

# Home Network Security Basics

Dennis Monroe  
dj.monroe@bitwaretech.com  
BitWare Technologies

Now more than ever computer and network security cannot be overlooked or diminished. “Computer security is the process of preventing and detecting unauthorized use of your computer” (Carnegie Mellon Software Engineering Institute, 2001). Our computers are used for everything from banking and finance, shopping or browsing the Web, or to send personal communications to our friends and relatives. A small amount of time spent securing one’s home network and computers can help protect confidentiality, integrity, and availability of sensitive data from the threats of intruders, spying eyes, identity thieves, malicious hackers, parasites, and viruses (Carnegie Mellon Software Engineering Institute, 2001).

“Always on” broadband technologies such as cable and DSL have created an array of readily available unprotected targets for Internet threats. Cable modem access’ “shared-medium” topologies create neighborhood-wide LANs susceptible to packet sniffing and unprotected windows shares. DSL is less susceptible to packet sniffing and the dangers of sharing a common collision domain, however, many other security risks still apply to DSL (Carnegie Mellon Software Engineering Institute, 2001).

Firewalls are a “system or group of systems that enforces an access control policy between two networks” (Carnegie Mellon Software Engineering Institute, 2001). “Home network” firewalls typically come in two forms, as a software application running on an individual computer, or as a network device such as a router (Carnegie Mellon Software Engineering Institute, 2001). Routers are essential devices for any home network that is connected to the Internet via cable modem. Even if they are not used to share a connection between multiple computers they can still act as a firewall, and provide the additional service of separating a home network into its own broadcast domain. This eliminates unnecessary traffic from other computers using the neighborhood shared-medium topology and reduces the ability of a hacker to “sniff” a home network. At a minimum, or in addition to a firewall device a firewall software application should be used to prevent unwanted access to a computer or the Internet from hackers or malicious applications. Free firewall software can be downloaded from <http://www.zonelabs.com> (Zone Labs, 2004).

Anti-virus software “look[s] for patterns in the files or memory of your computer that indicate the possible presence of a known virus” (Carnegie Mellon Software Engineering Institute, 2001). Anti-virus software uses the virus profiles provided by the vendor to identify viruses on a computer. Since new viruses are discovered every day, it is important to keep profiles up to date (Carnegie Mellon Software Engineering Institute, 2001). With the proliferation of viruses and Trojan horse programs on the Internet today a quality anti-virus package is essential. Free anti-virus software can be downloaded from <http://www.grisoft.com> (Grisoft, 2004).

A more recent and malignant threat comes in the form of “parasites” otherwise known as “unsolicited commercial software” “that is a program that gets installed on your computer which you never asked for, and which does something you probably don’t want it to, for someone else’s profit” (Clover, 2004). Parasites most commonly come in the following forms (Clover, 2004):

- Ad-ware-Typically plagues a browser with unwanted advertising;
- Spy-ware-Provides online viewing habits and personal information statistics to marketing companies;
- Scum-ware-Adds advertising links to web pages for which the author does not get paid;
- Homepage Hijackers-“Set browser homepage and search settings to point to the makers’ sites (generally loaded with advertising), and prevent you changing it back”;
- Dialers-Call “premium-rate” phone numbers from a computer’s modem;
- Other:
  - Leave security holes allowing software makers and others to download & run software on a computer
  - “Degrade system performance and cause errors thanks to being badly-written”
  - Hide code in unexpected places and prevent uninstall

Increasing your browser's security settings to the maximum, by being cautious when installing free-ware, and by running a spy-ware scanning utility, can help control the installation of parasites. Some companies that advertise spy-ware scanning utilities are the spy-ware companies themselves that hide their spy-ware and ad-ware inside of false spy-ware removal tools. Therefore, it is important to research and use a utility from a trusted organization. Two free spy-ware removal utilities that I use and recommend are Ad-Aware, and Spy-Bot. These applications can be downloaded from <http://www.safer-networking.org> (Safer-Networking.org, 2004) and <http://www.lavasoftusa.com> (Lavasoft, 2004).

Just as it is important to have antivirus software, anti spy-ware utilities, and a firewall, personal computing vigilance can help to ensure that security holes are prevented. Most hackers and parasite software creators use social engineering techniques to peddle their acrimonious wares across the Internet. It is important to use sound judgment before installing any freely distributed software. There is a good chance that the free smiley face software that you just installed on your computer is supported by ad-ware, or worse. If an item is questionable, or was marketed to you in a pop-up add do not install it. A hacker with a backdoor to your PC is likely to use your computer as a base for other attacks, or to serve questionable or illegal material (Carnegie Mellon Software Engineering Institute, 2001).

Additionally, it is imperative that operating system patches are kept up to date. Many operating systems—such as Windows—have automated update utilities that should be used whenever possible. Recent viruses such as Bagle, Sasser and Nimda illustrate how hackers can exploit operating system vulnerabilities in order to propagate malicious code (Grisoft, 2004). Furthermore, many recent viruses and exploits such as SQL Slammer have used open Windows directory shares to propagate. Therefore, open Windows directory shares should be eliminated wherever possible (Carnegie Mellon Software Engineering Institute, 2001).

The recent popularity of wireless home networks has ushered in a new set of security risks specific to the less secure nature of broadcasted wireless technologies. All of the precautions listed above should be strictly adhered to on a wireless network in addition to wireless specific precautions. Whether an integrated broadband router/wireless access point, or stand alone access point is being used, would be attackers can be easily thwarted if some basic steps are taken to secure and encrypt transmissions over a wireless medium.

When configuring a secure wireless access point it is important to begin by changing the default system ID called the SSID (Service Set Identifier) or ESSID (Extended Service Set Identifier). Since it is easy for hacker to find the default SSID for each manufacturer it is important to change it to something unique. Also, it is a good idea to disable identifier broadcasting (Bradley, 2004).

Announcing that you have a wireless connection to the world is an invitation for hackers. You already know you have one so you don't need to broadcast it. Check the manual for your hardware and figure out how to disable broadcasting (Bradley, 2004).

Also, make sure to change the administrative password while configuring the access point (Bradley, 2004). Use wireless encryption. There are currently two forms of wireless encryption WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access). WEP has many holes and is easily cracked, so whenever possible use WPA (most older wireless hardware is easily upgraded to use WPA) (Bradley, 2004). WPA overcomes WEP's security issues with its Temporal Key Integrity Protocol (TKIP) (Grimm, 2004).

TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all of WEP's known vulnerabilities (Grimm, 2004).

WEP and WPA can be configured on the access point and the wireless interface on the computer by enabling the encryption type and entering in a pass-phrase to generate a 128-bit key. Keys can also be manually entered. Once encryption is enabled the data portion of the frames sent between the access point and hosts will be encrypted. Also, computers that do not have encryption enabled and a matching key will not be given access through the access point.

Use MAC (Media Access Code) address filtering. Every network interface device is assigned a unique physical layer MAC address. MAC address filtering permits or denies access to a wireless access point based on the physical address of the interface. WEP and WPA do not prevent a computer from communicating with an access point, and only encrypt the data portion of the frame. Therefore, it is important to prevent unwanted access from hackers to the access point (Moran, 2004).

MAC address filtering can be configured on the wireless access point device. First enable the filtering, then chose to deny or permit MAC addresses. Lastly, add MAC addresses to the table. On my access point I have enabled filtering to permit the computers in my network. Any computer whose MAC address is not in the table will be denied access to the access point.

Home network security is not only essential it can be relatively easy to do. With the wide availability of free or reasonably price personal network security tools there is no reason to leave a home network unprotected. Threats to the internet and its users will not subside, however, with a little bit of effort to secure our home networks and computers hackers, virus writers, and parasite developers will find it increasingly difficult to exploit home users and their computers.