Global Information Assurance Certification Paper

DSL (Defending Someone's Lair) in the 'Always-On' World of High-Speed Internet from the Home
Mark Johnston
October 11, 2000

As a technology professional for a Fortune telecommunications company, I routinely hear all the ranting and raving when people get high-speed DSL installed in their home. They talk all day about their new toy and how fast they could download this, that, the other thing, and a few things I won't mention here. What I rarely hear is any concern or even recognition of the potential risk their new high-speed connection exposes them to. Most have probably never even heard of a personal firewall, and probably all aspire to the theory that hacking only happens to the military, government, and NASA.

Well, they're wrong and this paper is for those who would like to know why and how to mitigate the risk in the always-on world of DSL and cable modems. The bad news is that your home computer is now no longer safe with just a good anti-viral software package. Now folks, that doesn't mean you don't need anti-virus anymore so make sure you continue to keep it current. The good news is there are several products out there to help protect you from all the "hackers" and "script kiddies" probing and scanning the internet intent on electronically "breaking and entering" your home computer system and pilfering through your personal and professional information.

So, why are you at greater risk now? Well, first of all when we say "always-on" we mean just that. Unless you turn your computer off or disconnect your DSL or cable modem connection, your computer is now exposed in cyber-world with the same potential for being scanned and attacked as the corporations, military, and government organization's who spend millions protecting their systems.

But why would they break into my computer when they could break into a bank or some credit card company? Well, some might actually do that but consider the concept of "the path of least resistance". Criminals and hackers are going to seek out the path of least resistance to accomplish their objectives. If a criminal is doing surveillance in a neighborhood for a home to burglarize, they are most likely to pass on the one with the growling German Shepherd just inside the door and will opt for a home without a large menacing canine. If a hacker is intent on using his skills for financial gain, why invest the time and risk taking on the security of a bank or credit card company. Instead, they could hack into 20 or 30 unprotected and unmonitored "always-on" home computers and walk away with 50 to 100 credit card numbers. Viola'.

So, now we're thinking in terms of personal firewalls as the menacing canine for the always-on home computer. Good. You might also find it interesting that many of the attempts to compromise your computer will not be made by some shady figure in a dark room tapping on a keyboard, but by things like bots, spiders, lions, tigers, and bears. Oh my! Sorry, just kidding about the lions, tigers, and bears thing I got carried away. Seriously, bots and spiders are basically automated scripts for probing, scanning, and attacking computer systems. BOTS, short for ROBOTS, are scripts or programs for scanning and launching attacks in an automated manner. Spiders are also automated programs but don't launch attacks. They seek out specific vulnerabilities on specific types of systems logging them for a future assault. Not a list you want to be on. Once they have accomplished their mission they will somehow notify the shady character in the dark room by sending an e-mail reporting the results of the attacks or scans.

Okay, so I'm at risk what can I do about it? Well, there are quite a few products out there that can help us mitigate this risk. We going to take a brief look at three of them. They are NetworkICE's BlackICE Defender, Norton's Personal Firewall, and McAfee's Personal Firewall. So let's a look at each of these products. By the way, I'll refer to BlackeICE Defender, Norton Person Firewall, and McAffe's Personal Firewall as BID, NPF, and MFP respectively many times during the course of this document.

BlackICE Defender from NetworkICE is more that just a personal firewall http://www.networkice.com/html/blackice_defender1.html). It's both a firewall and an IDS or intrusion detection system. For the non-technical folks in the audience, that basically means that you can block or filter traffic to and from your computer (the firewall), as well as, monitor, detect, log, analyze, and report on suspicious activity or outright attacks on your system (the IDS). So let's take a look at some of the key components of BID.

One of the features I consider extremely important not only for the user, but for the proliferation of improving and encouraging security is the preset configuration and ease of installation of BID. By making the product work "out of the box" the user will benefit from a baseline configuration and immediate protection after installation. This feature will encourage more non-technical interneters to consider using security products beyond the traditional anti-virus software that is probably not current on their system anyway. BID is customizable for the more technical folks who want to tune their configuration to their liking.

Some of the more technical features of BID include the full-blown firewall and IDS that scans inbound and outbound traffic automatically calling upon the firewall to block a source when it detects anamolous activity. Alerts are simplified by color coding to warn you of the severity of an attack. A feature called advICE provides documentation on attacks that BID identifies and you can also enable audible alarming if you so choose. If the anomalous activity turns out to be an attack on your system, BID includes evidence logging of hacker or malicious code activity, as well as, back-track and identification features to track the hacker back to his lair. I found an excellent guide to protecting your home computer on NetworkICE's web site. It's entitled "Network ICE Guide to Home Protection" and can be found at http://www.networkice.com/html/networkice_guide.html. If you're a non-technical person interested in this subject, I encourage you to take a few minutes to read it. It should be very enlightening and it outlines in general terms what hackers do, how they do it, how to stop them, and why your home computer is now fair game. There's also another good article on why firewalls need intrusion detection you might consider reviewing at http://www.networkice.com/Docs/Firewalls%20Need%20IDS1.0.pdf.

You'll need Adobe Acrobat or a PDF viewer to read it. BID retails for $39.95, which isn't too bad considering the sensitive information that many of us are keeping on our home computer system.

BlackICE Defender doesn't have a monopoly here. McAfee who is well known for their anti-viral products also offers a personal firewall product. McAfee actually acquired the product from Signal 9 Solutions ConSeal Private Desktop and the URL for MPF is http://www.mcafee.com/myapps/firewall/ov_firewall.asp. The current version of McAfee.com Personal Firewall is pretty much a mirror image of the ConSeal product at this time. Basically, there is little user interaction required as the product starts up and runs minimized. If your computer invokes an Internet application, a window pops up asking you to confirm that the application can proceed through the firewall. It then builds rules into the firewall based upon your Internet applications and usage. It monitors inbound and outbound traffic, but the logs are apparently cryptic for anyone not familiar with packet data. One major drawback is that you do not have the option of filtering a specific address or list of IP addresses. It does however allow you to permit or deny traffic by application. It does not appear to have the IDS capabilities of BID, which I would prefer to have but looks like it will do the job and is competitively priced with BID.

Lastly, let's take a look at Symantec Corp's Norton Personal Firewall. The URL for NPR is http://www.symantec.com/sabu/nis/npf/. Several things caught my eye here. The first was a rule assistant or wizard. The wizard helps walk you through creating new firewall rules for applications. The second was NPF's standard configuration options. Basically, you can enable one of three levels of security out of the box. They include a minimal, medium, and high security setting. The minimal setting will allow all Internet traffic to pass unless a specific rule prohibits it. The converse of the minimal default is the medium setting, which prohibits all Internet traffic unless some specific rule allows it. I think novice users will like having those two options. Lastly, the high setting is very interactive with the product prompting the user for permission to perform certain functions. All good stuff for the non-technical users, but what about all us technology geeks who want to tune and tweak? Well, NPF provides access to the firewall rules and they can be customized based upon protocol, port, application, inbound, outbound, etc. NPF also appears to have good logging and reporting tools for reviewing history or getting a snapshot of what's going on. Another nice feature is the LiveUpdate feature that allows you to receive updates direct from Norton for a year. Like MPF, the NPF also doesn't appear to have the IDS capability of BID. NPF retails for $49.95 which is a little more expensive than the others we've considered, but still not too bad. O, one feature I almost forgot to mention. NPF also has an additional privacy protection feature for protecting private information such as your credit card or bank account numbers and they also come with high, medium, and minimal default settings and can be customized to your liking.

This concludes my research on personal firewalls for the home. If you're a member of the "always-on" community of Internet users, I encourage you to take a look at some of these links and do some research of your own. Let me close by saying that security is something we all do everyday and think very little about. We lock our cars and homes and we keep the majority of our financial resources in institutions we consider more capable of securing them for us. Security is a discipline that is ever evolving. Twenty years ago how many homes had security systems installed in them? Well, times have changed and now most homes being built today have security systems built into them with many older homes also having them installed.

Our home computer security and thus personal information is no different; it now needs to evolve. Until viruses became prevalent, we really didn't need to do much of anything to secure our home computer but to keep it locked up in the house. With the explosion of viruses a good anti-viral program is now a must for any computer. Well, times have again changed with the availability and popularity of high-speed always-on Internet services. For those using these services for business or personal use, a personal firewall is probably not a luxury item if you keep sensitive information on your computer. Remember that a personal firewall and intrusion detection package don't guarantee that a persistent hacker won't get into your system. It does however make it more difficult and time consuming, and

if you have an intrusion detection component you have a better chance of identifying and stopping it before it's too late.

I hope that you've found this information to be educational, helpful, and useful. Most importantly, I hope this has brought security of your home computer to a new, different, and hopefully higher level of thinking and importance.

References:

NetworkICE White Papers. "Network ICE Guide to Home Protection". (No Date)
URL: http://www.networkice.com/html/networkice_guide.html (4 Oct 2000)

NetworkICE Tech Notes. "Why Personal Firewalls Need Intrusion Detection". The Importance of Intrusion Detection. (No Date)
URL: http://www.networkice.com/Docs/Firewalls%20Need%20IDS1.0.pdf (4 Oct 2000)

Leemon, Sheldon. "Norton Personal Firewall". 23 August 2000
URL: http://www.zdnet.com/computershopper/stories/reviews/0,7171,2611116,00.html (3 Oct 2000).

Leemon, Sheldon. "BlackICE Defender". 23 August 2000.
URL: http://www.zdnet.com/computershopper/stories/reviews/0,7171,2611114,00.html (3 Oct 2000).

Leemon, Sheldon. "McAfee.com Personal Firewall". 23 August 2000.
URL: http://www.zdnet.com/computershopper/stories/reviews/0,7171,2611115,00.html (3 Oct 2000).

Last Updated: May 29th, 2017

Upcoming Training

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 San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
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 Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 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 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
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
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
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event