Global Information Assurance Certification Paper

Protecting Confidential Data and System Integrity while Allowing Reasonable Functionality to the Internet – A Families Point of View

Timothy Seigler
GIAC Version 1.2e
June 3, 2001

Introduction

The idea that no one can hack into my computer because I have a slow modem connection or that I only connect to the Internet when I am surfing or sending e-mail is an out of date and naive way of thinking about personal computer security. The threat to the security and integrity of personal computers goes far beyond some one trying to hack into my personal computer or my son downloading a word virus. With the introduction of affordable high speed connects to the Internet, new sophisticated viruses & Trojan horses, script kitties, web bugs, well educated and equipped hackers and many other threats to my family's home computer is becoming part of every day life.

Many owners of personal computers like myself install and use software packages like Microsoft Money and Quicken to manage household budgets, investments, bank accounts, loans, credit card accounts and many other highly personal and sanative types of data. Others depend on the Internet for their lively hood. Protecting your home computer from Internet threats has become an everyday concern.

The integration of the Internet into my family's daily life has reached a level I never dreamed of two years ago. My family's use of the Internet include but not limited to keeping in daily touch with other family members, checking cable listings, see what is showing on the theaters complete with show times and pricing, phone number and driving directions to a new department or moving money from our savings account to the checking.

The reason for this paper is to discuss one families concerns and possible solution to a question that many families may now be asking. How do I protect my family's personal data, integrity and availability of our personal computer and still insure reasonable functionality and access to the Internet?

First Things First – Defining the Objectives

Before I can answer the apposing question I first needed to ask several other questions before purposing and testing a solution that would accomplish my objectives. So what were my objectives?

- To protect my family's personal data from threats on the Internet
- To protect the integrity and availability of the family computer
- Continue to allow reasonable access to the Internet without loosing major functionality or performance
- To insure that if a threat does create a problem on the family's computer I can quickly and easily recover and restore access to the Internet

- To keep the impact of changes to the family's computing environment as transparent to my family as possible
- To accomplish my objectives using as much pre-owned hardware and free software as reasonably possible

Firewall in a Nutshell

The question of whether I need a personal firewall to protect my family's computer from threats on the Internet is pretty clear so the first thing a needed to do was find out more about firewalls and personal intrusion detection software.

According to an article on http://www.interhack.net/pubs/fwfaq a firewall is a system or group of systems that enforces an access control policy between two networks. This is about the simplest definition of a firewall I could find. So what are some different types of firewall?

- **Packet filtering** – Packet filtering route packets between internal and external hosts, but they do it selectively. They allow or block certain types of packets in a way that reflects a site's own security policy.
- **Proxy service** – A proxy is something or someone who does something on somebody else's behalf. Proxy services are specialized application or server programs that take users requests from Internet services and forward them to the actual service. Proxy services sit between a user on one side of a network and a service on the other side. Instead of talking to each other directory, each talks to a proxy.
- **Stateful inspection** - A newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded.

Packet Filtering

Some advantages of packet filtering

- One router can protect an entire network
- Extremely efficient
- Widely available hardware and software solutions

Some disadvantages of Packet Filtering:

- Packet filtering rules tend to be hard to configure
- Packet filtering capabilities of many products are incomplete
- A broken or bad implementation may allow packets that should have been denied
- Cannot enforce restrictions on particular users
- Reduced router performance

Proxy Services

Some advantages Proxy Services:

- Good at logging transferred data
- Can do intelligent filtering (Examples: HTTP filtering – removing Java or JavaScript, Virus detection)
- Cashing may provide increase performance
- User-level authentication
- Protection from weak IP implementations

Some disadvantages of Proxy Services:

- May require modifications to applications or procedures
- May require different servers for each service
- Proxy services lag behind nonproxied services

Choosing a firewall

After evaluating the way my family uses the Internet I decided that a dual-homed host (computer system that has at least two network interfaces) with proxy services offered the best protection from intruders and gave me the most flexibility and functionality.

Another reason I decided on proxy services is because I already had an older personal computer well equipped to host proxy services at no additional cost. With the ability to log transferred data I would be able to track what sites my family is going to and block sites or protocols deemed unsuitable or too dangerous for my family to visit.

My choice for an Operating System was Linux Redhat 7.1. Redhat 7.1 is not only free software but also has a built in firewall, which can be configured during installation along with proxy services. Linux runs very efficiently on older PCs so I did not have to upgrade any existing hardware. This meets one of my objects regarding free software and existing hardware.

Another objective was to have as little impact as possible to the current computing environment my family has grown accustom to. Proxy services installed on a dual-homed host will be virtually transparent to my family with very few exceptions.

Figure 5-2. Using proxy services with a dual-homed host

Intrusion Detection Software

Now that I have a dual-homed host configured with proxy services how do I protect this new computer from the same threats it was configured to protect aginst?

When I installed Linux Redhat 7.1 on my dual-homed host computer, I configured a default firewall now available as part of Redhat's installation process. I also went to http://www.redhat.com and downloaded any patches not currently part of Redhat's 7.1 default installation. The only services I configured were the proxy services, default firewall and networking. All other services like FTP and Send Mail were not configured.

I wanted to log activity like stealth port scans, CGI attacks, fingerprinting attempts or any other attacks that may be launched against my new proxy server. I started looking for a personal *Intrusion Detection* product that would help me log and analyze unwanted attacks against my firewall. I downloaded a free software product from http://www.snort.org/ called **Snort.** Snort was in my price range and advertised the type of capabilities I was looking to protect my new proxy server.

> Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plugin architecture. Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or WinPopup messages to Windows clients using Samba's smbclient.
>
> Snort has three primary uses. It can be used as a straight packet sniffer like tcpdump(1), a packet logger (useful for network traffic debugging, etc), or as a full blown network intrusion detection system.
>
> Snort logs packets in either tcpdump(1) binary format or in Snort's decoded ASCII format to logging directories that are named based on the IP address of the "foreign" host

Protection of Personal Data

I decided before I ever build a firewall that I would still treat any private and sensitive data on my personal computer as if other people may be able to see my hard drive. I also wanted to update my disaster recovery plan to reflect any changes that the firewall may have made to my computing environment.

Removable Media
I evaluated what data I didn't want other people to see and data I didn't want to loose in case of a desaster and moved **all data** from my local hard drive to removable media. The idea was the

ability to put personal and sanative data now only existing on removable media into the computer when and only when disconnect from the Internet. I already had a 1gig internal Jaz drive and ample Jaz media so cost was not a factor. Pointing default file locations to the Jaz drive letter turned out to be pretty simple task and did not seem to upset the way my family was using the computer. Labeling the Jaz Media was also a key part of this process.

The last step to this process was to make duplicate copies of all the jaz media, well label the Jaz drives and put the duplicate copies and the more sensitive data in a locked cabnet.

Maintaining System Integrity

Backing Up the Data
Now that I had all the family's important data stored on removable media I though about the piles of tapes I had been accumulating from backing up my hard drive faithfully every week, fighting old and stretch tapes, trying to restore files that were open or misplace, and dreading the day I would be forced to test the recovery of an entire hard drive from tape. The time it was taking to backup and restore from tape media was a very time consuming and tedious task often lead to putting off backups until it was convenient.

Now that all of my important data had been transferred to removable media, I realized that major changes to the operating system would not happen very often. This would also hold true for the Dual-Homed host acting as my firewall. I decided that backing up my two computers once a month was more the adequate. I also wanted a quicker and more reliable way to restore if I had a disaster so I started looking around for a better way to back my systems. The solution was to spend a little bit of the family budget and purchase a product called Norton Ghost 2001.

Norton Ghost 2001 gives me the ability to make a copy of an entire hard drive in a matter of minutes. Norton creates a single compressed image file small enough to fit on a jaz. This makes storing and protecting backups very simple and convenient. I have tested backing up and fully restoring hard drives on Windows 2000 as well as Linux Redhat 7.1. Norton Ghost is only one of many ways to backup and restore data but proved to be an essential tool for maintaining integrity of my personal computers.

Patches and Hot fixes
Staying on top patches and hot fixes can be both time consuming and dangerous. When a patch becomes available rushing to be the first person to install this fix may actually cause more damage then it fixes. When down loading and applying patches and hot fixes I have learned to only apply the ones required to fix a bug or curtail a vulnerability. A little research will answer any question you have about a new patch or hot fix. I make it a practice to visit http://www.redhat.com and http://www.microsoft.com about once a month to read up on any new updates. Keeping up with patches and hot fixes is a good way to stop unwanted attacks.

Check the Log Files
Analyzing the log files create by a firewall or proxy service can be a very time consuming task. Trying to understand what is in a log file can also be frustrating. It takes a little practice but

analyzing log files is the only way to tell who is trying to compromise my systems. The attacks being logged on my firewall have become a daily occurrence and are growing every day.

Virus Program
A good virus program has now become about as common on personal computers as the browser used to surf the Internet. Most people these days see a virus detection program as one of the most important applications on their computer for maintain system integrity. I will be the first to agree with this philosophy but only if data definitions are kept current. Too many people assume that their virus software is working when the data definitions are too out of date to catch the latest virus or script that may already be waiting in an e-mail. **Virus Definitions need to be update every two or three weeks**. This is vital to maintaining the integrity of any computer system with access to the Internet or not.

Educating My Family About Internet Security

The last and what I feel is the most important piece to protecting personal data and the integrity of my family's computing environment is education. With the changes I had made to the family's computing environment my family had to make a few changes in the way they used the computer. Below is the list of changes I felt were essential to the protection and integrity of our computer.

- Physically connect the cable modem to the firewall when access to the Internet is required and always disconnect the firewall when not access the Internet
- Never put removable media into the computers while access to the Internet is available
- Lock up **ANY** removable Media when not in use
- Never install or open any file that was download from the Internet including e-mail attachments
- Turn off the computer if you see anything that looks suspicious

After about two weeks I was able to take the sticky off of the monitor. These changes did not seem to cause any problems with the way my family currently used the Internet.

Conclusion

With the low cost of high speed connects to the Internet and the increasing numbers people using the Internet, home computers are quickly becoming a target of all kinds of attack designed to intrude, deny or destroy system integrity. Protecting your personal computer is going to become increasing important as attacks increase and become more sophisticated. Protecting your family's access to the Internet and the integrity of your home computer my start to clash some time in the future. Protecting the integrity of your home computer and giving your family access to the Internet is something that more families are going to be confronting some time in the future.

References

Elizabeth D. Zwichky, Simon Cooper, & Brent D. Chapman. Building Internet Firewalls.

Sebastopol, CA: O'Reilly & Associates, Inc., June 2000.

Firewall and Proxy Server HOWTO
Mark Grennan
v0.80, Feb. 26, 2000
http://www.linuxdoc.org/HOWTO/Firewall-HOWTO.html

Internet Firewalls: Frequently Asked Questions
Matt Curtin, Marcus J. Ranum
Revision: 10.0 Dec, 01, 2000
http://www.interhack.net/pubs/fwfaq/

Joel Scambray, Stuart Mcclure, George Kurtz. Hacking Exposed: Network Security Secrets & Solutions Second Edition, Obsbom/McGraw-Hill 2001

Marshall Brain's, How Stuff Works
Jeff Tyson
http://www.howstuffworks.com/firewall4.htm

Stephan Northcutt, Judy Novak, Donald McLachlan. Network Intrusion Detection An Analyst's Handbook Second Edition. New Riders, September, 2000

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event