AC 2007-2057: IDENTIFYING VULNERABLE SECURITY PRACTICES IN SMALL SCALE COMPUTER NETWORKS

Gary Steffen, Indiana University-Purdue University-Fort Wayne

Iskandar Hack, Indiana University-Purdue University-Fort Wayne

Identifying Vulnerable Security Practices in Small Scale Computer Networks

Abstract

Twenty years ago, the Internet and networking was technology only accessible to large corporations, educational institutions and researchers. In today's information marketplace high-speed Internet reaches into the smallest businesses and households. To extend Internet connectivity, individuals purchase small routers and wireless access points from local electronic stores. This allows sharing of the Internet connection with multiple employees and family members simultaneously.

Improper installation of such data equipment creates a vulnerability to personal information and security. In an effort to better serve this growing market, student training has been implemented in the security of small scale networks and routers. Traditional security training has typically concentrated on virtual simulation and larger scale routers/firewalls.

Small inexpensive routers/firewalls and access points can be a powerful tool, which possesses many of the same security principles as their more expensive counterparts. A majority of students already have this equipment available in their own homes because of the popularity of DSL and Cable Internet access. Students, many times, disconnect the principles of home security from that of corporate or large scale network security. They learn the practice yet fail to implement this knowledge into their own life. Even the smallest leak of information may result in catastrophic circumstances.

This paper will discuss the use of small scale routers and access points in the training of a security specialist in a Computer Engineering Technology program. Examples will be given on how these small inexpensive communication devices can be used to demonstrate extensive security principles. The result is a personal connection for the student to exercise good security practices on a daily basis.

Introduction

Broadband, a type of high speed Internet connection, access is now readily available through your local phone or cable companies. Phone companies offer DSL Internet service that comes through your telephone lines and the cable companies offer similar services through your coaxial cable. Comcast Cable, the largest broadband service provider in the nation, has over 5 million customers subscribing to their Internet service[1]. This type of service gives subscribers direct access to the Internet that in turn can give scrupulous individuals possible direct access to the subscriber's computer.

With this type of high speed access, many households and small businesses wish to share their Internet connection with everyone on the premises. This can be done by purchasing a small

router or wireless access point. A router is a networking device that connects multiple networks together, for example, your home network and the Internet[2]. The router allows each of your computers to share the same cable or DSL Internet connections. Similarly, a wireless access point allows the sharing of a cable or DSL Internet connection without a physical wire being connected to your computer. Both of these devices can be purchased for as little as $59.00 at any local electronics store.

The projected growth in both cable and DSL subscribers will go from a combined 24 million subscribers in 2003 to nearly 50 million subscribers by 2008[3]. The predicted worldwide router market will grow from $6.3 billion in 2003 to over $9.2 billion in 2008[4]. Currently over 85% of individuals surveyed with a home network use some form of home router (or access point), compared to only 78% surveyed just 18 months ago[5]. The small network market is experiencing staggering growth that will continue for many years to come.

The perceived problem is that communication equipment, routers and access points, once designed to be used by highly trained technicians are now being used by individuals with little or no technical training. Manufacturers for these "Home" routers include easy installation steps that many times discard security information for deeper readings. Most novice users are only concerned about obtaining the Internet connection by quickly plugging in the device while totally missing any security setup. Improper installation and setup of routers can lead to unwanted access to your computer and network by outside hackers as well as computer viruses and worms. According to statistics compiled by the CERT Coordination Center of the Software Engineering Institute, the number of reported attacks on business and government computers worldwide has doubled each year since 2000[6].

Security students, many of whom personally own these types of communication devices, disconnect the principles of home security from that of corporate or large scale network security. They learn good security practice yet fail to implement this knowledge into their own life. This paper will discuss the use of small scale routers, access points and operating systems in the training of a security specialist in a Computer Engineering Technology program.

Firewall

The word firewall has become synonymous with network and computer security. A firewall is an information technology (IT) security device which is configured to permit or deny connections set and configured by the organization's security policy. A firewall's basic task is to control traffic between computer networks with different zones of trust (figure 1). Typical examples are the Internet which is a zone with no trust and an internal network which is (and should be) a zone with high trust. The ultimate goal is to provide controlled interfaces between zones of differing trust levels through the enforcement of a security policy[7].

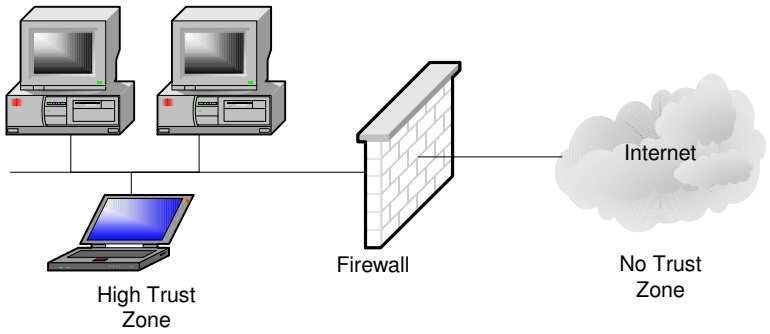

Figure 1 - Firewall

Firewalls fall into four broad categories: packet filter firewalls, circuit level firewalls, application level firewalls and stateful multilayer inspection firewalls.

Packet filtering firewalls work at the network level of the OSI model, or the IP layer of TCP/IP (figure 2). They are usually part of a router. A router reads the network layer address of all packets transmitted by a network, and forwards those addressed to other networks. In a packet filtering firewall each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet, forward it or send a message to the originator. Rules can include source and destination IP address, source and destination port number and protocol used. The advantage of packet filtering firewalls is their low cost and low impact on network performance.

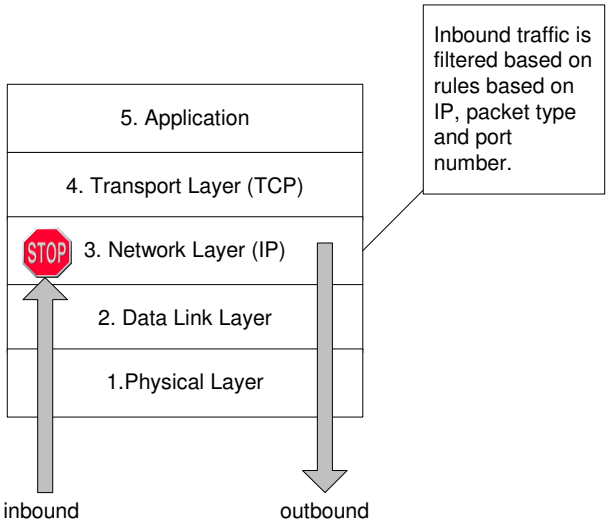

Figure 2 – IP Filtering Firewall

Circuit level firewalls, gateways, work at the session layer of the OSI model, or the TCP layer of TCP/IP (Figure 3). They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to remote computer through a circuit level gateway appears to have originated from the gateway. This is useful for hiding information about protected networks. Only valid entities or protocols based on the sessions rule set at the gateway will be allowed. Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect. They do not filter individual packets.

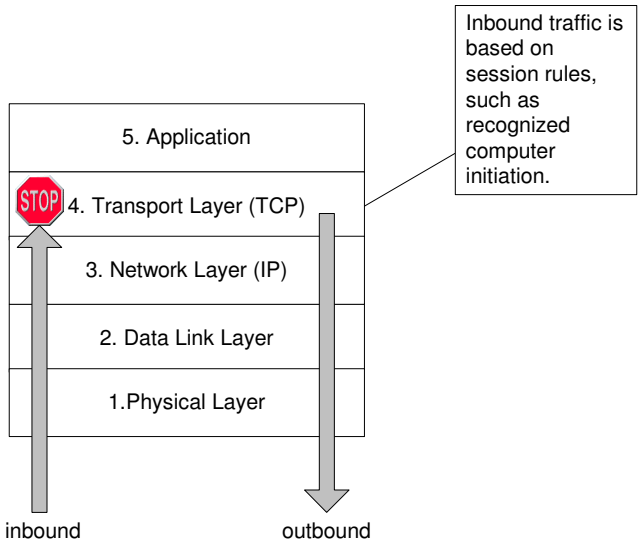

Figure 3 – Circuit Level Firewall

An application firewall, also called proxy, limit the access which software applications have to the operating system services, and consequently to the internal hardware resources found in a computer (figure 4). Incoming or outgoing packets cannot access services for which there is no proxy. In plain terms, an application level gateway that is configured to be a web proxy will not allow any ftp, gopher, telnet or other traffic through. Because they examine packets at application layer, they can filter application specific commands. Application level firewalls can also be used to log user activity and logins. They offer a high level of security, but have a significant impact on system performance. The reason that application firewalls are needed in today's Internet is that the other types of firewalls in existence do not control the execution of data, only the flow of data to the computer's processor.

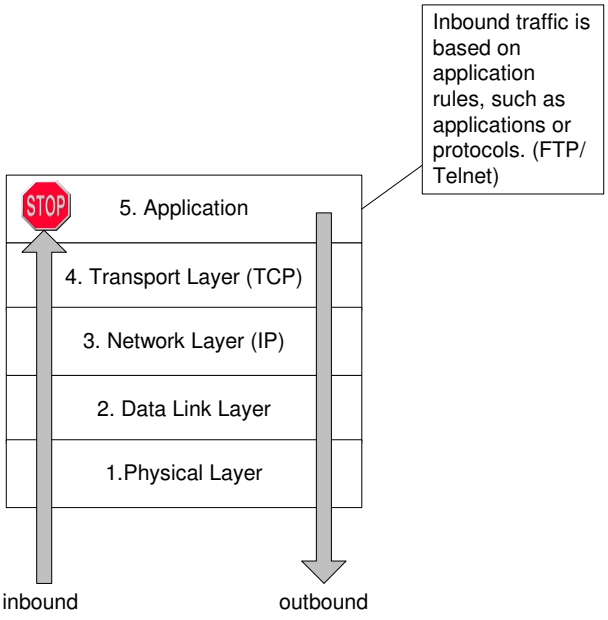

Figure 4 – Application Level Firewall

An additional type of firewall, known as a Stateful Multilayer Inspection Firewall, combines the aspects of the other three types of firewalls. They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer. They allow direct connection between client and host. This alleviates the problem caused by the lack of Stateful multilayer inspection firewalls that offer a high level of security, performance and transparency to end users but are expensive because of their complex implementation[8].

Firewalls under the first two categories can be demonstrated and explained using small inexpensive routers and access points, which have many of the same security principles as their more expensive counterparts. Routers, possessing the Network Address Translation (NAT) layer, offer the advantages of packet filtering firewalls but can also hide the IP addresses of computers behind the firewall, and offer a level of circuit-based filtering.

The application firewall can be associated with the use of a personal firewall. A personal firewall is traditionally a piece of software installed on an end-user's PC which controls communications to and from the user's PC, permitting or denying communications based on a Security Policy. The Operating System (OS) acts as the proxy to the applications. This can be simply demonstrated using the Microsoft personal firewall found in Windows XP and Vista.

Router as a Firewall

The small router market, as mentioned earlier, has exploded in recent years. The variety and types of routers is extensive. They range from simple routers/access points implementing NAT to routers containing the word “firewall”. Any of these types of routers contain characteristics of both IP filtering and Circuit Level Firewalls.

The idea behind using simple home routers is multifold. The first is the sheer number of simple routers found in small businesses and homes today. The students can use their own personal router if they own one. Furthermore, they can be easily purchased, or replaced because of the low cost of ownership. The author periodically is given free routers from students and faculty when they upgrade at home.

Implementing dynamic NAT automatically creates a firewall between your internal network and outside networks, or between your internal network and the Internet. NAT only allows connections that originate inside the stub domain. Essentially, this means that a computer on an external network cannot connect to your computer unless your computer has initiated the contact. You can browse the Internet and connect to a site, and even download a file; but somebody else cannot latch onto your IP address and use it to connect to a port on your computer.
In specific circumstances, Static NAT, also called inbound mapping, allows external devices to initiate connections to computers on the stub domain.

Most NAT routers provide for extensive filtering and traffic logging. Filtering allows your company to control what type of sites employees visit on the Web, preventing them from viewing questionable material. You can use traffic logging to create a log file of what sites are visited and generate various reports from it.

IP Filtering consists of examining incoming or outgoing packets and allowing or disallowing their transmission or acceptance on the basis of a set of configurable rules. Packet filtering policies may be based upon any of the following:

- Allowing or disallowing packets on the basis of the source IP address
- Allowing or disallowing packets on the basis of their destination port
- Allowing or disallowing packets according to protocol.

Depending on the type of router being used different aspects of IP filtering firewalls can be demonstrated. One such variation of IP filtering found in many routers is that of keyword filtration (figure 5). This rule allows for the blocking based on keywords or domain names specified by network users. In this case, the filtering blocks access to the "no trust zone" from someone in the "high trust zone". A firewall is an important learning tool when demonstrated in either direction (traffic-in or traffic-out).

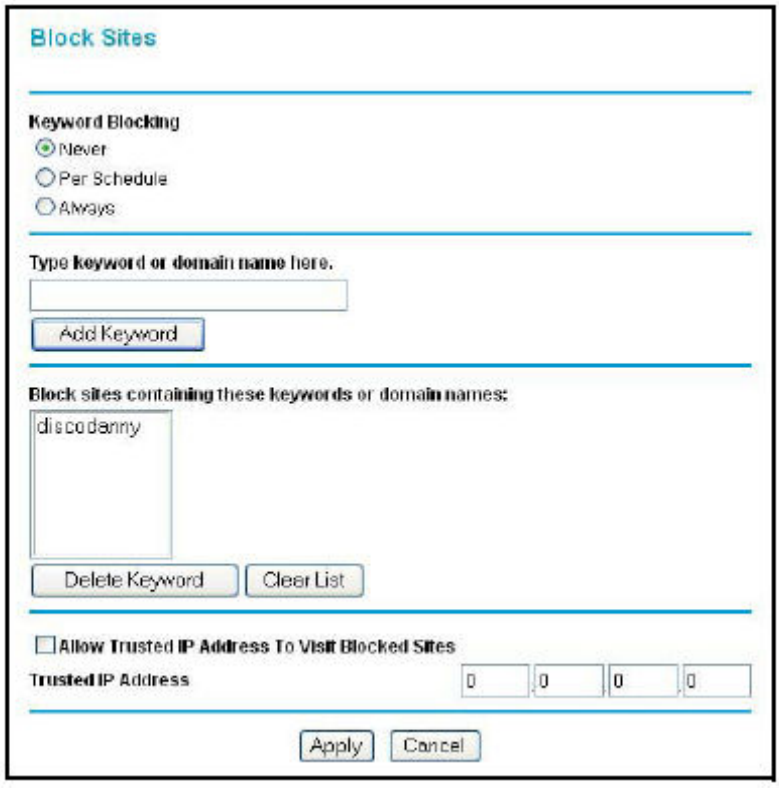

Figure 5 – Site Blocking

Another demonstration of IP filtering firewalls, demonstrated in simple routers, is with the use of services, or protocol blocking. Instead of targeting specific IP information, the objective is to stop specific protocols (figure 6). Explicit protocol types such as FTP or Telnet can be blocked for specific IP addresses within the trusted zone.

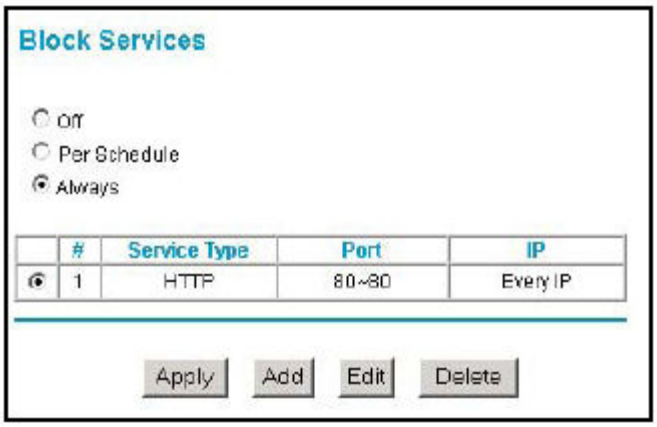

Figure 6 – Service Blocking

Circuit level firewalls can simply allow or disallow packets or can use rules of configuration to determine whether the connection between both ends is valid. Once validated, it will open a session and permit traffic only from the allowed source. The validity of a connection may be based upon:

- destination IP address and/or port
- source IP address and/or port
- time of day
- protocol
- user and/or password

Port forwarding, within some routers, uses a type of Circuit Level firewall. Forwarding sets up a specific address within the "high trust zone" that allows explicit incoming requests to be redirected (figure 7). Unless a precise port is specified by the "no trust zone" entity the session to the internal process will not be established. Port forwarding can be used to setup outside access to internal FTP, HTP or other services.

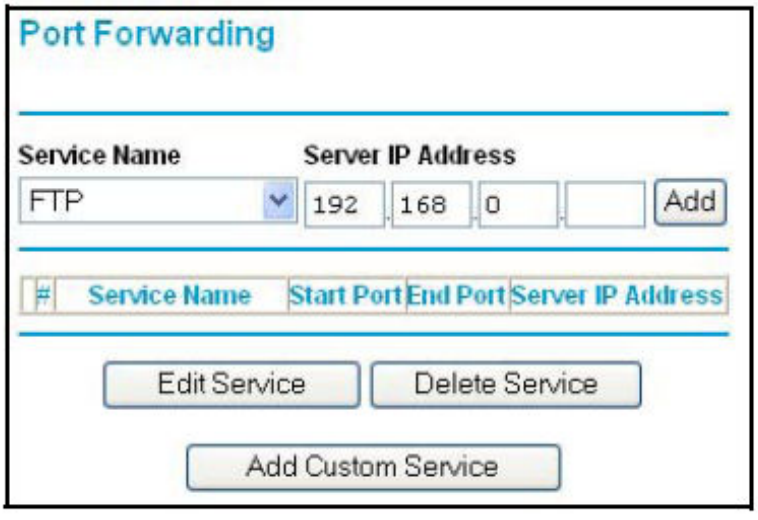

Figure 7 – Port Forwarding

Remote Management utilizes another form of the Circuit Level firewall (figure 8). Using Remote Management will allow a user or users on the Internet to configure, upgrade, and check the status of your router. This circuit level connection makes use of a source address, username and password. The IP address or address range for access can be specified with the remote management window.

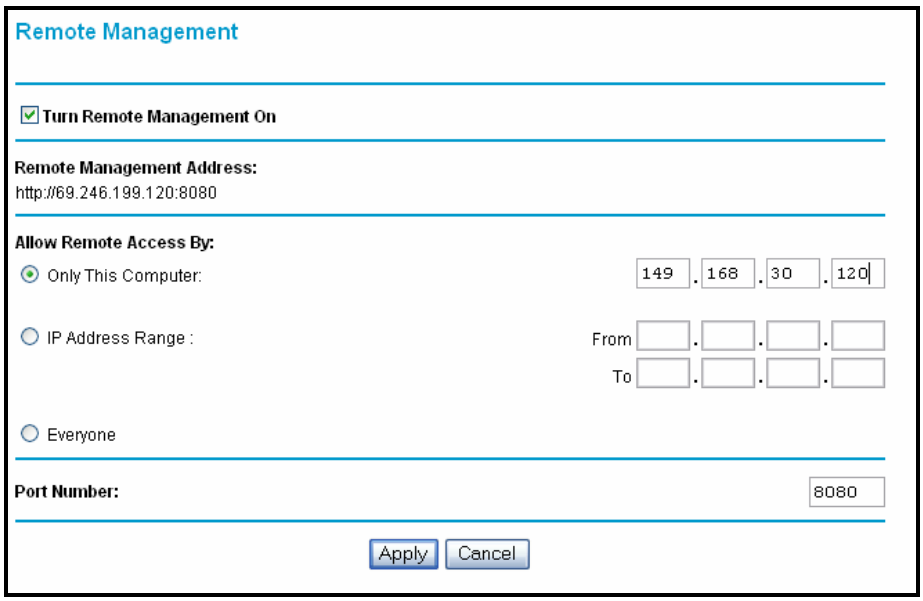

Figure 8 – Remote Management

Windows Firewall

The personal firewall is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy. A personal firewall differs from a conventional firewall in terms of scale. Personal firewalls are typically designed for use by end-users at the application layer. As a result, a personal firewall will usually protect only the computer on which it is installed.

This type of firewall works at the application layer of the TCP/IP stack, intercepting packets traveling to or from an application such as a browser. To be effective, personal firewalls must be tailored closely to the applications and the specific network environment they're protecting. Poorly configured firewalls can block legitimate users and applications or give hackers access to the system and data.

Many personal firewalls are able to control network traffic by prompting the user each time a connection is attempted and adapting security policy accordingly. Personal firewalls may also provide some level of intrusion detection, allowing the software to terminate or block connectivity where it suspects an intrusion is being attempted. These are similar to the types of controls that can be demonstrated within the Windows XP Operating System.

Windows XP when originally shipped in 2001 included a limited firewall called Internet Connection Firewall (ICF). ICF was disabled by default because of backward compatibility

issues, and the fact that it was stored away in a remote location within network configuration. It was rarely used. The Blaster worm and Sasser worms in 2003 attacked a large number of Windows machines, taking advantage of flaws in the RPC Windows service. Because of these incidents, Microsoft decided to significantly improve both the functionality and the interface of Windows XP's built-in firewall. They repackaged ICF simply as the "Windows Firewall".

The Windows firewall, turned on by default in service pack 2 or higher, can be accessed via the administrator account on any Windows XP or Vista machine. The firewall, once initiated, will block all outside sources from connecting to the computer, unless explicitly expressed (figure 9).

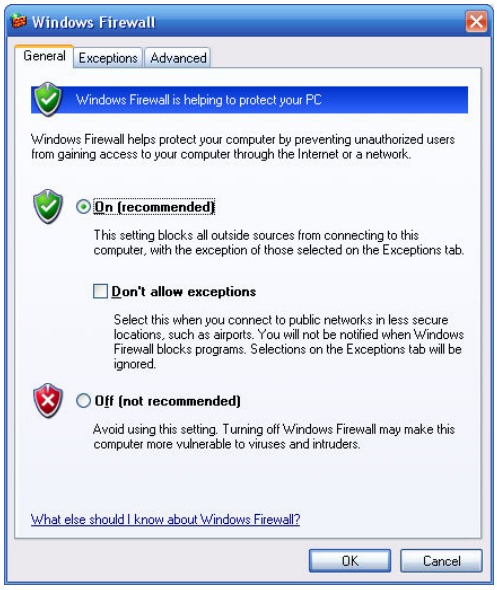

Figure 9 – Windows Firewall

The “Exceptions” list on the firewall shows allowable applications that can transverse the firewall through their appropriate I/O ports (figure 10). These explicit changes to the firewall can have direct adverse affect upon system security based on what applications you give access.

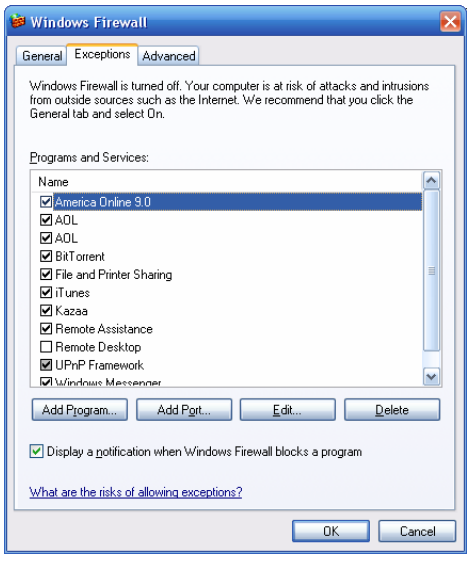

Figure 10 – Firewall Exceptions

The firewall exceptions can be added via two different implementations. The first implementation allows for the addition of an application to the "Exception" list by selecting "Add Program". This method gives control to the chosen application, allowing it to access I/O ports as needed. The second implementation, designed for more savvy users, allows you to open specified ports to specific protocols (figure 11). Selecting the "Advanced" tab on the firewall allows for the selection of specific services running on the network that the users can access (figure 12). This allows for the tightening of security by prohibiting user access to known faulty services, such as FTP and Telnet.

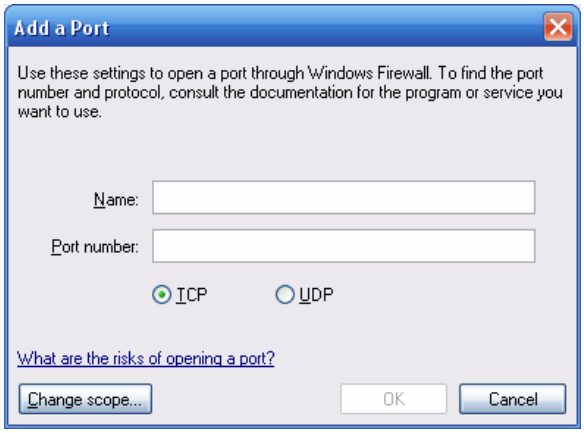

Figure 11 – Opening a Port

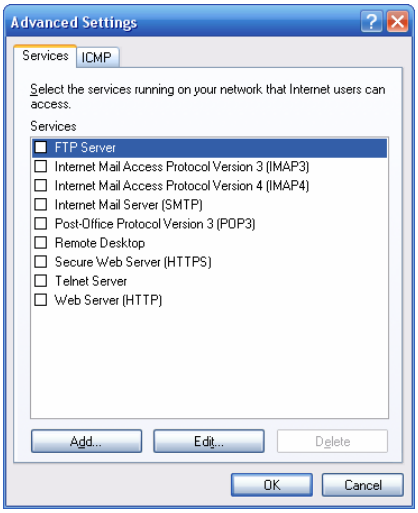

Figure 12 – Firewall Services

One final refinement that can be demonstrated on a personal firewall is the use of Scope (figure 13). A Scope is the range of valid values, in this case the range IP addresses or subnets. For any given exception, a scope of valid IP addresses or subnets can be assigned for computer for which this port or application in unblocked.

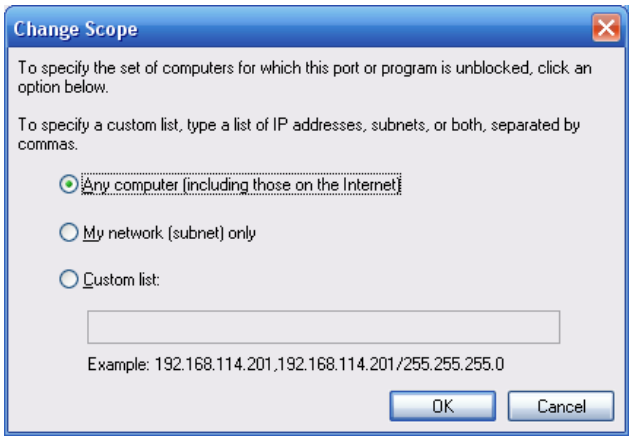

Figure 13 – Scope

Conclusion

Security students, many whom personally own these types of communication devices discussed in this paper, can now connect the principles of home security to those of corporate or large scale network security. They now recognize good security practice and can implement this gained knowledge into their own life.

Furthermore the cost of large scale, costly security equipment can be replaced and the student can even practice at home. Having such a wide variety of routers might seem to complicate instruction, but to the contrary, a variety of routers gives the student an opportunity to see multiple technology types. The student isn't asked just to perform basic tasks but is challenged to discover variations in the styles of routers found. This reinforces their need for lifelong learning.

1. Retrieved October 15th, 2007 from http://www.comcast.com/Support/Corp1/
2. "Applied Data Communications" 4th editions, by James E. Goldman and Phillip T. Rawles, Wiley, 2004
3. "Broadband is to this Decade What Cable TV was to the 1980s, Says In-Stat/MDR", In-Stat/MDR, October 21, 2004
4. "Worldwide Router Market to Grow to $9.2 Billion by 2008", Dell'Oro Group, August 2, 2004.
5. "The Home Network Owner 2004, A Survey of Current and Future Home Network Owners", In-Stat/MDR, May 2004
6. "The Internet Gets Serious: Security, Copyright Problems Must Be Resolved as the Medium Matures" By Jonathan Krim, Washington Post, June 19, 2002; Page H01
7. Retrieved December 2nd, 2006 from http://en.wikipedia.org/wiki/Firewall
8. Retrieved December 15th, 2006 http://www.vicomsoft.com/knowledge/