Out of Thin Air!

An introduction to wireless security at home, on the road and on campus

Sherry Callahan and Kyle Crane
University of Kansas Medical Center
October 5, 2009
Wireless Networking at Home
Sherry Callahan, Information Security Officer
What is Wireless Networking?

Wireless or Wi-Fi technology is another way of connecting your computer to a network without using wires. **Wireless networks** utilize radio waves and/or microwaves to maintain communication channels between computers. This gives people the freedom to connect computers anywhere in your home or office network.

Wireless networking works similarly to how cordless phones work, through radio signals to transmit data from one point A to point B. A basic wireless design typically consists of a wireless router that provides access to the Internet and/or network and a system that connects via a wireless adapter.
Home wireless networks typically consist of at least one Wireless Access Point/Router and one or more computers that connect to the wireless router. The Access Point/Router is the device that systems connect to for access to the internet or to another computer sharing the signal.
Here we see a typical wireless router with 4 available ports to plug computers directly into, the wireless antenna and one WAN port.

Computers need an adapter that is compatible with the router in order to connect. Most newer laptops and PDAs already contain a wireless adapter.

There are many different kinds of adapters. PCMIA, PCI, USB, and Firewire are a few shown below.
A, B.....G? Current Wireless Standards

802.11A
Supports bandwidth up to 54 Mbps. It has a very limited range and has more difficulty penetrating walls and other obstructions. These devices should be considered outdated and is not typically found in common retail stores.

802.11B
Supports bandwidth up to 11 Mbps. It has a much better range than 802.11a and is not as easily obstructed by walls or other objects. Devices that use this protocol can suffer from more interference from other electronic devices such as microwaves. These devices are quickly becoming scarce at retail stores as they are replaced by the newer 802.11G devices.

802.11G
Supports up to 54 Mbps and has a range that will cover most average homes. These devices are still typically common in retail stores but are quickly being replaced by the newer technologies such as 802.11N.

802.11N
One of the newest types of wireless devices found in retail stores. Supports up to 600 Mbps and can cover an extremely large home or small business.
Prior to purchasing a wireless network there are a few things that you can look for to ensure that the equipment will provide an adequate amount of security.

- Gather as much information about your wireless hardware’s security as possible. Advanced firewall protection, strong encryption protocols, web filtering, and MAC filtering are just a few items you should look for in a wireless router.

- Ensure you have access to phone, email, or knowledgebase support from the manufacturer.

- Check the documentation that comes with the router/network adapter. Verify that configuration and securing of the router is simple and easily understood.
That was easy!

Wireless networks have become extremely easy to setup these days. Many people find that they can simply plug the hardware in and in just a few minutes they can be surfing the web or transferring files to other computers with no wires attached.

But perhaps it was TOO easy….

Many people fail to setup appropriate security measures on their wireless once they are connected.

If you simply plugged in your network adapter, connected your laptop or PDA to your network, there’s nothing to prevent your neighbor or someone else from connecting just as easily as you did!
Recommendations for Securing Your Wireless Network at Home

1. Change the router’s default passwords.
2. Change the SSID name and disable SSID broadcast.
3. Setup MAC filters to limit which computers can connect.
4. Turn on WPA2 encryption – use a strong key.
5. Review your wireless logs.
6. Watch for upgrades from the manufacturer.
7. Practice good computer security.
**Step 1.** Change the router’s default passwords.

Most wireless router manufacturers provide Web pages that allow owners to enter their network address and account information. These Web tools are protected with a login screen (username and password) so that only the rightful owner can do this. Right out of the box, however, they are usually configured with a default password that simple and very well-known to hackers on the Internet. Change these settings immediately.

![D-Link Setup Wizard](image-url)
Step 2. Change the SSID name and disable SSID broadcast.

Access points and routers all use a network name called the SSID. Manufacturers normally ship their products with the same SSID set. For example, the SSID for Linksys devices is normally "Linksys." When someone finds a default SSID, they see it is a poorly configured network and are much more likely to want to snoop around.

In Wi-Fi networking, the access point or router typically broadcasts the network name (SSID) over the air at regular intervals. In the home, this feature may be unnecessary, and it increases the likelihood an unwelcome person will try to log in to your home network.
Step 3. Setup MAC Filters.

All network communication devices have unique hard coded numbers assigned to them. This number is called the “MAC” address.

If your router is capable of MAC filtering you should only allow devices that you expect to appear connect to your wireless network and deny all others.
Step 4. Turn on WPA2 Encryption.

All Wi-Fi equipment supports some form of "encryption", which scrambles the information sent over the wireless network so that it can’t be easily read. WEP or WPA are the most common encryption schemes found on home wireless systems. For most routers, you will provide a passphrase that your router uses to generate several keys. Make sure your passphrase is unique, not a dictionary word and at least 10 characters long – the longer, the better!

Understanding WEP vs. WPA2

WEP (wired equivalent privacy) was the encryption scheme included with the first generation of wireless networking equipment. It was found to contain some serious flaws which make it relatively easy to crack, or break into within a matter of minutes. However, even WEP is better than nothing and will keep casual snoopers and novice hackers out of your wireless network. Using encryption with a longer key length will provide stronger security, but with a slight performance impact.

WPA2 (WIFI protected access) is a much stronger security protocol than WEP and should be used instead of WEP if your wireless router and network adapters will support it. Some routers may refer to this as WPA-PSK.

You should always consider using the router’s strongest encryption mechanism.
Step 5. Review wireless logs.

Most routers will keep track of what systems have been successful or have failed to connect to your router.

Reviewing your logs can help identify a possible intruder or misconfiguration in your router's security.
Step 6. Watch for firmware upgrades for devices.

Network hardware is run by software called firmware. Just like computers, flaws may be found in the software that would allow people to bypass security mechanisms built into your router or network adapter. You should regularly check your wireless manufacturer’s website for updates and apply when appropriate.
Step 7. Practice good computer security.

Don’t rely only on your router/access point to protect your computers inside your wireless network. Even the most secure wireless network typically won’t stop a determined hacker.

- Enable System Firewalls
- Use accounts protected with a strong password
- Apply security patches to your OS in a timely manner
- Ensure you have antivirus up to date on your system
- Avoid using open shares on your computers to share files
- Be on the lookout for malicious websites, spyware/adware, phishing and scams

Windows Users
http://www.microsoft.com/protect/default.mspx

Mac
How can I confirm my setup is secure?

When connecting to your wireless network. Look for “Security-enabled wireless connection”.

If your home network connection is listed as “Unsecured”, you may be a sitting duck to individuals free-loading off your Internet connection or snooping around on your computer.
Demonstration

Hacking an Unsecured Home Wireless Network
Wireless Networking
“On the Road”
Kyle Crane, Network Security Specialist
Free Wireless On The Road

• Many businesses now provide some form of free wireless internet access.
  • Airports
  • Cafés
  • McDonalds
  • Starbucks
  • Panera Bread
  • Even some gas stations??
Can I connect?

Generally (but not always) the network will have a name that matches the business.

If in doubt, ASK!

- There are examples of places that have open access but never intended to provide that to the public.
- The laws on access to networks are strict and don’t fit well to the grey areas in wireless access but may well be applied to you anyway.
How to Find an Open Wireless Network with Windows XP

- *Windows normally provides notification of wireless networks in range and lists the names.*
- *You can then select the network you wish to connect with and click “Select”*
How to Find an Open Wireless Network with Windows Vista

– Windows normally provides notification of wireless networks in range and lists the names.
– You can then select the network you wish to connect with and click “Select”
How to Find an Open Wireless Network with Mac OS X

- **MAC OS X** provides a similar notice when the Airport icon is available and the airport is on.
- Click the Airport icon and select the network from the list to connect to it.
It Looks Open...but Should You Connect?

How do I know the terms of access?
- Many locations use a type of portal to gain access. You must read and agree to the terms before you are allowed on the net. Those terms are binding.

If you are not presented with any terms or acceptance screen?
- Be wary. You don’t have to know the networks terms of use to be held to them. It doesn’t have to make sense it’s just the law.
Wireless on the Road: The good...

• Convenient
  • It’s always nice to be able to stay connected on the road.
  • It is becoming more widespread and almost expected in hotels and other travel locations.

• More freedom when working on the road
  • Allows a teleworker the freedom to get out of the house.
  • Allows for easier use of vacation even if critical actions need to occur while you are away.
Wireless on the Road: The bad...

- **Legal grey areas**
  - Some businesses can be vague about what the terms are to use the access.
- **Often times can be poor quality**
  - Many locations implement wireless poorly and the signal is weak in the intended areas.
  - This makes it much easier for a hacker to setup a fake wireless router and fool you into thinking you are connecting to a legitimate wireless network.
- **You have no idea who your neighbors are**
  - Open wireless is by nature uncontrolled and any one with any intentions can be there with you.
  - Are you sure that “McDonalds” is really McDonalds?
**Really nasty stuff:**

- **Large open WiFi networks are just like being on the Internet**
  - There can be hundreds of people with unknown intent who are all on the same physical network as you, just as though they were inside your house.
  - Your system is wide open to anything if not using a firewall.
  - Detection and identification of the offender are harder than it would be on the net.

- **Automated tools are emerging to take advantage of systems on wireless networks**
  - While not necessarily simple today, they will improve with time.
  - Moving towards automatic discovery and exploitation of systems.
Recommendations for Using Wireless on the Road

- **Disable automatic connections even to preferred networks.**
  - This prevents scanners from gathering the list of wireless networks that Windows will automatically connect to.

- **Keep Antivirus products installed and up to date.** This is pretty general advice but it holds here too.

- **Enable the Windows firewall whenever you are working with public wireless.**
  - All but the most determined attacker will be seriously frustrated in attempts to attack a firewall enabled system. It raises the bar.
Recommendations for Using Wireless on the Road

• *Turn off or disable your wireless card when not in use.*
• *Ensure your system is patched and up to date.*
  • *Use the auto update features of your OS to reduce the number of possible exploits available to an attacker.*
• *Don’t access personal or sensitive information while on a public wireless network (e.g., banking sites.*)
Pushing the Limits: Wireless and the Law
So many unsecured networks!
Look, but don’t “touch”!

- Wardriving, warflying or war-anything is NOT illegal.
- Capturing traffic is also not illegal but, in some states, intent is the key.
- Just because a wireless network is unsecured, it’s not an invitation to use them.
- If you connect to a wireless network without permission, you are committing a felony under Kansas law.
Man charged with wireless trespassing

Florida man faces 3rd-degree felony charges after using another man's wireless network from his laptop.

July 7, 2005: 5:52 PM EDT
By Rob Kelley, CNN/Money staff writer

NEW YORK (CNN/Money) - Police have charged a Florida man with a third-degree felony charge, after he was arrested for violating a St. Petersburg resident's wireless network without permission.

According to the police, Benjamin Smith, 41, was seen by Richard Dignon outside Smith's home on the night of April 20, 2005, sitting outside Smith's home using a laptop computer. When the officer asked Dignon to deposit his trash, Smith quickly removed his computer and tried to hide it.

Dignon also stated that he later noticed icons on his home computer screen that Smith, 41, may have been using. He called police and an officer arrived at 11:30 p.m., two hours after the incident.

"The arresting officer wasn't in the right house when it took place," said George Kajs, the Petersburg Police Department's legal staff and they looked up the attorney general's statute.

The charge, unauthorized access to a computer network, applies to all varieties of computer network breaches, and gives prosecutors

Man Charged for Using Cafe's Free Wi-Fi

Posted May 29th 2007 4:14PM by Terrence O'Brien
Filed under: Computers

May 10th, 2007

Retailers haven't learned from TJX - still running WEP

Posted by George Ou @ 3:46 am
Categories: Security, Mobile/Wireless, Networking, Servers, Hardware, Desktop
Tags: WEP, Network, Retail Company, WLAN, Wireless, George Ou

When I blogged earlier this week about TJX's failure to secure their wireless LAN and how it may end up costing TJX a billion dollars, I knew that it was merely the tip of the iceberg with so many retailers still running WEP encryption. As if WEP wasn't already broken enough, WEP is now about 20 times faster to crack than in mid-2005 when TJX's WEP-based wireless LAN was broken and I knew from experience that most retailers were still running WEP. I decided to stroll through town and check on some of the largest retail stores in the country to see how they're doing today. The reason I looked at the large retailers is because they're the big juicy targets with millions of credit card transactions that the T.J. X hackers love. What I found was truly disturbing and I'm going to tell you what I found.

The law, called "Unauthorized Use of Computer Access," basically says that accessing a computer system without authorization is illegal. According to the Police Chief, this covers hopping on Wi-Fi networks. The law allows for a punishment of up to five years in jail and a $10,000 fine. Peterson was offered a drastically-reduced punishment, though, considering most people's ignorance of the law and the fact that the cafe's Wi-Fi network is free and unsecured.
Questions?