



Understanding
The Basics
of Wi-Fi Security

Threats, Deterrents, and Best Practices
for Keeping Your Information Safe



Table of Contents

Introduction 1

Section I: Network Threats 2

Sniffers **2**

Stumblers **3**

Crackers **4**

Worms, Firewalls, and Probes **6**

Section II: Exposed Secrets 6

Section III: The Limits of Trust 8

Network Trust **8**

Network Encryption Types **9**

Network Scenarios **10**

Hotspot 10

Home 10

Office 11

Data Encryption **11**

Section IV: Best Practices 12

Secure Your Passwords **13**

Secure Your Services **14**

Email 14

Web 14

Instant Messaging 15

Secure Your Session (Hotspots Only) **15**

Secure Your Network (Home Only) **15**

Secure All Your Network Traffic **16**

Section V: Why IPSec VPN is the Best

Security Solution 16

JiWire SpotLock: Powerful Wi-Fi Security Made Simple **18**

About JiWire 19

Introduction

A Wi-Fi network is the modern equivalent of a party line. In the same way that Sam and Ethel down the road could tap into your late night phone calls to L.L. Bean—or Victoria’s Secret—and then discuss your predilections with your neighbors, so, too, can neighbors, network crackers, and scammers access much of the information you pass over a Wi-Fi network and use it to your disadvantage.



The information that flows over Wi-Fi—whether on your home or office network or at a hotspot—is often privileged, private, or personal, or all three. It may be an email password that’s being sent to a colleague, a picture of a baby you’re sending to a family member, or a spreadsheet showing the next layoffs at your company. Most people want this information kept from all but the intended recipients.

Wi-Fi networking is inherently insecure. By that, we mean that the network is designed to connect you to a local network or the Internet—not to keep your particular information away from the eyes of others. Wi-Fi and its latest security and encryption updates described in this white paper try to protect network access but not necessarily the information that flows over that network.

In practical terms, this means that any network that you can easily connect to, such as a free or paid hotspot or a home network unprotected by a password, should be considered as open to the public as if you’d published your accounts, passwords, and correspondence in a newspaper.

Other risks abound, too, from the same root: open networks allow hobbyists and criminals alike to insert themselves between you and the Internet, simulating a Wi-Fi gateway and capturing information.

Even without snooping and spoofing, just having your computer on an open network means that others on the network can attack you with worms and viruses—intentionally or not—and browse shared folders you may have forgotten to fully protect.

An ounce of prevention is worth tons of cure in this case. In this white paper, we will outline the points of risk in Wi-Fi networks and how to avoid them by encrypting data that flows over them, whether through network encryption, service encryption, encryption and authentication, or our recommended best

practice: a virtual private network (VPN), an end-to-end network data protection solution that was formerly practical only for large corporations.

Section I: Network Threats

Two primary threats bedevil Wi-Fi users on any network: sniffers, who intercept data and extract information from it; and rogue access points, also described more recently as “evil twins,” that mimic a Wi-Fi network gateway and then fool you or your computer into providing secrets.

A third threat is more general but is aggravated by Wi-Fi networks: the proliferation of worms that spread viruses among machines on a network and the ability to probe other machines on a local network for weaknesses and information (including computers with active firewalls that are designed to protect such intrusion).

Sniffers

Wi-Fi uses radio waves to send data, and radio waves are notorious for penetrating beyond walls, floors, and ceilings. That’s why Wi-Fi has had such success in spreading itself into millions of homes and businesses and tens of thousands of hotspots.

That same penetration, however, makes Wi-Fi ripe for monitoring. Someone interested in the data passing over a network need only be in the vicinity. For a hotspot, they could be sitting next to you; for a corporation, they might be sitting in a car on a public street with a powerful antenna that’s not visible from the outside of their vehicle.

The basic fact is that unless you surround a building with a wire cage, signals leak and you must treat your access to the network as completely available to anyone within line-of-sight range.

And don’t fool yourself into thinking that only a high-end cracker with sophisticated radio gear, an expensive laptop, and specialized software will be looking into a network. A used \$200 laptop with a \$10 Wi-Fi card and free software is quite effective and often used for these purposes.

On a network that employs none of the security methods we discuss in Section III, a sniffer need only intercept the wireless signals by joining or associating with the Wi-Fi network. (They can also plug into an Ethernet port if one is available.)



Don’t fool yourself into thinking that only a high-end cracker with sophisticated radio gear, an expensive laptop, and specialized software will be looking into a network. A used \$200 laptop with a \$10 Wi-Fi card and free software is quite effective and often used for these purposes.



RISK: A sniffer can capture any unencrypted data and passwords passing across a Wi-Fi network, or an Ethernet to which the Wi-Fi access point is connected.

The sniffer can decode any data passing by into its original form, such as instant messaging conversations, Web site visits, email messages, and FTP (file transfer protocol) transfers (see Diagram 1).

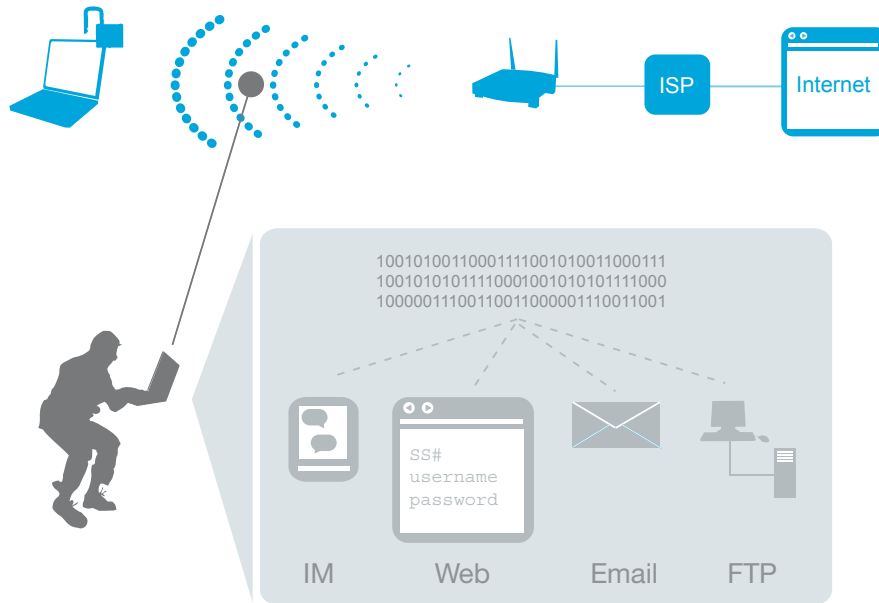


Diagram 1 - A Sniffer in Action

Unfortunately, there are a host of free software packages available on the Internet for many platforms, including Windows, Macintosh, GNU/Linux, and Unix, that specialize in finding networks, extracting passwords and other data that passes in the clear.

Stumblers

Stumbling software just alerts the person running it to the existence of Wi-Fi networks, detailing their signal strength, network name, encryption status, and channel number.

Stumblers are available for all platforms, including handhelds, and are often used for the hobby called wardriving in which people pass the time by driving around and recording available Wi-Fi networks in businesses and homes.

Windows: NetStumbler

Macintosh: MacStumbler, iStumbler

Unix/Linux: dstumbler

Pocket PC Stumblers: Ministumbler



Computer data can be easily intercepted using a number of free, readily available software packages commonly referred to as Stumblers, Snoopers, and Crackers.

Snoopers

If someone can connect to your network, they can view all of the data passing across it. This includes data that's encrypted: they may not be able to decipher what you're sending or receiving from a secure Web site, for instance, but they could snatch and use your email password if you aren't using APOP (Authenticated POP), which uses one-time passwords, or POP over SSL which encrypts a username, password, and all email messages in a session.

Unix and Linux distributions might employ **tcpdump**, a monitoring program that allows viewing of network data to determine which protocols are in active use, such as email or streaming media.

The Unix and Windows **ntop** utility collects data comprehensively, building a database as it works, and then presents a Web interface through which you can examine connections and traffic statistics. This is a way to learn more about which machines are on a network.

A dedicated password sniffer is called **ettercapNG**, and available for Unix, Mac OS X, and Windows. This program can automatically extract and capture passwords for many kinds of services.

Crackers

The original method of encrypting a Wi-Fi network, WEP (Wired Equivalent Privacy), has to be found to have deep flaws that render it easy to crack. Its replacement, TKIP (Temporal Key Integrity Protocol) that's part of WPA and WPA2, has an easy-to-avoid flaw as well. (Both protocols are discussed later in Section III.)

Several programs include modules that acquire enough data from a Wi-Fi network encrypted with WEP to crack the key which renders the network's traffic completely transparent to a sniffer. The amount of data needed can vary from megabytes to gigabytes depending on when all of the Wi-Fi adapters on the network were updated.

Unix/Linux: Kismet, AirSnort

Mac OS X: KisMAC

TKIP passphrases can be cracked when you choose very short phrases entirely composed of words found in dictionaries.

Windows: WPA Cracker

Mac: KisMAC

Rogue Access Points or “Evil Twins”

The sniffer listens to traffic over an existing network, but one level up is the “evil twin:” a Wi-Fi signal that is disguised as the network you want to connect to. Your computer associates with this rogue access point, which then intercepts all data and relays it back and forth to the legitimate network without your knowledge (see Diagram 2). In the process, the evil twin can extract even more data from your computer and perform “phishing” attacks.

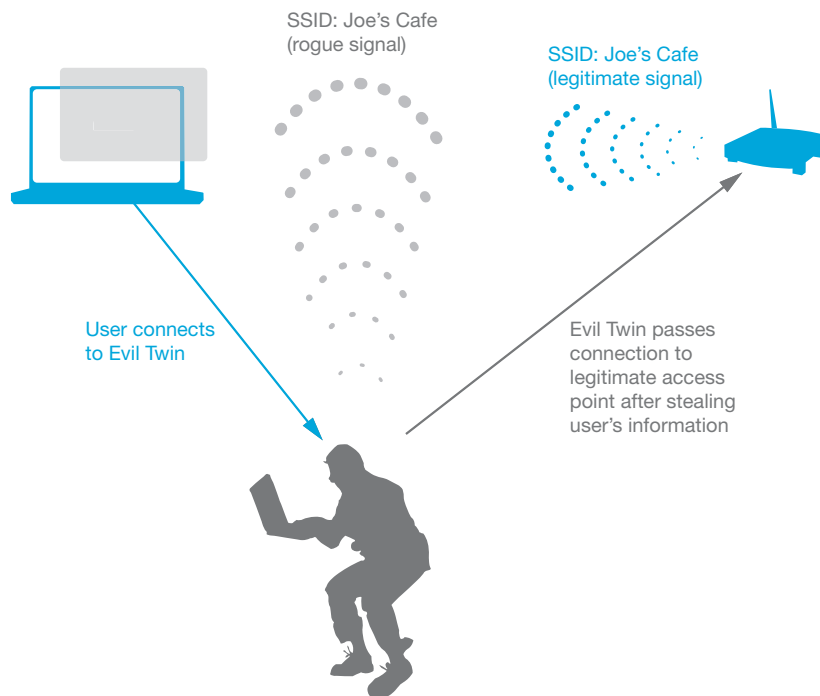


Diagram 2 - An Evil Twin in Action

For instance, the evil twin can control what Web site appears when you enter a domain name. Enter “paypal.com” and instead of being taken to PayPal’s secure Web page, the evil twin displays an unsecured page with a login prompt. An evil twin can also try to force software on your computer to re-connect to services that require passwords and extract them when they’re re-sent.

Evil twins can be set up using a piece of hardware near an existing network, but it’s more likely to be software running on a laptop computer. There’s no software that’s purposely designed to be an evil twin, but most operating systems allow a computer to be turned into an access point through the wireless driver.



“Evil Twins,” also commonly referred to as “rogue access points,” can be easily set up to trick your computer into connecting to the wrong network, at which point your data can be intercepted.



RISK: An evil twin can intercept and redirect network traffic in such a way as to fool software on your computer into revealing secrets, such as passwords and account information.

The evil twin is one of the greatest direct threats to a user's online identity and security, and has been seen more frequently as Wi-Fi becomes more popular.

Worms, Firewalls, and Probes

We don't need to describe in great detail the well-known damage and loss of productivity caused by Internet-based worms—malicious viruses that use resources on a computer to connect to other computers to spread themselves or other viruses.

A local network is a great place for viruses to spread, and on any Wi-Fi or Ethernet network, whether it has encryption enabled or not, all of your peers are as likely to infect you as you are them.

Even if you have a firewall installed, you may still be at high risk on a Wi-Fi network. Why? Because most users configure their firewall to allow machines on a local network, such as their home or work network, to have more privileges than computers or servers trying to reach your machine from the rest of the Internet.

Now think of the position in which a Wi-Fi network puts a laptop or handheld: it's on a local network, and your firewall permissions will give it the kind of access a trusted network would get.

Many Wi-Fi networks in public hotspots and other locations use the same range of private Internet protocol addresses that home and office networks employ, making those Wi-Fi networks appear exactly like each other to a firewall. (Many firewalls alert you to new networks, but you might ignore those prompts, turn them off, or click Yes when you should have clicked No.)

This allows entry for worms, as well as probes that try to find weaknesses in your system, or access shared network folders that you've failed to password protect.

A VPN can block this kind of subterfuge by rejecting or ignoring all attempts from machines on a local network to access your computer.

Section II: Exposed Secrets

It's easy to be lulled into a false sense of security until your email address is stolen, an ecommerce account or credit card is hijacked, and you find yourself

Expert Insight

“While using a laptop on a recent train ride across Europe, my computer was consistently able to detect one or more available Wi-Fi signals along the route. Based on the signal name (SSID), only a small fraction of these signals looked like public hotspots, but instead appeared to be Wi-Fi access points located in private homes or businesses. Trying to decide which Wi-Fi signals I could trust was practically impossible.

Had I connected to a Wi-Fi signal without any security protection, I could have immediately exposed the password to my corporate email account or given people using the same access point transparent access to my computer. As an added twist, had I started up the usual sniffer tools I use in my daily line of work as a security expert, I would have been able to eavesdrop on what my fellow train passengers were doing at the same hotspots. Bottom line, it's just too easy.”

- *Bjarne Jensen, CEO,
F/X Communications*

the victim of identity theft or misrepresentation.

All information your computer sends and receives is open to interception on a Wi-Fi network directly or via a connected Ethernet network unless you choose to use some form of encryption. You may think your password is protected, but the fact that your computer doesn't show it to you—it may show bullets or asterisks instead as you type it in—has nothing to do with what it sends over the Internet.

Here are just a few examples of what's exposed:

- Email passwords. There is no default protection for email passwords in email programs despite a widespread popular belief.
- The contents of email, including attachments like spreadsheets.
- Webmail. Most Webmail interfaces don't use encrypted Web sites and thus all email and often all account information is sent in the clear. (Some offer an encrypted login that just encrypts the password, but then encodes the password into a URL that's used for a non-secure site.)
- FTP passwords. FTP is commonly used to transfer files to Web site by graphic designers or others. Even if email passwords are protected, FTP passwords are often identical on small networks and thus expose the same amount of risk.
- Any Web site password for non-secure sites. Many media sites, like newspaper and online magazines, use a login that's sent over a non-secure link.
- Instant messages. This might include the connection that has your password embedded, but always includes the text of all messages.
- File server logins or transfers. When you access shared network files over the Internet, the account information may be encrypted, but the contents of files you send back and forth are generally not.

Often, each kind of service can be separately encrypted to protect itself over a local network or the Internet. However, encrypting each connection separately introduces complexity, points of failure, and usually additional cost per service for small office/home office workers and even workers



RISK: If your computer is available on a local network without blocks in place that prevent it from being accessed—a firewall or active VPN connection—it can be susceptible to worms and viruses.

whose corporate information technology departments don't support encryption for a particular service.

Section III: The Limits of Trust

As noted earlier, Wi-Fi networks are inherently designed to protect access, not to protect one user from another's ability to intercept data. Most networks are untrustworthy in the technical sense: this doesn't mean that a given hotspot, hotel, or other network has people running it with malicious intent.

Overlaying encryption for services or all data avoids any problems with trust at the network layer. Let's first look at network trust and then at encryption that a user can control on his or her own machine to overcome untrustworthy networks.

Network Trust

Network trust typically comes in two related forms: encryption and authentication. Network encryption on a Wi-Fi network means that everyone on the network shares the same encryption key that protects the network from people who do not have the key; they cannot see the data, but all users on the same network can.

Authentication couples encryption with uniqueness. On an authenticated network, each user has a separate account and is issued automatically a unique encryption key which protects each user's data from one another. But an authenticated network still has risk where it connects to an Ethernet network in most cases.

This breakdown of risk by network type (Table 1) shows all too clearly that trust is elusive even on networks with protection.



Network trust typically comes in two related forms: encryption and authentication.

Table 1

Location	Network Type	Network Encryption	Network Authentication	Trustworthy?
Hotspot	Wi-Fi	None	None	No
		WPA/WPA2	Yes	Mostly
	Ethernet only	None	None	No
Home	Wi-Fi	None	None	No
		WEP	None	Possibly
		WPA/WPA2	None	Yes
	Ethernet only	None	None	Yes
Work	Wi-Fi	None	None	No
		WEP	None	No
		WPA/WPA2	None	Possibly
		WEP/WPA/WPA2	Yes	Yes
	Ethernet only	None	None	Probably

Network Encryption Types

Wi-Fi network encryption comes in three forms:

- WEP (Wired Equivalent Privacy). WEP's encryption is broken, meaning that with a sufficient amount of network traffic, the WEP key may be extracted and used to connect to the network or sniff traffic. Using WEP doesn't assure security even for a single user on a home network.
- WPA (Wi-Fi Protected Access). WPA revised WEP's weakness, and is widely supported. WPA includes the TKIP (Temporal Key Integrity Protocol) key. A properly chosen TKIP provides perfectly adequate security for a home user.
- WPA2. This newer version of WPA adds a stronger encryption key format known as CCMP (Counter-mode CBC MAC Protocol) that is a form of AES

(Advanced Encryption System). CCMP is considered one of the most secure methods.

WPA and WPA2 are often coupled with a form of user authentication known as 802.1X. Combining WPA/WPA2 and 802.1X means that no two users on a network can see each other's data—until it hits an Ethernet connection at which point all data is once again visible.

Network Scenarios

In each kind of network listed in Table 1, you have different risks and opportunities to mitigate it at the network level. Let's look at each in turn.

Hotspot

Most hotspots employ no encryption on their Wi-Fi link, and even if they did, the encryption would be shared, meaning that all other valid users would have access to sniffing your data. Without encryption, your data is guaranteed to pass in the clear.

Whether you connect via Wi-Fi or Ethernet in a hotspot, you have to consider the security of the Ethernet network because Wi-Fi traffic is connected directly to a local Ethernet network.

The Ethernet network is often considered untrustworthy because without special precautions, anyone might have access to it and thus be able to view all unsecured traffic.

You can imagine that places that are designed to gather together people to use Wi-Fi networks are ripest for the picking for someone seeking to hijack online accounts or credit card numbers. Exercise the highest level of caution in hotspots.

Home

In the privacy of your home, unless you live in a very remote area, it's the unfortunate truth that you must take precautions against your neighbors.

It's extremely common for open Wi-Fi networks to be used by those who stumble across them. If you live near retail establishments, in an apartment building, or in a dense urban neighborhood, it is inevitable that an open network

will be used by others. You may find that acceptable, but recall our earlier advice about viruses and firewalls.

On an Ethernet-only home network, you should have no concerns.

Office

Businesses can control access to their network better than either home users or hotspot operators, but many do not. If you work in a business with an open network, convince them to change this immediately.

Many businesses have some form of protection enabled. WEP is clearly inappropriate for any business that has information they need to keep confidential. There's too much risk.

WPA or WPA2 are both acceptable if the business has a good policy of changing the key regularly and its employees know the importance of protecting the passphrase. A single outsider gaining access to the passphrase through social engineering jeopardizes the security of all users on the network.

Businesses should think strongly about using 802.1X or WPA Enterprise which combines simplicity with trust.

Ethernet-only business networks are generally trustworthy as long as no outsider can gain access to any Ethernet port.

Data Encryption

You can see the repeated theme here: even with network encryption enabled—even with the strongest form—most networks outside of corporations, especially Wi-Fi hotspots, still have weak points of access. This inevitably leads to encrypting one's own data as an overlay onto any additional network encryption and authentication that's available.

- Virtual Private Network (VPN), a catchall term for software that wraps up in encryption all network traffic entering and leaving a computer. It can be special software on the computer built into many operating systems, or it can be launched from within an appropriate Web browser; it always requires software on a server elsewhere on a local network or the Internet to handle the connection. Popular client-based VPNs use either PPTP (Point to Point Tunneling Protocol), considered weak because of a password extraction

flaw, or IPSec (IP Security), the most trusted encryption standard that runs over L2TP (Layer 2 Tunneling Protocol)



Because many networks, especially Wi-Fi hotspots, have little or no network encryption at all, it becomes necessary to also encrypt one's own data to ensure it is properly secured.

- SSL (Secure Sockets Layer) or TLS (Transport Layer Security) which protects sessions, such as between your browser and a secure Web site or between an email client and a secured mailer. SSL requires support in client and server software.
- SSH (Secure Shell) used for point-to-point usually persistent connections for a single kind of traffic, like a terminal session. SSH requires software to manage the connection on the client and a server that has general SSH connection support.
- PGP (Pretty Good Privacy) or GPG (GNU Privacy Guard), a way of protecting just the contents of a message or file so that only one or more parties with the right key can read it. Both parties must have compatible encryption software and have previously exchanged a public key that's been confirmed via fax or by voice for the highest security.

Section IV: Best Practices

The very reasons a public hotspot is so attractive—quick, easy, and open access—also makes it the location where your data is most vulnerable. A home network is as vulnerable as a neighbor or cracker's interest in what you're doing; add in the general feeling of safety you have from being in your own home and it's easy to feel secure, even though you're not without the proper protection.

Although firewall software and anti-virus software should always be used, that just protects your machine, not your data flowing to and from it. Here are four options, starting with the most basic level of security up to the most comprehensive level of encryption (see Table 2 for executive summary):

- Secure your passwords
- Secure your services, like email or FTP
- Secure your session (hotspots only) or secure your network (home only)
- Secure all your network traffic with a VPN

Table 2

Encryption Type	Protocol	Services Secured	Limitations
Password Only	APOP	Incoming Email	Password can still be intercepted but can't be reused; email data sent in the clear
	Authenticated SMTP	Outgoing Email	Login for sending an email, but password sent in the clear; email data sent in the clear
Web Services	SSL	Email, Browser, FTP, IM, file servers, others	Client configuration required; ISP or company must support service, may require multiple providers; extra fees generally apply
	SSH	Email, FTP, Browser	Requires special software and server configuration or command-line knowledge
Session (Hotspots)	802.11x plus WEP, WPA, or WPA2	Local Wi-Fi link	Requires client software or configuration for each hotspot network that supports it; only secures Wi-Fi link without securing Ethernet or link to Internet
Session (Home)	WEP	Local Wi-Fi link	WEP keys can be easily extracted by untrained crackers, rendering WEP protection useless
	WPA or WPA2	Local Wi-Fi link	Good protection for home network
Virtual Private Network (VPN)	PPTP (weak), IPSec (strong)	All services	Requires client software but is easiest method of reliably securing all data while acting as a de facto firewall

Secure Your Passwords

The path of least resistance avoids complexity but leaves most of your data in the clear. If you plan only to surf secure Web sites or sites without passwords,

and only send and receive email from an email client, you can just make sure your passwords can't be sniffed.

If your ISP or company supports APOP (Authenticated Post Office Protocol), you can typically check a single box in your email software and your password is scrambled uniquely each time you connect. The scrambled password is good only for a single session of retrieval.

Sending email is more complicated: if your ISP or company has Authenticated SMTP, then you can send email from anywhere by having your email client use a username and password to send outgoing messages. However, Authenticated SMTP still sends passwords in the clear. You may need to use Webmail to send email in this scenario, or use SSL-based SMTP, described next.

Secure Your Services

A wide variety of per-service encryption is available through ISPs, standalone services, and business information technology departments. To secure a service, both the client and the server software have to offer this as an option. This may require using different ISPs or providers for different services, installing special clients, and paying separate fees or purchasing third-party software. It also leaves all of your other services unprotected.

Email

Email is one of the easiest services to secure. Virtually all email clients support SSL, which allows session-based encrypted transactions. Many ISPs offer SSL for incoming and outgoing mail (POP/IMAP and SMTP). SSL email protects your account name, password, and all email contents.

You can also often employ a Webmail interface that supports SSL when an ISP or your client can't support direct email with encryption. Some of these Webmail services protect just the password, however, and only when you choose a secure login; the text of email is still sent in the clear.

Web

While all good Web sites that handle ecommerce and banking transactions have secured portions of their site, you can choose to encrypt all of your Web activities by using a third-party service that lets you connect to the Web using them as a secure proxy.

The connection from you to the service is encrypted, and they then conduct the transaction on your behalf from their network center.

Instant Messaging

It's rarely thought of, but instant messaging sessions are sent entirely in the clear by default and often contain private or confidential data.

Individual copies of instant messaging software can be secured through purchasing a personal digital certificate or using third party software.

Secure Your Session (Hotspots Only)

Some hotspots are starting to use a form of authentication known as WPA Enterprise or 802.1X with WPA. This method combines the advantages of a username and password with the security of WPA. With WPA Enterprise, you log in using either software built into your operating system (Windows XP, Mac OS X 10.3) or a connection package provided by the hotspot operator. Third-party 802.1X software is also available.

When you successfully connect with WPA Enterprise, the hotspot provides you with a unique WPA encryption key that you don't have to configure yourself. Since no one else on the network has the same key, your Wi-Fi traffic is protected.

This is considered reasonably good security as the hotspot operators who secure their local networks in this fashion also make promises about securing the Ethernet link on the back end. However, whenever it's possible for someone to plug into an Ethernet connection and gain access to the network, your data could be compromised.

Secure Your Network (Home Only)

Securing a home network is relatively easy. We recommend upgrading all of your equipment to WPA at a minimum. This requires Windows 2000 or XP or Mac OS X 10.3 as well as newer software drivers for the computers and firmware for the devices.

To keep an encryption key secure using WPA or WPA2, make sure your passphrase is at least 20 characters and includes a mix of letters, numbers, and punctuation—such as a favorite song lyric.

If you don't have a setup that will handle WPA, WEP is fine for home networks, but make sure you are using the latest firmware on all the devices on your network. Newer firmware has patched obvious vulnerabilities in WEP, and

up-to-date home networks are protected well enough with WEP against moderately interested intruders. Choose a WEP key that's full of random hexadecimal numbers rather than a short word found in the dictionary.

Secure All Your Network Traffic

The big guns can also be the easiest method of making sure none of your data is intercepted. A virtual private network (VPN) based on IPSec encrypts every bit of data that leaves your machine and decrypts every bit coming in. It also acts as a de facto firewall by disallowing any access from or to the local network.

A VPN doesn't affect the security of your local network: home users that choose to use a VPN should also turn on network encryption with WEP, WPA, or WPA2 as noted above. But if you choose to leave your network wide open to other users, they cannot intercept any of your data. On hotspot networks, which are open by default, this is obviously the crucial point.

A VPN creates a tunnel that extends from the client software across the local network, through the Internet, to the VPN concentrator. This can be in a business or ISP, or in a network operation center that's typically located in a secure co-location facility in which no one outside the VPN operator has access to the flow of traffic.

A VPN used to be an option reserved for large corporations; now it's a reasonable choice for even a home user, and it's the best practice for any traveler using hotspot networks, hotels, or Internet cafes.

Section V: Why IPSec VPN is the Best Security Solution

The majority of today's networks, including the Internet, are based on the Internet Protocol (IP). However, the IP protocol offers no security features and hence is susceptible to a variety of security threats, such as identity impersonation (spoofing), loss of privacy, loss of data integrity, data monitoring, and denial-of-service.

To achieve secure connections on the Internet, real security protocols need to work on top of IP. Such security protocols can get implemented within individual software applications, such as with SSL in the web-browser and POP3 authentication in the mail client. Whereas these application security protocols serve a perfectly valid purpose in the scope of getting the application to work as intended, the level of security will vary depending on implementation of each.

A VPN doesn't affect the security of your local network: home users that choose to use a VPN should also turn on network encryption with WEP, WPA, or WPA2 as noted above. But if you choose to leave your network wide open to other users, they cannot intercept any of your data. On hotspot networks, which are open by default, this is obviously the crucial point.

Note: The VPN tunnel is only as strong as the password that protects a user's identity when they login. The older PPTP protocol has a flaw in its password protection that allows a short password or one that contains common words to be cracked through brute force. A newer, stronger method for creating a VPN tunnel, IPSec over L2TP, uses algorithms that are acknowledged to be resistant to password choice problems and use more robust encryption as well.

As a consequence, application layer security is not a method wireless Internet users can rely on to protect their data from prying eyes.

Because of the variety of security threats in the IP protocol and the imperfection of the application layer security protocols, the Internet Engineering Task Force (IETF) defined a framework for IP security called IPSec.

IPSec is an end-to-end security model, establishing trust and security from a source to a destination, in what is known as a Virtual Private Network (VPN). IPSec works on the premise that to set up a common level of trustworthy end-to-end security, the security protocols need to work at the transport layer. In practice this means that IPSec layers somewhere between the network card and the Internet applications. All Internet traffic passes through this layer and by using IPSec for securing the IP layer, you secure the network. As IPSec provides security at the network layer rather than at the application layer, the security is transparent to applications.

For the user, the result of deploying IPSec is that all Internet traffic is secured in the same way, and the questionable safety of the traditional network applications is no longer depended upon. In effect, the IPSec VPN uses cryptography-based protection services, security protocols, and dynamic key management to create a secure tunnel between two or more network endpoints. Secure encryption keys are continuously negotiated between endpoints, in order to provide dynamic high-grade traffic encryption for the contents of your data packets.

In summary, IPSec provides application-transparent:

- Integrity, by guaranteeing data consistency between the source and destination.
- Authentication, ensuring that the received data is exactly the same as the data sent and the claimed sender is the actual sender.
- Confidentiality, by providing data privacy such that only the intended recipients can decipher the data crossing the VPN.

Because IPSec is designed to address all the issues related to keeping your data private over an unknown medium, it also becomes an ideal and proven solution for wireless hotspot users.

JiWire SpotLock: Powerful Wi-Fi Security Made Simple



On a global scale, wireless hotspot access is still in its absolute infancy. Despite progressive work on new security standards, it's clear that a simple way to overcome the many new threats hasn't been available—until now.

JiWire SpotLock simplifies wireless security by essentially applying its own secure Virtual Private Network (VPN) on top of any wireless connection. SpotLock bundles military-grade security features that encrypt your data, provide firewall protection, and ensures wireless networks won't block your outgoing emails (via SMTP relay).

How does JiWire SpotLock work?

Using powerful IPSec encryption technology, JiWire SpotLock creates a secure “tunnel” that protects all your inbound and outbound information between your computer and JiWire's security servers on the Internet. As a result, your information is not only protected between your computer and the wireless access point you're using, but all the way to JiWire's secure servers deep on the Internet. This ensures that your data can't be easily hijacked through the air or at the point it transitions to an Ethernet (wired) connection.

How does JiWire SpotLock address the security concerns previously addressed in this whitepaper?

Network Sniffers: Because JiWire SpotLock offers AES enterprise-level traffic encryption, network sniffers will only be able to see that your information is in fact, encrypted. According to the National Institute of Standards and Technology (NIST), it would take approximately 149 trillion years to crack this encryption with hardware available in 2000.

Evil Twins: As long as one wireless device can mimic another, it will remain a challenge for any security solution to deal with this threat. However, it remains extremely challenging for an evil twin operator to get in middle of the active IPSec tunnel used by JiWire SpotLock. While a data thief might eventually be able reverse engineer the many IPSec protocols used, decompress the IPSec traffic, extract the constantly changing encryption keys, remove packet encapsulation, and finally decipher the AES encryption, it would take an effort of gigantic proportions. While SpotLock cannot claim to offer the

catch-all solution to the evil twin problem, the sheer complexity of SpotLock's IPSec security makes it impossible for the average evil twin operator to pursue and highly unattractive for professional crackers. Bottom line, with so many people neglecting to secure their wireless connection, it's highly unlikely that even the most skilled cracker would spend the time trying to overcome SpotLock's defenses just to see an individual's private information.

Viruses and Worms: Traditional network-based attacks from unknown computers are unable to reach your Internet services, because all ports are blocked by SpotLock. This simple safety measure ensures protection against most "e-borne" viruses and worms.

About JiWire

Founded in 2003, JiWire provides information and services to help mobile professionals and computer enthusiasts find and connect to the wireless Internet. Through relationships with 400 Wireless Internet Service Providers (WISPs) and thousands of independent venues, JiWire offers the most comprehensive and up-to-date guide to free and commercial hotspot locations around the world as well as unbiased how-to guides, product reviews, and industry news. This critical information combined with services to manage and securely connect to any wireless network, offer users everything they need to safely and easily connect without wires -- anywhere. Customers include AvantGo, CNET Networks, Forbes.com, Intel, iPass, The New York Times, PC World, USATODAY.com, Wired.com and Yahoo!, among others. JiWire.com was named one of the "50 Coolest Websites" by Time Magazine and is a recipient of a 2005 Mobility Award presented by MobileTrax. With over one million people using JiWire's services, the company has created one of the world's largest Wi-Fi communities. To learn more, please visit www.jiwire.com.