Security Risks Associated With the Use of Web Browsing, Instant Messaging and File Sharing software

D.Bitsanis and M.Papadaki

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

This research has been conducted in order to associate the security risks of the computers with the use of applications of Web-Browsing, Instant Messaging and File Sharing. The research has been conducted by isolating the traffic that these applications have generated, allowing accurate results. Each type of application has generated isolated traffic for forty hours, leading to a one-hundred-twenty hours of research. The results from this research have indicated that the Web-Browsers are submitted to a large number of attacks while the Instant Messengers and the File sharing applications are much safer since they are only submitted to very few attacks.

Keywords

Security Risks, File Sharing, Instant Messaging, Web-Browsers

1 Introduction

This paper introduces the research which has been conducted in order to reveal the security risks that the Web-Browsers, the Instant Messengers and the File Sharing applications are vulnerable to, when they generate traffic. The security risks of each application are introduced from other authors, which have already conducted their research on this sector. This paper introduces the way that the research has been conducted, including the setup of the network and the applications which have been used. Finally the results of the research and their meaning are explained.

2 Applications Existing Vulnerabilities

The File Sharing applications, the IM (Instant Messengers) and the Web-Browsers are all vulnerable on attacks through the Internet. Some of the attacks are based on the traffic that these applications generate, while others are based on the actions of the user. The experiment was based on the vulnerabilities that the applications are exposed to, because of the traffic that they generate.

2.1 Web-Browsing

Denial of Service

The applications which connect to the Internet are vulnerable to DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks. When an application is submitted to such an attack, it fails to establish connections to other hosts or servers. Web-browsers cannot be submitted to DoS and DDoS attack directly. They can still be submitted to one through a server that provides critical services, such as the server of a web-site, e-mail or a DNS (Domain Name System) (Moseley, 2007). If one of these servers is submitted to a DoS or a DDoS attack, it will also render web-browsers useless since they will not be able to establish a connection with them and use the services that they provide.

Cross Site Scripting / Buffer Overflow

A XSS (Cross Site Scripting) attack occurs when a malicious script is executed in a trusted web-site. A script is composed from a combination of small commands, which are executed immediately upon the loading of a web-page. The attackers can place such scripts in the web-pages through the user input fields, when their size is not restricted, or when some symbols are not forbidden from the users. These scripts can have various functions, such as redirecting the input of the other users to the attacker, or capturing the session ID, that a user uses in order to connect to the web-site, so that the attacker can use it and pretend to be the legitimate user (Moseley, 2007).

Spoofing

A spoofing attack occurs when an attacker uses a fake IP (Internet Protocol) address, in order to pretend to be a legitimate user. The attack is successful when the attacker intercepts the traffic between a user and a server (Moseley, 2007). If that happens, the attacker can capture the messages that the user sends to the server and use them in order to communicate to the server as the legitimate user. Doing so, the attacker bypasses the security of the server and has the access rights that the legitimate user has.

Session Hijacking

A session hijacking is taking place when an attacker takes over control the session ID, of the application that a user uses in order to connect to the Internet with. Having the session ID, the attacker can control the users' application. The ID codes can be captured in different ways. One of them is a brute force attack, where the attacker is using every possible combination of letters, numbers and symbols (Moseley, 2007).

2.2 Instant Messaging

Denial of service

The IMs are also vulnerable to DoS attacks. The IMs can only process a limited number of messages that they accept from the users. A DoS attack can succeed when a large number of messages are sent to a user. Even though some IMs have a function that protects them against such attacks, there are ways to bypass it. The attacker can use many different accounts in order to launch the attack. If the number of messages that the IM is trying to process exceeds the limit, then there is a very high possibility that the IM will crash. In an even worst scenario, the IM will consume a large amount of CPU (Computer Processing Unit) that will cause the whole computer to become unstable and maybe crash. (Hindocha, 2003)

Eavesdropping / Spoofing

An eavesdropping attack occurs when an attacker intercepts the communication between two users. This kind of attack is possible because by default, the communication between two IMs is not encrypted (Piccard, 2003). This means that anyone who is tracking the traffic of the Internet will be able to capture and read the conversation between two users. The attacker knowing the IP (Internet Protocol) address from both the sender and the receiver can redirect the messages to each other and even send fake messages. (Moseley, 2007; Sagar, 2003).

2.3 File Sharing

Denial of service

In order for the File Sharing applications to function properly, they require to establish a connection to a server and then to other hosts over the Internet. On the other hand, the File Sharing application will accept connections from other hosts as well. However the number of connections that the application can establish is set. This feature creates a vulnerability to the File Sharing applications. By trying to establish a large number of connections, an attacker will launch a DoS or DDoS attack. If these attacks succeed, then the application will not operate properly and it may even crash. In an even worst scenario the application will consume a large amount of CPU and will cause the PC (Personal Computer) to become unstable and even crash. (Piccard, 2003)

Reveal of IP / Port

An attacker requires the IP address of a host and the ports that the host has unblocked, in order to launch an attack. Hiding these two pieces of information is enough protection for the user, in order to limit the number of attacks. The File Sharing applications neutralise this protection. When the File Sharing application connects to a server and then to a similar application on the Internet, the IP address of the host as well as the ports that the application is using is revealed on the other end of the communication (FaceTime, 2005; Piccard, 2003). This exposes the computer to attackers which can launch more sophisticated attacks.

3 Research Method

The experiment took place at the NRG (Network Research Group) lab, at the University of Plymouth. The purpose of the experiment was to determine what kind of Internet attacks a PC is exposed to, while using Web-Browsers, IMs and File Sharing applications. Two PCs have been used for the experiment. The First PC, the Host, has been used to generate traffic using the Web-Browsers, the IMs and the File sharing applications. The second PC has been used along with the first as a Firewall, in order to allow only traffic from specific ports to be generated and in order to capture all the traffic the Host has generated. The experiment has lasted for one-hundred-twenty hours in total. Forty hours have been spent on Web-Browsers, forty hours on IMs and forty hours on File Sharing applications. The duration of the experiment has been selected according to the number of hours that an average user connects to the Internet for, based on different authors and statistics (ComScore, 2007; JCMC, 2002 and Oxford, 2006).

3.1 Network Setup

The Host and the Firewall have formed a network. The Host was located to the Intranet (Internal Network) of the network which was formed for the experiment. In order to connect to the Internet (External Network), the Host first had to go through the Firewall and then if the rules allowed it, it would connect to the Internet. The Firewall was placed between the Internet and the Intranet. It was the PC which was providing to the Host, access to the Internet. Also the Firewall had the rules which allowed the traffic from all the ports to be allowed or denied. The final function of the Firewall was to capture all the packages which went through it, whether they were headed from the Intranet to the Internet or from the Internet to the Intranet.

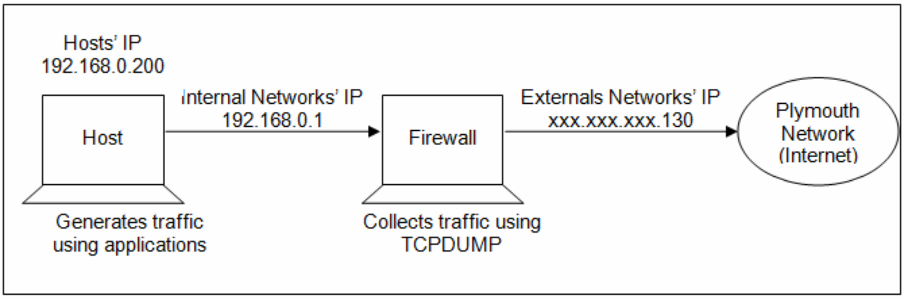

Figure 1: Experiments' Setup

The local IP of the Host, within the Intranet, was 192.168.0.200. However this has not been the IP that appeared in the Hosts' packages. When the packages were going to the Firewall, in order to be redirected to the Internet, the Firewall was changing the source IP, from the local IP of the Host, to the external IP address of the network. The external IP address was replaced with xxx.xxx.xxx.130 for security reasons. When a server was receiving the package, or when an attacker was encountering the package, the IP which would appear on the package was the external IP of the network (Figure 1).

3.2 Hardware

The hardware that the host has been consisted of was a processor 'Intel Pentium III' in 701 MHz (Megahertz) and 256 MB (Megabyte) RAM (Random Access Memory). The Host had one network card installed, which was using in order to connect to the Firewall.

The firewall had a bit stronger hardware than the host, since it had more demanding applications installed and it would be used for more demanding processes. Its' processor was an Intel Pentium III in 800 MHz. The RAM was 190. The Firewall had two network cards installed. One card was used to connect the Firewall with the Host, and create the Intranet. The other network card was used to connect the Firewall, and the Host through it, to the Internet.

3.3 Software

Web-Browser

Two Web-Browsers have been selected for the experiment. The first one was Microsofts' Internet Explorer and the second was the open source software, Mozilla Firefox. Both of these applications, had been selected as the most popular web-browsers that users prefer to use, according to the statistics that the web-site W3Schools (2007) has released. The Web-Browsers establish connections to other servers that provide web-sites through port 80, while they use other ports in order to connect to other services. Port 443 which has been used in the research is used for the e-mail service of the University of Plymouth (Table 1).

Application	Direction	Port No	Protocol	Action
Web-browser	Host->Firewall	80	HTTP	Allow
e-mail	Host->Firewall	443	HTTPS	Allow
General	Host->Firewall	All	All	Deny

Table 1: Rules setup for Web-Browsers

Instant Messenger

MSN has been the first application selected for the experiment for the IMs. MSN is Microsofts' messenger. MSN had been selected because according to the web-site FreebieList.com (2007), MSN is one of the most popular web-browsers of the Internet therefore it is probably targeted by attackers more often than other messengers. The main port that the MSN uses in order to connect to the server is

1863, using the TCP protocol. In order for two users to communicate, their communication goes through the server, and the server redirects the messages to the users (Hindocha and Chien, 2003) (Table 2).

Yahoo! Messenger has been the second application for the IMs. Yahoo! Messenger was also one of the most popular messengers according to FreebieList.com (2007). The ports that Yahoo! Messenger uses are 5000 using the TCP protocol for the voice chat, and port 5050 using the TCP protocol for the chat messages. The user connects to the server in order to register in the network. While it is connected to the server, the users' messages go through the server first and then are redirected to the contact (Hindocha and Chien, 2003) (Table 2).

Application	Direction	Port No	Protocol	Action
MSN	Host->Firewall	1863	TCP	Allow
Yahoo!	Host->Firewall	5050	TCP	Allow
Yahoo!	Host->Firewall	5000	TCP	Allow
General	Host->Firewall	All	All	Deny

Table 2: Rules setup for IM

File Sharing

eMule had been selected to represent the File Sharing applications. In eMule, the application first connects to server through a port that the server has specified. Usually each server has different ports, which will accept connections from. While in the server, the user can search for a file, by providing a name for the file. The server then provides a list of files, according to the word that the user provided. When the user selects the file/s to download, the server provides directly to the eMule application, the IP addresses of the hosts over the Internet which have and share the selected file/s. The eMule then connects to all the PCs directly, not through the server, and starts downloading the file/s.

Application	Direction	Port No	Protocol	Action
eMule	Firewall->Host	12679	TCP	Allow
eMule	Firewall->Host	12689	UDP	Allow
eMule	Host->Firewall	4242	TCP	Allow
General	Host->Firewall	All	All	Deny

Table 3: Rules setup for P2P

However in eMule, the user has to specify the ports from which the traffic will go through. A port has to be set for TCP (Transmission Control Protocol) and a port for UDP (User Datagram Protocol). eMule will communicate with other applications, sending the traffic through these ports. However the application at the other end might not have the same ports open. In this case eMule will redirect the traffic towards that application from another port, matching the applications open port (Table 3). During the experiment though, the firewall was setup to allow traffic from specific ports only. Because of this configuration, only a few other applications have been able to connect to the Host. It is not certain whether this has affected the results or not.

4 Results

4.1 Web-Browsers

Analysing the captured traffic from the Web-Browsers, has revealed one alert of 'MS-SQL Worm propagation attempt', one alert of 'MS-SQL Worm propagation attempt OUTBOUND', one alert of 'MS-SQL version overflow attempt', three alerts of 'DNS SPOOF query response with TTL of 1 min. and no authority', two alerts of 'ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited', three alerts of WEB-CLIENT Adobe Photoshop PNG file handling stack buffer overflow attempt, forty-five alerts of 'ATTACK-RESPONSES 403 Forbidden' and one-hundred-fifty-six (156) alerts of 'ATTACK-RESPONSES Invalid URL'.

4.2 Instant Messengers

After analysing the captured traffic from the IMs, the following alerts have been revealed. Eight alerts of 'MS-SQL Worm propagation attempt', eight alerts of 'MS-SQL Worm propagation attempt OUTBOUND', eight alerts of 'MS-SQL version overflow attempt' and three alerts of 'ICMP redirect host'.

4.3 File Sharing

Analysing the traffic generated by File Sharing applications has revealed twelve alerts of 'MS-SQL Worm propagation attempt', twelve alerts of 'MS-SQL Worm propagation attempt OUTBOUND', twelve alerts of 'MS-SQL version overflow attempt' and one alert of '(portscan) TCP portscan'.

5 Discussion

Web-Browsers

The analysis of the Web-Browsers' traffic has revealed that these applications are vulnerable to a variety of attacks. Within the forty hours of experiment, the Web-Browsers have accepted attacks of DoS, Cross Site Scripting/Buffer Overflow and

Spoofing. The MS-SQL related alerts that have been detected are not based on the traffic that the applications have generated, rather they are based on the random selection of an IP address by the ‘Slammer’ worm (CAIDA, nodate)

The users need to be very careful when they are using Web-Browsers because there are a lot of ways for an attacker to compromise their PCs and steal private information about or from them. Many of the attacks are easy to launch, especially because of the variety of tools that are freely available and from the fact that anyone from any place of the world can setup a fake server and use it for attacks. Most importantly the Web-Browsers are vulnerable to attacks which are not visible by the users hence there is no way to protect themselves from them.

Instant Messengers

The IMs have only accepted an eavesdropping/spoofing attack. The MS-SQL related alerts have not been generated by the traffic that the IMs have generated. The IMs are submitted to a low number of attacks because they communicate to other IM indirectly through the server, hence it becomes hard to detect and launch an attack on the traffic they generate.

According to the results of the experiment, the users have few reasons to be afraid of the attacks that are based on the traffic that the IM applications generate. What they need to be careful of is adding new users to their buddy list, and accepting files even when they are sent from contacts of the buddy list.

File Sharing

The File Sharing application has only been submitted to a portscan attack, which is based on the reveal of the IP/ports. Despite the fact that the reveal of such information should have increased the number of attacks, there has only been one alert of this kind. The MS-SQL related alerts have not been generated by the traffic that the application has generated.

According to the analysis of the results, the users who use File Sharing applications are not potential victims of an attack. The attackers do not appear to be interested on hosts which use such applications. There is a possibility that the outcome of the File Sharing applications has been affected by the fact that only a few ports have been opened, hence the application has established connections with a few other applications and has not generated enough traffic.

6 Conclusion

This paper has introduced the vulnerabilities that the users are exposed to when they are using applications of Web-Browsing, Instant Messaging and File Sharing. The results have revealed that the average users do not accept many attacks while using Peer-to-Peer and Instant Messaging applications. However the number of attacks and the level of aggressiveness are increased while they are using Web-Browsers. The data have been collected by isolating the traffic of the network, allowing only traffic by these applications to be generated. Any future work to improve the quality of the research would be to use more applications from each type, in order to increase the chances of an attacker detecting their traffic. Also adding more files to File Sharing applications could help. A last suggestion would be to allow the applications to generate traffic for more time than the time which had been allowed in this experiment.

7 References

CAIDA (nodate) “The Spread of the Sapphire/Slammer Worm” http://www.caida.org/publications/papers/2003/sapphire/sapphire.html (date accessed: 24/08/07)

ComScore (2007) “Press Release” http://www.comscore.com/press/release.asp?press=849 (date accessed: 06/04/2007)

FaceTime (2005) “Real-time Security for the Real-time Enterprise” http://www.spywareguide.com/whitepapers/wp_rtg500.pdf (date accessed: 29/11/2006)

FreebieList.com (2007) “Free Chat Programs and Chat Freeware Tools” http://www.freebielist.com/chatprograms.htm (date accessed: 01/06/2007)

Hindocha N. (2003) “Threats to Instant Messaging” http://www.symantec.com/avcenter/reference/threats.to.instant.messaging.pdf (date accessed: 29/11/2006)

Hindocha N. and Chien E. (2003) “Malicious Threats and Vulnerabilities in Instant Messaging” http://www.symantec.com/avcenter/reference/malicious.threats.instant.messaging.pdf (date accessed: 29/11/2006)

JCMC – Jounral of Computer-Mediated Communication (2002) “User Behaviour and the ‘Globalness’ of Internet: From the Taiwan Users’ Perspective” http://jcmc.indiana.edu/vol7/issue2/taiwan.html (date accessed: 06/04/2007)

Moseley R. (2007) “Developing Web Applications” John Wiley & Son, Ltd, Middlesex University, ISBN-13: 978-0-470-01719

Oxford University (2006) “Entwined in the network of networks” http://www.ox.ac.uk/publicaffairs/pubs/annualreview/ar05/02.shtml (date accessed: 06/04/2007)

Piccard P. (2003) “Risk exposure: Instant messaging and Peer-to-Peer Networks” documents.iss.net/whitepapers/X-Force_P2P.pdf (date accessed: 29/11/2006)

Sagar A. and Chakrabarty S. (2003) "Common attack methods" http://www.cert-in.org.in/knowledgebase/presentation/Commonattackmethods.pdf (date accessed: 12/03/2007)

W3Schools (2007) “Browser Statistics” http://www.w3schools.com/browsers/browsers_stats.asp (date accessed: 01/06/2007)