Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

SECURITY DANGERS OF USING OPEN WI-FI NETWORKS

There are several reasons why users should doubt the security dangers of using free wireless Internet access despite the ease and convenience this offers. When certain devices are enabled to connect to an open network that requires no password, the data that flows between them and the wireless router is at great risk.

Wi-Fi refers to a range of connectivity technologies, including WLAN.

The Attraction of Free Wireless Access

A household name and trademark of the Wi-Fi Alliance, Wi-Fi refers to a range of connectivity technologies, including WLAN. Wi-Fi devices are installed in laptops, portable video game consoles, MP3 players, and smartphones, to name a few. This allows a Wi-Fi-enabled device to access the Web when within range of an Internet-connected wireless network.

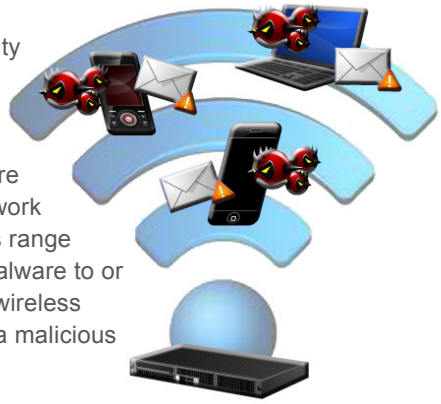
There are, however, security considerations when wirelessly accessing the Internet via a Wi-Fi-enabled device. A wired network's security is based on physical access control and trusting the other users on a local network. On a wireless network, however, anyone with a Wi-Fi-enabled device can easily connect to and infiltrate other users' systems.

Wi-Fi-enabled devices are prone to facing major security risks when browsing the Web via free wireless network access

TREND MICRO

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

The increased popularity of wireless networking devices is bound to spur more cybercriminal activity. Cybercriminals can easily grab the opportunity that a wireless network presents to gain access to unsecure systems. They can either perform passive attacks wherein they simply tune in to an open network and capture traffic or active ones wherein they join a network and target vulnerable devices. Active attacks range from accessing shared files to distributing malware to or spamming users connected to an unsecure wireless network, considering the difficulty of tracing a malicious activity's source.



A Growing Problem

Public wireless networks are generally designed for convenience than security. This is exactly where the problem lies.

The popularity of free and publicly available Wi-Fi network access and Wi-Fi-enabled devices is paralleled by the number of break-ins on unsecure networks and by the severity of cybercriminal activity involved. Telecommunications company AT&T has, in fact, seen significant growth in the number of Wi-Fi connections, which reached more than 100 million, in the third quarter of this year. The report also showed that the Wi-Fi access growth stemmed from the rapid rise in consumer use of Wi-Fi-enabled devices such as smartphones.

Early this year, the Wi-Fi Alliance also conducted a poll that showed that Wi-Fi connectivity has become a sought-after consumer electronics feature. The results also indicated a strong interest in a wide variety of Wi-Fi-enabled entertainment applications.

Apart from these, In-Stat statistics also showed that the next five years will see an increase in the number of Wi-Fi-enabled devices from more than 500 million in 2009 to nearly 2 billion by 2014.

Suffice it to say, the more users access free Wi-Fi hot spots with their mobile devices, the greater the risk they face. Ensuring that data shared over a network is encrypted is no longer enough, as a means for breaking Wi-Fi Protected Access (WPA) encryption wireless routers use has already been found. This has given hackers the ability to read encrypted traffic sent between PCs and certain types of WPA-encrypted routers.

Recent reports also revealed that *Google* publicly acknowledged that its open Wi-Fi network in Mountain View collected data that contained entire email messages, URLs, and passwords.

In addition, networks named "Free Public Wi-Fi" are not set up like most wireless networks are. These are usually ad hoc networks that allow users to directly access someone else's PC in the area. In most cases, these networks do not even provide Internet access.

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

An example of a security risk that users may face with using open Wi-Fi networks has to do with the newly developed browser add-on, *Firesheep*. *Firesheep* was originally developed for the purpose of spotting security holes in sites that do not encrypt their traffic. However, what may have seemed like an ideal security tool turned out to be one that even amateur hackers can use to access other people's accounts on *Facebook, Twitter,* and other popular services when on an open wireless network.

Firesheep allows users on a public Wi-Fi network to spy on others. It gives its users the ability to access sensitive information that can let them log in to their victims' accounts. As the add-on's developer explains, "As soon as anyone on the network visits an insecure website known to *Firesheep,* their name and photo will be displayed. Double-click on someone, and you're instantly logged in as them." With such a feature, it is not surprising that *Firesheep* has already been downloaded more than 104,000 times since its release.

Idiocy is another tool that bills itself as a warning shot to people who are unsecurely browsing the Internet.

> Trend Micro senior threat researcher Ben April said, "The sidejacking attack used by these tools is rather simple. Once you enter your user name and password to log in to a website, you will get a cookie back. Usually, it is a random token that only a successfully logged-in user and the site will have matching copies of. With this token, it becomes trivial to impersonate your browser and to own your session."

Trend Micro senior threat researcher Ben April said, "The sidejacking attack used by these tools is rather simple. Once you enter your user name and password to log in to a website, you will get a cookie back. Usually, it is a random token that only a successfully logged-in user and the site will have matching copies of. With this token, it becomes trivial to impersonate your browser and to own your session."

Why Should Users Care?

Firesheep poses a particular danger, as it can potentially compromise data and users' accounts every time they log in from public places like Internet cafes or access the Web using a publicly available network. This is alarming in that cybercriminals may easily collect personal information given the public venue that is an open network. Employees' systems are also at risk if they access their company networks from remote places via open networks, which also puts their companies at risk.

Even if a user is on a seemingly legitimate public network, the chances that other people will pry it are high. Unfortunately, there is no good way to tell whether a hot spot such as a coffee shop's Wi-Fi network is legitimate or if it was set up for malicious purposes. Users with malicious intent can also join the network and launch attacks on other connected systems. Still others may upload malicious executable programs for the purpose of stealing information.

TREND MICRO

The recent development of tools like *Firesheep* and *Idiocy* highlights an important security flaw that can expose users' systems to cybercriminals and hackers. These tools pose a serious threat to users accessing the Web via open or unprotected Wi-Fi networks. As for users who connect to or have set up their own open Wi-Fi networks, the risks involved in not properly securing these include data interception. This allows anyone within the coverage area of an open wireless network to potentially listen to communications sent over it. This is a serious problem for businesses, especially if the communications are meant to be confidential. An unsecure wireless network also gives hackers the perfect gateway to a business' internal network.

How to Stay Protected

Whether at home on private networks or at a local coffee shop or library, Internet users should always protect their systems while surfing the Web. Public hot spots that do not encrypt data transmissions put users' systems at risk. As the use of Wi-Fi networks in public places becomes increasingly popular, one can never be too sure of security. As such, users are advised to keep the following in mind:

- **Wireless networks are wide open.** They should generally avoid doing anything that they would not want to be seen doing on an open network such as conducting financial transactions.
- **When setting up an open wireless network, use a strong password.** The weakest point of security is typically the login. As when logging in to a website, a server checks to see if a matching account exists. If so, it replies with a cookie. However, when hackers get a hold of a user's cookies, they can do anything that user can do on particular sites. Moreover, anyone on an open wireless network will be able to read most of the Web traffic between other users and the access point.
- **Do not automatically connect to open networks.** Many Wi-Fi-enabled devices may pick up any open signal by default and that is convenient. However, doing so can leave these devices vulnerable to security risks.
- **Stay away from Wi-Fi hot spots altogether if at all possible.** For safety purposes, enable a system's firewall and make use of VPN technology. Doing so, according to April, prevents anyone on the same network from collecting one's credentials.
- **Configuring systems and Wi-Fi-enabled devices to stay secure is a user's best bet.** If systems are regularly patched and protected with an up-to-date antivirus and security software, they are on safer ground against bugs that hackers may leave just about anywhere behind.

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

Trend Micro Titanium Internet Security allows users to safely surf the Web, as it authenticates wireless hot spots and Wi-Fi networks. Enterprise users can also stay protected by using *Worry-Free Business Security,* which secures wireless connections.

Users should be careful and aware of what they send on an untrustworthy network. Unless messages sent over a network are encrypted, anyone with access to that network—wireless or not—can read them. In the end, it is important to exercise vigilance and caution before connecting to open Wi-Fi networks, especially those that come with the label "free."

References:

- AT&T. (October 22, 2010). *AT&T Recent Releases.* "Third-Quarter Wi-Fi Connections on AT&T Network Exceed Total Connections for 2009: Users Make 107 Million AT&T Wi-Fi Connections in Third Quarter, Up More Than Four Times Year-Over-Year." http://www.att.com/gen/press-room?pid=18686&cdvn=news&newsarticleid=31314&mapcode=consumer|financial (Retrieved November 2010).

- Ben April. (November 1, 2010). *TrendLabs Malware Blog.* "What's in Your Packets?" http://blog.trendmicro.com/whats-in-your-packets/ (Retrieved November 2010).

- Brian Prince. (October 25, 2010). *eWeek.com. "Firefox Firesheep* Extension Exposes Dangers of Lack of Encryption." http://www.eweek.com/c/a/Security/Firefox-Firesheep-Extension-Exposes-Dangers-of-Lack-of-Encryption-143340/ (Retrieved November 2010).

- Cade Metz. (October 22, 2010). *The Register.* "*Google:* Street View Cars Grabbed Emails, URLs, Passwords: 'Mortified' in Mountain View." http://www.theregister.co.uk/2010/10/22/google_acknowledges_street_views_wifi_data_contained_emails_urls_passwords/ (Retrieved November 2010).

- Elinor Mills. (November 1, 2010). *CNET News.* "The Unvarnished Truth About Unsecured Wi-Fi." http://news.cnet.com/8301-27080_3-20021188-245.html (Retrieved November 2010).

- Evelyn Rusli. (October 25, 2010). *TechCrunch.* "Lazy Hackers Unite: *Firesheep* Boasts +104,000 Downloads in 24 Hours." http://techcrunch.com/2010/10/25/lazy-hackers-twitter-firesheep-boasts-100000-downloads-faceboo/ (Retrieved November 2010).

- Evelyn Rusli. (October 24, 2010). *TechCrunch. "Firesheep* in Wolves' Clothing: Extension Lets You Hack into *Twitter, Facebook* Accounts Easily." http://techcrunch.com/2010/10/24/firesheep-in-wolves-clothing-app-lets-you-hack-into-twitter-facebook-accounts-easily/ (Retrieved November 2010).

- James Kendrick. (August 24, 2010). *GigaOM.* "Smartphone Wi-Fi Usage on the Rise." http://gigaom.com/mobile/smartphone-wi-fi-usage-on-the-rise/ (Retrieved November 2010).

TREND MICRO

- Marketwire, Incorporated. (July 29, 2010). *Marketwire.* "Wi-Fi-Enabled Devices to Exceed 1.9 Billion Units by 2014, Says In-Stat." http://www.marketwire.com/press-release/Wi-Fi-Enabled-Devices-to-Exceed-19-Billion-Units-by-2014-Says-In-Stat-1297168.htm (Retrieved November 2010).

- Robert McMillan. (August 27, 2009). *Network World.* "New Attack Cracks Common Wi-Fi Encryption in a Minute: Attack Works on Older WPA Systems That Use the TKIP Algorithm." http://www.networkworld.com/news/2009/082709-new-attack-cracks-common-wi-fi.html (Retrieved November 2010).

- Travis Larchuk. (October 9, 2010). *NPR.* "The Zombie Network: Beware 'Free Public Wi-Fi.'" http://www.npr.org/templates/story/story.php?storyId=130451369 (Retrieved November 2010).

- Wi-Fi Alliance. (January 27, 2010). *Wi-Fi Alliance Press Releases.* "Enthusiasm for Wi-Fi in Consumer Electronics Continues to Grow: Wi-Fi Direct Performance, Range, and Applications to Spur Increased." http://www.wi-fi.org/news_articles.php?f=media_news&news_id=946 (Retrieved November 2010).

- Wikimedia Foundation. (November 3, 2010). *Wikipedia.* "Wi-Fi." http://en.wikipedia.org/wiki/Wi-Fi (Retrieved November 2010).