Global Information Assurance Certification Paper

User Security and The Internet Service Provider

In August 2000, the U.S. Census Bureau reported on the increasing importance of computers in the American home. Fifty-one percent of U.S. households own a computer, and forty-one percent of households had Internet access (US Census Bureau, 2000). However, many of these home users are unaware of the risks associated with unsecured Internet service. These risks have severe consequences. For example, thousands of home PC's could be a part of a denial of service attack. On a much more drastic scale, an identity thief could possibly search the contents of the home user's hard drive, looking for social security, credit card, or bank account numbers entered into financial software or home budgets. The thief could also obtain the username and password needed for Internet access. With this information the theif could actually break into the Internet Service Provider's (ISP) server, opening up the account information of many users. The availability of broadband Internet access and many home computers running unsecured operating systems provides further fuel to the potential Internet firestorm.

It is often assumed that it is the user's responsibility to maintain security for their own machines. However, it is unlikely that most home users will have the technical expertise to properly patch or upgrade operating systems and software, update antivirus programs, and install hardware or software firewalls. It is in the area of technical security expertise that ISPs have a responsibility to their customers.

In order to agree with the statement that the Internet Service Provider is in a prime position to advance security measures for home users, one must look at the other options. Since September 11, the government has become increasingly interested in issues such as cyberterrorism, and as a result new legislation that effects the Internet has been discussed. However, the individuals trying to draft new legislation to require home computers to be secure are faced with two problems. Operating systems that were designed when the Internet was in its infancy only have security components that were added as the need arrived. This means that even a computer that was bought today would not have a totally secure operating system. Redesigning an operating system with security as the main component will take years to get to market. The other problem facing legislators has to do with computer software.

Legislation could be written that would force software makers to reengineer their software to be secure, but because of the large lobbying efforts of software companies, this option will also take some time to achieve the desired results. Without the protection of legislation, the next place to seek security for home Internet users is the Internet Service Provider. In fact, it is imperative that the ISP take steps to provide the needed security.

User Security: The ISP's Role

In many neighborhoods, people watch out for each other's homes. If they see a crime happening, they call the police. Other neighborhoods do not enjoy this goodwill. People watch out for themselves, not concerned about their neighbors. The same principle can be applied to the Internet. Currently, many ISPs promise to provide the subscriber with Internet access, but not secure Internet access. The ISP and the subscribers all are in the same neighborhood, but the ISP may have chosen to only be watching out for itself. Sadly, many subscribers do not know that they should be watching too. The ISPs who decide not to deal with user security actually have valid reasons for that choice. First of all, providing equipment and properly trained security professionals is a costly expense. Secondly, there could be legal consequences once an ISP provides the user with security. The ISP can be liable for attacks run though them (Plesco, Rosenberg, and Zimmerman (2002), and even if the ISP has maintained tight security, a compromise could result in suits filed by subscribers (Holtz, 2001). Finally, receiving cooperation from users in order to secure home machines could be difficult and time consuming for the ISP.

Law, ISPs, and Security

Before Internet Service Providers can tackle these issues, they must first examine current law to determine if the federal or state governments already require them to provide a certain level of security to their users. There is no law that specifically states that ISPs must provide users with secure access, but there are several laws that deal with privacy. If a user's home computer is compromised, their privacy, as well as their security, has been violated. The Electronic Communications Privacy Act of 1986 (ECPA) and The Computer Fraud and Abuse Act are applicable to these types of situations.

The Electronic Communications Privacy Act attempts to protect the privacy of users of electronic communication devices. It bans interception of any wire or electronic communication unless it is readily accessible to the general public. The law does allow for the exception of the providers of electronic communications, who may intercept any wire of electronic communication in the course of their day-to-day business. Also, service providers are given the right to record the fact that electronic communication occurred. Section 2511(2)(h)(ii)

states,

> "(h) It shall not be unlawful under this chapter --- (ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service" (1986, Law 99-508 (ii)).

Although the ECPA does not require ISPs to provide security to users, it defines lawful activity in regard to customer privacy, and attempts to control illegal interception by an unauthorized party (Electronic Communications Privacy Act, 1986).

The Computer Fraud and Abuse Act defines computer fraud as types of felony offenses. Crimes involving national defense, government computers, and the trafficking of passwords with intent to commit fraud are all described as a breech of security and, therefore, illegal (Staggs, 2000).

Internet Service Provider Ethics

These two federal laws define computerized crime, but do not provide the protection of security a user needs. Many home users are unaware of computer security concerns other than viruses that they hear about in the news media, and most likely assume that their ISP is taking care of computer security. Allowing the home user to connect to the Internet without knowing the possible risks is analogous to a business selling a product that could cause personal harm, but the customer has no knowledge of the potential danger. Ethically, ISPs should inform their customers of the risks involved with Internet connections. Better yet, ISPs can take simple, cost effective steps to provide security for the home users while protecting themselves from legal action.

Internet Service Provider Security Policies

One of the most important elements of a secure network is the written policy that governs it. Any measures an ISP implements to increase security for itself and its subscribers will be ineffective if there is no written policy to back the security measures up. A well written security policy that includes sections on subscriber security, policies for server installation and hardening, password policies, and network monitoring serves as a means to enforce

security at the ISP, while helping to show that the ISP was not negligent in any liability issues.

ISP Secure Network Design

Security must be the foundation of an ISP's network design. Without proper security, compromises could result in service disruptions to thousands of users. The steps that ISPs take to ensure security on their networks could also have a direct effect on the security of their subscribers.

The first step an ISP should take is to place all network access hardware on a subnet that is separate from the subnet that the ISPs main servers are located on. By placing modem pooles, DSL equipment, and other network access hardware on a separate subnet, an individual who might be attempting to sniff data would be forced to go through routing and switching equipment which would make it more likely that the ISP could detect that sniffing is taking place, and less likley that the individual would be successful. A network based intrusion detection system(IDS) is a tool that will give the ISP a good indication of any intrusive activity to which users might be exposed. However, if the users are on the same subnet as the intrusion detection system, the ISP becomes legally responsible for the users security, since they are aware of the existence of malacious activity. Instead, if the users are on a seperate subnet, and the ISP keeps routine logs of only the subnet it was running the IDS on, then the chance that the ISP can be held legally responsible for system compromises diminishes.

Other Secuirty Measures

Although the basic design of a network is important, the ISP can take other steps to further the security of the network. Access control lists will not allow incoming packets with a source ip address of any internal network, outgoing packets without a source ip of the internal network, and will deny incoming traffic access to unused lower port numbers. Potential risks such as IP spoofing are removed by placing an access control list on routers. Access control lists can also be used to deny access based on an ip range. For example, an ISP could deny all outgoing traffic on port 25 that is originating from the subnet their users are on. This could prevent viruses that contain their own SMTP server from replicating, thus cutting down a large number of virus infections. Here is an example access control list that ISPs might consider:

Subscriber Subnet: 999.999.999.0/24
ISP Main Subnet: 999.999.900.0/24:

```
#Deny everything, then
#Permit incoming traffic to www, smtp, pop3, and dns.
deny   tcp any any
permit tcp any host 999.999.900.55 eq 80
permit tcp any host 999.999.900.60 eq 25
permit tcp any host 999.999.900.65 eq 110
permit tcp any host 999.999.900.70 eq 53

#Permita all, then deny incoming traffic on ports 0-901 on #the subscribers
subnet
permit any any
deny tcp any host 999.999.999.0 255.255.255.0 range0-901

#Deny outgoing traffic from the subscribers subnet
#on port 25, while allowing all other outgoing.
allow any any
deny tcp 999.999.999.0 255.255.255.0 any eq 25
```

Access control lists can serve as a first line of defense against portscans and other malicious activity that originates from the Internet or from home users (Hatta, 2001).

Once a secure network has been designed and routers configured with access control lists, the ISP can move toward increased security with the installation of a firewall. Placing a firewall between the ISPs servers, the Internet, and the ISPs users, not only protects the ISP, but indirectly protects the users. Sensitive account information such as usernames, passwords, and bank or credit card numbers are stored on ISP servers. A firewall creates another level of security that must be overcome before gaining access to the servers on the interior. When security exploits are discovered, it also gives administrators valuable time to patch their servers.

Another step to user security is implementing a strong password policy. Many users want to use words or numbers that are familiar to them as passwords. This can prove to be dangerous. Many users' passwords include birthdates, nicknames, or passwords only four characters in length or less. Uninformed users have even been known to use their social security number as a password! The author ran John the Ripper, a password cracking program, against a client ISP's password file. Within four days, over 2000 passwords were cracked. All passwords, not just the users', should be at least six characters long, and contain alphas, numerics, and special characters (Hermens, 2001). Then if a user's password is sniffed, it will take much longer to break, and the attacker will likely move on to easier targets.

Many ISPs keep logs of information, such as which user was connected at what time, and from which ip address. This can be helpful in several ways. If the ISP consistently logs all activity on their servers, it can allow them to watch for trends in the logs. For example, if the logs showed a large number of connection attempts on an unused port, this might alert the administrator that someone was scanning the server, or trying to compromise it. Also, if a dial-up user continually tries to log in with several different passwords, it could mean that someone is trying to guess a password. Of course, it could merely be that the user forgot their password; but in either case, a simple telephone call to the user would quickly resolve the issue. Keeping consistent logs also helps protect the ISP. If legal action were taken against the ISP, log files could help the ISP to avoid penalties. Suppose a user of the ISP breaks into a computer on another network. The log files can help the user's ISP find out who was connected on that IP address and when, as long as it can be proven that the log files have not been altered, and that the ISP was in the habit of logging account information. To ensure that the log files located on each server are not lost, or purposefully edited, it is wise to setup a server that's sole purpose is to gather log information from each server and store it. This log information is stored on the log server in real time and can provide valuable information in the event of a compromise.

One of the services an ISP can provide for its subscribers is a webmail interface. However, many times this webmail system passes the users account name and password over the network in clear text. Users may be anywhere in the world when they access the webmail system, and because their account information is in clear text it has a greater chance of being intercepted. Another step ISPs can take to enhance user security is to implement SSL on mail and web servers. Setting up SSL wrapped POP, IMAP, and SMTP services on mail servers is easy and inexpensive. It also has enormous benefits, in that the user's account name and password are no longer traveling to the mail server in clear text. SSL is easy to configure, and popular email clients such as Microsoft Outlook Express and Eudora support its use. It is necessary to provide a secure HTTP server for the webmail interface so that the account information is encrypted. The connection from the webmail server to the mail server should then be made via SSL to complete the secure connection.

The network based intrusion detection system (NIDS) mentioned earlier is another security tool available to an ISP. The NIDS monitors network traffic, watching for packets that violate a specific set of rules. It then alerts the administrator and can proactively destroy any bad packets. By placing a NIDS outside of the firewall on the same subnet as their servers, the ISP will have a record of intrusion attempts which will allow them to take defensive measures whenever necessary.

The measures listed in this section are precautions that an ISP can take to ensure security of their network and servers. Some of these protect the ISP

from compromise and from legal action, while others help provide the user with a more secure environment.

Home Computer Security

Even though the steps that an ISP takes to secure their network effects the users, the most effective measures will take place at the home of the user. When users contract for Internet service, the ISP should make their customers aware of the security risks that exist for them as Internet users. This could be in the form of a disclaimer or ISP policy statement. The disclaimer and policy is also important legally for the ISP. It serves as proof that the user was informed of the risk of Internet use, and that they accepted that risk. The customer should also be given printed literature that explains the security risks and what they can do to prevent them. In addition to printed material, an ISP can also offer this security information on their website, along with links to other security-oriented websites and software.

Many ISPs have a setup CD that contains a configuration utility designed to help users access the Internet. These CDs also may contain other software such as web browsers or email clients. The setup CD could also include a personal firewall as an added benefit to the customers. Zone Alarm by Zone Labs, is an example of a popular personal firewall that is easy to configure and use. It is free for personal or educational use, making it possible for ISPs to include it on their setup CDs (Elliot, 2002). Other personal firewalls available for purchase are: Network ICE's Black ICE, McAfee Personal Firewall, Norton Personal Firewall, and Zone Alarm Pro by Zone Labs. However, getting users to install and properly configure a personal firewall may be difficult for an ISP.

Even after accurate security information and personal firewall software have been made available to users, it may still be a challenge to get the customers to use what they have been given. ISPs often give classes on Internet use or webpage publishing, it might be helpful to include classes or demonstrations on Internet security, covering issues such as viruses, installing and updating virus protection software, keeping their software patched and updated, and installing and configuring personal firewalls. By educating their users, ISPs can make a significant impact in the security of home Internet users.

Conclusion

There is a large and constantly growing number of home computer users who are connected to the Internet without any means of protection. The government, software manufacturers, Internet service providers, and security professionals need to act quickly to secure home computer systems. Because

a solution between all parties would take years to implement, ISPs are in the best position to quickly and effectively increase security measures for their users. By securing their networks and educating users about Internet security, the ISP provide significant assistance to home users. If all ISPs take interest in the security of their users, they can make the Internet a safe and secure place for all. However, it should be understood that before an ISP takes any of the steps suggested in this paper, they should consult their legal counsel to ensure that they will be protected in all legal matters.

Table of Contents

User Security and the Internet Service Provider

Prepared by

Ty Purcell

Assignment Version

1.4 Option 1

In Partial Fullfillment
of the Requirements
of

GSEC Certification

May 14, 2002

User Security and the Internet Service Provider

Abstract

Because more and more Americans are recognizing and utilizing the Internet as a valuable resource and tool, many home users and information technology professionals are questioning network safety. Is it truly safe to use your credit card number for computer transactions? How difficult would it be for someone to crack your username and password? These two questions are answered in this report, along with several possible solutions that begin with the local Internet service provider. Through the installation of proper equipment, sound and ethical policies, and the education of the home user as their

customer, this reports proves that ISPs are essential in order to alleviate these security dilemmas in the most efficient manner.

References

Elliot, C. Zone Alarm- A Free Solution for Home Security. 1 October 2002.
URL :http://www.sans.org

Hatta, M.S. Securing Routing and Remote Access on Cisco Routers. 20 September 2001.

URL :http://www.sans.org

Hermens, L. Inadequate Password Policies Can Lead to Problems. 10 October 2001.
URL :http://www.sans.org .

Holtz, G. System Security and Your Responsibilities: Minimizing Your Liability. 23 July 2001.
URL :http://www.sans.org

Plesco, R., Rosenberg, T., and Zimmerman S.C. (2002). Downstream Liability for Attack Relay and Amplification. RSA Conference 2002. San Jose, California.
URL:http://www.cert.org/archive/pdf/Downstream_Liabilit y.pdf

Staggs, J. Computer Security and the Law. 1 December 2000. URL :http://www.sans.org

United States. US Census Bureau. Home Computers and Internet Use in the United States: August 2000. Issued September 2001.

18 USC 2510 Electronic Communications Privacy Act of 1986.

Last Updated: July 25th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	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
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event