Table of Contents

Executive Summary .................................................................................................................................... 3
Threats to WLAN Environments ........................................................................................................... 3
Understanding Authentication and Access Control ................................................................................. 4
Dangers of Uncontrolled and Unauthenticated Access ........................................................................... 5
Standardized Attempts to Manage Authentication- and Access-Control-Based Dangers ......................... 6
Shortcomings of Standard Authentication and Access-Control Techniques ........................................... 6
Revised Standardized Approaches to Authentication ............................................................................... 6
Today's Real Solutions: Strong Authentication ....................................................................................... 8
Threats to Data Privacy and Integrity ..................................................................................................... 9
Standardized Attempts to Ensure Privacy .............................................................................................. 10
Revised Standardized Approaches for Protecting Confidentiality and Integrity ...................................... 11
Today's Real Solutions: Encryption ........................................................................................................ 12
Rogue Access Points .................................................................................................................................. 12
Shutting Down Rogue Access Points ..................................................................................................... 13
Denial of Service ........................................................................................................................................ 13
Today's Solutions: Denial of Service ........................................................................................................ 14
A Note About Residential WLANs for Enterprises ................................................................................. 14
General Lessons .......................................................................................................................................... 14
ActivCard Solutions for Secure WLANs ................................................................................................. 15
Additional Resources .............................................................................................................................. 17
Executive Summary

Wireless local area networks (WLANs) based on the Wi-Fi (wireless fidelity) standards are one of today’s fastest growing technologies in businesses, schools, and homes, for good reasons. They provide mobile access to the Internet and to enterprise networks so users can remain connected away from their desks. These networks can be up and running quickly when there is no available wired Ethernet infrastructure. They can be made to work with a minimum of effort without relying on specialized corporate installers.

Some of the business advantages of WLANs include:

- Mobile workers can be continuously connected to their crucial applications and data;
- New applications based on continuous mobile connectivity can be deployed;
- Intermittently mobile workers can be more productive if they have continuous access to email, instant messaging, and other applications;
- Impromptu interconnections among arbitrary numbers of participants become possible.

But having provided these attractive benefits, most existing WLANs have not effectively addressed security-related issues.

Threats to WLAN Environments

All computer networks, which by definition consist of autonomous computing nodes, are potentially subject to security problems. In the absence of central control of the sort offered by traditional mainframe computers, users with malicious intentions may be able to: undermine the confidentiality or integrity of your network-accessible data; use the capabilities of your networked components for illegal or unsavory purposes; or interfere with the legitimate activities of your network users. As the Internet and its protocols have come to dominate wide area connectivity, organizations wishing to secure their networks have established perimeter defenses—firewalls, VPNs, antivirus systems, and intrusion detection systems—to protect their networks, data, and applications from remote intruders and other threats.

The availability of inexpensive, easily installed WLAN equipment opens up new pathways for attacks and other security breaches. Unlike wired networks, where eavesdropping on network traffic will be apparent to watchful network administrators (unless the attacker has elaborate, military-grade detection equipment on site,) WLAN data streams can be passively observed using ordinary WLAN cards without being detected by administrators. Furthermore, the eavesdropper’s device may even be in the parking lot or on the sidewalk— unlike eavesdroppers on wired LANs, WLAN eavesdroppers need not be on site making an electrical connection to the network.

In fact, the spread of WLANs made possible a new sport known as “war driving”. War drivers have WLAN-equipped laptops, and sometimes, high gain antennas for the radio frequencies WLANs employ. In city after city, war drivers find they can connect to dozens or hundreds of WLANs, observe all the traffic on the network (which may include an entire corporate network), use the enterprise network’s Internet connection for any purpose (which may include anti-social activities such as broadcasting SPAM or releasing viruses), and damaging or defacing data and software on the exposed network. Wi-Fi WLANs have limited, though not entirely useless, security facilities. But war drivers consistently find that half or two-thirds of the networks they discover have all their security features disabled. One large retailer, which implemented its point-of-sale system on a WLAN without
enabling security features, found that conniving customers were changing the prices of items they purchased.

In addition, WLANs installed for the benefit of an organization’s internal users may not be protected by the network’s perimeter defense. Perimeter defenses focus on wide area connections, and assume that internal devices aren’t pathways for attacks and eavesdropping. Unprotected internal WLANs serve as a soft underbelly that is extremely vulnerable to attacks despite the careful deployment of security solutions at the perimeter. Since WLANs allow access from outside the physical security barriers of your office it is really a form of remote access to your network. Industry best practices for remote access include implementing strong 2-factor authentication.

This white paper describes the various security challenges for Wi-Fi wireless LANs, the attempts the industry has made to address those challenges, the shortcomings of those initial attempts, and the best possible practices, including ActivCard’s solutions, for organizations and residential users who want to take advantage of the real benefits of WLANs. ActivCard’s solutions integrate strong 2-factor authentication with standards-based WLAN security. ActivCard’s AAA Server is a full RADIUS and TACACS+ compliant AAA server that supports 802.1X authentication and also validates strong OTPs generated from ActivCard tokens, USB keys or smart card authentication devices. ActivCard provides solutions whether you choose to implement a VPN (Layer 3) or an 802.1X system (Layer 2) in order to provide the degree of authentication and access control your wireless network demands.

### Understanding Authentication and Access Control

Authentication is the foundation technology for protecting networks, servers, client systems, data, and applications from improper disclosure, tampering, destruction, and other forms of interference. The essence of an authentication system is discovering and confirming the identity of a person, an organization, a device, or more generally, of any software process on the network. In the non-digital world, we readily authenticate people we know personally by their appearance or the sound of their voice on the phone, and we authenticate people we don’t know personally by examining their documents, such as photo IDs. In the digital world, software processes exchange data at a sort of least common denominator level without these physical clues, and authenticating the identification of a person bound to a software process is a tricky problem.

Users can be authenticated by something they know, something they have, or something they are. The most common example of “something you know” is the traditional user ID and password combination. A common example of “something you have” is an access card that is swiped through a card reader. “Something you are” can be established with fingerprint readers, retinal scanners, facial recognition systems, and hand geometry analyzers.

Because all of these authentication techniques can be circumvented to one degree or another, many organizations that want higher levels of security combine two or more of these methods to create “two-factor” or “three-factor” authentication. For example, getting money from your ATM machine involves two-factor authentication that involves presenting your card—something you have—and entering a PIN—something you know.

Managing and deploying authentication will require you to commit resources, including management attention and employee training along with the monetary costs of the system. Important considerations that must be traded off include the protective strength of the solution, the up-front and ongoing costs of the components and system support, simplicity and transparency for users, and coverage for various operating systems and other infrastructural elements. A universally deployed public key infrastructure (PKI) can play a critical role in authentication for enterprises that are capable of making the necessary commitments of time, money, and effort. Specially chosen pairs of keys,
where one of the keys is kept secret and the other one is exposed publicly, can help provide strong authentication. However, the public key must be bound to an identity, usually either a person or an organization, or there is a potential for misuse. The most common form of this binding is via the issuance of digital certificates, which perform a function similar to that of a notary public. The administration of hierarchies of certificates can be time consuming.

Authentication provides a greater or lesser degree of assurance that users are who they say they are, but in itself it doesn’t control access to network resources. Access control is the job of authorization systems. Authorization can be thought of as a grid with each network resource along the x-axis and each user (or other entity) along the y-axis. At each intersecting cell, a list of privileges is created.

### Access Control Matrix

<table>
<thead>
<tr>
<th>Subject 1 (User A)</th>
<th>Object 1 (File X)</th>
<th>Object 2 (Printer Y)</th>
<th>Object 3 (Database Z)</th>
<th>Object 4 (Table T)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read only</td>
<td>Write only</td>
<td>Read and modify, but not create</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subject 2 (Application K, User L)</th>
<th>Object 1 (File X)</th>
<th>Object 2 (Printer Y)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read only</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subject 3 (Process G)</th>
<th>Object 1 (File X)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read and delete only</td>
<td></td>
</tr>
</tbody>
</table>

**Privileged Subjects.** Access control can be thought of as a matrix of subjects that have certain privileges with respect to various objects or resources.

Thus user Bob may be allowed to run and back up all the systems administration servers and applications, but blocked from reading personnel files and running the payroll application. Enterprise directories are the primary repositories of access control information, though it’s not uncommon for enterprises to have numerous standalone databases, Web applications, and security systems in addition to the directory or directories it has deployed.

### Dangers of Uncontrolled and Unauthenticated Access

Pretty much every potential security disaster can begin with failures of authentication and authorization. A wireless LAN installed by a naive user or even by an inexperienced network administrator may, for the sake of simplicity, refrain from forcing users to log in. Unauthenticated users may include: serious, money-motivated attackers or extortionists; vandals with time on their hands who treat unauthorized access as a sport; passers-by who would like to take advantage of free Internet access; spammers who are always seeking bogus source addresses for their material; fraud perpetrators; pornographers; and even, without stretching the point too far, terrorists.

Note that permitting unauthenticated and unauthorized users on the network opens up all these potential threats even if network traffic is encrypted and files and applications require authentication and authorization to be accessed. Of course, opening the entire network up to unauthorized users gives them opportunities to undermine the hitherto protected parts of the network. They can attack the encryption methods, run dictionary and brute-force attacks on passwords, and cast about for public or unprotected servers and clients where they can install Trojan Horse programs or so-called zombie software, even though the usual protections of wired networks remain intact, at least for a while.
Standardized Attempts to Manage Authentication- and Access-Control-Based Dangers

In order for wireless clients and access points to interchange data, they must be associated. The wireless nodes can only become associated once they are mutually authenticated. However, the standard default authentication method for 802.11 wireless networks, called open system authentication, performs authentication in name only—any node that requests authentication in an open system authentication environment will be authenticated. Obviously such a system can't provide a base for useful access control or authorization. As a security mechanism, open system authentication is, totally insecure. Open system authentication is, however, quite easy to use.

The 802.11 standard also provides for an alternative authentication method, known as shared key authentication. The standard 802.11 encryption method, known as Wireless Equivalent Privacy or WEP, uses 40-bit or 104-bit secret keys on access points and stations. Shared key authentication makes use of these shared secrets to implement a challenge and response exchange between potential authenticating stations and an access point.

Though it’s not part of the actual 802.11 standard, most access point vendors support another kind of access control by refusing to exchange data with stations whose MAC address is not on a list of welcome nodes. As with the other authentication and access control features of 802.11 networks, by default this feature is turned off, and only administrators who know about it in advance and want to employ it will be able to take advantage of it.

Shortcomings of Standard Authentication and Access-Control Techniques

We’ll put off the discussion of the shortcomings of WEP to the data privacy discussion later in this paper. But shared key authentication can’t be any stronger than the encryption algorithms underlying it. Furthermore, it’s considered poor security practice to employ the same keys for data encryption and authorization. One reason for this principle is that authentication can expose an algorithm’s shortcomings in a different fashion than ordinary data encryption does. For example, although shared authentication never passes keys in the clear, management frames aren’t encrypted, so information that can be captured from the authentication process may be useful in defeating encryption. In fact, there are specific attacks on WEP-based shared authentication. An attacker who manages to capture the management frames of a successful authentication session will have the raw material to authenticate repeatedly, even though he or she doesn’t actually capture the WEP key.

As mentioned earlier in this paper, there are numerous effective authentication systems with varying degrees of security assurance, including smart cards, cryptographic tokens, biometric readers, Kerberos, and others. However, none of these mechanisms is supported for 802.11 WLANs as they were initially deployed.

MAC address access control is very weak. Because WEP encryption protects only the data payload of each frame, MAC addresses are always in the clear. Anyone who can capture traffic—that is, anyone with a WLAN card-equipped PC and protocol analysis software—can simply read the
addresses that ostensibly serve as secret keys. In addition, practically all WLAN cards can have their MAC addresses changed via software. So attackers who have captured the MAC addresses can reset their network interfaces to a value that will give them full access. No decryption or brute force effort is required—this spoofing operation is practically foolproof.

A problem related to WEP keys is the difficulty of key management with 802.11 networks. There is no built-in mechanism for distributing keys to stations—they must be entered manually as a string of hexadecimal numbers or they can be derived from a password or other seed at the expense of some of the protective capabilities of the keys. In addition, sharing a single key among all users means that if a laptop or PDA that connects to the wireless network is lost or stolen, then all the users of that network must change their keys, the pain of which is multiplied by the need to do the job manually.

**Revised Standardized Approaches to Authentication**

There has been a substantial amount of effort by standards organizations since 1999 towards improving the authentication picture for WLANs. One important development was the IEEE’s approval of the 802.1X standard in June 2001. This standard extends authentication and authorization systems that already exist within the enterprise to the WLAN. It does this function by, in effect, establishing a temporary network that carries only 802.1X traffic, which consists primarily of authentication requests and responses. The access point, or a network access server connected directly to the access point, relays requests and responses between the client station and an authentication, authorization, and accounting server, typically implemented using RADIUS (Remote Dial-in User Service, originally designed to authenticate dial-up sessions over modems. Once the user has been authenticated over the dedicated, limited 802.1X link, then traffic can flow over the regular network. The beauty of the system is that the RADIUS server can be located anywhere that the wired network goes, but the connection to the authentication server is secure because any traffic other than 802.1X packets from the authenticating station (known as a “supplicant”), will be blocked. Furthermore, the access point, the access server, and other intervening devices (known as “authenticators”) need no knowledge of the details of the authentication operation—they simply relay requests and responses between the supplicant and the authentication server.

An 802.1X solution can be created with various types of key derivation systems used for authentication and encryption. The Extensible Authentication Protocol (EAP) is the foundation for 802.1X transactions. Some of these systems include Transport Layer Security (TLS, the successor to SSL or Secure Sockets Layer, the widely implemented protocol for authenticating Web transactions); MD5, a basic level challenge and response method that only authenticates in one direction; Tunneled TLS or TTLS, which performs TLS functions via an encrypted tunnel; and PEAP (Protected EAP), which operates much like TTLS. A proprietary Cisco version of EAP is LEAP (Lightweight EAP). LEAP has served as something of a stopgap for Cisco customers without PKI in place. It’s worth noting that a dictionary attack tool known as anwrap.pl is available from numerous Web sites, so if you must maintain a LEAP environment, use every effort to enforce the use of random-appearing passwords.
## Comparison: 802.1X Authentication Protocols

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>MD5</th>
<th>Cisco LEAP</th>
<th>EAP-TLS</th>
<th>PEAP and TTLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key length</td>
<td>None</td>
<td>128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Mutual authentication</td>
<td>No.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Authenticates user, but not authentication device</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall security</td>
<td>Weak</td>
<td>Stronger than MD5; weaker than other EAP solutions. Vulnerable to dictionary attack from “anwrap.pl”.</td>
<td>Strongest</td>
<td>Strong</td>
</tr>
<tr>
<td>Client software support</td>
<td>Native support in Windows XP. Other operating systems require client software.</td>
<td>Requires proprietary features in the NIC and AP. Wide range of operating-system support with Cisco 802.11 wireless card.</td>
<td>Native support available in Windows XP and Windows 2000. Other operating systems may require additional client software.</td>
<td>PEAP support available natively in Windows XP and Windows 2000. TTLS support available via third party software.</td>
</tr>
</tbody>
</table>

## Today's Real Solutions: Strong Authentication

Some enterprises want to offer free, unimpeded wireless Internet access to visiting customers and vendors. Thus, they use open system authentication and disable WEP on a wireless network accessible to these users. It’s critically important that such a network be connected to the enterprise network outside the firewall or in the DMZ, between a firewall that blocks all unrequested traffic and one that permits inbound traffic for Web servers and perhaps a few other sorts of outward facing server applications. Open wireless LANs outside the firewall are still subject to some of the problems listed earlier: your network will be implicated in the bad behavior of any unauthenticated user. But all things being equal, the internal network will be as secure from attacks over the WLAN as it is from Internet-based attacks.

The most direct way to extend the services of an outside-the-firewall WLAN to internal users is to employ a VPN. A VPN (Virtual Private Network) is an encrypted link into the internal network that runs over a public network, such as the open WLAN we have been describing. Accessing the VPN requires authentication, which can be gauged to the necessary degree of security. For non-critical facilities, a simple ID/password logon may be sufficient. Best practices for remote access security suggest deploying smart cards or tokens to raise the degree of protection. These techniques may be combined with biometric readers or other more esoteric systems for the most critical networks. Practically speaking, VPNs require software on the client and on a VPN server inside the network.

VPNs operate at Layer 3, the network layer of the ISO networking model, so a client needs an IP address and IP connectivity in order to log in to the network. An 802.1X system can kick off the authentication process without previously established IP connectivity. This capacity can also simplify deployment.
One of the advantages of an 802.1X authentication system compared to a VPN is that the wireless network need not be located outside the firewall. Because the access points won’t forward any data aside from the authentication process itself, there is next-to-no opportunity for wireless attackers to access the wired network, even if they can receive the wireless signals in the parking lot. However, this fact is not an argument for deploying wireless networks without solid encryption. Those parking lot intruders could still observe unencrypted wireless traffic and capture e-mail messages, passwords, and any other sensitive data that traverses the wireless network.

An 802.1X authentication system will sometimes be easier to deploy than a VPN if users sometimes need access at different sites. With VPNs, users may need different passwords or smart cards away from their home sites, while 802.1X and RADIUS can simplify multi-site logins.

**COMPARISON OF LINK LAYER (802.1X) AND NETWORK LAYER (VPN) PROTECTION**

<table>
<thead>
<tr>
<th></th>
<th>Link Layer (802.1X)</th>
<th>Network Layer (VPN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Services</td>
<td>Authenticates interface to the network. Normally based on user of the system.</td>
<td>Authenticates an IP address to the network. Normally based on user of the system.</td>
</tr>
<tr>
<td>Authentication Vulnerabilities</td>
<td>Dictionary, Man-in-the-middle, Replay</td>
<td>Dictionary</td>
</tr>
<tr>
<td>Data protection</td>
<td>PROTECTS ALL DATA FRAMES INTO AND OUT OF THE NIC.</td>
<td>Protects all IP datagrams based on the source or destination address.</td>
</tr>
<tr>
<td>Unprotected data</td>
<td>Management frames</td>
<td>Other IP addresses directed to NIC. Non-IP datagrams (e.g. ARP)</td>
</tr>
<tr>
<td>Scope of data protection</td>
<td>Link only</td>
<td>From system to gateway or endpoint</td>
</tr>
<tr>
<td>Interaction with other security layers</td>
<td>None</td>
<td>Potential problem if same layer (e.g. IPsec within IPsec)</td>
</tr>
<tr>
<td>Mobility Support</td>
<td>Re-authentication typically needed for each new link</td>
<td>Authentication stability across links and link state changes</td>
</tr>
<tr>
<td>Wireless System vulnerabilities</td>
<td>To other authenticated systems</td>
<td>To any other wireless system, authenticated or not</td>
</tr>
<tr>
<td>Provider Service theft</td>
<td>None practical</td>
<td>Authenticated system providing proxy services</td>
</tr>
<tr>
<td>Availability Now:</td>
<td>WPA</td>
<td>IPsec, L2TP, PPTP</td>
</tr>
</tbody>
</table>

For medium size and large enterprises deploying large scale WLANs, recent developments in hardware may be worth considering. So-called WLAN switches take many of the smarts out of access points, leaving them to handle only the basic physical layer functions. Authentication, encryption, and key management may be performed at the switch or passed along to the AAA server. WLAN switches are also useful for consolidating multiple access points, which can be tricky with standalone access points.

**Threats to Data Privacy and Integrity**

While failures of authentication and authorization can lead to dramatic and embarrassing outside attacks, failures of data privacy and integrity can be insidious. If the attacker is careful, you may not
notice that he or she is intercepting messages, capturing credit card or medical account data, or collecting information that could make it easy to access otherwise protected network components. Of course, data privacy and integrity failures can also be dramatic and embarrassing—for instance, when an attacker attempts to extort hundreds of thousands of dollars in exchange for not releasing your customers’ credit card information, or when a competitor gets a copy of an e-mailed proposal before it’s sent to a customer.

Because radio signals are useful for networking precisely because they radiate out from an antenna into the surrounding space, there is always a potential for data on the WLAN to be visible to a sufficiently sensitive receiver in an unexpected place outside the physical control of the network operators. Any data transiting the network—file transfers, mail, application transactions, Web browsing, instant messaging, music downloading, videoconferences, VoIP phone calls, and much more—is subject to being observed, copied, or conceivably, modified and re-injected onto the network.

**Standardized Attempts to Ensure Privacy**

The original privacy and integrity mechanism developed and deployed by the WLAN industry was WEP, for Wired Equivalent Privacy. The idea was that within the physically secure premises of an ordinary Ethernet network, most enterprises didn’t worry much about violations of data privacy and integrity. Thus the bar the industry set for itself wasn’t some kind of ideal hyper-security, but just a plain old wired network. You can’t walk through a building that has a wired Ethernet network with a laptop and an Ethernet card and capture all the data going by without physically connecting to the network. Physically connecting to the network would be visible to network administrators if they were paying attention, or if they had implemented a system of alarms when rogue nodes attached themselves to the network—not an especially difficult or uncommon thing to do. Except for the fact that an eavesdropper attempting to intercept Ethernet communications necessarily exposes his or her MAC address to the network and WLAN eavesdroppers don’t (as long as they don’t transmit), WLAN eavesdroppers have much the same access to network data as Ethernet eavesdroppers have.

However, the equivalence between WEP and wired networks breaks down quickly. WEP is primarily an encryption algorithm. When it is turned on, it encrypts the data payload of each frame that traverses the network. WEP also supports a form of data integrity checking by calculating a checksum for the encrypted data, appending the checksum to the data payload prior to the encryption operation. After the frame is received and decrypted, the checksum is recalculated and compared to the received checksum. If there is a match, the frame is accepted; if the checksums don’t match, the frame is rejected or otherwise flagged.

The first version of WEP used 40-bit shared secrets, partly because of the then-current export limits on strong encryption and partly to minimize the processing burden. The primary difference between WEP 1 and WEP 2 was the step up to 104-bit secret keys.
As processing power has gotten cheaper, breaking 40-bit keys by brute force has become nearly trivial. Pure 104-bit keys are still beyond the capabilities of brute force attacks. (The cryptographic strength of a key increases exponentially with the width of the key.)

**In Detail: Weaknesses of WEP Encryption**

RC4 security relies on using a different key for every encryption. The IV method of changing 24 bits of the key while leaving the other 40 or 104 bits constant means that keys will repeat after every 224 frames, that is, every 16,777,216 frames. It may take your home network a long time to see this much traffic, but a busy office or campus might wind up repeating IVs, and therefore repeating complete keys, every few hours. Furthermore, because of the “birthday paradox” (which demonstrates that the odds are better than even that two or more members of a random group of people will have the same birthday), there are better than even odds of an IV collision (that is, an instance of key re-use) after as few as 5,000 frames. By XOR-ing the two ciphertexts with the same key, you produce the XOR of the two corresponding plaintexts. If you can use pattern detection or otherwise guess one of the plaintexts, you can begin to create a decryption dictionary for every IV. Furthermore, the Integrity Check Value (ICV) will tell you whether your guesses are correct. Widely available tools, such as AirSnort automate this encryption breaking process. Once AirSnort has captured five or ten million frames, it can find the secret key in less than one second. WEPcrack is another publicly available key discovery tool.

If this situation weren’t bad enough, researchers Fluhrer, Martin, and Shamir published *Weaknesses in the Key Scheduling Algorithm of RC4*, which identifies a subset of especially weak keys in RC4. AirSnort and WEPcrack employ the discoveries in that article to improve their efficiency.

The main problem with WEP encryption is not that RC4 has shortcomings, but that WEP does a bad job of distributing keys to stations and access points. Because key distribution is out-of-band—that is, not performed over the WLAN—it’s difficult to change the keys, especially in a sizable organization with intermittently available users. In addition, features some vendors have added, such as deriving WEP secret keys from passwords, make it easier for attackers to recover the keys.

The ICV, the checksum intended to ensure the integrity of WEP-encrypted data, is even easier to defeat than WEP encryption. There are well known ways to manipulate checksums using the CRC32 method so that modified data can be compensated for, thus producing a bogus guarantee of the integrity of the ICV.

**Revised Standardized Approaches for Protecting Confidentiality and Integrity**

Wi-Fi Protected Access (WPA) is the Wi-Fi Alliance response to the shortcomings of earlier encryption, integrity, and authentication mechanisms. It is a subset of the forthcoming 802.11i wireless security standard. In fact, it makes up the parts of 802.11i that existing products will be able to upgrade to without replacing any hardware. The part of 802.11i that will only be possible with a hardware upgrade is the new Advanced Encryption Standard (AES) encryption algorithm.

On the shared key front, WPA embraces a dynamic key distribution protocol, the Temporal Key Integrity Protocol (TKIP). After 802.1X authentication is successfully concluded, the authentication server provides the user with a pair of unique session keys. These keys are employed to create a range of other keys that are used to protect various associations between authorization servers, access points, and stations. One of these types of derived keys, the temporal key, is combined with a 48-bit IV and used with the RC4 cipher to encrypt a frame.

TKIP also includes a new Message Integrity Code (MIC), which operates alongside the ICV but has a much higher degree of cryptographic strength. With its own 64-bit keys and a nonlinear algorithm, the
MIC provides much stronger assurances that data has not been modified. In fact, the MIC assures the integrity of frame headers as well as that of the payload.

Today's Real Solutions: Encryption

WPA-certified products are on the market now. In many cases, there are software and firmware upgrades for older network interface cards and access points. The issues related to authentication and authorization can be addressed to the required level of security you need by deploying 802.1X and one or more of the flavors of EAP. These authentication solutions support greatly enhanced systems for secure encryption and reliable integrity assurance, even though these systems wrap around the core RC4 cipher engine from the WEP days. It's worth noting that WEP and WPA systems can coexist in "mixed mode,” which is actually least-common-denominator mode—namely, WEP. Clearly it would not make sense to invest in an 802.1X infrastructure and upgraded access points and clients only to be held hostage to a non-upgraded part of the WLAN. The Wi-Fi Alliance claims that WPA addresses the encryption weaknesses of WEP-based products, and so far, there is little evidence to dispute these claims.

Rogue Access Points

There are two kinds of rogue access points worth noting. One is the employee-initiated internal kind. Employees who have WLANs at home decide they'd like to surf the Web from the lunch room, so they buy their own access point and plug it into an active Ethernet jack. Needless to say, this user won't be likely to turn on any sort of authentication or encryption. In spite of the probable innocence of these WLAN deployers, the danger is exactly the same as that of a purposely installed unencrypted, null-authenticated WLAN located inside the firewall.

The other sort of rogue access point is the external sort. It could be an inadvertent installation by another tenant in your building or someone in a neighboring building. One possibility in this situation is that the neighboring AP will associate with some of your users. In theory, someone on the neighboring network could capture such things as passwords and Web transactions from your users, but that prospect seems unlikely if the overlap of WLANs is accidental. More likely, your captured users will complain to the network manager because they lack expected access to the internal network’s servers and applications, and the problem can be solved.

The other external possibility is a true attacker who wants to capture your WLAN traffic in order to get some kind of confidential data. As with an inadvertent external rogue access point, users will soon observe odd behavior and ask the IT group for help. This sort of attacker would have to be extremely patient and stealthy to carry out such an attack for long, though they can do a lot of harm by simply collecting logon information from users as they attach to the network.

The primary danger of rogue access points appears when unencrypted and unauthenticated networks are installed inside the perimeter defenses. Such networks constitute about as severe a security breach as can be imagined, especially if their reception areas extend beyond the secure premises. In fact, open WLANs inside the firewall are subject to abuse by disgruntled, dishonest, or bored employees as well as by outsiders.
Shutting Down Rogue Access Points

Even WEP goes a long way toward preventing damage from external attackers installing rogue access points. Full WPA implementation on enterprise-configured client stations and access points will make it practically impossible for external attackers using unauthorized access points to capture data. The potential harm an open internal unauthorized access point could cause can’t be mitigated much by WEP or WPA because the worst vulnerability is to the wired part of the network, which hardly anyone ever encrypts.

In order to eliminate the gross risks of unauthorized internal access points, you need an auditing tool that can detect the devices and track them down. The most basic form these tools take is that of a wireless-capable protocol analyzer available as software or as handheld devices with useful features for finding rogues. There are many options available on the market. A free downloadable program for finding rogue access points is Network Stumbler. Some of these tools integrate with a GPS to pinpoint the physical location of identified access points. The problem is that there’s no substitute for walking around with your laptop or handheld auditing tool for anyone with more than a few hundred square feet of space in their facility. And you can’t just walk around once—you have to do it regularly.

Some vendors have come up with products designed to be installed permanently and watch for rogue access points and prevent authentication outside an administrator-defined boundary. These products may be able to limit the amount of walking around required to be sure there are no holes created by rogue WLANs.

Denial of Service

Denial of service (DoS) attacks are possible on any kind of network, not just WLANs. In their least sophisticated form, they consist of blasting traffic at a target network or component until the link is so full of traffic that no more can be accepted or until a server or other resource becomes overloaded and refuses additional data. Some attackers manage to take over hundreds or thousands of devices on unprotected networks and use these “zombie” nodes to focus spurious traffic on a target. WLANs could be attacked this way just as any other network could.

However, WLANs have some DoS vulnerabilities that they don’t share with other networks. The most brute-force DoS attack is an attack on WLAN radios. 802.11 networks operate on unlicensed Industrial, Scientific, and Medical (ISM) bands at 2.4GHz and 5.8GHz. The unlicensed bit is crucial to the cheapness and easy setup of WLAN equipment. The 2.4GHz band in particular must support a large number of other radio applications, including cordless phones, microwave ovens, Bluetooth devices, burglar alarms, RFIDs, and others. All of these devices, including WLAN components, are required to limit their power output in the interest of peaceful coexistence. However, it’s still possible for these devices to interfere with one another.

WLANs are also vulnerable to more targeted and stealthy DoS attacks such as:

- Simulated out-of-sequence frames may result in terminating all current connections and limiting re-attachment;
- Spoofed EAP logoff frames can be employed to terminate connections;
- Nodes configured to have more than their fair share of access time can prevent other nodes from accessing the network;
- Spoofed control frames can interfere with power-saving sleep mode to interrupt connections.
Today's Solutions: Denial of Service

As with wired networks, tracking down WLAN DoS attacks can be difficult, slow, and inefficient. Radio jamming can be tracked down fairly easily with the handheld or laptop tools used for detecting rogue access points, and some of the permanently placed detection systems will also be useful to track these problems down. Most of the other attacks can only be unmasked by careful monitoring and analysis with a protocol analyzer. Some of these vulnerabilities could be mitigated with changes to the standards, but none of them are on a standards track for now.

A Note About Residential WLANs for Enterprises

Enterprises don’t care much whether their employees have secure WLANs at home, unless the employees have access to the enterprise network. Then the issue of security at home becomes an extension of the enterprise issue. Even employees connecting through VPNs can’t be considered secure if there is a WLAN connecting the employee’s laptop to a cable modem or DSL line. A competitor or attacker parked on the street or located on another floor of the building may be able to capture the VPN login or other enterprise data. Preventing employees from creating home networks is probably unrealistic. Convincing them that the data they can access on the enterprise network must be protected is a good first step. Educating them on the types of attack they may encounter can help encourage them to at least turn on the security features of their WLANs.

General Lessons

WLANs should only be deployed with full awareness of the potential security breaches they can introduce. In fact, an enterprise’s security policy should define: who is allowed to use WLANs; who is permitted to install and configure WLANs; what standards of authentication, access control, encryption, and integrity assurance must be met in varying types of facilities; what current and future features must be available in wireless products that will be deployed; how unauthorized access points will be discovered and corrected; and numerous other wireless-oriented issues. If you don’t have a written, up-to-date security policy, putting one together ought to be your highest priority.

If there are unprotected WLANs connected to an enterprise network, it’s crucial that these WLANs be located outside the firewall and other perimeter defenses. Wherever WLANs are attached to the enterprise network, it’s crucial to install and maintain a secure authentication system that is commensurate with the security risks the enterprise faces. In addition, it’s crucial to find and secure any unauthorized access points. In most cases, enterprises will want to update their existing access point firmware and software, client driver software, and authentication servers to the WPA standards, and only purchase WPA-compliant products going forward. These steps will go a long way towards ensuring that you don’t sacrifice essential security in order to reap the benefits of WLANs.
ActivCard Solutions for Secure WLANs

When you move to deploy a secure WLAN, or to enhance the security of an existing one, the most important components you’ll need aside from the wireless access points and client interface cards is the authentication and authorization system. ActivCard is a premier provider of these solutions, whatever your environment may be and whatever degree of security you require.

ActivCard provides many standards-based solutions to help secure WLANs depending on the level of security you are looking for and on your specific network configuration. ActivCard is the only strong authentication vendor in the market to offer an integrated 802.1X compliant RADIUS server combined with a One-Time Password (OTP) validation server that allows you to create a simple, integrated, single server solution. ActivCard AAA Server is a full RADIUS and TACACS+ compliant AAA server that supports 802.1X and also validates strong OTPs generated from ActivCard tokens, USB keys or smart card authentication devices. For enterprises that want to protect their WLAN and require 2-factor authentication for remote access, ActivCard provides the easiest-to-deploy and lowest total cost alternative on the market.

ActivCard supports environments where you may want to mix and match your security solution depending on user population. For example, R&D employees may have a PKI Certificate Authority deployed. They may be required to use a PKI certificate on a smart card for 2-factor authentication and EAP-TLS for Layer 2 (Link Layer) protection. A contractor, who may have only limited access rights to the network, may best be protected by a simple username/password and a PEAP 802.1X connection may be appropriate. However, a mobile professional who needs to get e-mail access from the local coffee shop may require a VPN solution with a OTP token.

ActivCard AAA Server manages authentication requests and administers authorization policies across enterprise networks. User identities can be verified via static password, synchronous, or challenge/response authentication. Unlike other strong authentication providers, ActivCard AAA Server’s standards-based server platform meets enterprise-specific needs by leveraging the enterprise’s existing LDAP directory structures as well as integrating 802.1X authentication to protect...
WLANs. ActivCard AAA Server runs on Windows or Solaris platforms and provides a much lower total cost of ownership than the competition.

**Features**

**Integrated 802.1X Authentication** - Enables centralized authentication for all WLAN connections based on Wi-Fi Alliance-approved Wireless Protected Access (WPA) standards. Integrating 802.1x authentication and 2-factor authentication management into a single server saves time and money. Supports EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC. Supports Microsoft and Cisco clients.

**LDAP User Management** - Enables centralized management of users in a single LDAP directory and assignment of authentication devices via directory server or ActivCard AAA Server console.

**Integrated in existing infrastructure** - Uses standard best of breed solutions such as RADIUS, TACACS+, 802.1X (WPA) and ODBC, which allow quick and powerful interoperability with existing network infrastructure.

**Device Independence and Manageability** - Supports multiple authentication devices including keypad tokens, soft tokens, USB keys, and smart cards.

**Scalable for Large User Base** - Provides secure simultaneous remote access to multiple servers distributed across large-scale enterprises.

**High-Availability & Roaming** - Provides 24/7/365 uptime and multi-site authentication with advanced roaming credentials system.

**Benefits**

**Compelling ROI** - Eliminates the need to manage yet another static password that changes every 30 days. A lower total cost of ownership is achieved even if competitive token technology is already in place. ActivCard devices come with perpetual licenses that do not expire. Lower administrative costs for secure WLAN with a single server solution instead of supporting both an EAP compliant RADIUS server and a token management server.

**Smooth Bridge and Migration** - The ActivCard solution supports all current and future authentication needs. It allows enterprises to deploy a mixed environment of static passwords, tokens, USB keys, and smart cards. You can easily deploy both OTP and PKI authentication as well as migrate smoothly from competitive token deployments already in place.

**Familiar and Easy to Use** - ActivCard simplifies the user experience by using the universally accepted PIN entry method. PIN entry consolidates multiple authentication credentials on a single smart card device and allows the user to manage it without administrative involvement.

**Enhanced Security** – ActivCard allows local initialization of 2-factor authentication devices, ensuring that no one else has the ability to discover what secret keys are deployed. PIN numbers are validated on the user’s device and are not sent over the network. When deploying smart card devices, all private keys are generated and stored on the smart card providing strong storage and protection from hackers.

**Easy Implementation and Administration** – The ActivCard solution supports LDAP directories and SQL compatible databases, therefore requiring no proprietary database. The ActivCard AAA Server is designed for easy installation and deployment.
Additional Resources

The Unofficial 802.11 Security Web Page
http://www.drizzle.com/~aboba/IEEE/ In-depth explanations of 802.1X, EAP, and RADIUS, with many links to original sources.

Security of the WEP algorithm

802.11 Security Vulnerabilities
http://www.cs.umd.edu/~waa/wireless.html A comprehensive list of original documents about 802.11 vulnerabilities.

Authentication and Authorization: The Big Picture with IEEE 802.1X

Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks
http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf The official discussion of how WPA overcomes the problems with WEP.
Legal Information and Notice

ActivCard Intellectual Property: This document or deliverable(s) contain proprietary information of ActivCard Corp. and/or its subsidiaries and affiliates (collectively, “ActivCard”) embodying confidential information, ideas, and expressions, no part of which may be reproduced or transmitted in any form or by any means, electronic, mechanical, or otherwise, without prior written permission from ActivCard. This document may not be modified, copied, distributed, transmitted, displayed, performed, reproduced, published, licensed, derivative works created therefrom, transferred, or sold unless expressly agreed by ActivCard. The furnishing of this document does not imply or expressly provide a license to any of ActivCard’s intellectual property.

Copyright Notice: Copyright © 2004 ActivCard, Inc., 6623 Dumbarton Circle, Fremont, California 94555 USA. All rights reserved. This document and ActivCard software products are protected by United States copyright laws and international treaty provisions.

Trademarks: ActivCard, ActivCard (logo), ActivCard Identity Management System (AIMS), ActivCoupler, ActivEngine, ActivKernel, ActivKey, ActivLoader, ActivPack, ActivCardOne, ActivReader, BioMouse, Corporate Wallet, Corporate Access Card, Gold, mID, Return on Identity, Trinity and/or other ActivCard products or marks referenced herein are either registered trademarks or trademarks of ActivCard in the United States and/or other countries. The absence of a mark, product, service name or logo from this list does not constitute a waiver of ActivCard’s trademark or other intellectual property rights concerning that name or logo. The names of actual companies, trademarks, tradenames, service marks, images and/or products mentioned herein may be the trademarks of their respective owners. Any rights not expressly granted herein are reserved.

Patents: ActivCard may have patents, pending patent applications, and/or other intellectual property rights covering subject matter contained in this document or deliverable(s).

Export Control: ActivCard products, programs, or services referenced in this publication may not be available in all countries in which ActivCard operates due to export restrictions or changes in market conditions. Recipient agrees to comply fully with all relevant export laws and regulations, including but not limited to the U.S. Export Administration Regulations (collectively, “Export Controls”). Without limiting the generality of the foregoing, Recipient expressly agrees that it shall not, and shall cause its representatives to agree not to, export, directly or indirectly, re-export, divert, or transfer the software, programs, documentation, materials, specifications or any direct product thereof to any destination, company or person restricted or prohibited by Export Controls. In the event that Recipient provides the software, programs, documentation, materials, specifications or any direct product thereof to a third party located in any destination outside the country of delivery by ActivCard, Recipient shall ensure that it enters into a written agreement with such third party that protects ActivCard's rights and interests to the same extent protected hereunder and specifies ActivCard as a third party beneficiary. Recipient agrees to provide a copy of such agreement to ActivCard at ActivCard's request and to assist ActivCard, at Recipient's expense, in enforcing ActivCard's rights if ActivCard is not recognized as a third party beneficiary in the applicable jurisdiction.

Disclaimer: This publication is intended for informational purposes only. ActivCard makes no warranties, express or implied in this document. Furthermore, the information contained in this document has not been submitted to any formal testing and is distributed ‘AS IS’. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the recipient’s ability to evaluate and integrate them into an operational environment. While each item may have been reviewed by ActivCard for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Attempts to adapt these techniques to any environment are done so at their own risk. Information in this publication was developed in conjunction with the use of the hardware, software, and networking arrangements specified and is thus limited in application to those specific hardware and software products and levels. The information contained herein is not intended as a specification of any programming interfaces that are provided by ActivCard. This document is subject to change without notice and does not represent a commitment on the part of ActivCard. This document may contain information about product functionality not available in your product release.