Wireless Security

Executive Summary

Today's mobile workforce increasingly demands convenient and secure access to the Internet using mobile devices (such as notebook and handheld PCs) with HP Wi-Fi and other mobile connectivity solutions. A secure solution enables a mobile worker to gain safe network access in areas where it is traditionally hard to deploy "wired" networks. It also enables such services as wireless access for CRM Data, file and database synchronization, and convenient network access to corporate resources on the intranet.

However, as users find it easier than ever to connect to, synchronize with, and download corporate data, the need for device security becomes crucial. This paper addresses the security implications of Wireless LANs (WLANs), and makes recommendations regarding some available, but underutilized, security solutions and tools.

A brief description of the evolution of wireless security is provided as an introduction to the available WPA and 802.11i solutions.

Problem Statement

Equipping today's mobile workforce with wireless equipment has the potential to increase productivity by providing mobile and wireless users access to corporate data from any remote location. The key to securing a wireless network lies in understanding the issues and available solutions through the entire system – from the moment the mobile user powers on the mobile device…through log-in…through application initiation….through the network firewall…through access to the network and data download. At every step, there are vulnerabilities.

In addition, this paper highlights security issues for mobile devices that are unrelated to the wireless nature of the solution, but may be associated with other aspects of Mobility and Connectivity.

Historical information/background

Most security issues for mobile devices have little to do with using wireless connectivity, but with the mobile aspect of the devices – the fact that they are moved from place to place. Confidential data may be located on a device that can be physically stolen or misplaced outside secure corporate buildings. Other security issues stem from the fact that the devices are connected to the Internet or a corporate intranet. But regardless of whether the connection is DSL, GPRS, Phone Line Dial-up, 1XRTT, EDGE or UMTS – securing that connection is the issue.

Before we discuss the tools developed for wireless security, it's important to address requirements for wireless solutions. All wireless devices must be supported using Encryption and Authentication. Recognizing that security needs to be addressed holistically, we have added client device security as a requirement.

The aim of encryption is to provide a mechanism to ensure data privacy and integrity. Data should only be decrypted by authorized means. All transmitted packets should be originated from senders. Data integrity must be maintained under all circumstances.

Authentication should be mutual – enabling wireless device clients and access points to authenticate one another. Authentication messages between clients, access points and authentication servers must be possible. Access points should be able to validate client credentials in order to grant access to the network

Mobile device security is required not only to protect the client devices, but also to help ensure that client devices themselves do not become points of vulnerability that could be used to threaten the entire IT infrastructure. This is on important aspect of data integrity.

Mobile Device Security and HP Protect Tools

HP saw the need for better security solutions very early, and started devoting resources to addressing this issue. As a result of this proactive effort, HP has developed a solution – the HP ProtectTools Security Manager – that not only meets mobility and wireless requirements, but is also extensible and therefore can easily grow to handle new threats and offer new technologies as they become available.

Businesses trying to implement client device security face a dizzying number of choices that may not always work well together. In addition, security solutions can be difficult to deploy and use. If a technology is difficult to use, most users will avoid using it. This further complicates the task of making client devices secure.

Client device security options feature a number of capabilities based on a variety of technologies:

- Notebook and desktop computers can be configured with Smart Card readers.
- Handheld devices now offer integrated biometric readers and incorporate security solutions for data encryption and user authentication
- The Trusted Platform Module – or TPM – embedded security chip designed to the Trusted Computing Group (TCG) standard, is available on a range of HP commercial products.
- Biometrics are expected to become more important as those technologies mature and become more suitable for enterprise deployment.

In addition, many client devices include security features that exist within the device BIOS. These include features such as:

- Pre-boot authentication – the ability to authenticate users before allowing the system to boot
- Device configuration lock down
- Remote management capabilities

While these security features increasingly rely on established industry standards, and therefore better integrate with other elements of IT security, there are still challenges that keep these features from being widely deployed and used. These challenges include:

- **Usability:** technologies and features that are difficult to use
- **Manageability:** technologies and features that are difficult to manage, particularly on a large scale
- **Awareness:** IT managers and users are not aware of a feature or do not understand its purpose
- **Interoperability:** features or services need to span multiple technologies
- **Extensibility:** solutions must adapt as security needs grow and newer technologies and features become available
- **Services:** implementation support to assist the customer in enabling product-based security attributes is often expensive and complex

The HP ProtectTools Security Manager is a security platform that addresses these challenges by using add-on software modules, which provide important client security features. New features may be added easily by installing new modules. This architecture gives users an easy-to-use, all-in-one security solution.

Wired Equivalent Privacy

Although most wireless security concerns have little or nothing to do with the wireless nature of the devices, there is some validity to the apprehension regarding the vulnerabilities of the Wired Equivalent Privacy key. WEP is an encryption algorithm designed to provide wireless security for 802.11 wireless networks. It was developed by IEEE volunteers. WEP security issues can be summarized in four main points:

- Web Key Recovery
- Unauthorized decryption and violation of data integrity
- Poor key management and
- Access Point association

All wireless vendors have taken steps to address these concerns. The IEEE response to the WEP key issue is 802.11i (802.1x Authentication) and Wi-Fi Protected Access (WPA). In fact, all HP devices will support Wi-Fi Protected Access, and the high-level authentication provided by 802.1x Enhanced Authorization Protocol. Also, these devices support TKIP and AES Encryption. We are focused on what is available today, as it is hard to predict future changes in wireless technologies as they are emerging and IP networks are evolving to IPv6.

The table below addresses the various solutions that vendors have developed to address the weaknesses discovered in WEP vulnerability.

Vendor Solutions for WEP Vulnerability	
Virtual Private Network Implementations **HP solutions:** HP Production WLAN HP Wireless Internet Access	Although VPN provides adequate security, there may be issues with roaming, cost, throughput and usability. Some solutions include: HP Production WLAN: Provides a routable IP address controlled by Security Policies allowing only access to Corporate VPN servers. Because you have to implement VPN using secure ID to gain Internet access, this is more secure HP Wireless Internet Access Solution: Provides full Internet access for on-site customers/vendors. Access is vended via Network Access Controllers that only allow Internet access after the client accepts a Legal Disclaimer. VPN is required if some intranet data is needed. In most cases, this is not needed as most productivity applications can be accessed using reverse proxy. This is very flexible and resilient to "edge of the network" changes.
Dynamic WEP key CISCO Hewlett Packard Microsoft	Implementation of Dynamic WEP re-keying of Access Points. In this solution, short-lived WEP keys are dynamically generated and broadcast. The time interval is short enough that the attacker will not have enough data to crack the web key. Initially, this solution introduced interoperability issues. Now it is the standard for Wi-Fi Security and was the seed for the WPA and 802.11i.
Enhancements of WEP Key (40-64 bit WEB) Lucent 128 bit Agere 152 bit WEB US Robotics 256 bit WEP	This extension of the WEP key did not help with security, as the WEP vulnerability issues persisted (for more information, click here). It might take longer to crack the key but it does not help.
MAC Address Filtering Server based Access point based	Filtering solutions are difficult to manage. Spoofing the MAC address is possible, but some Access Points can hold 30 MAC addresses, which requires you to feed in to all Access Points and tack them.

Vendor Solutions for WEP Vulnerability	
Other security measures Hiding the SSID Limiting the RF propagation	Hiding the Service Set Identifier (SSID) is not a valid security measure. Because management frames on 802.11 Wireless LANs are always sent in the clear, this mode of operation does not provide adequate security Limiting propagation is hard, although it is possible in certain environments

Wi-Fi Protected Access

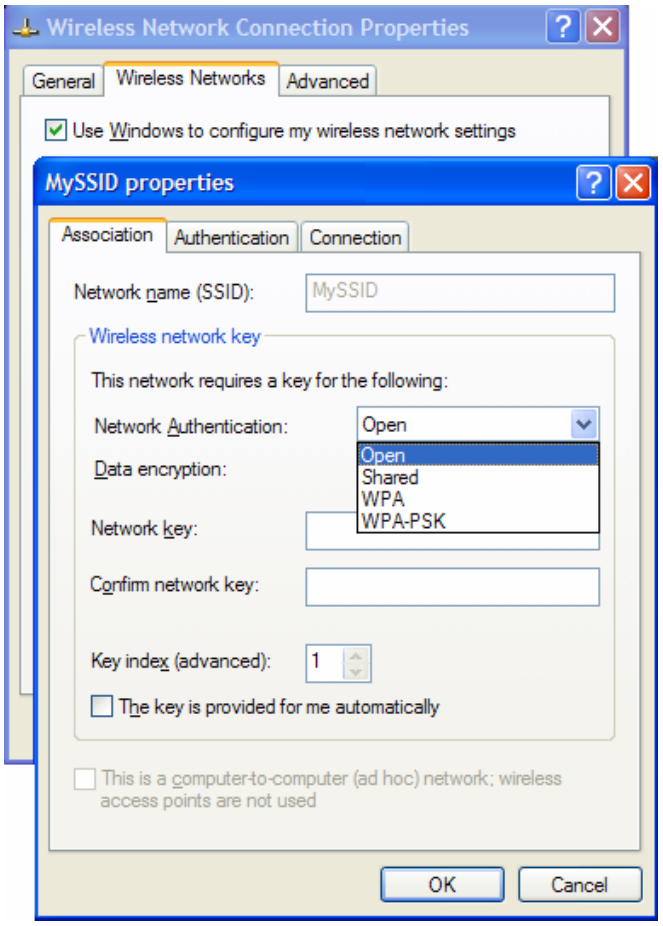
Fortunately, the Wi-Fi Protected Access (WPA) subset of the 802.11i solution is available to address the vulnerabilities in WEP key access, until the full 802.11i solution – driven by the industry – is available. WPA was developed expressly to increase the level of security for new wireless LANs, and manage existing solutions with software or firmware updates. This solution targets all known WEP vulnerabilities and is forward compatible with the upcoming 802.11i standard. This is a robust security solution with the following features:

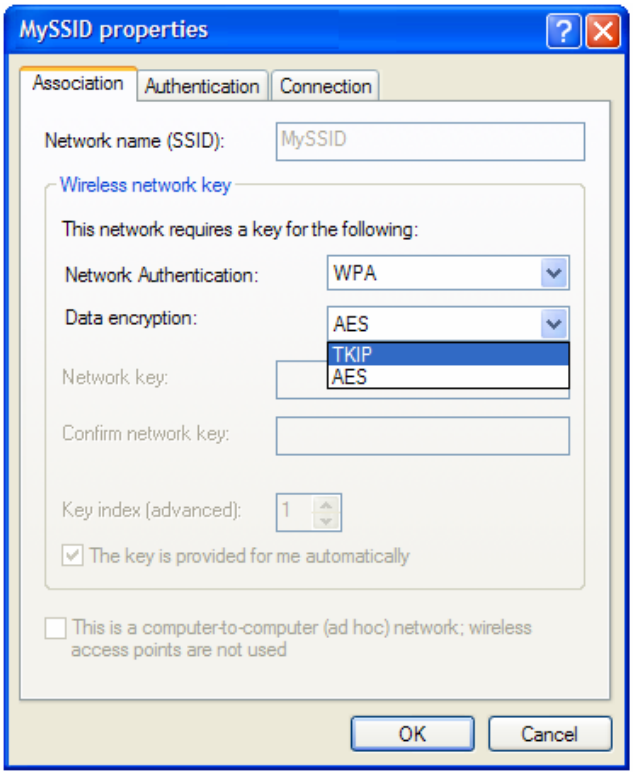
- Implements 802.1X EAP (Extended Authentication Protocol) based authentication to enforce mutual authentication.
- Applies Temporal Key Integrity Protocol (TKIP) on existing RC4 WEP to impose strong data encryption for key management
- Enhanced Message Integrity (using Michael Message Integrity Check)

The table below lists the advantages and issues of WPA, in comparison to WEP,

Advantages	Issues
• Uses dynamic keys in TKIP for better key management • Supports mutual authentication for stronger network access control. Previous methods authenticated the device, but not the source, for less security • Supports better authentication technologies such as 802.1X, EAP, RADIUS and Pre-shared key • Imposes data integrity through Integrity Check • Forward compatibility with 802.11i	• There are still potential encryption weaknesses in TKIP. It would be possible to crack the system, but it would be very difficult. • Slight performance degradation, mainly due to more complex and computation-intensive authentication and encryption protocols. However, with enhancement of hardware and introduction of 802.11g and a, we are gaining greater performance

The following screen shots show available WPA authentication and encryption supported on HP notebook PCs.





WPA Pre-Shared Key

While WPA and 802.11i allow EAP Authentication, this solution may not be affordable or available for home users. In addition, home users don't typically have access to an authentication server. In these instances, most available consumer devices offer authentication within the device with a WPA pre-shared key.

This makes a great solution for home use and office or small business use. It offers a straightforward replacement to WEP keys while offering all the WPA features – TKIP, AES, and others.

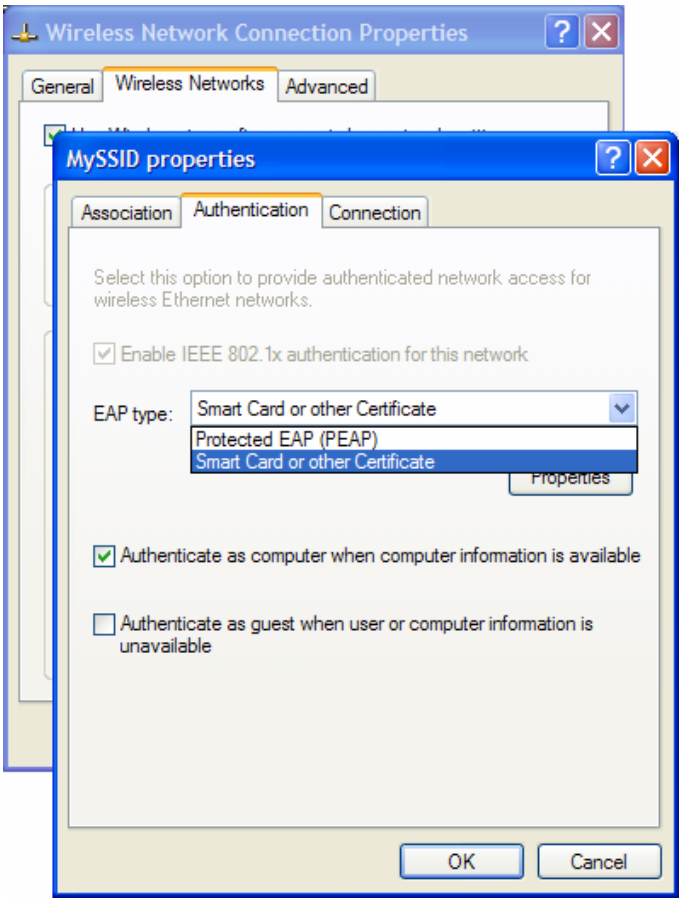
IEEE 802.11i

To address WEP security issues, IEEE formed a Task Group — "I"— and challenged it to develop the 802.11i standard. The group was asked to produce a detailed specification to enhance the security features for wireless LANs. The IEEE 802.11i standard was approved and ratified June 25, 2004, for authentication, authorization and key management.

The IEEE 802.11i standard is generally recognized as the future benchmark for the industry and will be available on all wireless devices. IEEE 802.11i products are currently in development and will be available soon.

Because authentication is available using digital badges, companies must protect the badges, leading to the need for certificate authentication. The screen shot below shows that EAP authentication can be extended or certificate-based, in addition to other EAP types. HP products are focused on delivering "out-of-the-box" support for a broad range of EAP types, such as CISCO

EAP and many other EAP implementations. For more details please visit http://www.hp.com/products/security



In addition to the advantages of WPA, 802.11i has the following advantages and issues:

Advantages	Issues
• Stronger Encryption dictates use of Advanced Encryption Standard (AES)	• An extra hardware upgrade is required, in order to implement AES.
• Supports roaming	• *Products are not widely available (Products will carry WPA2 logo as a certification of 802.11i)

* HP Notebooks with WPA2 Certification are available

Emerging Mobile Applications

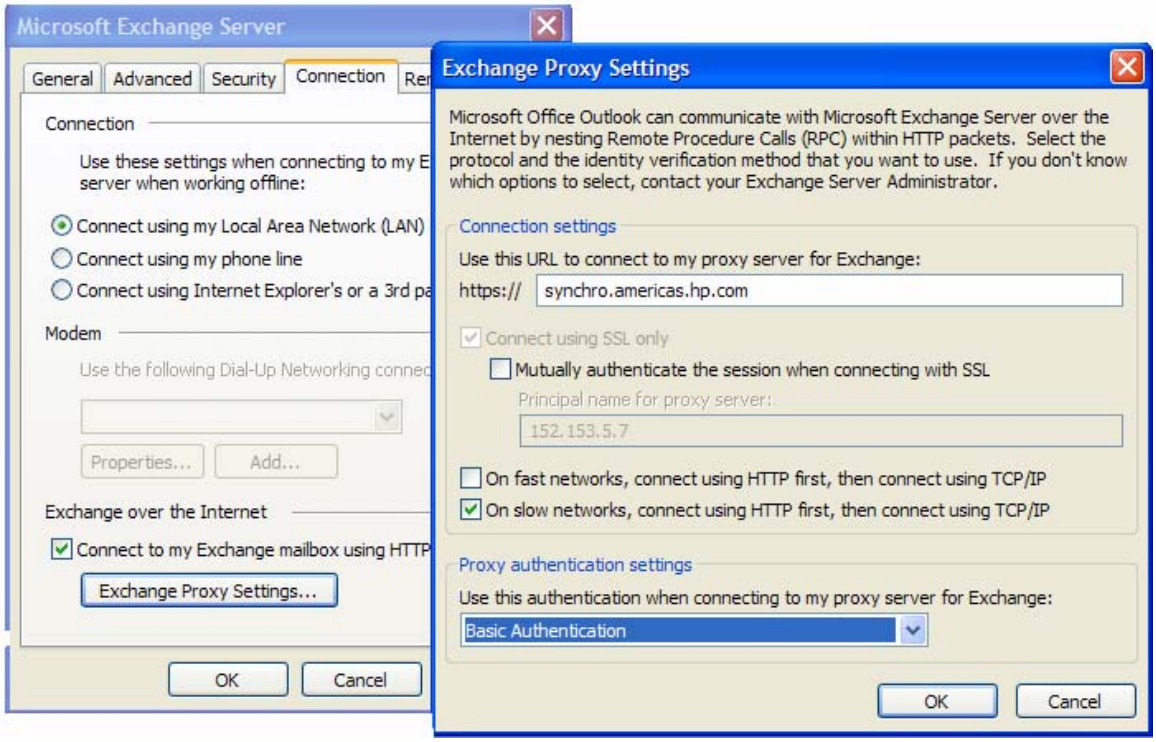
The rise of the Internet and wireless connectivity increased the demand for security and pervasive access to data from heterogeneous networks. The risk grew as static web pages evolved into dynamic and active server pages, or even remote procedure calls over http.

Hewlett Packard has had the optimal solution for this complicated problem since 1980, and can provide more robust security to mail, database and web servers. The HP solution is based on Trusted Operating system (TOS). One aspect of using this is reverse proxy.

Virtual Private Network vs. Reverse Proxy

Most people are using Virtual Private Network (commonly known as Tunnels) to connect to their corporate networks. Even consumer-grade wireless and wired routers have VPN and some Firewall and DMZ capabilities. An alternative to VPN that is rapidly gaining acceptance is the use of reverse proxy to obtain pervasive access. Reverse proxy passes http traffic back and forth across the firewall from the device to the back-end servers and web services – such as Microsoft Exchange, database servers, file servers and any web application.

This is all done using http, https or http with AES, 3DES or other encryption to secure transmitted data. The following screen shots demonstrate how Microsoft Exchange Server can connect to the network without VPN, using HTTPS. This is an ideal solution for notebooks accessing wireless and mobile networks.



Microsoft Exchange Server supports access to full PIM using Reverse Proxy when clicking "more settings."

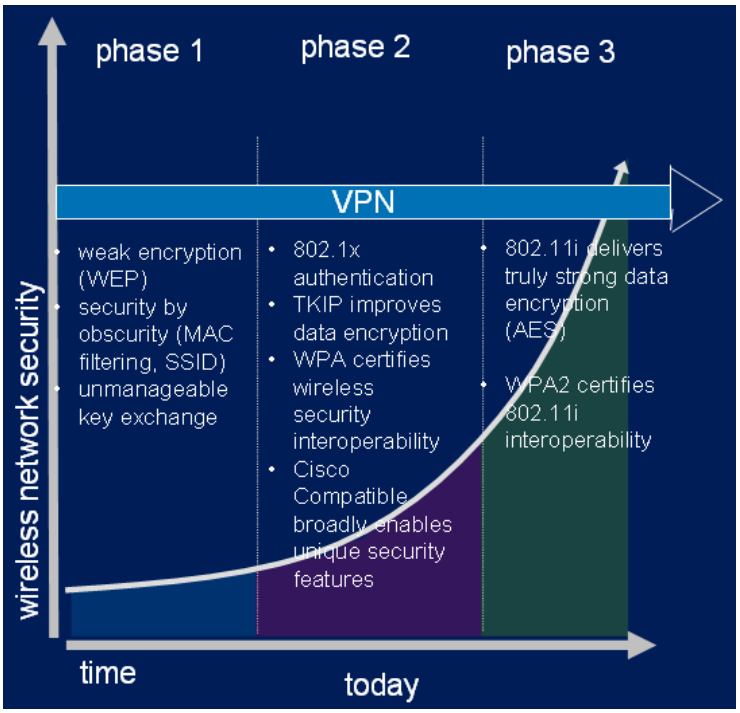
Nearly all applications – and many software solutions – use this method, including: device management, security solutions, PIM Synchronization, file sharing (such as Microsoft SharePoint) and database synchronization. This can include rich media and voice applications as well as Instant Messaging.

Microsoft SQL 2005 and Microsoft VisualStudio 2005 will be tightly integrated and will support subsequent generations of the needed proxy code to enable synchronization of the database over http, where developers can add the needed security – such as Advanced Encryption Standard (AES), Secure Socket layer (SSL) or Data Encryption Standard (DES). AES is proving to be the optimal encryption for mobile devices, due to its low requirements of memory and CPU processing power. This has a huge impact on mobility in terms of battery life, time, price and total customer experience.

Conclusion

A high-level understanding of the issues associated with wireless security is key to protecting your data and network. This is true of any kind of connection – wire-line or wireless.

Over the past eight years, wireless security has undergone major changes to address the vulnerabilities in Wired Equivalent Privacy. Wireless LAN *can be more* secure, provided that we apply the new available solutions.



The IEEE 802.11 Group, the Wi-Fi Alliance and major network equipment vendors such as Hewlett-Packard, CISCO and Microsoft are working together to develop new levels of security standards. WPA, an interim solution to WEP vulnerability, is available on almost all HP mobile devices. WPA, which is a subset of the 802.11i standard, addresses all WEP vulnerability issues. In addition, WPA-Pre-Shared Key was developed for use in a home or home office situation, where there is no need for an authentication server.

The 802.11i standard was released June 25th, 2004, and products based on this standard will be available shortly. With the 802.11 standard, the authentication server can be part of the Access Point. Users should ensure all Access Points and routers have WPA or 802.11i certification.

Products designed to be interoperate with other products designed to the 802.11i standard will be certified by the Wi-Fi Alliance. Certified products will carry the WPA2 certification label.

HP officially supports the Cisco-Compatible Extensions program. This is a formal certification program that attests to certified HP products interoperating with unique features of Cisco wireless LAN infrastructure

As wireless LAN security improves over time, users will continue to find stronger data protection and user authentication, as well as improved interoperability. Microsoft Windows XP Service Pack 2 offers enhancements for wireless security that address many wireless concerns related to WPA, 802.11i – and connectivity in general. Reverse Proxy has returned, and almost any web application can be accessed from any network without VPN, using this access method.

Now and into the foreseeable future, mobile consumers and users can feel safer in implementing wireless solutions by remembering that standards-based wireless network security plus HP ProtectTools security technology equals a more secure mobile computing environment.

For more information

http://www.hp.com/products/security

5983-0863EN Rev 2, 2/2005