Hacking tricks toward security on network environments

Tzer-Shyong Chen[1], Fuh-Gwo Jeng[2], and Yu-Chia Liu[1]

[1] Department of Information Management, Tunghai University, Taiwan

[2] Department of Applied Mathematics, National Chiayi University, Taiwan

E-Mail: fgjeng@mail.ncyu.edu.tw

Abstract

Mounting popularity of the Internet has led to the birth of Instant Messaging, an up-and-coming form of Internet communication. Instant Messaging is very popular with businesses and individuals since it has instant communication ability. As a result, Internet security has become a pressing and important topic for discussion. Therefore, in recent years, a lot of attention has been drawn towards Internet security and the various attacks carried out by hackers over the Internet. People today often handle affairs via the Internet. For instance, instead of the conventional letter, they communicate with others by e-mails; they chat with friends through an instant messenger; find information by browsing websites instead of going to the library; perform e-commerce transactions through the Internet, etc. Although the convenience of the Internet makes our life easier, it is also a threat to Internet security. For instance, a business email intercepted during its transmission may let slip business confidentiality; file transfers via instant messengers may also be intercepted, and then implanted with backdoor malwares; conversations via instant messengers could be eavesdropped. Furthermore, ID and password theft may lose us money when using Internet bank service. Attackers on the Internet use hacking tricks to damage systems while users are connected to the Internet. These threats along with possible careless disclosure of business information make Instant Messaging a very unsafe method of communication for businesses. The paper divides hacking tricks into three categories: (1) Trojan programs that share files via instant messenger. (2) Phishing or fraud via e-mails. (3) Fake Websites.

Keywords: Hacking tricks, Trojan programs, Phishing, Firewall, Intrusion detection system.

1. Introduction

Increasingly more people are using instant messengers such as MSN Messenger, Yahoo! Messenger, ICQ, etc as the media of communication. These instant messengers transmit alphanumeric message as well as permit file sharing. During transfer, a file may be intercepted by a hacker and implanted with backdoor malware. Moreover, the e-mails users receive every day may include Spam, advertisements, and fraudulent mail intended to trick uninformed users. Fake websites too are prevalent. Websites which we often visit could be counterfeited by imitating the interface and the URL of the original, tricking users. The paper classifies hacking tricks into three categories which are explained in the following sections.

2. Hacking Tricks

The paper divides hacking tricks into three categories: (1) Trojan programs that share files via instant messenger. (2) Phishing (3) Fake Websites.

2.1 Trojan programs that share files via instant messenger

Instant messaging allows file-sharing on a computer [9]. All present popular instant messengers have file sharing abilities, or allow users to have the above functionality by installing patches or plug-ins; this is also a major threat to present information security. These communication softwares also make

Proceedings of the Seventh International Conference on
Parallel and Distributed Computing,Applications and Technologies (PDCAT'06)
0-7695-2736-1/06 $20.00 © 2006 IEEE

IEEE COMPUTER SOCIETY

it difficult for existing hack prevention methods to prevent and control information security. Therefore, we shall discuss how to control the flow of instant messages and how to identify dangerous user behavior.

Hackers use instant communication capability to plant Trojan program into an unsuspected program; the planted program is a kind of remotely controlled hacking tool that can conceal itself and is unauthorized. The Trojan program is unknowingly executed, controlling the infected computer; it can read, delete, move and execute any file on the computer. The advantages of a hacker replacing remotely installed backdoor Trojan programs [1] with instant messengers to access files are:

When the victim gets online, the hacker will be informed. Thus, a hacker can track and access the infected computer, and incessantly steal user information.

A hacker need not open a new port to perform transmissions; he can perform his operations through the already opened instant messenger port.

Even if a computer uses dynamic IP addresses, its screen name doesn't change.

Certain Trojan programs are designed especially for instant messengers. These Trojans can change group settings and share all files on the hard disk of the infected computer. They can also destroy or modify data, causing data disarray. This kind of program allows a hacker access to all files on an infected computer, and thus poses a great threat to users. The Trojan program takes up a large amount of the resources of the computer causing it to become very slow and often crashes without a reason.

Trojan programs that access a user computer through an instant messenger are probably harder to detect than classic Trojan horse programs. Although classic Trojan intrudes a computer by opening a listening or outgoing port which is used to connect to a remote computer, a desktop firewall can effectively block such Trojans. Alternatively, since it is very difficult for the server's firewall to spot intrusion by controlling an instant messenger's flow, it is extremely susceptible to intrusion.

Present Trojan programs have already successfully implemented instant messengers. Some Trojan programs are Backdoor Trojan, AIMVision, and Backdoor. Sparta.C. Backdoor Trojans use ICQ pager to send messages to its writer. AIMVision steals AIM related information stored in the Windows registry, enabling a hacker to setup an AIM user id. Backdoor. Sparta.C uses ICQ to communicate with its writer and opens a port on an infected host and send its IP Address to the hacker, and at the same time attempts to terminate the antivirus program or firewall of the host.

2.1.1 Hijacking and Impersonation

There are various ways through which a hacker can impersonate other users [7]. The most commonly used method is eavesdropping on unsuspecting users to retrieve user accounts, passwords and other user related information.

The theft of user account number and related information is a very serious problem in any instant messenger. For instance, a hacker after stealing a user's information impersonate the user; the user's contacts not knowing that the user's account has been hacked believe that the person they're talking to is the user, and are persuaded to execute certain programs or reveal confidential information. Hence, theft of user identity not only endangers a user but also surrounding users. Guarding against Internet security problems is presently the focus of future research; because without good protection, a computer can be easily attacked, causing major losses.

Hackers wishing to obtain user accounts may do so with the help of Trojans designed to steal passwords. If an instant messenger client stores his/her password on his/her computer, then a hacker can send a Trojan program to the unsuspecting user. When the user executes the program, the program shall search for the user's password and send it to the hacker. There are several ways through which a Trojan program can send messages back to the hacker. The methods include instant messenger, IRC, e-mails, etc.

Current four most popular instant messengers are AIM, Yahoo! Messenger, ICQ, and MSN Messenger, none of which encrypts its flow. Therefore, a hacker can use a man-in-the-middle attack to hijack a connection, then impersonate the hijacked user and participate in a chat-session. Although difficult, a hacker can use the man-in-the-middle attack to hijack the connection entirely. For example, a user may receive an offline message that resembles that sent by the server, but this message could have been sent by the hacker. All at once, the user could also get disconnected to the server. Furthermore, hackers may also use a Denial of Service (DoS) tool or other unrelated exploits to break the user's connection. However, the server keeps the connection open, and does not know that the user has been disconnected; thus allowing the hacker to impersonate the user. Moreover, since the data flow is unencrypted and unauthenticated, a hacker can use man-in-the-middle attacks that are similar to that of ARP fraud to achieve its purpose.

2.1.2 Denial of Service (DoS)

There are many ways through which a hacker can launch a denial of service (DoS) attack [2] on an instant messenger user. A Partial DoS attack will cause a user end to hang, or use up a large portion of CPU resources causing the system to become unstable.

Another commonly seen attack is the flooding of messages to a particular user. Most instant messengers allow the blocking of a particular user to prevent flood attacks. However, a hacker can use tools that allow him to log in using several different identities at the same time, or automatically create a large number of new user ids, thus enabling a flood attack. Once a flood attack begins, even if the user realizes that his/her computer has been infected, the computer will not be able to respond. Thus, the problem cannot be solved by putting a hacker's user id on the ignore list of your instant messenger.

A DoS attack on an instant messenger client is only a common hacking tool. The difficulty of taking precautions against it could turn this hacking tool into dangerous DoS type attacks. Moreover, some hacking tools do not just cause an instant messenger client to hang, but also cause the user end to consume large amount of CPU time, causing the computer to crash.

2.1.3 Information Disclosure

Retrieving system information through instant messenger users is currently the most commonly used hacking tool [4]. It can effortlessly collect user network information like, current IP, port, etc. IP address retriever is an example. IP address retrievers can be used to many purposes; for instance, a Trojan when integrated with an IP address retriever allows a hacker to receive all information related to the infected computer's IP address as soon as the infected computer connects to the internet. Therefore, even if the user uses a dynamic IP address, hackers can still retrieve the IP address.

IP address retrievers and other similar tools can also be used by hackers to send data and Trojans to unsuspecting users. Hackers may also persuade unsuspecting users to execute files through social engineering or other unrelated exploits. These files when executed search for information on the user's computer and sends them back to the hacker through the instant messenger network.

Different Trojan programs were designed for different instant messaging clients. For example, with a user accounts and password stealing Trojans a hacker can have full control of the account once the user logs out. The hacker can thus perform various tasks like changing the password and sending the Trojan program to all of the user's contacts.

Moreover, Trojans is not the only way through which a hacker can cause information disclosure. Since data sent through instant messengers are unencrypted, hackers can sniff and monitor entire instant messaging transmissions. Suppose an employee of an enterprise sends confidential information of the enterprise through the instant messenger; a hacker monitoring the instant messaging session can retrieve the data sent by the enterprise employee. Thus, we must face up to the severity of the problem.

2.2 Phishing

The word “Phishing” first appeared in 1996. It is a variant of ‘fishing’, and formed by replacing the ‘f’ in ‘fishing’ with ‘ph’ from phone. It means tricking users of their money through e-mails.

Based on the statistics of the Internet Crime Complaint Center, loss due to internet scam was as high as $1.256 million USD in 2004. The Internet Crime Complaint Center has listed the above Nigerian internet scam as one of the ten major internet scams.

Based on the latest report of Anti-Phishing Working Group (APWG) [8], there has been a 28% growth of Phishing scams in the past 4 months, mostly in the US and in Asia. Through social engineering and Trojans, it is very difficult for a common user to detect the infection.

To avoid exploitation of your compassion, the following should be noted:

(1) When you need to enter confidential information, first make sure that the information is entered via an entirely secure and official webpage. There are two ways to determine the security of the webpage:
   a. The address displayed on the browser begins with https://, and not http://. Pay attention to if the letter ‘s’ exists.
   b. There is a security lock sign on the lower right corner of the webpage, and when your mouse points to the sign, a security certification sign shall appear.

(2) Consider installing a browser security software like SpoofStick which can detect fake websites.

(3) If you suspect the received e-mail is a Phishing e-mail, do not open attachments attached to the email. Opening an unknown attachment could install malicious programs onto your computer.

(4) Do not click on links attached to your emails. It is always safer to visit the website through the official link or to first confirm the authenticity of the link. Never follow or click on suspicious links in an e-mail. It is advisable to enter the URL at the address bar of the web browser, and not follow the given link.

Generally speaking, Phishing [3] [5] is a method that exploits people’s sympathy in the form of aid-seeking e-mails; the e-mail act as bait. These e-mails usually request their readers to visit a link that seemingly links to some charitable organization’s website; but in truth links the readers to a website that will install a Trojan program into the reader’s computer. Therefore, users should not forward unauthenticated charity mails, or click on unfamiliar links in an e-mail. Sometimes, the link could be a very familiar link or an often frequented website, but still, it would be safer if you’d type in the address yourself so as to avoid being linked to a fraudulent website. Phisher deludes people by using similar e-mails mailed by well-known enterprises or banks; these e-mails often asks users to provide personal information, or result in losing their personal rights; they usually contain a counterfeit URL which links to a website where the users can fill in the required information. People are often trapped by phishing due to inattention

Besides, you must also be careful when using a search engine to search for donations and charitable organizations.

2.3 Fake Websites

Fake bank websites stealing account numbers and passwords have become increasingly common with the growth of online financial transactions. Hence, when using online banking, we should take precautions like using a secure encrypted customer’s certificate, surf the net following the correct procedure, etc.

There are countless kinds of phishing baits, for instance, messages that say data expired, data invalid, please update data, or identity verification intended to steal account ID and matching password. This type of online scam is difficult for users to identify. As scam methods become finer, e-mails and forged websites created by the impostor resemble their original, and tremendous losses arise from the illegal transactions.

The following are methods commonly used by fake websites. First, the scammers create a similar website homepage; then they send out e-mails with enticing messages to attract visitors. They may also use fake links to link internet surfers to their website. Next, the fake website tricks the visitors into entering their personal information, credit card information or online banking account number and passwords. After obtaining a user's information, the scammers can use the information to drain the bank accounts, shop online or create fake credit cards and other similar crimes. Usually, there will be a quick search option on these fake websites, luring users to enter their account number and password. When a user enters their account number and password, the website will respond with a message stating that the server is under maintenance. Hence, we must observe the following when using online banking:

(1) Observe the correct procedure for entering a banking website. Do not use links resulting from searches or links on other websites.
(2) Online banking certifications are currently the most effective security safeguard measure.
(3) Do not easily trust e-mails, phone calls, and short messages, etc. that asks for your account number and passwords.

Phishers often impost a well-known enterprise while sending their e-mails, by changing the sender's e-mail address to that of the well known enterprise, in order to gain people's trust. The 'From' column of an e-mail is set by the mail software and can be easily changed by the web administrator. Then, the Phisher creates a fake information input website, and send out e-mails containing a link to this fake website to lure e-mail recipients into visiting his fake website.

Most Phishers create imitations of well known enterprises websites to lure users into using their fake websites. Even so, a user can easily notice that the URL of the website they're entering has no relation to the intended enterprise. Hence, Phishers may use different methods to impersonate enterprises and other people. A commonly used method is hiding the URL. This can easily be done with the help of JavaScript.

Another way is to exploit the loopholes in an internet browser, for instance, displaying a fake URL in the browser's address bar. The security loophole causing the address bar of a browser to display a fake URL is a commonly used trick and has often been used in the past. For example, an e-mail in HTML format may hold the URL of a website of a well-known enterprise, but in reality, the link connects to a fake website.

The key to successfully use a URL similar to that of the intended website is to trick the visual senses. For example, the sender's address could be disguised as that of Nikkei BP, and the link set to http://www.nikeibp.co.jp/ which has one k less than the correct URL which is http://www.nikkeibp. co.jp/. The two URLs look very similar, and the difference barely noticeable. Hence people are easily tricked into clicking the link.

Besides the above, there are many more scams that exploit the trickery of visual senses. Therefore, you should not easily trust the given sender's name and a website's appearance. Never click on unfamiliar and suspicious URLs on a webpage. Also, never enter personal information into a website without careful scrutiny.

3. Conclusions

Business strategy is the most effective form of defense and also the easiest to carry out. Therefore, they should be the first line of defense, and not last. First, determine if instant messaging is essential in the business; then weigh its pros and cons. Rules and norms must be set on user ends if it is decided that the business cannot do without instant messaging functionality. The end server should be able to support functions like centralized logging and encryption. If not, then strict rules must be drawn, and carried out by the users. Especially, business discussions must not be done over an instant messenger.

The paper categorized hacking tricks into three categories: (1) Trojan programs that share files via instant messenger. (2) Phishing (3) Fake Websites. Hacking tricks when successfully carried out could cause considerable loss and damage to users. The first category of hacking tricks can be divided into three types: (1) Hijacking and Impersonation; (2) Denial of Service; (3) Information Disclosure.

Acknowledgement: This work was supported by the National Science Council, Taiwan, under contract No. NSC 95-2221-E-029-024.

References

[1] B. Schneier, "The trojan horse race," *Communications of ACM*, Vol. 42, 1999, pp. 128.

[2] C. L. Schuba, "Analysis of a denial of service attack on TCP," *IEEE Security and Privacy Conference*, 1997, pp. 208-223.

[3] E. Schultz, "Phishing is becoming more sophisticated," *Computer and Security*, Vol. 24(3), 2005, pp. 184-185.

[4] G. Miklau, D. Suciu, **"**A formal analysis of information disclosure in data exchange," *International Conference on Management of Data*, 2004, pp. 575-586.

[5] J. Hoyle, "'Phishing' for trouble," *Journal of the American Detal Association,* Vol. 134(9), 2003, pp. 1182-1182.

[6] J. Scambray, S. McClure, G. Kurtz, *Hacking exposed: network security secrets and solutions*, McGraw-Hill, 2001.

[7] T. Tsuji and A. Shimizu, "An impersonation attack on one-time password authentication protocol OSPA," to appear in *IEICE Trans. Commun*, Vol. E86-B, No.7, 2003.

[8] Anti-Phishing Working Group, http://www.antiphishing.org.

[9] http://www.symantec.com/region/tw/enterprise/article/icq_threat.html.