

University of Michigan

NETWORK WORKING GROUP

Recommendation for Wireless Network Security
At the University of Michigan

CONTENTS

ABSTRACT.....3
WEB BROWSER ACCESS CAPABILITIES AND LIMITATIONS.....4
VIRTUAL PRIVATE NETWORK CAPABILITIES AND LIMITATIONS.....5
WEB BROWSER ACCESS TECHNICAL DESCRIPTION7
VIRTUAL PRIVATE NETWORK TECHNICAL DESCRIPTION10
WIRELESS SECURITY - CURRENT STATE AND FUTURE DIRECTIONS13
APPENDIX – SUMMARY OF UM WIRELESS INSTALLATIONS.....18

ABSTRACT

The Network Working Group proposes a solution for wireless network security consisting of a core authentication system with access-control devices to enforce security policies. We propose two configurations for the access-control devices: as wireless gateways for access via web browsers or as Virtual Private Network (VPN) servers. These two configurations will allow units to optimize their wireless networks to emphasize either very high levels of security (VPN access) or very low barriers to usability (web browser access). Both of these configurations are in service at other institutions of higher education, with no clear consensus favoring one or the other. Users will be able to move from one environment to another, but not completely transparently. Both configurations may be extended to include portions of the wired network, such as publicly accessible network jacks.

VPN access is designed to enforce a policy that all users must use strong encryption to guarantee the highest level of security. All types of network activity would be protected. Users must install compatible client software on their computers: software bundled by manufacturers may not work. Personal Desktop Assistants (PDAs) and other devices may be more problematic with this method.

Authenticated browser access permits VPNs but does not require them. It offers “quick start” access via a web browser to common applications such as email, class web pages, and web research; but several other network activities must be forbidden in the less secure quick start mode. Web browsers are ubiquitous on users’ computers, and PDAs and other wireless devices probably will work.

Standards and technologies to help resolve the security vs. usability conundrum are emerging. Therefore we recommend that our proposals be frequently re-evaluated; perhaps annually, but certainly prior to any future large-scale wireless network installation.

The authentication architecture for both types of devices requires a University of Michigan account for everything but the most restricted access to the wireless network: but visiting scholars and lecturers, corporate visitors, conference attendees and others will be among those for whom the wireless network will be most useful. We therefore strongly recommend that procedures be established to permit the easy creation of temporary accounts for short-term guests who can legitimately be allowed to use University resources.

The next part of this report discusses the two configurations in terms of their capabilities and the compromises each entails: it is intended for decision makers in units contemplating wireless network installations. A detailed technical description of each recommendation follows. Last is a discussion of the emerging standards that we think could eventually lead to a satisfactory campus-wide wireless security solution.

WEB BROWSER ACCESS CAPABILITIES AND LIMITATIONS

Web browsers are ubiquitous on laptop computers: they are also provided on PDAs and other devices. To gain access to the wireless network users merely launch a browser, and select the access type from a page that is presented to them automatically. Wireless gateway devices are used for authentication and filtering.

The advantage to this method is that it ensures that users can get adequate network access quickly and easily. Because it uses familiar mechanisms it should generate a minimal user support requirement. In developing this configuration as an alternative to the highly secure VPN method we considered a scenario in which a large wireless network was installed during the summer, a likely event given the cycle of the academic year. Students coming to campus in the fall would be motivated to "try out" the new facility. Even if these students experienced only minor difficulties, the sheer volume of calls could quickly overwhelm support facilities, such as 4-HELP.

We are unable accurately to assess the likelihood of the above scenario. The College of Engineering deployed VPN access in November 2002 and they report few difficulties, but their population may not be representative of the larger University community. An investigation by Medical Center Information Technology concluded that VPNs would impose an unacceptable support burden. We suggest that web browser access could be considered for large early installations to serve a technically heterogeneous population, where a positive initial user experience is an important criterion.

With the web browser access method the range of services and capabilities offered must necessarily be limited to reduce risks, because of the inherent insecurity of this method. Nevertheless we believe that this offering would be satisfactory for the initial experience of most people and would be likely to remain so for the continuing daily needs of many. All users would have the option to install additional software for secure access gradually as their own knowledge and requirements increased.

Both authenticated and unauthenticated access would be offered:

Unauthenticated access would not require an account to gain access to the wireless network. Capabilities offered would be similar to authenticated access except that the Internet would not be available. University of Michigan web servers would be accessible. This access type might be useful to prospective students and their families visiting the campus; members of the general public come to campus to take advantage of publicly available resources; and members of the University community wanting the quickest possible access.

Unauthenticated access to the Internet is denied for two reasons. The first is that the University is charged for Internet access by traffic volume. The second is that under the terms of our agreement with MERIT we are obliged to be able to identify all users of our Internet connections.

Authenticated access would require users to provide a University of Michigan username and password, which would be encrypted and secure from eavesdropping. All other traffic would not be encrypted. To ensure that University accounts would not subsequently be compromised by this lack of encryption protocols that transmit passwords in clear text would not be permitted.

Although the rudimentary encryption currently available in the wireless access points could conceivably be used, we recommend against this. The encryption keys used would be so widely shared and so difficult to change among the entire University community that the encryption would offer no security at all; on the contrary it might instill a false sense of security in users. This approach (no encryption) is currently adopted by the School of Information.

Most University of Michigan web services could be made available over an unencrypted connection without incurring serious risks, as could fully encrypted services such as mail.umich.edu or Wolverine Access. We recommend taking an exclusive rather than inclusive approach: making a set of known “safe” services available initially and allowing other service providers to “opt in” according to their own risk assessments.

Blocking of protocols that use clear text passwords would not be a significant detriment to the utility of the wireless network when accessed via a web browser, since alternatives using encryption are readily available and are distributed on the campus “Blue Disk”. Access to campus Microsoft Windows networks is more problematic. Early Windows systems, such as NT3 and Windows 95, use clear text passwords: unfortunately these early authentication methods remain imbedded in the protocols currently used by Windows and are difficult explicitly to filter out. The College of LS&A is blocking this type of insecure authentication *at its servers* and they report no difficulties for their users. We strongly recommend that other Windows providers should be consulted, and until then we recommend that the Windows protocol suite should be blocked over the unencrypted wireless network. Windows users would have the option to use a VPN for secure access to their networks, after they had authenticated with their web browsers.

The wireless gateway devices used for web browser access have the capability also to provide VPN access, which could be implemented as part of the initial deployment or later. Care should be taken that the VPN method chosen will be compatible with other units offering or requiring VPNs. An attractive alternative might be for a unit requiring VPNs to provide that service to the rest of the campus under the aegis of the IT Commons. How much of a burden this might entail is not clear, since we really do not know how people will use a wireless network and what tradeoffs of security for convenience they will consider acceptable. If a variety of wireless security options is available on campus usage statistics might enable us better to know people’s requirements and to tailor future network architectures appropriately.

VIRTUAL PRIVATE NETWORK CAPABILITIES AND LIMITATIONS

Virtual Private Networks were developed to allow secure transmission of data from an insecure network to a secure network. When the weaknesses of wireless network security became apparent this mature technology was easily adapted to solve the problem. VPN servers are used for authentication and encryption. The method discussed in this report is designed to support a unit policy mandating the strongest security for all wireless connections.

The advantage to this method is that it offers the best possible security available for wireless networking. By requiring a VPN, users do not particularly need to be aware of the risk or restrict the types of activities they use the wireless network for. We considered the historical difficulties of educating people in good security procedures, and the possibility that users, judging their own risk to

be minimal, would inadvertently expose other parts of the network to damage through careless practices. With the VPN access method the physical security provided on the wired portion of the network is not compromised in any way by the wireless access link.

Conventional wisdom has been that end user support for VPNs is difficult but this is arguably less true today as the technology has matured. The College of Engineering has been using this model since November 02 to provide wireless access throughout the Media Union, Lurie Engineering center and a number of hotspots across the College.

We suggest that VPN wireless access should be considered by units with a concern for data security and who are confident of their ability to meet the support requirements of their user population. VPN client software for given VPN servers is available for all computer and operating systems commonly found on campus, but not all available VPN client software will work with a given VPN server. Clear instructions on which client software to install and where it may be found should be provided. The College of Engineering has built a support web site devoted to wireless networks that can be access both from the wired and wireless networks.

To provide flexibility and access for the wide range of users and guests a number of access levels has been identified:

Encrypted Access for U of M Students, Faculty and Staff:

All students, faculty, and staff will be required to encrypt their traffic on the wireless network by use of a VPN client on their computers. When users would connect to the wireless network they would get a private IP address on a network that contains a web server. Upon opening a web browser they would be directed to a web site that maintains information for the wireless network. This web site would provide detailed information to access the wireless network and also act as a single point of information for campus happenings on the wireless network. Users would be able to download and install pre-configured VPN client software by using their unqiename and password. Once the client has been installed users would simply start the client to connect to the VPN server and authenticate with their unqiename and password.

Unauthenticated Access

A web proxy server would provide very limited unauthenticated access. Users who do not use a VPN client would only be able to access selected web pages indirectly through the proxy server. No other types of network activity would be possible. This access type might be useful to prospective students and their families visiting the campus; members of the general public come to campus to take advantage of publicly available resources; and members of the University community wanting the quickest possible access to general University information.

Authenticated Guest Access

Allowing guests access to the wireless network is a critical step to providing a favorable first impression of the University. To require guests to install software or configure a VPN client on their machine would be impractical; instead short-term guests would use a temporary unqiename and

password to access the network through a wireless gateway device similar to that used for web browser access. Corporate guests and others who need to connect to off-campus VPNs could do so through the gateway. Access would be granted to the Internet and to selected University resources. To enforce the mandatory VPN policy, the authentication mechanism for the wireless gateway would not allow U of M students, faculty, and staff to access the network this way.

VPN Pass-through Access for UM Users

Currently a number of members of the University of Michigan community use VPN access to corporate networks. In the future some University units (MAIS, perhaps) may require the use of VPNs to access particularly sensitive resources. VPN technology does not permit a VPN tunnel within another VPN tunnel, so a separate mechanism is required for University users who need a VPN that does not terminate at the wireless VPN servers. A wireless gateway device would permit U of M users to authenticate to the wireless network. A firewall (possibly incorporated into the gateway) would permit only VPN protocols, enforcing the mandatory VPN policy.

WEB BROWSER ACCESS TECHNICAL DESCRIPTION

From the user perspective a web browser is used to authenticate and gain access to the wireless network. The view from the network is that the wireless gateway is the multi-function box that controls access. This one box contains:

Firewall	Blocks or permits traffic from each user based on their role
Redirection	Monitors web traffic from unregistered users and redirects them to the gateway's server
Web Server	Presents user with login web page
Authentication	Authenticates using servers such as Active Directory, LDAP or RADIUS
Role Based Access Control	Registered users are assigned a role. Roles can control access based on IP address, network, protocol, time and location.
QOS Server	Bandwidth per user can be limited by role.
VPN Server	A Virtual Private Network protects the privacy of all traffic from a user with encryption.

The proposed configuration would be a single system providing three options for a client to authenticate and select encryption (refer to the figure on page 9):

Option 1: Unauthenticated Guest

Anyone on campus can use this option – no association with U-M is needed. From a web browser on the login page the user enters an e-mail address. The gateway assigns the user the role of ‘guest’, which only permits access to a limited number of Umich web servers. Since they cannot connect to the Internet, no direct costs are associated with their traffic.

This option has PR value as visitors can gather information about campus. A student could use this option to read e-mail by connecting to a secure web server such as mail.umich.edu. This option does not encrypt the data connection and it blocks the use of protocols that present a known security risk.

Option 2: No VPN

This option requires a Kerberos identity. From a web browser on the login page the user enters a username and password. This option does not encrypt the data connection (only the web authentication is encrypted). Since the connection is not encrypted, this option also blocks protocols that present a known security risk. Users can connect to the Internet. If the user runs a VPN connecting to some other VPN server they can run any protocols through the VPN tunnel. This would permit visitors to get a temporary Kerberos identity and connect to a VPN server at their home institutions.

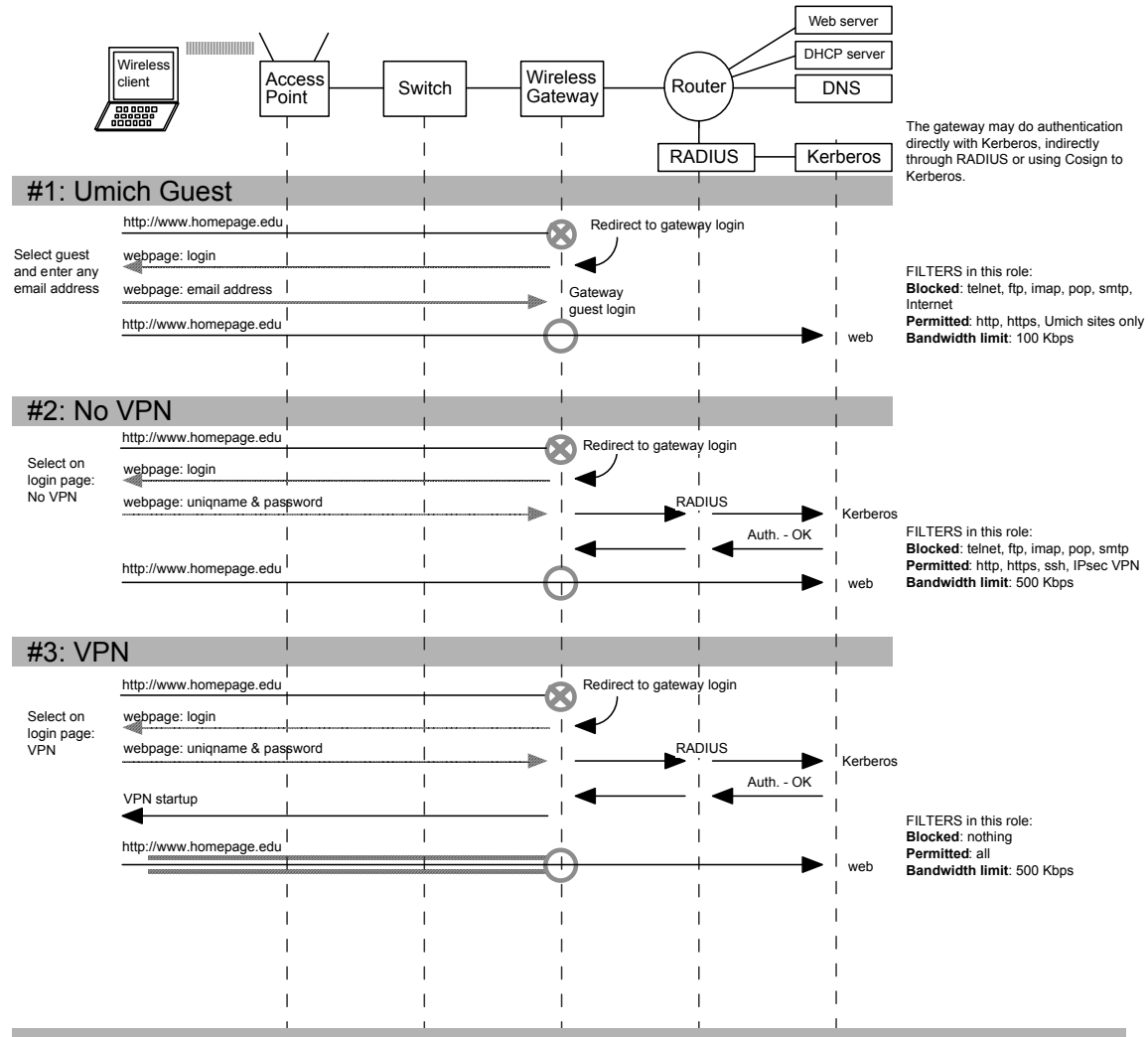
Option 3: VPN

After a web authentication this option encrypts the data connection with a VPN. This option requires a Kerberos identity and the user will need to have the VPN client software. Users can connect to the Internet and are permitted to use any protocol.

Wireless LAN Security Authentication and Encryption Using Wireless Gateway and VPN

Goal: Authenticated wireless LANs with encryption to protect sensitive information.
Avoid using mandatory VPN because of cost, support overhead and interference with connecting to other VPN server (departmental, corporate, MAIS).

This diagram is of a single system providing three options for a client to authenticate and select encryption. All clients use a web browser with SSL to authenticate. Options 2 and 3 require a Kerberos identity, either as a registered visitor (temporary Kerberos ID) or as a normal faculty-staff-student.
#1: Umich Guest • Anyone present on campus can use this option. It allows visitors to connect to Umich websites but since they cannot connect to the Internet there are no direct costs associated with their traffic. This option does not encrypt the data connection.
#2: No VPN • This option does not encrypt the data connection (only the web authentication is encrypted). Since the connection is not encrypted, protocols that present a security risk are blocked by filters. If the client runs a VPN connecting to some other VPN server they can run any protocols.
#3: VPN • After web authentication this option encrypts the data connection with a VPN. The wireless client will need to have VPN client software.



KEY

- Browser SSL encryption (dashed line with arrow)
- VPN tunnel encryption (thick solid line)
- Filter for unregistered user: DNS only (circle with X)
- Filter for registered user: Selective based on role (circle with dot)

GLOSSARY

- SSL** - Secure Sockets Layer, a protocol for encryption built-in to all web browsers.
- VPN** - Virtual Private Network, an encrypted connection from a client to the VPN server. All applications on a client can use the VPN to protect the privacy of their traffic.

VIRTUAL PRIVATE NETWORK TECHNICAL DESCRIPTION

Overview

Virtual Private Networks (VPNs) were first used to provide secure data transmissions through an insecure network to a secure network. For the purpose of this discussion insecure networks are those in which you don't necessarily know who is on them, or how the networks are put together. The Internet for instance is an insecure network because you don't know the route your data traffic takes before reaching its destination. Wireless falls into this category because of its broadcast nature. Wireless is based on transmission of data over a radio frequency (RF) spectrum. Those same transmissions are heard by others using the same spectrum with up to 500ft. of your location. This combined with the general "clear text" or unencrypted nature of most network applications makes wireless a very insecure environment.

VPNs can solve this insecurity issue by forcing all traffic from your machine to be encrypted while traveling over the wireless network. VPNs work by building a secure tunnel between your machine (the client) and a termination device (the server) elsewhere on the network. The server is responsible for decrypting your traffic and sending it out onto the secured network. The session created by the VPN is called a tunnel, because traffic between you and the VPN server can only be read by the two stations. Others on the network still see the encrypted traffic, but it is not readable by their machines.

In the early days of VPNs, they were very difficult to configure and could only be used to set up very static, manually configured tunnels. Since the advent of the mobile telecommuter uses for VPNs have expanded to allow for remote secure access on a dynamic basis. This has greatly improved the usability and the feature set of VPNs.

Technical Details (refer to the figure on page 12)

Three main flavors of VPNs have developed over the last five years. Two were originally developed by Microsoft for building secure connections between their products. These are Point to Point Transfer Protocol (PPTP) and Layer 2 Transfer Protocol (L2TP). The third and most commonly used VPN standard is called IPsec, and has been around for over 10 years. Recently PPTP has been added to the base load for Apple computers in addition to most Microsoft Windows platforms. Both of these protocols are very basic VPN systems with very limited feature sets. While they are limited in what they can do from an encryption standpoint, they would provide the level of security that is needed for access, and they come standard on most laptop computers. Both of these protocols have one major problem however; they can't be used to authenticate against Kerberos user databases. The University uses Kerberos as a password authentication mechanism for most systems and thus stops us from being able to use PPTP and L2TP as encryption mechanisms.

IPsec is a networking standard, however the way it was written makes it more useful as a guideline than a standard. IPsec has optional parts to the standard that some vendors implement and others do not. This requires an examination of clients supported by the VPN server in a large scale deployment. Most VPN servers don't support clients from every vendor, and to make use of

advanced features in the VPN you have to be using a client and server manufactured by the same company.

How IPSec works

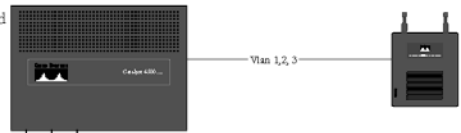
A remote user IPSEC connection is initiated by the client machine either at boot or by starting an application. The client and server then exchange identification to verify who they are. This is done by one of two methods: Pre-shared Keys or Digital Certificates. Digital Certificates are the most secure means but implementation them on a campus basis is not practical at this time. Pre-shared keys are just passwords the server and client exchange to get their connection established. Once the keys are exchanged, a uniquely encrypted connection is established allowing the user to enter their username and password. Once the user's credentials are accepted traffic can begin to be exchanged between the server and client. Encryption Keys are automatically changed at set intervals to insure that they cannot be broken.

While IPSec provides the structure for this mechanism, the actual encryption algorithms can vary with the VPN server. Very common today are DES and 3DES, which have been long standing encryption algorithms that have proved almost impossible to break. Emerging is a new encryption standard called AES that promises to be equally secure but requires a lot less work from computers to encrypt/decrypt the traffic.

VPN Wireless Access Model

Generic Wireless Infrastructure

Requirements Access Points have to support VLANS
 Need switches capable of Vlans
 A&A servers are centralized
 VPN Servers and Gateways are Centralized

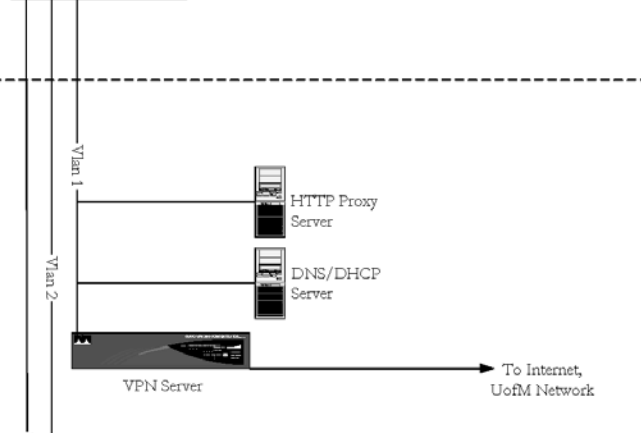


U of M Students, Faculty and Staff

Wireless Setup Vlan 1--General-USE
 SSID = UofM Wireless
 SSID Broadcast = YES
 Private Network= YES

Authentication Radius Server w/Uniquename
 and Passwords

Authorization Radius Server, all UofM Student,
 Faculty and Staff

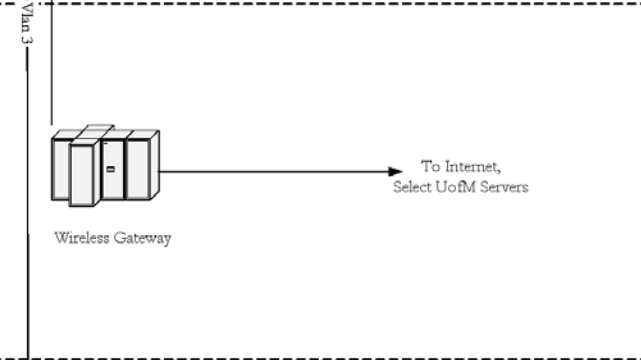


Authenticated Guests

Wireless Setup Vlan 2--Guest-Wireless
 SSID = UofM Guest Wireless
 SSID Broadcast = NO
 Private Network= NO

Authentication Radius Server w/Uniquename
 and Passwords

Authorization Radius Server, Only Guest User
 accounts are allowed

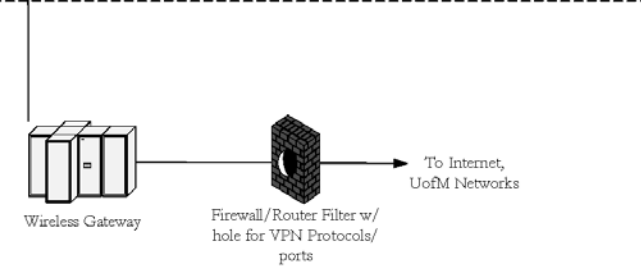


VPN Pass-through Access

Wireless Setup Vlan 3--VPN-Wireless
 SSID = UofM VPN Wireless
 SSID Broadcast = NO
 Private Network= NO

Authentication Radius Server w/Uniquename
 and Passwords

Authorization Radius Server, all UofM Student,
 Faculty and Staff



WIRELESS SECURITY - CURRENT STATE AND FUTURE DIRECTIONS

Wireless security is a moving target with both theoretical and proven security exploits. The industry has responded with several possible solutions, but most have theoretical exploits developed shortly after being documented. Both the IEEE and the Wi-Fi Alliance are developing security recommendations.

The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. Currently the Wi-Fi Alliance has 182 member companies from around the world, and 698 products have received Wi-Fi® certification since certification began in March of 2000. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability. - www.wi-fi.org

Currently the Wi-Fi Alliance is working to enhance security through deployment of the Wi-Fi Protected Access scheme or WPA. WPA employs the use of IEEE standard 802.1x for authentication and authorization and temporal key integrity protocol (TKIP) for encryption. 802.1x employs the Extensible Authentication Protocol (EAP) that is designed to sit inside of PPP's authentication protocol and provides a generalized framework for several different authentication methods. TKIP encryption is often referred to as WEP2. This is due to the fact that TKIP also uses RC4 to perform the encryption, but corrects many of the vulnerabilities in WEP. TKIP even resets the keys based on the number of packets exchanged in a session. Future standards are expected to embrace Advanced Encryption Standard (AES) based encryption as the system becomes more widely deployed. The goal of the Wi-Fi standards are to allow for non-vendor based security systems at the wireless level rather than requiring a security mechanism at a higher layer. As of late April 2003 the first designs for AP and client radios for 802.11 a/b/g were approved by the Wi-Fi.

The IEEE is working on 802.11i that covers areas of security. Specifically the draft covers the security of data in transit and the access control to the wireless network. The draft is still in process, although many expect it will be ratified by fall 2003. The current draft includes the use of TKIP for encryption and the IEEE 802.1x protocol for access control. However, the IEEE does not look to TKIP as a long-term solution. Again AES encryption is expected to be used in the future because it is considered more robust than TKIP. The move to AES will require most hardware to be upgraded due to the computational requirements. Again AES devices are designed to have backwards compatibility allowing for older less secure encryption methods for old clients.

However, 802.1x is not without problems. With the openness of the standard and the availability of multiple EAP types there are issues with hacks as well as compatibility on multiple platforms and vendor hardware. There are known vulnerabilities depending on the EAP type used, see <http://www.cs.umd.edu/~waa/1x.pdf>. By employing EAP types that require mutual authentication many of these attacks are not effective. These EAP methods include TLS, IKE, and GSS_API (Kerberos).

Use of security solutions developed specifically for wireless and that take advantage of the hardware can enhance security. These can also allow for the ability for systems administrators to require the use of the other higher layer security protocols for specific applications. Deployment of these new

solutions will be hindered until a common solution is in place that multiple vendors support on both the access points and in operating systems.

Related Documents

http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

<http://www.nwfusion.com/research/2002/0506whatisit.html>

<http://www.ieee802.org/1/files/public/docs2000/8021xSecurity.PDF>

<http://www-106.ibm.com/developerworks/library/wi-wifi.html?dwzone=wireless>

Here we summarize the various methods used to secure data on IEEE 802.11 networks as well as the strengths and weaknesses of each approach.

MAC address filter: Limits access to the AP by filtering incoming traffic based on MAC address.

- Allow only registered MAC addresses to communicate to the AP.
- Better than a completely unsecured net.
- Authorized MAC addresses easily discovered and spoofed.
- No encryption of the data stream.
- No user authentication when used alone.
- Does not scale beyond a small installation.

WEP (Wireless Equivalent Privacy): Encrypts data using a standard length key (40, 64, 128 or 256 bit)

1. Encrypted data stream
 - 40 bit key standard
 - 128 bit key supported by most vendors
2. Easily cracked keys:
 - An intruder eavesdropping on wireless transmissions can monitor network traffic and gather enough information to decipher the key and decrypt the data
3. Better than no security but not much.
4. No user authentication.
5. Does not scale well.
 - Limited set of keys (4).
 - All users must know at least on key.
 - No easy mechanism to change and distribute keys.
6. No Key rotation
 - Big Weakness
7. Key weaknesses
 1. The use of RC4 encryption algorithm
 - a. Relatively simple to crack
 2. The inability to have per user/session keys
 3. The lack of frequent changing of the encryption key

- *“Statistical attacks become increasing practical as more ciphertexts that use the same key stream are known.” (Borisov, Nikita; Goldberg, Ian; Wagner, David. (In)Security of the WEP Algorithm. ISAAC Group Home Page, Computer Science Division, University of*

California, Berkeley.

<http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>)

WPA (Wi-Fi Protected Access): designed to take the place of WEP and address many of its shortcomings

WPA requires the user to provide a master key, but this does not become a static encryption key. Instead, the master key is simply a password used as a starting point through which WPA derives the key it will use to encrypt network traffic. Moreover, the key is regularly and automatically changed (and never reused), reducing the likelihood that it will be compromised. The master key also serves as a password by which users can be authenticated and granted network access.

IEEE 802.11i: defines the encapsulation of EAP (extensible authentication protocol) on 802.11 WLAN's. Incorporates authentication and encryption to secure wireless network.

- *Official standard not yet released. To be ratified 3rd quarter 2003*
- The framework of LEAP* (Cisco solution to WEP vulnerabilities) is the basis for the 802.11i standard.
- Uses WPA – potentially upgradeable (hardware).
- Will use 802.1X for key hierarchy and key handshakes
- defines new encryption key protocols including the Temporal Key Integrity Protocol (TKIP**) and the Advanced Encryption Standard (AES). AES will require new hardware when it is completed.
- Proposed protocol conformance standards:
 - RSN Information Element (Tx'd in management frames)
 - Group Key Cipher Suite
 - Pairwise Key Cipher Suite
 - Authenticated Key Management Suite List
 - Unspecified EAP/802.11i Key Management
 - Preshared key/802.11i Key Management
 - (See Appendix for more Protocol Implementation Conformance Statements)

(ref:http://grouper.ieee.org/groups/802/linksec/meetings/MeetingsMaterial/Nov02/halasz_sec_1_1102.pdf)

*Cisco introduced LEAP authentication in November 2000. It is an authentication algorithm that leverages the 802.1x authentication framework. 802.11i will provide an alternative to WEP for it will offer new encryption methods and authentication procedures. "LEAP introduces a number of WEP enhancements like preventing replay attacks, preventing bit flipping attacks; dynamic per user, per session WEP keys, etc."

**TKIP – initial "Quick fix" used in 802.11i. Firmware upgrade to fix WEP vulnerabilities. Upgraded units should be backward-compatible with hardware that still uses WEP. Later AES hardware upgrade for greater security. Helps overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP changes temporal keys every 10,000 packets.

(Ref: <http://www.landfield.com/isn/mail-archive/2002/Oct/0120.html>)

IEEE 802.1X: Authentication Protocol for wireless implementations.

- IEEE standard (approved, June 2001) that enables authentication and key management for IEEE 802 Local Area Networks
- Specifies authentication and key management protocols (NOT an alternative to WEP, AES, 3DES)
 - Key-distribution mechanism overcomes the static-key problems of WEP
- Uses EAP framework
 - Inherent Weaknesses in EAP
 - Lack of protection of the user identity or the EAP negotiation
 - No standardized mechanism for key exchange
 - No built-in support for fragmentation and reassembly
 - Lack of support for fast reconnect
 - PEAP (Protected EAP Protocol)
 - By wrapping the EAP protocol within TLS, Protected EAP (PEAP) addresses the above deficiencies
 - (<http://www.globecom.net/ietf/draft/draft-josefsson-pppext-eap-tls-eap-02.html>)
 - Provides an end-to-end tunnel to transfer the user's credentials, such as a password, without having to use a certificate on the client.
 - Not supported for VPN clients.
- Adds no per-packet overhead and can be implemented on existing switches and access points with no performance impact
- Difficult to implement across a wide variety of clients.

Cisco's LEAP uses the structure that's defined by 802.1x to provide port access authentication in WLANs. The 802.11i committee for the authentication part is very strongly leaning towards 802.1x as the authentication mechanism for WLANs.

PROPOSED PICS for IEEE 802.11i

PICS - Protocol Implementation Conformance Statement

A.4.4.1 MAC Protocol Capabilities

Add the following, (Where "X" in PCX is the next number for the protocol capabilities)

Item	Protocol Capability	References	Status	Support
	Are the following MAC protocol capabilities supported?			
PCX PCX.1	Robust Security Network RSN IE	7.3.2.17	O PCX:M, FT1:M, FR1:M, FT3:M, FR3:M, FT6:M, FR6:M, FT7:M, FR7:M	Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.1 PCX.1.2	Group Key Cipher Suite Pairwise Key Cipher Suite List	7.3.2.17 7.3.2.17	PCX.1:M PCX.1:M	Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.2.1 PCX.1.2.1.1 PCX.1.2.1.2 PCX.1.2.1.3	CCMP data privacy protocol CCMP encapsulation procedure CCMP decapsulation procedure CCMP Security Serv. Mng.	8.3.4 8.3.4.1.1 8.3.4.1.2	PCX:M PCX.1.2.1:M PCX.1.2.1:M	Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.2.2 PCX.1.2.2.1 PCX.1.2.2.2 PCX.1.2.2.3	TKIP data privacy protocol TKIP encapsulation procedure TKIP decapsulation procedure TKIP counter measures	8.3.2 8.3.2.1.1 8.3.2.1.2 8.3.2.4.2	O PCX.1.2.2:M PCX.1.2.2:M PCX.1.2.2:M	Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/>

Item	Protocol Capability	References	Status	Support
PCX.1.2.2.4	TKIP Security Serv. Mng.		M	Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.2.3	WRAP data privacy protocol	8.3.3	O	Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.2.3.1	WRAP encapsulation procedure	8.3.3.1.1	PCX.1.2.3:M	Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.2.3.2	WRAP decapsulation procedure	8.3.3.1.2	PCX.1.2.3:M	Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.2.3.3	WRAP Security Serv. Mng.		M	Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.3	Auth. Key Mng. Suite List	7.3.2.17	PCX.1:M	Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.3.1	Unspec. EAP/802.11i Key Mng.	7.3.2.17	PCX.1:M	Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.3.2	Preshard key/802.11i Key Mng.	7.3.2.17	PCX.1:M	Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.3.3	802.11i Key Mng.	8.5	PCX.1:M	Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.3.3.1	Key Hierarchy	8.5	PCX.1:M	Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.3.3.1.1	Pairwise Key Hierarchy	8.5.1.2	PCX.1:M	Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.3.3.1.2	Group Key Hierarchy	8.5.1.3	PCX.1:M	Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.3.3.2	4 way handshake	8.5.3	PCX.1:M	Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.3.3.3	Group key handshake	8.5.4	PCX.1:M	Yes <input type="checkbox"/> No <input type="checkbox"/>
PCX.1.4	RSN Capabilities	7.3.2.17	PCX.1:M	Yes <input type="checkbox"/> No <input type="checkbox"/>

Links:

<http://www.mail-archive.com/cryptography@wasabisystems.com/msg03079.html>

802.1X specification: <http://standards.ieee.org/getieee802/download/802.1X-2001.pdf>

<http://support.asl.co.uk/observer/wireless/EAP-LEAP.htm>

Regarding WAP (WTLS)

<http://www.hut.fi/~jtlaine2/wtls/>

APPENDIX – SUMMARY OF UM WIRELESS INSTALLATIONS

College/ School/ Dept	Security Choice	Authen- tication	Access Control	Rate Control	Encryption	Supported Client Platforms	AP Type	RADIUS	Future Features
Taubman College of Architecture & Urban Planning	MAC address (802.11a/b)	n/a	MAC address	n/a	WEP 128 bit	Apple			
College of Engineering	VPN	Radius Server with Uniqname and Passwords			Data encryption with VPN	Windows 95, 98, ME, 2K, XP, Linux and Apple 10.1 or higher.	CISCO	Kerberos	Gateway with VPN?
School of Education (SEB or SoE)	MAC address registration	n/a	MAC address	n/a	none	Windows 95, 98, ME, 2K, XP and Apple.	Intel, Apple (Airport) and CISCO	None	Expand with more AP coverage
IT-COM	Wireless gateway with no VPN (currently Bluesocket)	Radius Server with Uniqname and Passwords		500kbits/s	SSL web encryption during authenticatio n only	Windows, WinCE, PalmOS, Unix, Apple (any SSL web browser)	CISCO	Merit RADIUS with Kerberos proxy	Cosign integration in gateway. Enable VPN in gateway.
Law School	MAC address registration	n/a	MAC address		WEP 128 bit	Windows 95, 98, ME, 2K, XP and MAC OS 9x, 10x	Lucent		Bluesocket gateway has been purchased and planning in early stages.
MCIT	MAC address (Cisco ACS)	n/a	MAC address	Internet Usage HTTP, HTTPS only	WEP 128 bit	Windows 2000, XP, WINCE, MAC OS	CISCO		802.1x, Checkpoint gateway, VPN support
School of Information (SI)	MAC address	n/a	MAC address						Gateway (Reefedge)
Business School	MAC address registration (m-track login)	n/a	MAC address	n/a	WEP 128 bit but only recommende d	W2k, WXP	Lucent	n/a	Gateway, 802.1X, role based access control
College of Literature, Science and Arts (LS&A)	n/a	n/a	MAC address	n/a	n/a	Windows	Lucent, CISCO	n/a	Assessing new technologies, such as, gateways and VPNs. Moving towards CISCO APs.
School of Natural Resources	MAC address/80 2.11a	n/a	MAC address	n/a	WEP?	W2K, XP and Mac OS 10 and above	CISCO	n/a	Centralized user authentication . Will more than likely not provide student support. Waiting for UMNWG

College/ School/ Dept	Security Choice	Authen- tication	Access Control	Rate Control	Encryption	Supported Client Platforms	AP Type	RADIUS	Future Features
									recommendati ons.
School of Public Health (SPH)	Wireless gateway (BlueSocket)	undecided	MAC address	undecided		Windows 2000	??	??	Cosign integration into Gateway
School of Art & Design	MAC address (must be a student in the college to register)	n/a	MAC address	n/a	n/a	MAC 9x 10, W2K, WXP	Apple Airport		Looking to extend coverage.
School of Music	n/a	n/a	n/a	n/a	Apple??	Apple Airport			Intending on adopting the CAEN model (VPN and radius server)
Institute for Social Research (ISR)	SSID (802.11g)		n/a	n/a	WEP 128 bit	W98 and WXP	Wavelan??	n/a	Expand to other areas but not needed for all locations