International Journal of Educational Planning & Administration.
Volume 1, Number 1 (2011), pp. 43-53

http://www.ripublication.com/ijepa.htm

Types of Hacking Attack and their Counter Measure

Minakshi Bhardwaj and G.P. Singh

Galley discusses three types of attacks against computer systems: Physical, Syntactic and Semantic. A physical attack uses conventional weapons, such as bombs or fire. A syntactic attack uses virus-type software to disrupt or damage a computer system or network. A semantic attack is a more subtle approach. Its goal is to attack users' confidence by causing a computer system to produce errors and unpredictable results.

Syntactic attacks are sometimes grouped under the term "malicious software" or "malware". These attacks may include viruses, worms, and Trojan horses. One common vehicle of delivery formal ware is email.

Semantic attacks involve the modification of information or dissemination of incorrect information. Modification of information has been perpetrated even without the aid of computers, but computers and networks have provided new opportunities to achieve this. Also, the dissemination of incorrect information to large numbers of people quickly is facilitated by such mechanisms as email, message boards, and websites

Hacking tricks can be divided into different categories elaborated below:

1. Trojan programs that share files via instant messenger.
2. Phishing
3. Fake Websites.
4. Spoofing
5. Spyware
6. Electronic Bulletin Boards
7. Information Brokers
8. Internet Public Records
9. Trojan Horses
10. Wormhole Attack

Trojan programs that share files via instant messenger

Instant messaging allows file-sharing on a computer. 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 software also make it difficult for existing hack prevention method to prevent and control information security. 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 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.

Hijacking and Impersonation

There are various ways through which a hacker can impersonate other users. 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.

Denial of Service

There are many ways through which a hacker can launch a denial of service (DoS) attack 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.

There are many ways in which a hacker can cause a denial of service on an instant messenger client. One common type of attack is flooding a particular user with a large number of messages. The popular instant messaging clients contain protection against flood-attacks by allowing the victim to ignore certain users. However, there are many tools that allow the hacker to use many accounts simultaneously, or automatically create a large number of accounts to accomplish the flood-attack. Adding to this is the

fact that once, the flood-attack has started and the victim realizes what has happened, the computer may become unresponsive. Therefore, adding the attacking user accounts to the ignore list of the instant messenger client may be very difficult DoS attacks are very easy to generate and very difficult to detect, and hence are attractive weapons for hackers. In a typical DoS attack, the attacker node spoofs its IP address and uses multiple intermediate nodes to overwhelm other nodes with traffic. DoS attacks are typically used to take important servers out of action for a few hours, resulting in DoS for all users served by the server. It can also be used to disrupt the services of intermediate routers.

Phishing

The word phishing comes from the analogy that Internet scammers are using email lures to fish for passwords and financial data from the sea of Internet users. The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords from unsuspecting AOL users. Since hackers have a tendency to replacing “f'” with “ph” the term phishing was derived.

Phishing 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.

Phishing Techniques

Phishing techniques can be divided into different categories, some of which are elaborated below:

Link manipulation

Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishers, such as this example URL, http://www.yourbank.com.example.com/. Another common trick is to make the anchor text for a link appear to be valid, when the link actually goes to the phishers' site.

An old method of spoofing used links containing the '@' symbol, originally intended as a way to include a username and password (contrary to the standard). For example, the link http://www.google.com@members.tripod.com/might deceive a casual observer into believing that it will open a page on www.google.com. whereas it

actually directs the browser to a page on members.tripod.com, using a username of www.google.com: the page opens normally, regardless of the username supplied. Such URLs were disabled in Internet Explorer, while the Mozilla and Opera web browsers opted to present a warning message and give the option of continuing to the site or canceling.

A further problem with URLs has been found in the handling of Internationalized domain names (lDN) in web browsers, that might allow visually identical web addresses to lead to different, possibly malicious, websites. Despite the publicity surrounding the flaw, known as IDN spoofing or a homograph attack, no known phishing attacks have yet taken advantage of it. Phishers have taken advantage of a similar risk, using open URL redirectors on the websites of trusted organizations to disguise malicious URLs with a trusted domain.

Filter evasion

Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing emails.

Website forgery

Once the victim visits the website the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar or by closing the original address bar and opening a new one with the legitimate URL.

An attacker can even use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, although it is very difficult to spot without specialist knowledge. Just such a flaw was used in 2006 against Pay Pal.

A Universal Man-in-the-middle Phishing Kit, discovered by RSA Security, provides a simple-to-use interface that allows a phisher to convincingly reproduce websites and capture log-in details entered at the fake site.

Phone phishing

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Voice phishing sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

Solutions

Social responses

One strategy for combating phishing is to train people to recognise phishing attempts,

and to deal with them. Education can be promising, especially where training provides direct feedback.

People can take steps to avoid phishing attempts by slightly modifying their browsing habits. When contacted about an account needing to be "verified" (or any other topic used by phishers), it is a sensible precaution to contact the company from which the email apparently originates to check that the email is legitimate. Alternatively, the address that the individual knows is the company's genuine website can be typed into the address bar of the browser, rather than trusting any hyperlinks in the suspected phishing message.

Technical responses

Anti-phishing measures have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures. The following are some of the main approaches to the problem.

Helping to identify legitimate sites

Since phishing is based on impersonation, preventing it depend on some reliable way to determine a website's real identity. For example, some anti-phishing toolbars display the domain name for the visited website. The pet-name extension for Fire-fox lets users type in their own labels for websites, so they can later recognize when they have returned to the site. If the site is suspect, then the software may either warn the user or block the site outright.

Fake Web sites

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.

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:

Observe the correct procedure for entering a banking website. Do not use links resulting from searches or links on other websites.

Online banking certifications are currently the most effective security safeguard measure.

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.

Solutions

Internet Explorer 7 and Fire-fox 2 both have sophisticated filters that can detect most fake websites.

Here are some other clues that might give away a fake:

- Look for evidence of a real-world presence: an address, a phone number, an email contact. If in doubt, send an email, make a phone call or write a letter to establish whether they really exist.
- The website's address is different from what you are used to, perhaps there are extra characters or words in it or it uses a completely different name or no name at all, just numbers.
- Right-clicking on a hyperlink and selecting "Properties" should reveal a link's true destination - beware if this is different from what is displayed in the email.
- Even though you are asked to enter private information there is NO padlock in the browser window or 'https://' at the beginning of the web address to signify that it is using a secure link and that the site is what it says it is.
- A request for personal information such as user name, password or other security details IN FULL, when you are normally only asked for SOME of

them.

- Although rare, it is possible for your computer to be corrupted by viruses in such a way that you can type a legitimate website address into your browser and still end up at a fake site. This problem is known as 'pharming'. Check the address in your browser's address bar after you arrive at a website to make sure it matches the address you typed. Subtle changes ('eebay' instead of 'ebay' for example) may indicate that your computer is a victim of a pharming attack.

Pharming

Similar in nature to phishing, Pharming (pronounced farming) is a Hacker's attack aiming to redirect a website's traffic to another, bogus website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real addresses - they are the "signposts" of the Internet. Compromised DNS servers are sometimes referred to as "poisoned". The term pharming is a word play on farming and phishing. The term phishing refers to social engineering attacks to obtain access credentials such as user names and passwords. In recent years pharming has been used to steal identity information. Pharming has become of major concern to businesses hosting ecommerce and online banking websites.

Spoofing

A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.

A closely interconnected and often confused term with phishing and pharming is spoofing. A "spoofer", in Internet terms, is defined generally as the "cracker" who alters, or "forges", an e-mail address, pretending to originate a message from a different source address than that which he or she truly has. There are many ways an attacker may do this, and there are many types of attacks. The attacker may do this to gain access to a secured site that would accept the "hijacked" address as one of few permissible addresses, or more maliciously, the reason may be to hide the source of any type of attack. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

Spoofing Attacks Techniques

Spoofing attacks can be divided into different categories, some of which are elaborated below:

Man-in-the-middle attack and internet protocol spoofing

An example from cryptography is the man-in-the-middle attack, in which an attacker spoofs Alice into believing they're Bob, and spoofs Bob into believing they're Alice, thus gaining access to all messages in both directions without the trouble of any.

Spyware

Spyware is computer software that can be used to gather and remove confidential information from any computer without the knowledge of the owner. Everything the surfer does online, including his passwords, may be vulnerable to spyware. Spyware can put anyone in great danger of becoming a victim of identity theft. Moreover, some forms of spyware can be installed on the computer from a remote location without the identity thief ever having physical access to the victim's computer.

While the term spyware suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting Web browser activity, accessing websites blindly that will cause more harmful viruses, or diverting advertising revenue to a third party. Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of Internet or other programs. In an attempt to increase the understanding of spyware, a more formal classification of its included software types is captured under the term privacy-invasive software.

In response to the emergence of spyware, a small industry has sprung up dealing 1ll anti-spyware software. Running anti-spyware software has become a widely recognized element of computer security best practices for Microsoft Windows desktop computers. A number of jurisdictions have passed anti-spyware laws, which usually target any software that is surreptitiously installed to control a user's computer.

Routes of infection

Spyware does not directly spread in the manner of a computer virus or worm: generally, an infected system does not attempt to transmit the infection to other computers. Instead, spyware gets on a system through deception of the user or through exploitation of software vulnerabilities.

Most spyware is installed without users' knowledge. Since they tend not to install software if they know that it will disrupt their working environment and compromise their privacy, spyware deceives users, either by piggybacking on a piece of desirable software such as Kazaa or Limewire, tricking them into installing it (the Trojan horse method). Some "rogue" anti-spyware programs masquerade as security software, while being spyware themselves. The distributor of spyware usually presents the program as a useful utility - for instance as a "Web accelerator" or as a helpful software agent. Users download and install the software without immediately suspecting that it could cause harm.

Spyware can also come bundled with shareware or other downloadable software, as well as music CDs. The user downloads a program and installs it, and the installer additionally installs the spyware. Although the desirable software itself may do no harm, the bundled spyware does. In some cases, spyware authors have paid shareware authors to bundle spyware with their software. In other cases, spyware authors have repackaged desirable free software with installers that add spyware.

A third way of distributing spyware involves tricking users by manipulating security features designed to prevent unwanted installations. Internet Explorer prevents web sites from initiating an unwanted download. Instead, it requires a user action, such as clicking on a link. However, links can prove deceptive: for instance, a pop-up ad may appear like a standard Windows dialog box. The box contains a message such as "Would you like to optimize your Internet access?" with links which look like buttons reading Yes and No. No matter which "button" the user presses, a download starts, placing the spyware on the user's system. Later versions of Internet Explorer offer fewer avenues for this

Solutions

As the spyware threat has worsened, a number of techniques have emerged to counteract it. These include programs designed to remove or to block spyware, as well as various user practices which reduce the chance of getting spyware on a system. Nonetheless, spyware remains a costly problem. When a large number of pieces of spyware have infected a Windows computer, the only remedy may involve backing up user data, and fully reinstalling the operating system.

Security practices

To deter spyware, computer users have found several practices useful in addition to installing anti-spyware programs.

Many system operators install a web browser other than IE, such as Opera or Mozilla Fire-fox. Although these have also suffered some security vulnerabilities, their comparatively small market share compared to Internet Explorer makes it uneconomic for hackers to target users on those browsers. Though no browser is completely safe, Internet Explorer is at a greater risk for spyware infection due to its large user base as well as vulnerabilities such as ActiveX.

Electronic Bulletin Boards

Chat rooms and electronic bulletin boards have become breeding grounds for identity theft. When criminals have obtained personal identifying information such as credit card numbers or social security numbers, they visit hacker chat rooms and post messages that they have personal information for sale.

In April 16, 2004, a Manchester, New Hampshire man was sentenced on eight felony counts related to a website and electronic bulletin boards where he posted for sale thousands of Social Security Numbers and other personal information belonging to employees of Global Crossing, as well as threats to injure or kill.

Information Brokers

Information brokers have been around for decades, however, a new breed of information broker has emerged in recent years; the kind that sells personal information to anyone requesting it electronically via the Internet Driven by greed, some information brokers are careless when they receive an order. They fail to verify the identity of the requesting party and do little, if any, probing into the intended use

of the information.

In one case, a 24-year old Indian man who at the time (March 2005) worked for Gurgaon-based online marketing firm named Infinity eSearch, allegedly sold information on 1,000 bank accounts to an undercover journalist working for The Sun for £ 2,750. The victim has since claimed that he was only a middleman and that he did not sell data collected by his employer. Infinity eSearch has said the company does not handle any data for the banks named in the Sun report, and that the victim did not have access to confidential data of any kind through his employment with the company, according to press reports. But the case has raised fears of an anti outsourcing blacklash if Indian firms are seen to be careless with the data they handle.

Internet Public Records

There are two ways public records are accessible electronically. Some jurisdictions post them on their government web sites, thereby providing free or low-cost access to records. Government agencies and courts also sell their public files to commercial data compilers and information brokers. They in turn make them available on a fee basis, either via web sites or by special network hookups.

Identity theft

The crime of identity theft and other types of fraud will be fueled by easy access to personal identifiers and other personal information via electronic public records. Such information includes Social Security numbers, credit card and bank account numbers, and details about investments.

Solutions

What can be done to mitigate the negative consequences of making public records containing personal information available on the Internet and from other electronic services? Governments are not likely to make the decision to keep such records off the Internet altogether. Indeed, they should not. The public policy reasons for making public records available electronically are irrefutable - promoting easier access to government services as well as opening government practices to the public and fostering accountability.

But there are several approaches government agencies and court systems can take to minimize the harm to individuals when sensitive personal information is to be posted on the Internet while at the same time promoting government accountability.

Regulating the information broker industry

The information broker industry must be regulated. At present, information brokers purchase public records from local, state, and federal government agencies and repackage them for sale to subscribers. They add data files from commercial data sources such as credit reports and consumer survey data. Virtually anyone can obtain access to these files, although many information brokers claim they limit access to professions such as private investigators, attorneys, law enforcement, media, debt collectors, landlords, and employment background checkers. However, the effectiveness of such self-regulation is limited at best.

Requiring more accountability of the private investigator industry

The private investigator profession, a major user of public records information, must be regulated in those states where there are no oversight agencies. Further, existing regulations must be tightened and made uniform nationwide, perhaps by federal law. Private investigators must be held to strong standards regarding their access to and use of sensitive personal information. They should be held accountable when they misuse personal information.

Trojan Horses

In this context, a Trojan horse could be defined as an application that appears to be benign, but instead performs some type of malicious activity. A Trojan can be disguised as a game, an e-mail attachment, or even a Web page. As soon as the victim runs or opens the camouflaged application, the Trojan installs itself on the hard drive and then runs each time Windows is started.