noted earlier, changes to 802.11 security will be made as part of TGi. Kerberos also has exceptionally low overhead, making it well suited for wireless-LAN applications.

Kerberos' mutual authentication uses a technique that involves a *shared secret*, which works much like a password. Many authentication techniques (including RADIUS) actually send passwords in the clear, allowing them to be compromised if intercepted by an unauthorized party (such as an eavesdropper using a wireless LAN card operating in "promiscuous mode", which allows all traffic within range to be intercepted). Kerberos solves this problem via encryption – rather than sending the password, an encrypted key derived from the password is communicated and thus the password is never sent in the clear. This technique can be used to authenticate a client, but can also be used for mutual authentication of a server as well. Once authentication takes place, all further traffic is be encrypted, allowing even new encryption keys to be communicated without undue fear of compromise.

The implementation of Kerberos includes a number of key features and benefits:

- Encryption-key distribution is *dynamic*, and keys can be changed and securely distributed whenever desired. Key lifetimes can be set from minutes to infinity.

- Keys are generated at the start of every session and are allocated per client – *no sharing of keys among clients is allowed*. Key generation also works seamlessly with roaming between access points - new keys are generated upon user roaming or when a load-balancing operation is performed (i.e., when two access points mutually move a given user connection between them so as to allow better performance).

- Mutual authentication assures that rogue access points cannot capture user data, and encryption prevents a wireless node operating in promiscuous mode from seeing any user data in the clear.

- Kerberos can scale to support potentially very large networks, and the Kerberos server can be located anywhere in the network.

While the details can be complex, the structure of Kerberos is actually quite elegant and designed for general application in a (wired or wireless) network. As shown in Figure 1, the Kerberos "Key Distribution Center" (KDC) software runs on secure hardware. Suppose a roaming user wishes to access an application running on a server somewhere in the network. The user first establishes a secure connection with the Kerberos KDC. After exchanging authentication information, the user, if authorized, gets a "ticket" which grants access to the desired application.

Kerberos is thus particularly well suited to authentication, encryption, and key distribution on a WLAN. Note that it is also transparent with respect to both the lower-level features of 802.11, as well as other installation-specific techniques – like 802.1X and virtual private networks – that might be put in place at the discretion of specific organizations.

Future Directions

It's important to point out here that no matter how good a given authentication and encryption technique might be, hackers and crackers are getting smarter all the time. It's probably impossible to ever develop a security technology that could even be remotely described as impenetrable.

The goal, then, of any security philosophy is to make it at least extremely difficult for unauthorized individuals to obtain access to network resources and information. A Kerberos-based approach does exactly that, with an efficient, proven, standards-based implementation that supports roaming users while addressing all of the known security deficiencies in the current 802.11 standard.

And there is one other key benefit that we alluded to above. Kerberos is a proven technology that is also flexible and extensible to future developments in network security. The work now underway in IEEE 802.11 Task Group i, for example, will correct many of the known deficiencies in WEP. For example, future 802.11 security implementations will feature much stronger encryption, and support of multiple encryption techniques. But the 802.11i extensions to the standard, when approved, are expected to provide for an extensible framework, allowing a variety of techniques, including Kerberos, to be included with a specific security solution implemented at a given site.

As we noted at the beginning of this white paper, security should be of paramount concern to network managers and users alike. We believe that wireless LANs need be no less secure than their wired counterparts provided appropriate techniques are used to implement a flexible and transparent solution – and that's exactly what Compsee provides in our wireless LAN products.

Compsee is a leader in mobile data transaction systems, providing innovative wireless LAN solutions for data and voice, application-specific mobile computing, and bar code data capture. Compsee systems and products are used to increase productivity from the factory floor to the retail store, to the enterprise and out to the home.

Compsee provides a wireless local area network (LAN) solutions, featuring high-speed data communications for applications in industries ranging from education to manufacturing. Compsee wireless solutions support IEEE standards, and offer all the advantages of industry-leading intelligent network traffic management, fast wireless Internet access, worldwide roaming, powerful data security, large file transfer capabilities, and rugged equipment designed for combined voice/data communications in real time.

For further information contact:

Compsee, Inc.
International Sales Office
2500 Port Malabar Blvd. NE
Palm Bay, FL 32905

(800) 628-3888 (V)
(321) 724-4321 (V)
(321) 723-2895 (F)
sales@compsee.com

Corporate Headquarters
PO Box 1209
Mt. Gilead, NC 27306

Compsee

International Sales Office
2500 Port Malabar Blvd.
Palm Bay, FL 32905

(800) 628-3888 ● (321) 724-4321 – V ● (321) 723-2895 – F ● sales@compsee.com ● www.compsee.com