Global Information Assurance Certification Paper

Online home users Defense in Depth
GSEC V1.4
Hatim Ali Badr

Abstract

Home users are increasing everyday and most of them have little knowledge about information security. Information security is new area that home users are not aware of its risks and threats and how to protect their data from. Also they do not know that they may contribute in attacking others if they did not apply proper security measures. Online information security is everyone's responsibility. Home users are responsible to implement the security measures to secure their data and to play important role in securing our cyber world. On the other hand security specialists are responsible for home users' education and awareness in information security, in easy and understandable language to non IT users.

Home users concerns are "how to protect my data" which is the information security and 'how to stop the leakage of my personal and private information without my knowledge or permission" which is known as online privacy. Information security and online privacy are usually addresses separately. In this paper we will address both of them to provide a complete defense in depth solution for the home users. We will have a look at risks and threats to both computer security and online privacy and the recommended protection measures to have a secured home computer environment.

Introduction

Home user is a person who uses his computer to access the internet from home. The majority of home users have very little knowledge and awareness of the security breaches that may occur when connecting to internet and "The current situation shows many home PCs have become victims of virus and worm infections, DDOS agents and many others" [1]

In general information security is addressing three main areas:
1. Confidentiality: Only authorized person has access to his information.
2. Integrity: Only the authorized person is allowed to change the information.
3. Availability: Information is available for the authorized person when he needs it.

On the other hand privacy of online users means that personal data like (Name, e-mail address, location …) will not be disclosed without their permission. There are ways that let people to know others' personal data without their permission. These ways and tools will be discussed as threats and the protection measures for it will be highlighted as well.

Home users are targets of attackers because of the following reasons:
1. Steal confidential or personal information.
2. Attackers can use home users as agents in attacks such as Distributed Denial of service (DDOS) or to hide them selves while attacking other sites with the victim identity (Spoofing).
3. The places that unprofessional attackers (Script Kiddies) can easily attack. "They view this class of user as "soft targets" and a new group to exploit, of which only about 3% has any type of personal firewall to protect against an intrusion"[2]

1. How home users are connecting to Internet

Connecting to internet has two parts physical which means what technology used to connect to internet and logical which means how computers communicate after physical connection Put in place.

1.1 Physical Connectivity

There are three known types of physical connectivity to internet
1- Dialup Connections: Use normal telephone line to dial to an ISP. This is the traditional and the most commonly used way to connect to internet.
2- DSL: Use Digital subscriber lines technology that is faster than dialup lines, up to 2 Mbps, to connect to Internet, it is more expensive.
3- Cable Modem: Use the TV cable systems to connect to internet; it is the fastest way to connect to internet among these three techniques, it can reach up to 27 Mbps.

DSL and cable modem connections are called Always-on connections since they have 24x7 connections to internet. They are more vulnerable to internet threats because they are always connected to internet.

1.2 Logical Connectivity

TCP/IP (Transmission Control Protocol / Internet Protocol) is a suite of protocols that can governs any computer network communications. It is the de facto of the internet communications; TCP/IP is a layered model protocol; that mapped to OSI (Open System interconnect) reference model which "describes how information from a software application in one computer moves through a network medium to a software application in another computer" [3]. UDP, ICMP and ARP are other protocols that are part of the TCP/IP.

IP (Internet protocol) "provides the basic delivery mechanism for packets of data sent between all systems on an internet" [4]. IP address is a unique identifier for every computer in the network; it consists of four decimal numbers separated by dots for example 192.168.13.20. Every computer should have an IP address when connected to internet.

TCP and UDP are protocols working on top of IP that provides data transfer service between computers in the internet. Since there are a lot of application running on top of TCP and UDP, each application uses a separate port number. While IP addresses are used as node (computer, router …) identifier in the internet, Port numbers are unique identifier for each application running in a computer. Web traffic which is HTTP is using TCP port number 80, when downloading a file from the internet FTP protocol (TCP Port number 21) is used, when using e-mail clients to download e-mails to local computer either POP3 (TCP port number 110) or IMAP (TCP port number 143) are used. So in the same time users can browse the internet, download file and downloading his e-mail because of the modularity of the TCP/IP.

2. What are the threats?

Knowing the risk is the first step to avoid or prevent it. This section describes the most common and current computer security and online privacy threats that may face the home users.

2.1. Malicious codes

It is any code of malicious intent to damage or interrupt computer operations. Known malicious codes are:

2.1.1 Viruses and worms

Although there is no standard definition for a virus we will consider SANS institute definition "A virus is a piece of parasitic code (or program) written specifically to execute on behalf of the user without the user's permission (or knowledge)"[5]. Viruses are the most known security threat. There are several types of viruses:

1. File virus which can infect executable file or double them.
2. Boot virus which infect the computer boot sector which is responsible for booting the computer, boot virus will change the normal boot sequence and may crash the system
3. Macro virus which infect documents such as word documents, spreadsheets and databases, the most common macro viruses are Microsoft Word macro viruses. Macro.Word97.Mellisa is well known macro virus that infects word 97 and word 2000 documents and templates and it sends itself to others through Microsoft outlook.

While the virus requires some user action, Worms spread automatically to other machines without any action from the user side. By other words it is a malicious code that does not require any user to interact with it. Worms spread faster than virus to other computers in the network.

Tanatos, also known as Bugbear, is one of recent worms. Tanatos ranked number one in the Virus top twenty October 2002 list by Kaspersky Labs [6] with 44.9% of occurrence. Tanatos spread as attachment in an e-mail and it copies itself to the windows directory (folder), configures itself to start when windows start at next time, create DLL files that will sniff all keyboard inputs, send itself to all contact list if the user is using Outlook or outlook express with different subject and body text, opens port 36794, this is known as backdoor, so that the administrator of this worm can connect to victim's machine through this port and execute applications and also it will tries to terminate some applications and especially security protection applications.

Another well known worm is LOVELETTER, "The infection affected millions of computers and caused more damage than any other computer virus to date"[7]. If a user opens the worm, which usually comes as e-mail attachment, (named LOVE-LETTER-FOR-YOU.TXT.vbs) then it creates some files in Operating system directory, overwrites some files types (e.g. jpg, mp3), modifies Internet Explorer start page with an script which will start at windows startup and sniffs passwords and it will send a copy of itself to all listed contacts, if user using outlook to send and receive e-mail.

2.1.2 Trojan horses

A Trojan horse is "An unauthorized program contained within a legitimate program. This unauthorized program performs functions unknown (and probably unwanted) by the user" [8]. Trojans have two components server and client, the attacker will install one of these components in victim's machine and will connect from his machine to victim's system through the internet. There are several variations of Trojan horses; the common ones are listed below: [8]

- Remote access (Backdoor): It gives attacker administrator remote access to victim's system.

- Password sending: Search for cached passwords and entered passwords and send them to Attacker's e-mail.
- Denial of service attacks Trojan: Use victims systems as agents for Distributed Denial of service attacks
- Proxy Trojan: Uses the victim's system as a proxy to access other websites. Attacker's activity, which will be most probably illegal, will be logged with victim's IP address.
- Destructive: Destroy and Delete files from victim's system.

Well known Trojans are Subseven, netbus and Back Orifice. If a user finds his screensaver has been changed, CD-ROM door opens and closes, mouse moves by itself then most probably the machine is infected by a Trojan.

2.2 E-mail Spoofing

E-mail spoofing is a message originated from a person that is pretending to be known person or trusted entity while he is actually an attacker tries to send malicious code or trying to get confidential or private information.

Usually we open e-mail messages from our friends or colleagues without even thinking about any security risks since the message is coming from well known person. Attackers can spoof user's friend e-mail ID and sends an attachment which is actually a virus, or user's ISP administrator e-mail asking about personal information or requesting him to send his password.

2.3 Denial of Service (Dos) and distributed Denial of service attacks (DDoS)

Denial of service (DoS) is the process of preventing authorized users from using their system. DoS can be by sending a flood of packets from attacker to victim that will utilize all the bandwidth or by taking advantage of weaknesses in operating systems and applications that can disrupts the normal service.

If more than one attacker are contributing in the DoS attack, this will be named as Distributed Denial of Service DDoS attack. Home users can contribute in DDoS without their knowledge; if the attacker is able to install a specific Trojan horse in several home users' machines then he can control all these machines and use them as DDoS agents to attack other sites. "WinTrinoo is a DDoS tool that has become really popular recently, and if the attacker has infected many ADSL users, major Internet sites could be shut down as a result"[8]

2.4 Unprotected Windows shares

Windows Operating systems file and print sharing service is one of good features that will allow network users to share their resources across the network. On the other hand it can be harmful since an attacker can exploit systems from this share. Attackers can use the unprotected windows shares and download malicious codes. This threat is applicable only in network media like cable modem networks.

2.5 Packet sniffing

Packet sniffing is the process of capturing traffic passing through the network. It is applicable only in network media like cable modem networks. If attacker is able to sniff the traffic then

he can read unencrypted data sent via the network even the sensitive data such as username, passwords and credit cards. If a cable modem user installs a packet sniffing software, then he can see other cable modem users' traffic connected to the same network

2.6 Internet Chat Applications

Chat clients such as instant messaging services (MSN messenger, and Yahoo messenger) and Internet relay chat networks (mIRC) enable users to chat, talk and send files to others. "15% of all IM users said they accepted file transfers from unknown parties. These people are just asking for viruses, worms and other dangerous programs to invade their computers" [9]. These files may be a malicious code that may affect user's system if he is not protected. Worm, Trojan horses, information disclosure and denial of services are the common threats that can affect systems through chat applications.

2.7 Peer-to-Peer (P2P) Applications

P2P applications such as Kazaa allow users to share their files across the internet. With P2P applications users can download files that are infected with malicious codes. Also user may unintentionally share private or confidential files that others can download. "The automatic queries occurred every 90 seconds for 12 hours and revealed 443 instances of unintentional file sharing. In that 12-hour period, 156 Kazaa users were found to have e-mail files open for public review. Sixty-one percent of the searches revealed at least one e-mail file" [10]. Users have to take care when dealing with such applications. Several malicious codes are written especially to Kazaa and distributed through Kazaa. Unintentional file sharing can leak user's private and confidential data.

2.8 Malicious Mobile codes (java script, Java applets and Active X)

Mobile codes are programs executed by web browser locally directed by the visited web site (Java applets and ActiveX components) or scripts, like java scripts, that embedded in the web pages to perform simple tasks such as calculations or data manipulations. In general Mobile codes are very useful tools that create more functionality and interactive that can not be achieved with normal HTML language. Mobile codes can automate any task or operation the user can perform in his machine, Java applets are limited in its functionality by the Java Virtual machine which provides a security guard for the system. ActiveX execute as normal executable files. Some malicious websites can use the advantage of the mobile codes to execute or perform tasks that may harm systems or they can be used get information about user's machine settings and configuration and other information like the visited websites. It sends it to back to the website. By default mobile codes are enabled in Internet Explorer and Netscape Navigator.

2.9 Hidden file extension

By default Windows operating systems hide certain file extensions. File extensions identify the file type. Attackers are taking advantage of hiding the file extension by creating viruses and worms and spread them as risk-free files such as text file or multimedia file while it is actually a malicious executable code. "The first major attack incorporating an element of file extension obfuscation was the VBS/LoveLetter worm which contained an email attachment named "LOVE-LETTER-FOR-YOU.TXT.vbs" [11]. Since file extension .vbs is hidden be default in windows, the user thinks that this is a text file because of .TXT at the end of the file

name while it is a malicious file. In fact this issue is not a threat by itself but it can be considered as a trick that will ease the threat to attack systems.

2.10 Cookies

Cookies are text file stored locally in users' systems when they visit some websites. HTTP is session less protocol, cookies makes it session aware. Cookies contain unique identifier and data you entered into the browser such username, real name passwords or any other data you normally provide when web sites ask for it. Ideally, websites can access only their stored cookies and not others; this is a security measure in cookies that will not allow others to access what other websites are storing locally. "Typically the server uses the cookie to remember the user and to maintain the illusion of a "session" that spans multiple pages"[12], because if this, Cookies are used extensively in online shopping and to personalize browsing by saving your information and settings and use them the next time you visited the website. "Cookies cannot be used to "steal" information about you or your computer system. They can only be used to store information that you have provided at some point"[12].

As mentioned earlier that websites can access only their cookies but what will happen if a websites can access others' cookies? Cookies can store usernames, real names, postal addresses and even passwords (NYTimes.com saves password in their cookies if the user asked the website to do so) [13], so it is really a security risk. There are vulnerabilities in cookies that can make cookies public to all websites; Open Cookie Jar is one of these vulnerabilities in Microsoft internet explorer.

"However cookies can be used for more controversial purposes. Each access your browser makes to a Web site leaves some information about you behind, creating a gossamer trail across the Internet. Among the tidbits of data left along this trail are the name and IP address of your computer, the brand of browser you're using, the operating system you're running, the URL of the Web page you accessed, and the URL of the page you were last viewing"[12], some websites and especially advertisement companies are collecting information about users without their knowledge. Advertisement companies are placing their ads in many websites that will create a large network of websites. If you visited anyone of them, an advertising material will be downloaded from the advertisement company site, not from the site you are visiting. Over the time, advertisement companies will create a profile for individuals with their interest and habits by tracing the user's internet surfing history. Collecting all these information time will identify the user's interest and habits. So if a user visited other site that is part of that network, the advertising company will check its cookies to check you profile and then download advertising material of his interests. This data may not be confidential but it is personal and may be user is not willing to provide others about his browser type or his interests.

3. Defense in Depth

"Defense in depth is the practice of layering defenses to provide added protection. Defense in depth increases security by raising the cost of an attack"[14]

Form the previous section we have seen how online home users are vulnerable to security threats whether through operating systems and applications weaknesses (Active X and windows sharing), lack of technical knowledge and awareness (E-mail spoofing), through intentional attacking tools (Malicious codes, DoS, DDoS) or collecting private data (cookies, scripts, internet chat and P2P applications). To have a proper secured computing

environment we will explore the techniques that will provide secured environment for home users.

3.1 Harden the system by applying security patches

"The best defense is a good offense. From a security standpoint, that means the most valuable thing you can do is take proactive measures to keep your system software up to date"[15] Attackers are looking for vulnerabilities whether in operating system or applications and especially web browser (Internet Explorer or Netscape navigator) and e-mail client (Microsoft Outlook, Eudora). They are trying to find some vulnerability in systems to get advantage from that one and exploit it.

On the other hand vendors and security professionals are trying to fix any vulnerability found by them or reported to them from customers before the bad guys exploit it. When vendors detect certain vulnerability it immediately starts develop a fix or patch and release it to the customers. Usually these patches can be downloaded from the vendors and major software companies' websites, some vendors have automatic mechanism for patches update (for example Microsoft provided its Windows Operating -starting from Windows 98- systems with windows Update feature that connects to Microsoft website checks your machine for required patches, displays the patches required and gives you the choice to download them or not). Every user must make sure that machine's operating system, web browser, E-mail client and other applications are updated.

3.2. Install Antivirus Software

Antivirus software is application that scans files for the presence of virus across, delete virus and recovers the infected files. It has a list of all known viruses signature "A unique string of bits, or the binary pattern, of a virus. The virus signature is like a fingerprint in that it can be used to detect and identify specific viruses"[16]. It scans the files against theses signatures, if a file matches the signature, antivirus will respond with one of the following options, cleaning (it will remove the pattern from the files), Delete the file or Quarantine, isolate, the infected file .

There are plenty of antivirus software. Users can choose the product that he can relies on and fits into his requirements. ICSA Labs (a division of TruSecure Corporations), is an independent entity that certifies security products, has a list of certified antivirus products. ICSA Labs developed a certain criteria which products should meet to be certified.

"The objective of ICSA Labs' Anti-virus Certification Program is to make available to the user community a selection of products that provide the following security services:

1. Provide protection to computer systems and media from computer virus intrusion.
2. Provide detection of computer viruses on an infected computer system or media.
3. Provide for recovery from a computer viruses infection" [17]

Also there is West Cost Lab's CheckMark [18] which is another independent organization that certifies security products. The advantage of West Coast Lab's Check-Mark over ICSA labs that it has separate certification for the Anti-Trojan software. All well known antivirus software are certified by both ICSA lab and Check-Mark Lab and certified as Anti-Trojan as well. If you have already antivirus that it does not detect and clean Trojans it is recommended to install anti-Trojan software or replace it with a certified antivirus product that works as

anti-Trojans as well. The following link lists the certified West Cost Lab's Check-Mark Anti-Trojan product http://www.check-mark.com/checkmark/products_troj.html .

Beside the basic functions of Antivirus, others features are to be considered when choosing Anti-virus software

- Automatic update feature that will be used to download the new virus signatures automatically from the internet
- Agents for other applications such as Instant messages application, for example Norton Antivirus 2003 has agent for Instant messaging applications.

As per the ICSA Labs 7th annual computer virus Survey 2001 [19], the most used Anti-Virus software are Norton Antivirus from Symantec and McAfee Antivirus from Network Associates.

3.3 Install Personal Firewall

Antivirus will protect systems from the malicious codes, but what about other threats like Denial of services, File sharing or unauthorized access to the system that Anti-virus can not protect from. Firewall protects the stand alone systems or computer networks from intruders by blocking unwanted traffic.

In general Firewall can be a software or hardware device. Almost all companies connected to internet are protecting their networks by firewall. Personal firewall is software installed in systems.

As for the Antivirus, ICSALABS as well as other independent product Certification bodies are helping users to select the proper firewall product. ICSALABS selection criteria for personal firewall are as follows [20] :

- Ability to support Microsoft Networking capabilities while providing end point protection
- Ability to support concurrent dial-up and LAN connectivity
- Ability to block common external network attacks
- Ability to restrict outgoing network communications
- Ability to maintain consistent protection across multiple successive dial-up connections
- Ability to log events in a consistent and useful manner

ICSA labs are certifying only two products, one from Symantec and the other is from Mcafee[21] . There are plenty of personal firewalls in the market and some of them are popular and good as well, for example ZoneAlarm Pro from Zone Labs, Tiny Personal firewall from Tiny software, BlackICe PC protection from Internet security Systems.

Firewall sits between user's machine (trusted area) and the internet (Un-trusted area) and will allow or deny traffic based on the rules created whether manually or through wizards. In general it allows outgoing traffic (traffic initiated from trusted) and block all incoming traffic (traffic initiated from un-trusted area). It uses the port numbers in allowing and permitting traffic since each application has different port number.

Firewall rules can be customized to the user needs. If a user requires incoming traffic from a trusted person or entity in the un-trusted area (Internet) or want to block some outgoing

traffic, then he can customize the firewall rules to allow specific incoming traffic or deny specific outgoing traffic. Since these rules require some technical knowledge, rule and filters are based on Source and destinations IP addresses as well as ports, most of personal firewalls shipped with predefined levels of settings that you can change with a click, with most restrictive and protective that will deny all incoming internet traffic and the least one which allows all incoming traffic.

Beside the selection criteria of the basic features of personal firewall from ICSALABS listed above, there are other features and tools bundled with the commercial products available in the market that extends the functionality of traditional personal firewall. To select a product is recommended to look for the following features and tools as well:

- Application control: It can control all applications trying to access the Internet. It will give the user he rights to allow of block any application from accessing the internet.
- Automatic configuration and update: Since personal firewalls are targeting non IT people who do not have technical background, the automatic configuration and wizards are one of the nice features, also auto update of application will help users to make sure that personal firewall application is updated.
- Certified products: ICSA labs certification will provide end users with confidence that the technical experts had tested the product and certified it.
- Presentable Logging feature: Firewalls are logging traffic, event, changes and attacks. It is important to have easy to understand logging feature to know what is going there.
- Intrusion detection system (IDS): Although IDS is a separate product; most of the vendors had embedded IDS. An ID is application that will detect any intrusion and act based upon configured rules.
- Malicious Mobile code protection: Several Personal firewalls are adding a module that will control the malicious mobile codes execution and can block them or warn users before executing them.

3.4 Disable mobile codes (java script, Java applets and Active X)

Mobile codes as mentioned earlier are useful tools but some malicious mobile codes or scripts may attack your system. It is recommended to disable them, if the personal firewall is not having a module that controls the mobile codes. Disabling mobile codes will reduce browsing functionality and features of some websites, instead user may force the system to prompt before downloading such components and he have to read carefully before accepting it. CERT Coordination center has a detailed documents on how to disable mobile codes [22].

It is recommended also to disable mobile codes in e-mail clients. E-mail clients such as Microsoft outlook, Outlook express and Eudora can also be attacked by malicious mobile codes.

3.5 Take precautions before opening E-mail attachments

Most of the malicious codes are coming as e-mail attachments, the ICSA Labs 7th annual computer virus Survey 2001 [19] stated that 83% of the malicious codes in 2001 are coming from e-mail attachments while it was only 9% in 1996. Fig 1 shows source of infections for viruses from 1996 to 2001 [25].

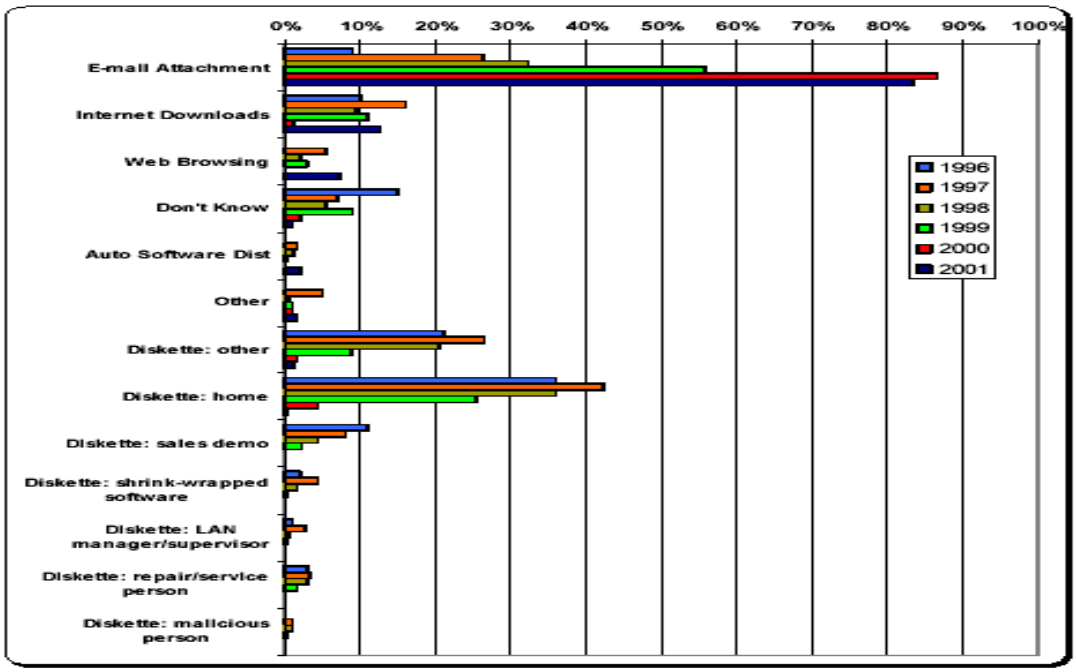

Fig 1: Source of infections for viruses from 1996 to 2001 [19]

This means that users have to make sure that e-mail attachments are not containing viruses, worms or a Trojan. Malicious codes can appear that it is coming from trusted parties (E-mail spoofing) or from others. Each user should take some precautions when opening attachments:

- Make sure that the message is coming from trusted party.
- User is expecting an attachment with the received message.
- Make sure that subject name and the attachment file name are related.
- If you suspect a virus contact the sender -by phone or by e-mail- before opening the attachment.
- Make sure that anti-virus software is updated
- Save the attachment in the hard disk, scan it with antivirus and then open it.

On the other hand when a user wants to send attachment to others, it is recommended to send a message without attachment stating that you want to send attachment and then send the attachment after receiving a confirmation from the recipient.

3.6 Take care when downloading and installing programs

Downloading applications from internet is getting easier than before with the increase in the bandwidth as well as the availability of free software and sharewares. Downloading applications from un-trusted parties can contain viruses, worms, Trojan horses that may destroy your machine or may give control of your machine to intruders. It is recommended not to download or run un-trusted or unknown origin applications.

3.7 Protect online privacy

Today, Online Privacy is a concern because a lot of sites can collect data from people without their knowledge or permission. Even if a user provided a site with his personal information, he does not know what this site will do with it and how it is secured. There are websites that

provide information and awareness about online privacy "such as Privacy Foundation, Privacy Net, Electronic Frontier Foundation, Electronic Privacy Information Center and Online Privacy Alliance" [23]. To protect online privacy it is recommended to:

3.7.1. Install personal proxy

There are several personal proxies in the market or internet that controls online information collection. It mainly controls cookies, web bug (1x1 pixels image embedded in another image or a webpage that can not be seen and it can run scripts that collect information about computer settings) referrers (tells the website what was the last site the user had visited) and advertisements. There are a lot of free personal proxies on the internet such as proxomitron, webwasher, privoxy etc. Some personal firewalls products are having personal proxy features as part of their personal firewall such as ZoneAlarm , Norton Internet Security 2003 and MacAfee Internet security 2003 .

3.7.2. Read the privacy policy of websites you visit

Privacy policy will show how the site will handle personal information. TRsute.org is an independent, non profit initiative that has TRUSTe Privacy Seal Program that "All Web sites that display our trust mark must disclose their personal information collection and privacy practices in a straightforward privacy statement, generally a link from the home page"[24]. This program is mainly for United state websites, if you are browsing other regions websites you have to search for the privacy policy.

The P3P (Platform for Privacy Preferences Project) "developed by the World Wide Web Consortium, is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit."[25].

AT&T developed a tool, beta version, called Privacy bird ; it will read the privacy policy based on the P3P standard format. If it finds it matching your settings it will show a green bird and if not It will show a red one. It will show yellow one if it did not find privacy policy written in the P3P standard. It gives the ability to customize the options that match your privacy concerns.

3.8 Backup important files

User can not feel the importance of the backup unless he looses some data and can not recover it. Previously people were using floppy disk to backup their files but Currently CD writers are becoming very cheap that anyone can afford to have one or you can use zip drive to backup your data.

3.10 Awareness and education

Security is an ongoing process and it is active filed that requires computer users to be updated and aware of the new threats and defense methods. The weakest link in information security is people. Intruders are taking the advantage of lack of awareness and education as well as lack of security measures implementation. For home users, Installing personal firewall and antivirus may prevent from known risks but may not protect from new threats. Awareness and education will help users to take precautions when dealing with such risk. Several sites that will provide home users with valuable information about computer security such as

www.staysafeonline.info sponsored by the National Cyber security alliance, http://www.cert.org , http://www.sans.org.

Conclusion

Home users must know that there are always risks when using computer even if you follow and implement all security measures. The only way to have full information security is to switch off the computer. Using computers introduce a risk, connecting to internet is a threat that adds more risks to data and assets. Risks are always there even in our life. We always take the necessary measures to protect ourselves from them. In online environment there are threats to our information and privacy that we try to implement defense solution to protect them.

Information security and online privacy are two faces for one coin. To have a secured online environment, both of them should be protected. Everyone is responsible for information security and online privacy. Home users must deploy security measures and keep updated with risks and threats and the protection techniques. Websites should implement the adequate security and privacy protection measures. IT and security professionals, beside their role of identifying risks, finding threats and developing security solution, are responsible for representing the security risks and associated solutions and measures to home users in friendly way to understand it.

References

1- Malaysian Computer Emergency Response Team, **"Home User PC Security: Know the Threats and Countermeasures"**
URL: http://www.mycert.org.my/homepcsecurity.html 22nd October 2001

2- Internet Security Alliance, Inc, **"Internet Security Background for Personal Computers"**
http://www.isa-llc.com/company/wpaper.php

3- Cisco Systems, **"Introduction to Internet"**
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm#xtocid1 , Feb 20, 2002

4- Mike Oliver, **"TCP/IP FAQ; Frequently Asked Questions (1999-09) Part 1 of 2"**
http://isc.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part1/ 1999-09-06

5- SANS Institute, **"SANS Security Essentials IV: Encryption and Exploits"**

6- Virus List, **"Virus Top Twenty – October"**
http://www.viruslist.com/eng/index.html?tnews=1001&id=57691 November 01, 2002

7- Frank Thorsberg, "**The World's Worst Viruses"**
http://www.pcworld.com/features/article/0,aid,103992,00.asp August 23, 2002

8- Dancho Danchev, **"The Complete Windows Trojans Paper"**
http://www.frame4.com/content/pubs/comp_trojans.html

9- Bob Woods, "**Half of IM Users Accept Downloads"**
http://www.instantmessagingplanet.com/security/article.php/1470691 September 26, 2002

10-Steven Musil, **"File swappers expose themselves"**
http://zdnet.com.com/2100-1105-933836.html June 7, 2002

11- CERT Coordination Center **"Exploitation of Hidden File Extensions"**
http://www.cert.org/incident_notes/IN-2000-07.html June 19, 2000

12- Lincoln D. Stein and John N. Stewart **"The World Wide Web Security FAQ, 9. Client Side Security"**
http://www.w3.org/Security/faq/wwwsf2.html July 28, 2001

13- New York Times Customer service **"Frequently Asked Questions about Cookies"**
http://www.nytimes.com/ref/membercenter/help/cookiesfaq.html

14 Brooke Paul, **"Building an In-Depth Defense"**
http://www.networkcomputing.com/1214/1214ws1.html July 9, 2001

15 Microsoft TechNet, **"5-Minute Security Advisor - Essential Security Tools for Home Office Users"**
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/5min/5min-105.asp

16- Virus Signature- EarthWeb.com: The IT Industry Portal: Network ... Enterprise Storage Forum **"virus signature"**
http://enterprisestorageforum.webopedia.com/TERM/V/virus_signature.html February 05, 2002

17- ICSA Labs **"Antivirus Certification Criteria"**
http://www.icsalabs.com/html/communities/antivirus/certification.shtml 14 February 2002

18- West Coast Lab's Checkmark **"Checkmark - The system which tests and certifies computer security products."**
http://www.check-mark.com/cgi-bin/redirect.pl

19- Lawrence M. Bridwell and Peter Tippett, "**ICSA Labs 7th annual computer virus Survey 2001"**
http://www.trusecure.com/download/dispatch/vps-survey-2001.pdf?ECDE=W0001 2001

20- ICSA Labs "Welcome to ICSA Labs PC Firewall Community"
http://www.icsalabs.com/html/communities/pcfirewalls/index.shtml February 1, 2003

21- ICSA Labs "**ICSA Labs Certified PC Firewalls"**
http://www.icsalabs.com/html/communities/pcfirewalls/cert_prods.shtml February 1, 2003

22- CERT Coordination center, **"Frequently Asked Questions about Malicious Web Scripts Redirected by Web Sites"**
http://www.cert.org/tech_tips/malicious_code_FAQ.html February 3, 2000

23- Tony Yao, **"Personal Proxy – Online Privacy Protection for Home Users "** http://www.sans.org/rr/privacy/personal_proxy.php September 10, 2002

24- Truste, **"The TRUST e Program: How It Protects Your Privacy"** https://www.truste.org/consumers/users_how.html

25- W3C, **"Platform for Privacy Preferences (P3P) Project"** http://www.w3.org/P3P/ Jan 21, 2003

26- CERT® Coordination Center, "**Home Network Security"** URL**:** http://www.cert.org/tech_tips/home_networks.html **,** December 5, 2001

27- Virus Encyclopedia, Virus List "**I-Worm.Tanatos (a.k.a BugBear)"** http://www.viruslist.com/eng/viruslist.html?id=52245 Feb 21, 2003

28- Eugene Kaspersky **"Computer Virus Classification"** http://www.viruslist.com/eng/viruslistbooks.html?id=21

29- CERT Coordination center, **"Results of Security in ActiveX Workshop"** http://www.cert.org/archive/pdf/activeX_report.pdf December 21, 2000

30- Lawrence R. Rogers, **"Home Computer Security"** http://www.cert.org/homeusers/HomeComputerSecurity/ 2002