Threats to Computer Security
Physical Security, Internal Security, Firewalls, Key-logging and Phishing

James Harryman: jh3e09@ecs.soton.ac.uk
Joshua O’Donovan: jodig09@ecs.soton.ac.uk
Peter West: pw9g09@ecs.soton.ac.uk
David Wigram: dw6g09@ecs.soton.ac.uk
Jamie Wilyman: jw14g09@ecs.soton.ac.uk
Computer Security

Abstract

Security of information is a topic that affects all computer users, from large companies to individuals who use computers casually, many of whom are unaware of the vast number of security issues that face them. This folder considers the modern threats to information by providing profiles on some of the most common threats: Physical Security, Internal Security, Firewalls, Key-logging and Phishing. Each document investigates the dangers of these “criminals” and provides methods to avoid becoming a victim. Provided with this information, users can be made aware of the dangers in order to take precautions to avoid them.

Background

In a world where computers are becoming more and more prevalent, information security is of vital importance to everyone. As more information is being stored in computer systems, criminals have created a variety of techniques to try and illegally access this information.

Failure of appropriate computer security can cause millions of pounds of damage - both to hardware and information. Subsequently, it is essential to both organisations and individuals to take steps to prevent security issues from affecting them. As the criminals’ techniques improve, so should the security of information.

Introduction

Information security is of increasing importance. It is an issue that nobody can completely avoid, as all computer users’ information is at risk of theft or manipulation. A broad topic, this profile folder considers a number of the most common risks to information.

Considered first are the threats of physical security. This is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. Threats can arise in multiple forms however there are simple solutions to combat those and keep data safe. Internal Security involves safeguarding against threats from corrupt, or even careless employees. To avoid the possibility of workers stealing the company information, techniques such as hierarchical access levels and employee monitoring are required.

A firewall, a hardware or software package that restricts access to a local network, provides vital security from threats on the internet, blocking harmful viruses and worms from planting themselves on computers and damaging information.

Key-logging is the act of intercepting keystrokes and storing them such that someone may steal information from a computer user. Finally, Phishing is considered. Phishing is the forgery of websites, and is to blame for many cases of internet fraud. This is perhaps one of the most widespread security problems, as it affects nearly all users, especially those who use email.

This folder contains documents that educate you on each of these issues to security and provides methods of preventing dangers.
Profile

Name:

Physical Security

Known Associates:

Disgruntled Employees, common thief

Evidence: Exhibit A

Criminal Background

Physical security is described as "the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled" (Mittal, 2009). This loss of data can be due to common theft or degradation due to environmental conditions. The following procedures can be implemented to negate these possibilities and keep your data safe and secure.

Environmental Conditions

These are often overlooked with respect to physical security; however, there is an easy process to combat this. Backing-up:

Regular backups of your data will reduce the problem of damaged/data but not stolen data. These backups can be on a multitude of physical platforms:

a) Optical DVD Media - Susceptible to light degradation and as such should be kept in dark conditions, cheap however for small amounts of data. Lasts for up to 10 years (Podio, 1991)

b) Disk Drives - Extremely long life time, 136 years and cheap for large amounts of data, however if knocked can result in data loss. (Schroeder, 2007)

c) Magnetic Tape - Long-term preferred option due to low cost of very large amounts of data. Last 30 years but requires special software. (Crespo, 2000)

All of these options though share some common concerns:

a) Keeping offsite - the advantage of this is that reduce risk of natural disasters in more than one location however as you will not be connected to the process of backing up can be inconvenient. Data may be lost in rough transportation.

b) Fireproof Safes - The risk of fire is a prevalent one and this simple procedure could stop this, safes are expensive for large amounts of data though.
a) Physical security—This is still a consideration wherever you keep your data and will be investigated further in this report.

**Physical Security**

Data can be obtained by a variety of malicious means, however these all involve in some capacity the action of theft. The question you have to ask yourself is this:

Who has physical access to your hardware?

If you know the answer to this question, life will be a lot easier however not full proof! The measures contained below detail how physical removal of your hardware can prevent theft.

b) Locks—Door locks for your Office/Room can range from the high-tech to the simplest deadlock. High-tech locks such as key card, keypad or fingerprint print scanners have the added advantage of being harder to break into. The copying of key cards also requires a more technically advanced criminal. The physical theft of a key card or keypad code, however, may open many doors within an office space, as opposed to a singular doorframe. Finger scanners or retina scanners are almost full-proof despite what you have seen in films but are extremely restrictive due to their price. The mortice deadlock should be regarded as the lowest form of security and should conform to British Standard number BS3621: 1998 for Thief Resistant Locks. These locks will protect against lock picking, force, drilling, manipulation and hacksaw attack. (Winchester, 1982)

c) Secure Workspaces—The next step within the office or home workspace security layer. These consist of the simple concept of attaching your hardware to a desk thus stopping removal of said device. The cage is normally locked and as such these locks should adhere to the above specifications otherwise rendering them useless. The beauty of this design is that it will deter the opportunist thief. With any closed box or cage the threat of overheating should always be considered.

d) Cable Type security cable If the thought of buying secure workspaces is prohibitive to your situation a much cheaper option is available. This cable security cable fits into the security lock slot present on most laptops and loops around an immovable object such as your desk. The PVC coated steel cables make it harder for bolt cutters and the like to be used.

e) Audible alarms—If already removed from a working area, the audible alarm is most effective at stopping the continued theft of a piece of hardware.

f) Video Surveillance—Moving to the higher end of the security scale is video surveillance. This will not stop thievery however, it does has the ability to put off the thought of theft. This would work well in a large office where
a) the possibility of worker theft (due to unanimity) is a threat. There may be ethical issues as to the filming of employees and it would also generate a lot of film that may need to be stored or looked through.

b) Wires / Cabling - These wires should be passed through walls and ceilings. As physical security is concerned with data loss, the hijacking of a system falls within this remit. Networks could easily be hacked through the tapping of cables incorporating an outside device.

c) Disposing - With the disposal of secure documents the possibility of theft is still prevalent. Thus shredding of all important documents should be compulsory. Even the formatting of disk drives is not full proof and the disposal of hard disk should employ disk wiping.

References


Profile

Name: Internal Security

Known Associates:

Employees, privacy and Corruption

Evidence: Exhibit B

Criminal Background

This is a relatively unknown danger to the security of a company. Although protection of data from outside threats is vital, there is a definite need for security internally as well. A company’s employees have access to all the data the company holds, and so it should be clear that measures need to be taken to guarantee the privacy of that information. Whether due to employees just being careless or actually being corrupt, this information could be leaked without proper internal security.

Threats

Whilst careless employee behaviour can be addressed by educating them on the dangers, as with physical and other security, dealing with corrupt employees is more challenging. There are many reasons why an employee might start misusing company information, and it can be done at many levels. The crime is usually done for some personal benefit for that employee, but it may be purely situational (Willison, 2006). The employee themselves may not even consider what they are doing to be an actual crime, and so a big part of the prevention of information misuse would again be to educate the employees further.

There are certain situations where employees may feel less loyal to their companies, and resort to stealing information as a safeguard against dismissal. During the recent recession, Mansfield-Devine, the editor of Network Security, explained how workers who fear they are about to lose their jobs were doing just that, or at least putting less effort into their work because they no longer cared about the consequences (2009). Even if employees who may be driven to such activities are in the minority, the consequences can be such that preventative measures must be taken.
Common Defences

Most companies will have a large amount of employees, many of whom will not need access to all of the data the company holds. In order to reduce the likeliness of employees misusing company information, access to secure data should be limited to only those employees who need to use that data. The method used for doing this is to provide access levels, usually using some sort of key code for different employees. These access levels follow a hierarchical system so that more important employees in the company, and therefore more trusted employees, will have access to more information than employees lower down in the company. The system used to assign access levels usually uses some sort of cryptographic key method, as outlined by Hwang and Yang (2000). The method allows easy assignment of access privileges to different employees. It will also mean that user relationships between different users of the system, referred to as Key-to-Key relationships, can be defined (Vrobleski, et al., 2005).

Even with access levels, however, there are still issues. If employees lose their commitment to their company, then even the employees who are considered trustworthy may be tempted to misuse the information they have access to. There are steps that can be taken to protect the data, including safeguards which involve trying to prevent employees who attempt to commit these crimes from succeeding, and deterrence, which involves trying to prevent employees from considering committing the crime in the first place (Willison, 2006). As valuable as these methods may be, there is no proof they are working without employee monitoring, which is the most valuable defence available.

Employee Monitoring and Related Issues

Employee monitoring can be achieved simply by examining their activities through the use of workplace, and by examining their work output, or it can be done through electronic tools. Monitoring tools have become fairly widespread, to the extent where many employees expect only a small level of privacy (Mitrou and Karydas, 2005). Monitoring tools can include examining websites accessed, time spent on each webpage, files accessed, and even employees’ personal communication. As such there needs to be a distinction between what is necessary to keep information secure, and what is too far and encroaching on invading privacy.
CASE STUDY

(Mansfield-Devine, 2007): The European Court of Human Rights decided in 2007 that a publicly funded Welsh college had violated an employee’s human rights by monitoring her email, phone and internet use. The Government stated that the monitoring was necessary to ensure the resources were not being used for personal use, but the Court found the argument unpersuasive. The employee was awarded €3000 in damages and £6000 in costs.

As the above case study shows, care needs to be taken in limiting the extent of the monitoring. It should be such that any criminal activity can be identified, without invading what could be personal and private information. There are also possible side effects of such extensive monitoring. Stoney (2000) explains how employee satisfaction can decrease significantly if they feel they have no freedom. There is clearly a balance that needs to be found.

References


What is a firewall? It's a hardware and/or software solution that restricts access from your internal network to the Internet -- and vice versa. (Chapman, 1995) A firewall uses a set of instructions within a system or network that is designed specifically to block unauthorized or unwanted access while still allowing the system to function. Firewalls are set up by the user and outline the criteria and strength of the protection they offer. For example, you wouldn't want a firewall that blocks all communication between systems. Only the unwanted transmissions. Firewalls when used properly can provide a significantly increase in computer security. Commonly firewalls can be classified into four categories, often more than one of which are used at the same time. (Bellovin, 1994).

**Threat Prevention**

The threat that firewalls prevent from entering our systems could affect any user of the Internet. More than a million systems are now connected to the Internet, and something like 15 million people in 100 countries on all seven continents use Internet services. More than 100 million email messages are exchanged each day, along with countless files, documents, and audio and video images. (Chapman, 1995) This alone shows that if one virus or worm entered a single email, with no firewalls, victims could reach potential be over 1 million users.

**Packet filtering.**

The main way that information is transferred across the Internet is in groups of data called packets. A single packet can be destined to many different sources and as it is received it must be quickly determined as to whether it should be accepted, forwarded or discarded. These decisions are made by nodes in a network system. Every node is responsible for examining every packet and accepting only those of interest. In this case the hardware performs a partial filtering and then passes the packet to the software for the full packet filtering. The criteria for the filtering is defined by the user and can be anything from very basic to high level filtering. The benefits of this firewall is that it is highly transparent to the user although is fairly difficult to configure. (US Patent, Hausman, 1995)
Application Layering.

This system is more effective that packet filtering as it works at all levels of an application. The idea being that it can understand certain application protocol that is desirable and detect unwanted protocol sneaking through into the application. This is especially useful for applications such as web browsers. A huge benefit of application layer is that it can be easily deployed onto the internet and needs no infrastructure support. Dealing with multicasting (distribution to more that one host) (Banerjee, 2002) is a simple function of this method and therefore ideal for nodes in a large network (i.e. the world wide web). In order to access how functional the application layer is, a number of tools are used: (Banerjee, 2002) The quality of data path; defined as how trustworthy a host is and its applicable redundancy. And the control overheads; which constitutes the stages and details of routers. Links and segments that are linked with the packet of data.

Stateful Filters.

Developed by AT&T and more commonly known as circuit level firewalls. This firewall performs Stateful Packet Inspection (SPI) and in basic terms it keeps track of the state of network connections. Three colleagues from AT&T and Bell Laboratories, developed this technique and defined it as a solution to preventing attack which exploit existing connection or denial of service attacks (Sharma, 2009). The principal being it maintains all records of connections and checks them against a series of static rules. Proxy Server. Perhaps considered the most junior aspect of firewalls. The proxy server intercepts all messages entering or leaving the network and hides the true network address. (Yadav, 2009)

Known Associates.

Worm

A computer worm is a software program that is designed to copy itself from one computer to another. Without human interaction. Unlike a computer virus, a worm can copy itself automatically. Worms can copy themselves in a large volume. For example, a malicious worm may be able to send out copies of itself to everyone in your email address book. However, worms are not always harmful as such. (Microsoft Security, 2018) They often do not access data or apply any functions. But merely by their volume and spreading ability they can clog up networks and cause system to slow severely. The spread of worms is likely to accelerate as networks become more high speed (Chen, 2004) As rates increase the time available to respond to worm threats becomes less and less and may shorten only a few seconds before the entire vulnerable population is saturated.

Virus

The detection of computer viruses is becoming commonplace in system as firewalls learn and adapt to new threats. It is also interesting to note that many viruses are benign or only mildly destructive. (Adleman, 1990) However this does not lessen the likelihood of serious high level viruses existing. A virus itself is defined as a program which reproduces itself and attaches to other programs. It often causes data corruption, data change, or performance degradation. Viruses can be arranged into boot sector, master boot record, file infector or macro virus types. Those that use more than one of this type are known as multi partite viruses. (Tech Community, 2018)
Case Study

Melissa Macro

Beginning as newsgroup promising account names and passwords for erotic websites, the melissa virus became one of the most infamous in the history of early computing. In March 1999 the virus spread to over 100,000 hosts. Up to this point it was thought that viruses couldn't be caught by simply opening an email, the melissa proved this theory wrong. Downloaded into Microsoft the word the virus attached itself so that any future saved document would carry the virus. Effectively it reduced the security setting of the program and infected all of the outlook recipients at the same time. (Chen, 2003)

Love Letter Worm

In May 2000, the love letter worm was spread using a social networking attack. It formulated as a message saying "I love you" that would encourage the user to read the attachment. (Chen, 2003) Upon execution, the worm installs copies of itself into the Windows System directory and modifies the Registry to ensure that the files are run when the computer starts up. The worm also infects various types of files (for example, .VBS, .JPG, .MP3, etc.) on local drives and networked shared directories. The worm then attaches itself to contacts in outlook and sends copies of itself to email contacts.

These threats are two of many that exist in the computing world. Others include the familiar Trojan Horse, the bugbear, Klez, ExploreZip and the concept of virus. It is estimated that worms and virus cost the industry billions of dollars every year. The love letter alone costing an estimated $960 millions in clean up (CNET, 2001).

References

Profile

Name: Keylogging
Known Associates: Hackers, Creditcard fraud
Evidence: None

Criminal Background

Keylogging is where the keystrokes typed on your keyboard are recorded. This is usually done covertly without your knowledge. Criminals frequently make use of keylogging technology to steal username/password pairs and other information so that they may impersonate credit card or bank customers.

The trouble with keylogging is that without understanding how it works, it is almost impossible to detect let alone to prevent it. This article will explain the different kinds of keylogging technology in existence and also advise on best practice to foil this kind of data theft.

Interception of keystrokes can be achieved by either software or hardware.

Hardware Interception:
Hardware keyloggers generally come in two forms, either USB or PS/2, depending on what connection your keyboard has to the computer. A microcontroller circuit physically copies the electrical signals generated from your keystrokes and maintains a store of them in memory. These keyloggers are designed to look very much like adaptors in the event that a user looks behind their computer, which excepting computer enthusiasts is fairly unlikely (when is the last time you looked behind yours?). Their main advantage is that they are 100% undetectable from anti-malware software as they are completely hardware based. They also work across any kind of computer or operating system as long as USB or PS/2 is supported. The main disadvantage of this technique, is that it requires physically installing and removing the device. Typically these devices can store up to 4Mb of data, which doesn’t sound like much, but that’s approximately 2 years worth of typing.

Even computer savvy users may be fooled by hardware keyloggers, because it is possible to install them into the keyboards themselves either in the bait & switch technique or by implanting a keylogger circuit inside your keyboard. Needless to say, only the most paranoid user would consider constantly rechecking for such a thing!

Software Interception:

Software keyloggers are frequently installed by trojan viruses. Fortunately there is an arms race between the purveyors of anti-malware software and those producing software keyloggers. However this form of keylogger is physically undetectable and far more common than its hardware equivalent. Software keyloggers are also generally far more sophisticated than hardware keyloggers, enabling criminals to take screenshots and sometimes to monitor specific applications, as well as being able to store far more data.
Advice:
Most of these methods to avoid being a victim of keylogging fraud are low tech, inexpensive and easy to implement.

1. Change your password as frequently as possible.
2. Use online banking systems that allow you to use 'one time passwords'. One time passwords are generated by a small device that resembles a calculator. After the password from the OTP device is used, it is no longer useful.
3. It does little harm to take a peek behind your computer to see if there's any weird looking adaptors about.
4. If you use Alt-Numpad characters in your password, it is unlikely that a hardware keylogger will pick them up. For example; ALT+112, ALT+97, ALT+115, ALT+115, ALT+119, ALT+111, ALT+114, ALT+100 would type the word 'password'.
5. Typing a bunch of rubbish input e.g. adffsd, and then selecting characters from this to cut and paste into your login.
6. Use a virtual keyboard, where you click on the screen to input characters.
7. Use an encrypted keyboard. This is where an input from the keyboard is encrypted and then decrypted by software when it reaches the application on the computer you're using. This works against most attacks, but can be expensive.


Phishing

Known associates: password theft, identity theft, fraud
Victims: Online Banking, Email, Online shopping

What is phishing?
Phishing - pronounced "fishing" - is the forgery of websites in order to obtain your passwords, personal information or even bank details. Starting off as an authentic-looking email, a user simply clicks on a provided link and is taken to a website that looks similar to the genuine one. It is not immediately obvious that the website is a fake, so the user enters their details, which are then passed on to the fraudsters who may use the information maliciously.

Most individuals who have email can be targeted, and subsequently, millions fall victim to phishing every year, and it’s becoming more and more common. (June Janrich Parsons 2010, 28)

Details often targeted are (James 2009):
• Bank details or credit card information, which may be used for fraud. By providing this information, it may be used to transfer money from the user’s account to another individual’s account. (Kole, Moon and Fjostheim 2006)
• Personal details, which may be used for identity theft.
• Passwords, which may be used to access email, social networks and other services, which could provide personal details that could be used for identity theft.

The following is an example of a phishing email. An individual receives an email claiming it’s from Barclays bank (Figure 1). It explains that the service is undergoing review, and that the individual should follow link to a website. After visiting the link, the individual will no doubt be asked to enter their bank details, which may then be used for fraud.

Figure 1: A phishing email claiming it is from Barclays bank, however, despite it appearing genuine, it is fake. Notice that the URL that the recipient is asked to visit is “i-barcleys.com”. A genuine address is more likely to be simply “barclays.com”.
Avoid phishing

For almost all victims of phishing, they will first be linked to a website. The most common method is by email, where an authentic-looking email will request the user follow a link where they will be asked to enter details, such as a password, bank details or personal details.

There are many common characteristics of phishing emails, allowing you to identify what is genuine and what is not:
1. Most services, especially banks, will never send you emails requesting details
2. The URL of the link will not be genuine. Ensure you know the website address to the company that is being forged. If, for example, you bank with hsbo, you must know that the website will begin with www.hsbo.co.uk, and never something else like www.hbbo.co.uk.
3. Install security software, such as AVG or Avira. These often include software that will prevent users from accessing phishing websites, or scan email for fake links.
4. Install an anti-phishing toolbar (Wu, Miller and Garfinkel 2006), which, similar to above, prevent users from accessing phishing websites.
5. More recent browsers, such as Mozilla Firefox and Google Chrome include protection against some phishing websites, which will provide a warning before allowing access to the site.

Relevant Laws

• Fraud Act 2006 specifically makes unlawful any activity of participating in fraudulent activity and false representation. Those who participate in theft through fishing are in breach of these laws. Offenders may face up to 10 years in prison (Dunn 2007).
• Data Protection Act 1998 protects data that an organization may hold on an individual. Organizations should make precautions to ensure that data is sufficiently protected that from phishing attacks. Employees should be taught to recognize genuine services so they do not provide individuals’ information to fraudsters. (Kumaraguru, et al. 2008)
• The Theft Act 1968 protects individuals by making theft unlawful. This covers data, however, this has been largely superseded by the Fraud Act 2006 (Dunn 2007).

References


Phishing ctd.