Global Information Assurance Certification Paper

Home Security:
How to Make It Work

GSEC Practical v 1.4b
Submitted by Kevin Fournier

Last year, as businesses focused more on network security, hackers and virus writers, once satisfied to point their destructive tools at large companies, began to turn their sights to home computers that are faster, more powerful and less secure than ever before. The continued vulnerability of this segment of the Internet reveals a critical need to create and promote a system for improving home security that is different and more effective than the one currently in place.

The Problem

The number of Internet users continues to increase.
Even as we were witnessing the spectacular bust of the dot.com boom, Internet usage was rising spectacularly in all segments of individual electronic commerce and personal Internet usage. That growth trend is continuing and it is not only youth that is being served by the Internet. We are seeing growth in every gender, ethnic, and age demographic in every country worldwide as millions of users incorporate the medium into their daily routine of communicating, browsing, and shopping. The number of users on the Internet today is estimated to be over 600 million worldwide – quadruple what it was just five years ago.

The content of the Internet is changing and home computers are a more attractive target.
And these users aren't using the Internet for just for entertainment and information. Statistics show that the numbers for the 2002 holiday online shopping season increased an astounding 40 percent over the 4th quarter of 2001[1]. Almost two-thirds of Internet users have by now purchased a product or service online. That's up dramatically from 36 percent in 2000. Online banking has also experienced a significant jump – almost doubling in the last couple of years. In Canada, U.K., Germany and the U.S. more than 40 percent of Internet users have banked online[2]. This growth in the economic participation of users is a reflection of the powerful appeal and growing maturity of the Internet. And it's growing economic importance. The emphasis is no longer on building out the physical infrastructure of the Internet but has now has shifted to developing a broad array of services, finding more effective ways to market to existing users and adding new electronic customers. This increase in web services and the consumers that purchase them has made the Internet an important commercial

[1] Ecommerce, March 2003. URL:http://www.nua.ie/surveys/index.cgi?f=FS&cat_id=14
[2] Financial Services, March 2003. URL: http://www.nua.ie/surveys/index.cgi?f=FS&cat_id=4

enterprise and brings new security challenges not just for businesses as the providers of value but, equally, to users as the purchasers of value. Now it is not just business that has it's financial assets exposed to the Internet. Home users also have personal and financial information online and it makes them much more attractive targets for hackers to steal data, credit card numbers and identities.

A growing number of computers are connected directly to the Internet through high-speed DS and cable lines.
Security challenges are even more difficult because of the fact that as Internet services have increased, users are demanding a faster connection then the agonizingly slow 56k modem can provide. They are dropping dial-up connections in favor of broadband – DSL and cable modem - at an increasing rate. Studies show that the percentage of U.S. homes using broadband connections, instead of dialup, will increase from 27% to more than 70% by 2008 — 59 percent of all U.S. homes. European households are also making the conversion, with expectations that 38 percent of them will have broadband Internet services by 2008. And around the world, annual sales of 60 million units a year are predicted by 2008[3]. High bandwidth links do not only provide end users with faster download times--they also give hackers a broader target audience to attack with a wider array of tools.

This large number of powerful personal computers is left exposed because the majority of home users are negligent about securing their computers. Users don't install antivirus or firewall software. They don't plug security holes by applying the necessary fixes from software vendors. Generally, security is not comprehended by these non-technical users and their lack of attention toward protecting their systems makes home users even more susceptible to attacks than financial, government and commercial institutions who at least have professional staffs trying to make an effort. Moreover, it's not just themselves that are being put at risk. Individual users are more likely to be unwitting accomplices in exploits that can affect every other user connected to the Internet. Studies have shown that a significant number of Internet attacks originate from home PCs through broadband or cable ISPs. Infiltrated by worms and Trojans or infected with email viruses, these PCs often act as the platforms from which large scale Internet attacks are launched. Millions of novice users with always-on, always-connected, always-vulnerable broadband hookups could be used to mount an attack that would be able to paralyze most of the Internet traffic. We should not and cannot leave a threat like this unattended.

There is nothing that can be done about the first three developments. As a matter of fact, they are essential to the continued evolution of the Internet as a commercial enterprise. However, home security, or, more correctly, the lack of home security is a critical problem and something must be done to improve it.

[3] Greenspan, Robyn, "Broadband's Reach Gets Broader", Feb. 2003. URL: http://cyberatlas.internet.com/markets/broadband/article/0,,10099_1580601,00.html

Surprisingly, this is not as difficult a task as some might think. In reality, the majority of successful attacks on Internet connected systems target only a few vulnerabilities. This is because most 'hackers' are unskilled and take the easiest and most convenient route to exploit well-known flaws because that's the only thing their scripted attack tools can do. They usually attack indiscriminately, scanning the Internet on autopilot for vulnerable systems and are successful only if they find computers that are not patched or protected properly. So if users would just take the time and follow the advice of computer experts then this security problem would be solved. That advice typically contains the following three points:

1. *Awareness*. Obviously, if users don't see security as a problem they won't join in to be part of the solution. For the most part, this message is being heard. Studies show that people are concerned about their financial information being exposed and are disturbed by the thought of someone destroying their data through a virus or hacking into their computer.
2. *Education*. This is the area stressed the most and rightfully so. Detailed explanations are given about what a user should do to protect their system. The list normally includes the following:
    - Install and use an anti-virus program
    - Keep your system patched
    - Don't open unknown email with attachments
    - Install and use a firewall program
    - Make backups of important files and folders
    - Use strong passwords
    - Download and install programs cautiously
3. *Action*. Users are strongly urged to act on the above suggestions. Nothing is accomplished if the firewall, antivirus, etc. is not installed. Awareness and education alone accomplish nothing.

At first glance, these suggestions seem reasonable and would solve most of the security problems facing the home user. And yet, making the Internet safer has proved to be elusive. So you have to ask yourself, " Why aren't we any closer to a secure Internet?". The answer is obvious. Users have not and will not take the time to implement even these reasonable precautions.

Let me share a personal experience that was very enlightening to me concerning this issue. Last year, I gave a series of home security seminars to parents in my community. I live in a middle class suburban area and the people are generally well educated. Those that attended the meetings were very concerned about protecting their computers and the information it contained. They were inquisitive about finding ways to prevent attacks against their systems and I spent a good deal of the seminar explaining the threats and how to prevent them. I even took one of the more popular anti-virus/firewall products on the market went through a detailed step-by-step presentation on how to install, configure and update all of

its features. I talked as plainly as possible and purposely avoided technical terms and jargon. However, in the Question & Answer period at the end of the seminars, the tone and type of questions asked by the parents revealed a total lack of conviction about what to do about security, a lack of confidence about how to do it and a lack of certainty about doing it at all. After giving these talks, it became obvious to me that while home users recognize the need for security, they want the problem to be dealt with rather then dealing with it themselves.

On the surface, it doesn't seem that home users are being asked to do that much. There is no sophisticated operating system, no infrastructure, no database, network protocols or web software to protect. With just a little bit of time and effort, following the clear instructions provided through different media, the home PC could be made secure and, along with it, a big part of the Internet. But while configuring antivirus software might seem simple to a computer professional, it is a daunting and frustrating task to the average user who uses his computer as a tool. It's surprising to me that our expectations are set so high. We don't expect this level of involvement in any other area of people's lives. People don't fix their own cars. They don't repair their household appliances. They use them for the purpose they are intended and if they don't work, there is a support system in place where they can be fixed. This support system isn't a website or a manual telling them how to fix it yourself. Someone is actually there to do the job for them. We don't expect people to become experts in all areas of their lives. Why should computers be the exception? There is also the problem of maintenance. Computer security is dynamic not static and requires constant attention. If you put a lock on your front door, you'll be protected for years without ever having to do anything else because the tactics of a burglar never change. If you install a firewall on your computer and leave it alone, in a few months it will have become useless. New vulnerabilities will have been discovered and exploits developed that will turn your firewall into a welcome mat.

Something else to consider is the sheer numbers involved. With the world Internet population estimated to be 600 million people, we can't reasonably expect them all to effectively police their own computers. And yet, even if only a small fraction leave their computers exposed, that would create millions of vulnerable targets. These numbers are will only increase and the situation will get even worse as technology taps into markets in lesser developed countries and penetrates existing markets in developed countries more deeply. These new users will be even less technically motivated then the old ones and security concerns will rise to dramatic new levels. It will probably be many years before this becomes a reality but it's wiser to put a system in place that can deal with the problem now and be applicable in the future as well. An integral part of any effective system must be the recognition of the general public's inability to handle their own security. This change of attitude is the first step in making a fundamental change toward a resolution of the problem of Home Security.

If the present approach is failing then what can we do that would work better? If we look to the changing business network security model we'll find three components that could be used to create a system that could be effective, consistent and scalable over the long term.

In the business community, there are Network and System Administrators whose job it is to recognize security threats and put in place the means to deflect them. They are aware that security is a problem. They have access to information – mountains of it - to help them deal with it. Usually, they have had training and education in dealing with security issues. But even these professionals have failed to keep to keep current with the avalanche of security alerts and patches. A stunning example of this is the recent SQLSlammer Worm that exploded across the Internet in January of 2003. Within 10 minutes, the Worm had infected more than 90% of the vulnerable hosts around the world. It's exponential replication and propagation overloaded the capacity of large parts of the Internet, disabling networks and database servers. After one day an estimated 75,000 computers had been infected worldwide. Was this a newly created sophisticated attack against a previously unknown vulnerability? No. As a matter of fact, the worm exploited a known vulnerability that was first discovered in July 2002. And a patch had been available for months. It's clear that even professionals left to their own devices cannot cope with the demands of maintaining a secure network environment. It is a human failure not a technical one and the solution is to put a process in place to help deal with the enormity of the task.

As any administrator knows, security solutions that rely on manual installations or that require frequent physical patching require huge amounts of time to be effective. From 1999 to 2001, the number of newly published vulnerabilities increased from about 400 to more than 2,400[4]. The number of patches and hot fixes grew at roughly the same rate. In the meantime, Web site defacements, corruption and loss of data due to network penetrations, denial-of-service attacks, viruses and Trojans continue at a constant rate. Facing this reality, network professionals are demanding that software vendors and developers become more aware of security concerns and that this awareness be translated into solutions that would bring efficiencies to creating and managing a secure environment. The clamor is bringing about some much needed change. Security has become a buzzword in the industry and software companies are bringing to market applications and utilities that integrate and simplify security jobs. Other vendors are developing centrally managed security systems that can collect, organize and interpret all manner of network log information. For companies that lack the in-house staff, corporate security can be outsourced to firms that will monitor and manage systems remotely. Even Microsoft, afraid that its indifference to security would result in a loss of market share for its web initiative and server software, came out with its Trustworthy Computing Initiative and has developed utilities such as Windows Update, Baseline Security Analyzer, and

4

Software Upgrade Server to help analyze and automate the patching and upgrading of computer systems.

Recognizing the need to put a process in place to compensate for the failed human element, businesses are embracing a move toward systems that emphasize the implementation of an automated or managed security model. Since the root cause of home security problems is also the human factor, a similar process – an automated, centrally managed system – could be applied as a solution there as well.

Here are some examples of the possible methodologies:

D_WARD: In a paper released by the Computer Science Department at UCLA, a security model called D_WARD is described which suggests that security is more effective if it is implemented closer to the source rather than the destination. In this plan, deployment is on source network routers at Internet gateway points. Incoming and outgoing traffic to and from the end user and the Internet is monitored and compared against predefined models of normal traffic to and from that source. Any discrepancy between the current traffic and historical traffic pattern is classified as a potential attack. The source router applies algorithms to distinguish between 'good' and 'bad' traffic flow and will stop the attack while letting legitimate data through. The important point to note, for the purposes of this paper, is that security is taken out of the hands of the end users.

The diagram below shows a schema of this model.

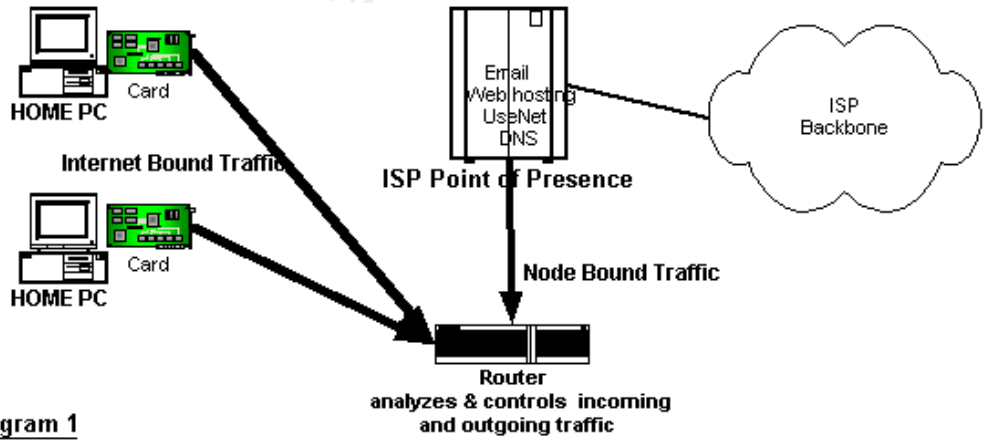

Diagram 1

Network-1 Security Solutions: This company has developed an application that installs security policies to the individual users computer to stop attacks at the

point of origin. In this 'distributed firewall' approach, a preconfigured firewall is pushed out to a host machine connected inside a local area network or outside on the Internet. The product combines a packet filtering firewall, full stateful inspection, and integrated intrusion prevention. When installed on a machine, the software will protect the network from the host, and also protect the host from the network. The product blocks exploits that attempt to take advantage of operating system vulnerabilities, such as port scans looking for open services and DDoS attacks. Since the software filters all outgoing traffic, the user's machine can't be used as a launch pad for attacks by running malicious code such as a Trojan. The user is protected whether the source of attack is from inside or outside. A security administrator uses tools from a central console to manage policies and events. Configuration, installation, administration and maintenance are all transparent to the owner of the host computer.

Check Point: In yet another example, Check Point Software Technologies Ltd., makers of the Check Point Firewall, recognized that network administrators needed to connect, protect and manage increasingly large numbers of remote client systems - laptops, PDAs, home computers, etc. - linked back to the corporate environment with remote devices over VPN. To solve the problem they added a secure client that includes a personal firewall that restricts access to the remote machine to prevent a backdoor attack into the company network. This firewall component is centrally controlled and managed, allowing rules to be added or deleted to as needed strengthen the restrictions on the remote desktop. There is a commonality to all of these methods – they are centrally administered, offer individualized security and require little or no intervention on the part of the managed user.

The diagram below shows a schema of this model.

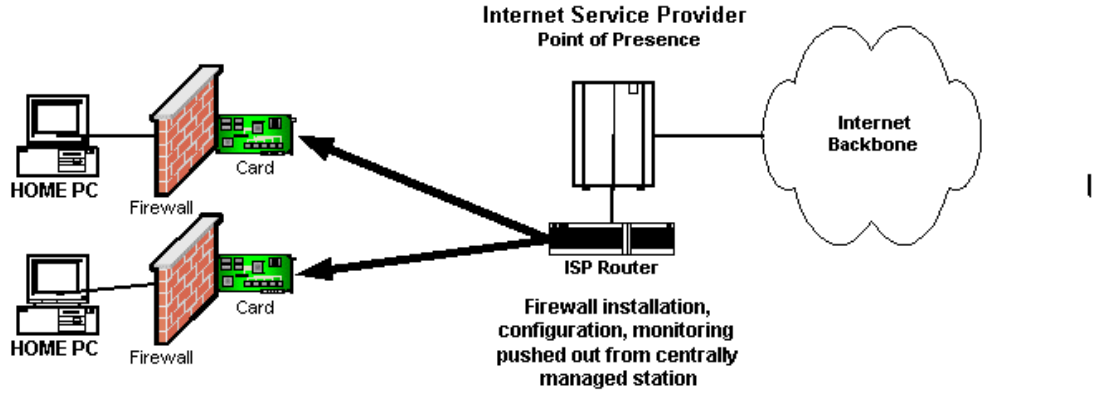

Diagram 2

In the system I'm suggesting, the user no longer has the responsibility of implementing and maintaining home security and the methodologies above can be adapted to take over that job transparently from remote locations.

The last element in the plan is finding an entity that has the skills, incentive and resources necessary to create and administrate the process. Given the physical and business structure of the Internet, there is one obvious candidate for the job – the Internet Service Provider. They are uniquely positioned to handle this job because they are the gatekeepers to the Internet. They provide the physical point of access for their subscribers and all traffic must go through their infrastructure. This being the case, they could implement security on a gateway router and filter packets going into and out from their network. Or they could push out security to their subscribers as in the 'distributed firewall' model. They also have the technical support staff that is qualified to install and manage such a system.

From a business perspective, it is the ISP that already has a captive relationship with the home user - a relationship that could be leveraged in a marketing campaign to promote managed security as a value added service. In addition, competitive pressure has already pushed most of the Internet Service Providers into the security business. Researching the top 10 broadband ISP's in the United States shows that most of them offer email and limited web hosting services to their subscribers. Since they control these functions, they are compelled to make them secure and so they are forced to provide firewall protection for the web servers and filter the subscriber's email through antivirus and antispamming software. Earthlink, Yahoo! And Cox Communications have moved even further into security. They each are selling a service called 'Home Networking' that follows the D-WALL model that was described earlier where firewall is configured on a source network router allowing safe communications between the subscriber and the Internet.

Conclusion:

The current lack of home security is a serious and growing problem that must be solved to preserve the integrity of the Internet and foster it's growth. The first step in moving toward a solution is to recognize that the responsibility of home computer security needs to be taken out of hands of the end user and given to more skilled and attentive people. It is obvious that the current expectation that home users bear the responsibility of personally maintaining the security of their home system is unrealistic and unproductive. Effective technologies exist that can remotely install, configure and manage the home users PC. Using these technologies, Internet Service Providers can assume the role of security administrators of the Internet and provide and manage essential security services for their subscribers. By taking over this responsibility, ISP's would have control over the integrity of the traffic originating from their networks and the number of vulnerable points on the Internet would drop from hundreds of millions to tens of thousands. Security problems would not disappear but the Internet would be a safer place and a more pleasant experience.

LIST OF REFERENCES:

Moore, David, et al. “The Spread of the Sapphire/Slammer Worm” Feb. 2003.
URL: http://www.caida.org/outreach/papers/2003/sapphire/.

Matrix NetSystems. Event Advisories, January 2003.
URL: http://www.matrixnetsystems.com/ea/2003/20030130.jsp#Item2.

Cox, Beth. “E-Commerce as a Way of Life”, February 2003
URL: http://www.internetnews.com/ec-news/article.php/1583721.

King, Peter. “Residential Broadband Modems and Gateways:Global Market Forecast”, December 2002.
URL: http://www.strategyanalytics.com/cgi-bin/greports.cgi?rid=172002120621.

“Continuing Threats to Home Security”, CERT Advisory CA-2001-20.
URL: http://www.cert.org/advisories/CA-2001-20.html.

The World Fact Book, 2002.
URL: http://www.cia.gov/cia/publications/factbook/.

World IT Report, February 21, 2003.
URL:http://www.worlditreport.com/main/index.ie.php3?sid=93619&lang=e&dir=home,

J. Mirkovic, et al. “Attacking DDoS at the Source”, Proceedings of ICNP 2002, Paris, France, November 2002.
URL: http://www.lasr.cs.ucla.edu/ddos/.

Morrissey, Brian, “Yahoo! Plans Bundled Services”, Internet Advertising Report, February 13, 2003
URL: http://boston.internet.com/news/article.php/1583711.

Barry, David. “Service Provider Solutions”, Packet, First Quarter 2003.

Tippett, Peter. “Myths of Infosecurity”, Information Security, Nov. 2002,
URL: http://www.infosecuritymag.com/2002/nov/executiveview.shtml.

Fusco, Patricia. “Top U.S. ISPs by Subscriber– First Quarter of 2002”. May, 2002.

URL: http://www.isp-planet.com/research/rankings/usa_history_q12002.html.

Simonis, Drew, et al. CheckPoint NG: Next Generation Security Administration. Massachusetts: Syngress, 2002.

Last Updated: July 25th, 2017

Upcoming Training

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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS