Некоммерческое

акционерное

общество

АЛМАТИНСКИЙ

УНИВЕРСИТЕТ

ЭНЕРГЕТИКИ И

Кафедра
иностранных
языков

ПРОФЕССИОНАЛЬНО-ОРИЕНТИРОВАННЫЙ АНГЛИЙСКИЙ ЯЗЫК

Security of Information Systems

Методичекие указания для студентов специальности 5В100200

Алматы, 2014

СОСТАВИТЕЛИ: Г.С.Ахетова, Ж.Е.Иманкулова. Профессионально-ориентированный английский язык, Security of Information Systems. Методичекие указания для студентов специальности 5В100200.– Алматы: АУЭС, 2014. – 44 с.

Данные методические указания предназначены для студентов специальности Система информационной безопасности. Методическая разработка содержит аутентичные тексты на английском языке, посвящённые различным проблемам обеспечения информационной безопасности, а также задания и упражнения, позволяющие овладеть терминологией и языковыми оборотами, необходимые для понимания и перевода научно-технической литературы.

Рецензент канд. филол. наук Козлов В.С.

Печатается по плану издания некоммерческого акционерного общества «Алматинский университет энергетики и связи» на 2014г.

Text.1

Can We Make Operating Systems Reliable and Secure?

1.1 Look through the text and say:

- Are unreliability and insecurity the same from the OS point of view?
- What are the main causes of unreliability and insecurity of operating systems?
- How many approaches to the problem are discussed in the text? What are their main ideas?

Microkernel's – long discarded as unacceptable because of their lower performance compared with monolithic kernels – might be making a comeback in operating systems due to their potentially higher reliability, which many researchers now regard as more important than performance.

The worst offender when it comes to reliability and security is the operating system. Although application programs contain many flaws, if the operating system were bug free, bugs in application programs could do only limited damage.

A few words about the relationship between reliability and security are to be said. Problems with each of these domains often have the same root cause: bugs in the software. A buffer overrun error can cause a system crash (reliability problem), but it can also allow a cleverly written virus or worm to take over the computer (security problem). Although we focus primarily on reliability, improving reliability can also improve security.

Why are systems unreliable?

Current operating systems have two characteristics that make them unreliable and insecure: They are huge and they have very poor fault isolation. The Linux kernel has more than 2.5 million lines of code; the Windows XP kernel is more than twice as large.

The large size of current operating systems means that no one person can understand the whole thing. Clearly, it is difficult to engineer a system well when nobody really understands it.

Operating systems do not have isolation between components. A modern operating system contains hundreds or thousands of procedures linked together as a single binary program running in kernel mode. Every single one of the millions of lines of kernel code can overwrite key data structures that an unrelated component uses, crashing the system in ways difficult to detect. In addition, if a virus or worm infects one kernel procedure, there is no way to keep it from rapidly spreading to others and taking control of the entire machine.

Fortunately, the situation is not hopeless. Researchers are endeavoring to produce more reliable operating systems. There are four different approaches that researchers are using to make future operating systems more reliable and secure.

Language-based protection.

The most radical approach comes from an unexpected source – Microsoft Research. In effect, the Microsoft approach discards the concept of an operating

system as a single program running in kernel mode plus some collection of user processes running in user mode, and replaces it with a system written in new type-safe languages that do not have all the pointer and other problems associated with C and C++.

Thus, each of the four different attempts to improve operating system reliability focuses on preventing buggy device drivers from crashing the system.

It is not yet known which, if any, of these approaches will be widely adopted in the long run. Nevertheless, it is interesting to note that micro kernels – long discarded as unacceptable because of their lower performance compared with monolithic kernels – might be making a comeback due to their potentially higher reliability, which many people now regard as more important than performance.

1.2 Translate the vocabulary used in the text below.

a flaw	sandboxing
fault isolation	entire
to endeavor	interrupt
armored	to discard
to wrap	type-safe language

1.3 What approach to more reliable and secure OS is more acceptable? Why?

Match the terms in table A with the statements in table B.

Table	Table
1Operating system	a) The software that manages the sharing of the resources of a computer and provides programmers with an interface used to access those resources.
2 Kernel	b) The core of an OS that handles memory allocation, talks to hardware devices, and makes sure everything keeps running.
3 Micro kernel	c) A kernel architecture where the entire kernel is run in kernel space in supervisor mode.
4 Monolithic kernel	d) microkernel is a minimal computer operating system kernel which, in its purest form, provides no operating-system services at all, only the mechanisms needed to implement such services

1.4 Complete the gaps in this summary of the text using passive forms.

to discuss to wrap to intend to replace to use

to make to develop to move to adopt to know

The problem of operating systems unreliability and insecurity _____ in the text. Current operating systems _____ unreliable and insecure due to two characteristics: they are huge and they have very poor fault isolation. Fortunately, the situation is not hopeless. More reliable operating systems _____by researchers. There are four different approaches to the problem solving. In the Nooks approach, each driver _____ in a software jacket to carefully control its interactions with the rest of the operating system, but it leaves all the drivers in the kernel. In the Para virtual machine approach the drivers _____ to one or more machines distinct from the main one. Both of these approaches _____ to improve the reliability of existing operating systems.

In two other approaches legacy operating systems. with more reliable and secure ones. The multiserver approach runs each driver and operating system component in a separate user process. Finally, in the most radical approach, a type-safe language, a single address space, and formal contracts _____ to carefully limit what each module can do. Thus, micro kernels in three of the four research projects, but it not which of these approaches widely.

Text 2
Read and translate the text

Data Theft: How Big a Problem?

Data theft is, quite simply, the unauthorized copying or removal of confidential information from a business or other large enterprise. It can take the form of ID-related theft or the theft of a company's proprietary information or intellectual property.

ID-related data theft occurs when customer records are stolen or illegally copied. The information stolen typically includes customers' names, addresses, phone numbers, usernames, passwords and PINs, account and credit card numbers, and, in some instances, Social Security numbers. When transmitted or sold to lower-level criminals, this information can be used to commit all manner of identity fraud. A single data theft can affect large numbers of individual victims.

Non-ID data theft occurs when an employee makes one or more copies of a company's confidential information, and then uses that information either for his own personal use or transmits that information to a competitor for the competitor's use. However it's done, this is a theft of the business' intellectual property, every bit as harmful as a theft of money or equipment. A company's confidential information includes its employee records, contracts with other firms, financial reports, marketing plans, new product specifications, and so on. Imagine you're a competitor who gets hold of a company's plans for an upcoming product launch;

with knowledge beforehand; you can create your own counter-launch to blunt the impact of the other company's new product. A little inside information can be extremely valuable — and damaging for the company from which it was stolen.

Data theft can be a virtual theft (hacking into a company's systems and transmitting stolen data over the Internet) or, more often, a physical theft (stealing the data tapes or discs). In many ways, it's easier for a thief to physically steal a company's data than it is to hack into the company's network for the same purpose. Most companies give a lot of attention to Internet-based security, but less attention is typically paid to the individuals who have physical access to the same information.

One would expect data theft to be somewhat widespread. And it probably is — if we truly knew all the numbers. The problem with trying to size the data theft issue is twofold. First, many companies do not report data theft to the police or do not publicize such thefts; they're trying to avoid bad publicity. And even when data theft is reported, the dollar impact of such theft is difficult to ascertain.

Whichever number is correct, that's a lot of stolen data. Add to that the immeasurable cost of intellectual property data theft, and you get a sense of the size of the problem — it's big and it's getting bigger.

Unfortunately, there's little you as an individual can do to prevent data theft; the onus is all on the company holding the data. You could reduce your risk by limiting the number of companies with which you do business, but that may not be practical. Being alert is your only defense against this type of large-scale theft.

2.1 Give definitions to the following word combinations.

Data theft, ID-related data theft, non-ID data theft, virtual theft, physical theft, company's confidential information.

2.2 A: Translate the following words with negative prefixes.

Unauthorized, illegally, immeasurable, unfortunately.

B: Make the words negative with the help of prefixes and translate them:
un- reliable, able, pleasant, intentionally, likely, suspecting, wanted, questionable;
in-visible, dependent, accurate, compatible, adequate, appropriate;
im-possible, perfect, proper, mobile;
ir-regular, rational, resistible, responsible;
mis- lead, understand, pronounce, print, direction;
anti- virus, spyware, glare;
dis- continue, appear, connect, advantage, agreement.

2.3 Find in the text English equivalents for the following word combinations.

Интеллектуальная собственность; в некоторых случаях; информация может быть чрезвычайно ценной; во многом; с той же целью; уделять большое внимание; меньше внимания уделяется; это довольно широко

распространено; пытаться избежать дурной славы; проблема в два раза серьезнее; во-первых; трудно установить; к сожалению; предотвратить кражу информации; вся ответственность лежит на компании; быть осторожным.

2.4 Answer the questions.

1) Why is it easier for a thief to physically steal a company's data than to hack into the company's network?
2) How widespread is the data theft problem?
3) How do thieves steal corporate data?
4) What happens to the stolen data?
5) What can you do to prevent data theft?

2.5 Speak about the data theft problem.

2.6 Translate the following sentences paying attention to the words in bold type.

1. The malicious code problem will continue to grow *as* the Internet grows.
2. *As* cyber criminals get smarter and smarter, staying one step ahead of emerging security threats is getting harder and harder.
3. *As* you might guess from the name, the decryption key is different from the encryption key.
4. The threat has grown to the point where using a password *as* the sole form of authentication provides you with almost no protection at all.
5. Most folks devise simple passwords, *such as* the names of their pets or the names of their favorite sports teams.
6. *As a result,* phishing has become big business, and very profitable for attackers with little fear of being caught for their crimes.
7. *While* new security technologies and products are developed *in order to* meet the changing needs, the bad guys are coming up with new technologies and strategies *as well*. As has been said many times, there is no silver bullet in the security world.
8. Over time, the threats have grown in *both* number *and* complexity, *while* the timeframe for response has been shortened dramatically.
9. Failure is *the only* thing *one can* achieve without effort.

Text 3

Read and translate the text

What is Malicious Code?

Malicious code is any code added, changed, or removed from a software system in order to intentionally cause harm or subvert the intended function of the system. Though the problem of malicious code has a long history, a number of recent, widely publicized attacks and certain economic trends suggest that

malicious code is rapidly becoming a critical problem for industry, government, and individuals.

Traditional examples of malicious code include viruses, worms, Trojan Horses, and attack scripts, while more modern examples include Java attack applets and dangerous ActiveX controls.

Viruses are pieces of malicious code that attach to host programs and propagate when an infected program is executed.

Worms are particular to networked computers. Instead of attaching themselves to a host program, worms carry out programmed attacks to jump from machine to machine across the network.

Trojan Horses, like viruses, hide malicious intent inside a host program that appears to do something useful (e. g., a program that captures passwords by masquerading as the login daemon.)

Attack scripts are programs written by experts that exploit security weaknesses, usually across the network, to carry out an attack. Attack scripts exploiting buffer overflows by "smashing the stack" are the most commonly encountered variety.

Java attack applets are programs embedded in Web pages that achieve foothold through a Web browser.

Dangerous ActiveX controls are program components that allow a malicious code fragment to control applications or the operating system.

Recently, the distinctions between malicious code categories have been bleeding together, and so classification has become difficult.

Any computing system is susceptible to malicious code.

The growing connectivity of computers through the Internet has increased both the number of attack vectors, and the ease with which an attack can be made. More and more computers, ranging from home PCs to systems that control critical infrastructures (e. g., the power grid), are being connected to the Internet. Furthermore, people, businesses, and governments are increasingly dependent upon network-enabled communication such as e-mail or Web pages provided by information systems. Unfortunately, as these systems are connected to the Internet, they become vulnerable to attacks from distant sources. Put simply, it is no longer the case that an attacker needs physical access to a system to install or propagate malicious code.

A second trend that has enabled widespread propagation of malicious code is the size and complexity of modern information systems. Complex devices, by their very nature, introduce the risk that malicious functionality may be added (either during creation or afterwards) that extends the original device past its primary intended design. An unfortunate side effect of inherent complexity is that it allows malicious subsystems to remain invisible to unsuspecting users until it is too late.

A third trend enabling malicious code is the degree to which systems have become extensible. From an economic standpoint, extensible systems are attractive because they provide flexible interfaces that can be adapted through new components. Unfortunately, the very nature of extensible systems makes it hard to

prevent malicious code from slipping in as an unwanted extension.

3.1 Find in the text English equivalents for the following words.

Причинить вред; намеренно; несмотря на; недавно; кроме того; к сожалению; больше не; вместо; например; различия между категориями; становиться уязвимым; широкое распространение; сложность современных систем; побочный эффект; оставаться невидимым для доверчивого пользователя; слишком поздно; с экономической точки зрения.

3.2 Complete the table.

Noun	Verb	Adjective
access	—	—
action	—	—
—	apply	—
—	assess	—
—	—	behavioral
—	—	computational
—	depend	—
harm	—	—
—	perform	—
protection	—	—
—	—	strong

3.3 Answer the questions.

1. What is malicious code?
2. What are traditional examples of malicious code? Give examples of more modern malicious code.
3. What are the key trends that are making malicious code a critical national problem?
4. What is an unfortunate side effect of inherent complexity of modern information systems?
5. What are the advantages and disadvantages of extensible systems?

Text 4
Read and translate the text

Defense against Malicious Code

Creating malicious code is not hard. In fact, it is as simple as writing a program or downloading and configuring a set of easily customized components. It is becoming increasingly easy to hide ill- intentioned code inside otherwise innocuous objects, including Web pages and e-mail messages. This makes

detecting and stopping malicious code before it can do any damage extremely hard.

To make matters worse, our traditional tools for ensuring the security and integrity of hosts have not kept pace with the ever- changing suite of applications. For example, traditional security mechanisms for access control reside within an operating system kernel and protect relatively primitive objects (e. g., files); but increasingly, attacks such as the Melissa virus happen at the application level where the kernel has no opportunity to intervene.

In general, when a computational agent arrives at a host, there are four approaches that the host can take to protect itself.

1. *Analyze* the code and reject it if there is the potential that executing it will cause harm.

2. *Rewrite* the code before executing it so that it can do no harm.

3. *Monitor* the code while its executing and stop it before it does harm, or

4. *Audit* the code during executing and take policing action if it did some harm.

Analysis includes simple techniques, such as scanning a file and rejecting it if it contains any known virus, as well as more sophisticated techniques from compilers, such as dataflow analysis, that can determine previously unseen malicious code. Analysis can also be used to find bugs (e. g., potential buffer overruns) that malicious code can use to gain a foothold in a system. However, static analysis is necessarily limited, because determining if code will misbehave is as hard as the halting problem. Consequently, any analysis will either be too conservative (or reject some perfectly good code) or too permissive (and let some bad code in) or more likely, both. Furthermore, software engineers working on their own systems often neglect to apply any bug-finding analyses.

Code rewriting is a less pervasive approach to the problem, but may become more important. With this approach, a rewriting tool inserts extra code to perform dynamic checks that ensure bad things cannot happen.

Monitoring programs, using a reference monitor, is the traditional approach used to ensure programs don’t do anything bad. For instance, an operating system uses the page-translation hardware to monitor the set of addresses that an application attempts to read, write, or execute. If the application attempts to access memory outside of its address space, then the kernel takes action (e. g., by signaling a segmentation fault).

If malicious code does damage, recovery is only possible if the damage can be properly assessed and addressed. Creating an audit trail that captures program behavior is an essential step. Several program auditing tools are commercially available.

Each of the basic approaches, analysis, rewriting, monitoring, and auditing, has its strengths and weaknesses, but fortunately, these approaches are not mutually exclusive and may be used in concert.

4.1 Find in the text English equivalents for the following words and word combinations.

На самом деле; так же просто, как; так же сложно, как; в противном

случае; в довершение всего; не отставать от чего- либо; вообще; более сложные методы; следовательно; слишком нестрогий; более вероятно; часто забывают использовать; менее распространенный метод; например; важный этап; каждый метод имеет свои сильные стороны и недостатки; не являются несовместимыми.

4.2 Answer the questions.

1. What makes detecting and stopping malicious code extremely hard?
2. Do the defenses keep pace with the ever-changing suite of applications? Give examples.
3. What are the main methods to protect the host?
4. What are the strengths and weaknesses of each of the basic approaches?

4.3 Speak about the malicious code problem and main approaches to dealing with it.

Text 5
Read and translate the text

Authentication, Authorization, and Accounting

Whether a security system serves the purposes of information asset protection or provides for general security outside the scope of IT, it is common to have three main security processes working together to provide access to assets in a controlled manner. These processes are: authentication, authorization, and accounting.

Identification and Authentication.

The process of authentication is often considered to consist of two distinct phases: (1) identification and (2) (actual) authentication.

Identification provides user identity to the security system. This identity is typically provided in the form of a user ID. The security system will typically search through all the abstract objects that it knows about and find the specific one for the privileges of which the actual user is currently applying. Once this is complete, the user has been identified.

Authentication is the process of validating user identity. The fact that the user claims to be represented by a specific abstract object (identified by its user ID) does not necessarily mean that this is true. To ascertain that an actual user can be mapped to a specific abstract user object in the system, and therefore be granted user rights and permissions specific to the abstract user object, the user must provide evidence to prove his identity to the system. Authentication is the process of ascertaining claimed user identity by verifying user-provided evidence.

The evidence provided by a user in the process of user authentication is called a *credential*. Different systems may require different types of credentials to ascertain user identity, and may even require more than one credential. In

computer systems, the credential very often takes the form of a user password, which is a secret known only to the individual and the system. Credentials may take other forms, however, including PIN numbers, certificates, tickets, etc.

User identification and authentication are typically the responsibility of the operating system. Before being allowed to create even a single process on a computer, the individual must authenticate to the operating system. Applications and services may or may not honor authentication provided by the operating system, and may or may not require additional authentication upon access to them.

There are typically three components involved in the process of user authentication:

Supplicant. The party in the authentication process that will provide its identity, and evidence for it, and as a result will be authenticated. This party may also be referred to as the authenticating user, or the client.

Authenticator. The party in the authentication process that is providing resources to the client (the supplicant) and needs to ascertain user identity to authorize and audit user access to resources. The authenticator can also be referred to as the server.

*Security authority/database***.** A storage or mechanism to check user credentials. This can be as simple as a flat file, or a server on the network providing for centralized user authentication, or a set of distributed authentication servers that provide for user authentication within the enterprise or on the Internet.

In a simple scenario, the supplicant, authenticator, and security database may reside on the same computer. It is also possible and somewhat common for network applications to have the supplicant on one computer and the authenticator and security database collocated on another computer. It is also possible to have the three components geographically distributed on multiple computers.

It is important to understand that the three parties can communicate independently with one another. Depending on the authentication mechanism used, some of the communication channels might not be used — at least not by an actual dialogue over the network. The type of communication and whether or not it is used depends on the authentication mechanism and the model of trust that it implements.

Authorization.

Authorization is the process of determining whether an already identified and authenticated user is allowed to access information resources in a specific way. Authorization is often the responsibility of the service providing access to a resource.

Before authorization takes place, the user must be identified and authenticated. Authorization relies on identification information to maintain access control lists for each service.

User Logon Process.

Authentication and authorization work very closely together, and it is often difficult to distinguish where authentication finishes and where authorization starts. In theory, authentication is only supposed to ascertain the identity of the user.

Authorization, on the other hand, is only responsible for determining whether or not the user should be allowed access.

To provide for the logical interdependence between authentication and authorization, operating systems and applications typically implement the so-called user logon process (or login process, also sign- in process). The logon process provides for user identification; it initiates an authentication dialogue between the user and the system, and generates an operating system or application-specific structure for the user, referred to as an access token. This access token is then attached to every process launched by the user, and is used in the process of authorization to determine whether the user has or has not been granted access. The access token structure sits in between user authentication and authorization. The access token contains user authorization information but this information is typically provided as part of the user identification and authentication process.

The logon process can also perform non-security-related tasks. For instance, the process can set up the user work environment by applying specific settings and user preferences at the time of logon.

Accounting.

Users are responsible for their actions in a computer system. Users can be authorized to access a resource; and if they access it, the operating system or application needs to provide an audit trail that gives historical data on when and how a user accessed a resource. On the other hand, if a user tries to access a resource and is not allowed to do so, an audit trail is still required to determine an attempt to violate system authorization and, in some cases, authentication policies.

Accounting is the process of maintaining an audit trail for user actions on the system. Accounting may be useful from a security perspective to determine authorized or unauthorized actions; it may also provide information for successful and unsuccessful authentication to the system.

Accounting should be provided, regardless of whether or not successful authentication or authorization has already taken place. A user may or may not have been able to authenticate to the system, and accounting should provide an audit trail of both successful and unsuccessful attempts.

Furthermore, if a user has managed to authenticate successfully and tries to access a resource, both successful and unsuccessful attempts should be monitored by the system; access attempts and their status should appear in the audit trail files. If authorization to access a resource was successful, the user ID of the user who accessed the resource should be provided in the audit trail to allow system administrators to track access.

5.1 Find in the text English equivalents for the following words.

Защита информационных ресурсов; обеспечить доступ к ресурсам; система защиты; пользователь должен представить доказательства; доказать подлинность; проверить имя пользователя и пароль; персональный идентификационный номер; обязанность

операционной системы; важно понимать; в зависимости от; независимо друг от друга; по крайней мере; до того как произойдет авторизация; полагаться на; часто сложно различить; с другой стороны; так называемый процесс регистрации пользователя; называемый маркером доступа; определить, был ли пользователю разрешён доступ; выполнять задачи, не связанные с системой защиты; попытка проникнуть в систему; в некоторых случаях; полезный с точки зрения безопасности; невзирая на; как успешные, так и безуспешные попытки; отслеживать доступ.

5.2 Translate the following derivative groups.

Depend, dependent, dependence, interdependence. Distinguish, distinguishable, distinguished.

Identity, identical, identify, identification. Prefer, preferable, preferably, preference. Responsible, responsibly, responsibility. Secure, security.

Set, settings.

Success, successful, successfully, unsuccessful. Use, user, useful, useless.

5.3 Complete the sentences giving definitions to.

1. Authentication is often considered to consist of …
2. Identification provides …
3. Authorization is …
4. Accounting is sometimes referred to as …
5. Supplicant is the party …
6. Authenticator is …
7. Credential is …
8. A user password is …

5.4 Decide whether the following statements are true or false.

1. User identity is typically provided in the form of a user ID.
2. Different systems may require different types of credentials to ascertain user identity.
3. In computer systems, the credential always takes the form of a user password.
4. There are typically two components involved in the process of user authentication.
5. The authenticator can also be referred to as the client.
6. The supplicant, authenticator, and security database reside on the same computer.

5.5 Answer the questions.

1.What does authorization rely on?
2.What is the difference between authentication and authorization?
3.What does the access token contain?
4.What tasks does the logon process perform?

5.What information does an audit trail contain?

5.6 Speak about three main security processes.

5.7 Translate the following sentences paying attention to the words.

1) There are doubts about *whether* the system is safe.

2) It is difficult to establish *whether* this problem can be solved at all.

3) The results of the test are to be recorded *whether* successful or not.

4) Theft is theft, *whether* the target is money, jewels, or information.

5) If a user tries to access a file that resides on a file server, it will be the responsibility of the file service to determine *whether* the user will be allowed this type of access.

6) *Whether* you're a beginner or an expert, you'll learn something from the course.

7) *Once* operational requirements have been defined, the next step is to ensure that the SIM (Security Information Management) solution can support what will be needed today and tomorrow.

8) *Once* your password is no longer secret, it no longer protects access to your valuable information.

9) Keep a close watch on your credit reports and accounts for at *least* the next year after a problem has been resolved.

10) Cracking passwords is too large a topic for one article, but I can highlight at least a couple of methods.

11) For instance, using my e-mail address for the password might be a long password, but a fairly easy *one* to crack.

12) The key for any organization — *regardless of* its size or the industry in which it plays — is to implement a data protection program.

Text 6

Read and translate the text

Understanding Denial of Service

A denial-of-service attack is different in goal, form, and effect than most of the attacks that are launched at networks and computers. Most attackers involved in cybercrime seek to break into a system, extract its secrets, or fool it into providing a service that they should not be allowed to use. Attackers commonly try to steal credit card numbers or proprietary information, gain control of machines to install their software or save their data, deface Web pages, or alter important content on victim machines. Frequently, compromised machines are valued by attackers as resources that can be turned to whatever purpose they currently deem important.

In DDOS attacks, breaking into a large number of computers and gaining

malicious control of them is just the first step. The attacker then moves on to the DOS attack itself, which has a different goal—to prevent victim machines or networks from offering service to their legitimate users. No data is stolen, nothing is altered on the victim machines, and no unauthorized access occurs. The victim simply stops offering service to normal clients because it is preoccupied with handling the attack traffic. While no unauthorized access to the victim of the DDOS flood occurs, a large number of other hosts have previously been compromised and controlled by the attacker, who uses them as attack weapons. In most cases, this is unauthorized access, by the legal definition of that term.

While the denial-of-service effect on the victim may sound relatively benign, especially when one considers that it usually lasts only as long as the attack is active, for many network users it can be devastating. Use of Internet services has become an important part of our daily lives. Following are some examples of the damaging effects of DOS attacks.

- Sites that offer services to users through online orders make money only when users can access those services. For example, a large book-selling site cannot sell books to its customers if they cannot browse the site's Web pages and order products online. A DOS attack on such sites means a severe loss of revenue for as long as the attack lasts. Prolonged or frequent attacks also inflict long-lasting.

- Site's reputation — customers who were unable to access the desired service are likely to take their business to the competition. Sites whose reputations were damaged may have trouble attracting new customers or investor funding in the future.

- Large news sites and search engines are paid by marketers to present their advertisements to the public. The revenue depends on the number of users that view the site's Web page. A DOS attack on such a site means a direct loss of revenue from the marketers, and may have the long-lasting effect of driving the customers to more easily accessible sites. Loss of popularity translates to a direct loss of advertisers' business.

- Numerous businesses have come to depend on the Internet for critical daily activities. A DOS attack may interrupt an important videoconference meeting or a large customer order.

- The Internet is increasingly being used to facilitate management of public services, such as water, power, and sewage, and to deliver critical information for important activities, such as weather and traffic reports for docking ships. A DOS attack that disrupts these critical services will directly affect even people whose activities are not related to computers or the Internet. It may even endanger human lives.

- A vast number of people use the Internet on a daily basis for entertainment or for communicating with friends and family. While a DOS attack that disrupts these activities may not cause them any serious damage, it is certainly an unpleasant experience that they wish to avoid. If such disruptions occur frequently, people are likely to stop using the Internet for these purposes, in favor

of more reliable technologies.

6.1 Find in the text words which have the same or a similar meaning.

To change, to happen, to consider, to cause, usually, often, aim, serious, now, extremely large, every day, problem.

Now find words that mean the opposite of.

Malicious, rare, short, able, authorized, same, illegal, gain, pleasant.

6.2 Make adverbs from the following adjectives and translate them.

Intentional, frequent, direct, certain, wide, rapid, usual, common, recent, unfortunate, easy, extreme, relative, necessary, perfect, consequent, proper, previous, current, simple.

6.3 Find in the text English equivalents for the following word combinations.

Пытаться взломать систему; обманом заставить предоставить услуги; изменить важную информацию; цель, которую они в данный момент считают важной; в большинстве случаев; действие может казаться сравнительно безвредным; стал важной частью нашей повседневной жизни; пользователи могут иметь доступ; серьёзная потеря; длительные или частые атаки; прервать важную видеоконференцию; подвергать опасности жизнь людей; вызывать серьёзные повреждения; для этих целей.

6.4 Answer the questions.

1.What is the difference between a denial-of-service attack and most of the attacks that are launched at networks and computers?
2. What is the goal of DOS attacks?
3. Are DOS attacks a real threat to some Internet sites?
4. What is the effect of DOS attacks? Give examples.

6.5 Read the text and decide on a suitable title for it.

"Phishing" is a new term widely popularized in mainstream media in the second half of 2003. Microsoft defines it as any type of attack that attempts to lure users to a fake Web site to enter in sensitive information that is then used for identity and banking theft. This normally occurs via an e-mail, directing users to a phishing Web site.

Originally, phishes obtained passwords by tricking users into supplying the passwords in response to an e-mail request. Although this method is still prevalent today, with firms such as the major banks, eBay, and PayPal being among the largest targets, more complex and creative methods have been developed to attempt to fool the end user. These include such methods as directing users to fake Web sites that appear as if they are issued by the same company (i. e., eBay, Chase,

U.S. Bank), man-in-the-middle proxies to capture data, Trojan-horse key

loggers, and screen captures. Phishing activity has been increasing dramatically over the past few years.

The United States leads as the country hosting the most phishing sites, with 24.27 per cent. The other top countries are China (17.23 per cent), Republic of Korea (11 per cent), and Canada, with 4.05 per cent. These statistics point out that this is a growing activity and increasingly used as a criminal activity to open an account, make an unauthorized transaction, obtain log-in credentials, or perform some other kind of identity theft.

A First Data survey in 2005 revealed that over 60 per cent of online users had inadvertently visited a spoofed site. A Consumer Reports survey indicated that 30 per cent of users had reduced their overall use of the Internet and 25 per cent had discontinued online shopping. Where once there was trust in the major brands, as indicated earlier, this trust is eroding with respect to online transactions, in large part due to a lack of trust in Web sites and fear of identity theft.

Educating consumers about the dangers of phishing is a delicate balance. On the one hand, consumers need to be vigilant in not responding to e-mails with links to sites requesting their personal information; on the other hand, consumers should not be afraid to participate in online commerce and use e-mail wisely. Phishing has become so prevalent that the Federal Trade Commission (FTC) issued a consumer alert advising consumers how not to get hooked by a phishing scam. The key points from the FTC included the following.

- If you get an e-mail or pop-up message that asks for personal or financial information, do not reply. And do not click on the link in the message, either.
- Area codes can mislead (and may not be in your area due to Voice-over-IP technology).
- Use antivirus and antispyware software, as well as a firewall, and update them all.
- Do not e-mail personal or financial information.
- Review credit card and bank account statements as soon as you receive them.
- Be cautious about opening any attachment or downloading any file from e-mails.
- Forward spam that is phishing for information to spam@uce.gov and to the bank or company that was impersonated with the e-mail.

If you believe you have been scammed, file a complaint at www.ftc.gov.

However, the entire burden cannot be on the consumer. There are multiple known delivery methods, attack vectors, and solutions to help minimize the risk. Organizations must be vigilant in their education of internal and external customers, the design of secure software, the maintenance of appropriate patch levels, and providing a phishing reporting and remediation capability and must remain continuously aware of the techniques and threats related to this type of attack.

6.6 These are answers to questions about the text. Write the questions.

1. Phishing is a variant of the word “fishing”, describing the use of sophisticated techniques to “fish” for sensitive information.
2. The United States, China, Republic of Korea, and Canada.
3. Via an e-mail, directing users to a phishing Web site.
4. Such methods as directing users to fake Web sites, proxies. to capture data, Trojan-horse key loggers, and screen captures.
5. Due to a lack of trust in Web sites and fear of identity theft.
6. Use antivirus and antispyware software.

Text 7

Read and translate the text

Database design principles

Users enter into the database system through the database application program when users firstly access the database, database applications deliver the username and password which is submitted by the user to the database management system for certificating, after determining their legal status, users are allowed to enter. They also must pass the authentication when operate objects, tables, views, triggers, stored procedures etc. in the database. How can users operate in application and database is depended on rights allocation and constraints of accessing control.

1. Secure Database System Model.

Criteria based on security database, you can create a simple security database system model which is divided into four layers: system layer, including data access, encryption and decryption algorithm; function layer is the key to the whole system, including key distribution mechanism, fast indexing mechanism and derive control; interface layer is directly user-oriented, which includes the function of user authentication, authorization

a) Access Control.

Access control is the rights control of user access to all kinds of resources of the database, which is divided into two stages: one is security account identification, the other is the access the database access mechanism will control the legal users to operate the data objects. First of all, statements in the database license will limit the database user to carry out some SQL statements. Secondly, objects in the database license will limit the database user to carry out some tasks of the database objects.

b) Establish Data Security by Using System Stored Procedures.

As the database administrator, if you want a user to have a select right rather than the delete right, at this time you can achieve the goal by establishing stored procedures, thus protecting the safety of the data.

c) Establish Data Security by Using the View.

If the administrators give users the permission to access the database tables and form a too large user access area, it will cause threats brought by users to data security of the database. To avoid this situation, you can achieve data security view

through the way of establishing data view.

d) Establish Data Security by Using the Database Role.

This role is used for setting license at a time that number of database users can access to the database, if permission is not deployed properly, it will threat data in the database directly. As an administrator, you should be very careful when you give permission to the public role.

e) Data Backup.

Data backup is principal work in the course of daily management of the database. When the server or database system breaks down, the original data is difficult to recover without a backup strategy. Therefore, the database should be installed in security zone of their intranet, and can not be connected to the Internet directly. In addition, different computers should implement backup strategies to protect data security when people deal with abnormal failure.

f) Database Encryption.

Database encryption requires that database cryptography changes plaintext into cipher-text, and cipher-text data stored in the database. Cipher-text is decrypted to get clear information when queries, so data will not be leaked even if the hardware store is stolen, thus the database system security is greatly improved, of course, the cost also increases. Response to attacks from the network level, the database mainly uses many ways e.g. installing a firewall, doing intrusion detection etc. to improve its safety performance. Firewall resists the incredible connections from outside. Intrusion detection systems are generally deployed in firewall, and detect abnormalities on the network and the host through Network packet interception analysis or Analysis of log.

g) Audit Trail and Attack Detection.

The audit function records all database's operation in the audit log automatically when the system works, attack detection system analyses and detects attempt of internal and external attackers according to the audit data, and reproduces events which leads to the status of the system, find vulnerabilities of the system by analyzing, and then trace the relevant responsible person.

7.1 Translate the following words and word combinations.

1) Database application program—
2) Access control---
3) Fast indexing mechanism----
4) Interface layer----
5) Security account identification----
6) Data backup---
7) Database encryption---
8) Intrusion detection system-----
9) Internal external attackers-----
10) Network packet interception-----

7.2 Give the synonyms to the following words.

Application, user, determine, allow, operate, distribution, to carry out, select, protect, incredible, goal.

7.3 Match the following word combinations.

1) To protect	internet
2) To avoid	stored procedures
3) To establish	the situation
4) To give	audit data
5) To connect	data security
6) To install	useful information
7) To attack	permission
8) To get	in security zone
9) To cause	the goal
10) To achieve	threats

7.4 Put the verbs in the correct forms.

1) We can achieve the goal by establishing (to store) procedures thus (to protect) the safety of the data.

2) When the server or database system (to break) down the original data is difficult (to recover) without a backup strategy.

3) Firewall (to resist) the incredible connections from outside.

7.5 Read the following sentences and translate.

Поддержка программного обеспечения - одно из важнейших средств обеспечения целостности информации. Прежде всего, необходимо следить за тем, какое программное обеспечение установлено на компьютерах. Если пользователи будут устанавливать программы по своему усмотрению, это может привести к заражению вирусами, а также появлению утилит, действующих в обход защитных средств. Вполне вероятно также, что "самодеятельность" пользователей постепенно приведет к хаосу на их компьютерах, а исправлять ситуацию придется системному администратору.

Text 8
Read and translate the text

Encryption for Confidential Information

This method is particularly effective to protect confidential information, which can prevent wiretapping and hacking. Transmission encryption in Web services is in general achieved in the application layer. When WWW server sends confidential information, firstly, it selects keys to encrypt the information, based on the receiver's IP address or other identification; After browser receives the encrypted data, it decrypts the encrypted data according to source address or other identification of the information in IP packet to get the required data. In addition,

transmission, encryption and decryption of information at the IP layer also can be achieved by encrypting and decrypting the whole message to ensure information security at the network layer.

Currently some network security protocols e.g. SSL and PCT have appeared, which are based on the existing network protocol. These two protocols are mainly used for not only protecting confidential information but also preventing other unauthorized users to invade their own host.

SSL protocol is a private communication and includes technology of authentication, signature, and encryption for the server, which can not only provide authentication for the server but also provide authentication for the client according to the options of the server.

SSL protocol can run on any kind of reliable communication protocols, e.g. TCP, and can also run in application protocols e.g. HTTP, FTP, Telnet etc. SSL protocol uses X.509 V3 certification standards, RSA, Diffie-Hellman and the Fortezza-KEA as its public key algorithm and uses the RC4-128, RC-128, DES, 3-layer DWS or IDEA as its data encryption algorithm. The authentication scheme and encryption algorithm provided by PCT are more abundant than SSL, and it makes improvements in some details of the agreement.

IPSec protocol is used to provide end to end encryption and authentication services for public and private networks. It specifies all kinds of optional network security services, and the organizations can integrate and match these services according to their own security policy, and they can build security solution on the framework of the IPSec. The protocol provides three basic elements to protect network communications, the basic elements are "Authentication Header", "Encapsulating Security Payload" and "Internet Key Management Protocol".

HTTPS protocol (Secure Hypertext Transfer Protocol), which is built on its browser for compressing and decompressing the data, and returns the result which is back to the network.

Digital Signatures for the Software.

Many large companies use digital signature technology for their software, and claim that they are responsible for the security of their software, especially e.g. Java applets, ActiveX controls, which will bring risks to Web services. Digital signatures are based on public key algorithms, using their private key to sign its own released software, and are authenticated by using the public key. Microsoft's Authenticode technology is used to identify a software publisher and prove that it has not been damaged. Authenticode is software for client, which monitors the ActiveX control, Cab files, Java applets, or download of executable file, and look for the digital certificate to verify in these files, and then show warning words, the certificate organization's name and other information to the user for possible security problems**.** Digital signature can protect the integrity of the software, and it is sensitive to illegal change of the software in the transfer process.

8.1 Translate the following words and word combinations.

1) confidential Information;

2) transmission encryption;
3) to encrypt the information;
4) decryption of information;
5) existing network protocol;
6) unauthorized users;
7) public key algorithm;
8) authentication services;
9) optional network security;
10) certification standards.

8.2 Give the antonyms to the following words.

Effective, confident, encryption, receive, authorized, private, reliable, agreement, integrate, compress, responsible, bring, illegal, optional, public.

8.3 Match the following word combinations.

1) to protect	wiretapping and hacking;
2) to prevent	optional network.
3) to receive	information security;
4) to ensure	own host;
5) to invade	encrypted date;
6) to bring	authentication services;
7) to provide	risks to web services;
8) to look for	the public key;
9) to use	digital certificate;
10) to specify	confidential Information;

8.4 Read the following sentences and translate.

Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с законодательством страны и уровнем доступа к информационному ресурсу. Конфиденциальная информация становится доступной или раскрытой только санкционированным лицам, объектам или процессам.

Нарушение безопасности информации - событие, при котором компрометируется один или несколько аспектов безопасности информации (доступность, конфиденциальность, целостность и достоверность).

Text 9
Read and translate the text

Security audit

Definition of security audit.

Security audit is based on certain security policy, improving systems

performance and safety by recording and analyzing historical events and data**.** Security audit includes all actions and instruments, e.g. testing, assessing and analyzing all of the weak links in the network information system to find the best ways to let the business run normally, based on the maximum guarantee of safety. It is to ensure the safe operation of network systems and prevent confidentiality integrity and availability of the data from being damaged, prevent intentional or unintentional human error and detect criminal activity on the network. The network status and processes can be targeted to recorded, tracked and reviewed by using the audit mechanism, and find safety problems. In addition, the audit can provide the basis of making filtering rules for online information, if the harmful information is found in the website, it will be added into the list of route filtering, to reject all information of IP addresses on the filtering list through information filtering mechanism.

Situation of Security Audit System in Network.

Security audit techniques use one or several security testing tools (generally referred to as scanner), first of all, it will scan loopholes and inspects security vulnerabilities of the system, then achieve the inspection report about the weak link of system, at last it will take security protection and emergency measures according to the response strategies.

Traditional security audit has the function of "old records", pay attention to the audit afterwards and emphasize the deterrent of the audit and verification of security incidents. With the change of United States national information security policy, doing the so-called "defense in depth strategy information" in the information infrastructure is put forward by Information Assurance Technical Framework (IATF), this strategy requires security audit system to participate in the active protection and response. In modern time, network security audit is an all-round, distributed, and multiple-level strong audit concept, which breaks the previous concept of "log" and other shallow level security audit, and it's consistent with the requirements of protecting, detecting, replying and recovering (PDRR) dynamic process, which is put forward by IATF. It can protect and response to the information actively on the basis of improving the breadth and depth of audit.

1. Based on the objects of audit, security audit is divided into:

- Operating system of audit.
- Application system of audit.
- Equipment of audit.
- Network application of audit.

2. Based on the ways of audit, security audit is divided into:

Distributed audit: audit information is stored in the server and security equipment, and system security administrator will review it. Distributed audit is applied to enterprise information system.

9.1 Translate the following words and word combinations.

1) Security audit

2) Harmful information

3) The weak link of system
4) Defense in depth strategy information
5) Information Assurance Technical Framework (IATF)
6) PDRR
7) Testing tools
8) Multiple-level strong audit concept
9) Distributed audit
10) Security vulnerabilities

9.2 Give the antonym to the following words.

Intentional, weak links, traditional, modern, active, to find, to store, certain, to damage, maximum, to defeat, safety.

9.3 Match the following word combinations.

1) to find	harmful information
2) to analyze	criminal activity
3) to defect	historical events
4) to use	emergency measures
5) to scan	the concepts of "Log"
6) to take	testing tools
7) to break	loopholes
8) to achieve	the security policy
9) to change	the inspection report
10) to have	the best ways

9.4 Read the following word combinations and translate.

Меры обеспечения информационной безопасности, механизм обеспечения информационной безопасности, нарушитель информационной безопасности, система обеспечения информационной безопасности, угроза безопасности информации, угроза информационной безопасности коммуникационной системы, конфиденциальность информации, криптографическая защита, легальные пользователи, надежность сети.

9.5 Put the verbs in the right form.

1) Audit information is (to store) in the server and security equipment, and system security administrator will (to review) it.
2) Distributed audit is (to apply) to enterprise information system.
3) The network status and processes can (to target) by using the audit mechanism.

Text 10

Read and translate the text

Key technologies of network security audit system

Analysis of Data Source of Network Security Audit System.

For security audit system, selection of incoming data is the key problem to be solved, data source of the security audit can be divided into three categories: Based on the host, based on network and other channels. In order to select the appropriate data sources, it analyzes each class of data source respectively as follows.

Data Source Based on the Host.

Data sources of the network security audit based on the host, including audit records of the operating system, system log, log information of application system and information based on the target.

Data Source Based on the Network.

Network data is the most common source of information in the current network security audit system and commercial intrusion detection system. The basic principle is that when the network data stream transmitting in the network, using a special data acquisition technology to collect the data transmitted in network as the data source of security audit system.

Other Data Source.

Data source from other safe products mainly refers to log files produced by safe products.

Firewall, authentication system which is operated independent in the target system. These data sources also should be considered by security audit system.

Data source from network device e.g. a network management system, using information provided by SNMP (Simple Network Management Protocol) as data source. Out-of-band data source refers to data information provided by the artificial way, which is contrived and non-systematic, e.g. recording what happened in system environment manually, including hardware error information, system configuration information, system crash, other kinds of natural hazard events etc. Out-of-band data source may play an important role for later analysis.

In general, it will improve the performance of security audit system if active log of the network and its safe device are used as audit data source.

Functions of Network Security Audit System.

Data Acquisition and Storage Capability.

Data collection captures data-packets based on the data link layer. It filters out the packets without audit and saves selectively according to the defined policies and system analysis requirements**.** Data acquisition and data files are generated to provide data source the network security audit system. It is the key link of the network security audit system, and is the basis of data analysis and processing. Because the system only access the external computer and the user network audit, it is not necessary to collect or store internal network data.

10.1 Translate the following words and word combinations.

1) network security;
2) audit system;
3) data acquisition;

4) current network security;
5) basic principle;
6) acquisition technology;
7) target system;
8) simple network management protocol;
9) out-of-band data source;
10) natural hazard.

10.2 Complete the table.

Noun	Verb	Adjective
detection	—	—
transmition	—	—
—	operate	—
—	manage	—
—	—	active
—	—	capable
—	perform	—
requirement	—	—
—	generate	—
—	—	special

10.3 Answer the questions.

1) What are the key technologies of network security?
2) What do you know about categories of security audit?
3) What is the main purpose of security audit?

10.4 Read the following sentences and translate.

Контроль доступа - процесс защиты данных и программ от их использования объектами, не имеющими на это права.

Система обеспечения безопасности - совокупность стандартных защитных мер: криптографическое кодирование, паролирование, присваивание идентификатора, электронная цифровая подпись и т.д.

Text 11

Read and translate the text

Log Data Management Capabilities

The log data with sustainable growth are very large, even a small network produces over 3 G network logs per day. Integrated mechanism of backups, recovery and processing is constructed for management of network security logs rather than simply delete.

Feature of Automatic Analysis and Statistical Reports Generation.

The network will generate a lot of daily log information, and it is difficult for administrators to process these huge amount of work. A visualized analysis and statistical reports automatically generated mechanisms need to be provided to ensure that administrators can find a variety of network anomalies and security events effectively.

Data Analysis and Processing Functions.

System access to external networks, achieve the user's computer and the contents of the audit network behavior via processing and analyzing to the data collected and preserved. The core is protocol analysis. Web content audit system includes web audit, mail audit, FTP audit and user log etc. The function data play a decisive role in audit results.

Function of Real-time Network Status Monitoring.

Real-time monitoring function mainly includes analysis, identification, judgment and record of typical protocol in network traffic, intrusion detection for Telnet, HTTP, Email, FTP, Internet chat, file sharing etc. flow monitoring, and identification and alarming of unusual flow.

Network Service Control Function.

Network service control function achieves control of host and service for user access to network services, to be able to support the operations of user authorization, settings of white list host and user access rules.

Network Security Audit System Architecture.

Network security audit system mainly consists of three modules.

Data Collection Module.

Data collection module acquires network packet of users' operation by monitoring and core filtering technology depending on imaging feature of switchers and user-defined strategies. The key to realize this module is to acquire accurate and complete packet. Data integrity of data acquisition modules is determined by the exactness and completeness of audit results.

Packet Processing Module.

Protocol analysis is a key step in the data packet processing. Main job of packet processing module is to capture the data packets and determine the protocols e.g. TELNET, FTP and other protocols it belongs based on their header information. According to the formats, transmission mode and message content, it make the user's operation to restructure, restore, and finally it restore user data and submit to the audit module.

Data Audit Module.

According to the rules defined format, the achieved user information e.g. TELNET and FTP commands, SQL statements, manipulate objects, operating keywords will match with the user-defined strategy in rule base. Responses are made according to the matching results, and the audited data are recorded into audit logs. The rule base is generated based Security audit approach.

Rule base based security audit method is the process below. Administrators extract feature of attack behaviors, and then push them into rule base after represent by script language. When executing security audit, network attack behaviors are

detected after the comparison and matching operations e.g. keywords, regular expression, fuzzy approximation degree between the above rules base and network data. But these rules are only fit for certain specific types of attacks or attack software, and failures of rule base are generated when new attack or upgraded software turns up.

11.1 Translate the following words and word combinations.

1) sustainable growth;
2) network security logs;
3) function of real-time network;
4) network security audit system;
5) data collection module;
6) packet processing module;
7) data audit module;
8) statistical reports.
9) fuzzy approximation degree
10) upgraded software .

11.2 Match the following words and word combinations.

1) to construct	external networks
2) to find	to users authorization
3) to include	while list host
4) to acquires	a decisive role
5) to determine	the data packets
6) to capture	the exactness and completeness of audit
7) to play	network packet of users
8) to set	web audit, mail audit, user log etc.
9) to support	network anomalies
10) to access	network security logs

11.3 Read and learn the following abbreviations.

FTP (File Transport protocol) is a TCP/IP - based service which provides transmission of text and binary files. It is often used on the Internet for sharing access to information organization.

SMTP (Simple Mail Transfer Protocol) is a postal transport service protocol.

DNS (Domain Name System) is a TCP/IP - based service (Domain Name System). It is a distributed database which converts "word" names of network computers to their digital IP-addresses and vice versa.

Telnet is an internet service, using which the user should be registered (username and password) in the Telnet - server.

Sendmail is a popular e-mail program on the internet.

11.4 Read the following sentences and translate.

Система управления информационной безопасностью (ISMS или

Information Security Management System) позволяет управлять комплексом мер, реализующих некую задуманную стратегию, в данном случае - в отношении информационной безопасности. Отметим, что речь идет не только об управлении уже существующей системой, но и о построении новой/перепроектировке старой.

Text 12
Read and translate the text

How to do security audit

An audit system which leads to excellent audit should to be developed to ensure that auditors do their work on a regular basis. In the audit system, auditors should clearly know what the audit objects are. The main focus is the enterprise's information protection e.g. the server, backbone switches, routers and security devices.

Focus on Safety Auditors fostering.

Safety audit involves massive products and wide content. The basic information of the audit comes from operating system, network systems, security devices, applications system etc. Security auditors are not only necessary to understand the operating system knowledge, but also should be familiar with network protocols, database, and virus infection mechanism. Moreover, auditor should understand the basic situation of application systems as well as master the work principles of servers, switches and security devices, especially the understanding a variety of security policies of information systems deeply. Thus, in the audit processing, the analysis of massive information can be developed and the observing and thinking ability can be cultivated.

However most of the enterprise information system security audit work is just begin without any own professionals. Although security audit can be conducted by professional security company or buying excellent audit software, it is still harmful in term of the safety and long term development. The audit process involves a number of important enterprise information especially the system security weaknesses. Serious threaten will occur when criminals turn up or the workers are in low ability to analyze the weak links**.** From the above analysis, the security audit work should be accomplished by the professionals in the enterprises.

From the angles of security audit requirement for auditors and situation enterprise internal personnel’s, the enterprise should lay emphasis on the foster of information system administrators, network administrators, security guards especial the safety audit personals. Because all security policy, security system and security measures are developed by human beings, personnel’s with high quality and ability are required in developing management standards of enterprise information system and ensuring enterprise information security.

Reasonable Structure of the Security Audit System.

The premise of improving the safety audit is to build a security audit system in

line with business needs. In building a security audit system, the follow issues should be considered:

The profundity and scope of audit. The audit profundity and scope determine the complexity of the audit system, which are also the basis of audit products selection.

Problems of data sources. An audit system operation is based on data from the system at all levels, and how to obtain the data sources of audit system is the most critical issue.

Relationship with the original systems. To ensure the normal operation of the original system go smoothly in the realization of the audit, and the least modification and the minimum impact on system performance make the audit perfect.

Eliminate of audit function ignore. If the audit system is easily bypassed, it would lead to serious problems.

Effective utilization of audit data. In establishing an audit system, the lack of deep utilization of audit data will lead to weak audit system effection.

Network security is accompanied with the production of computer, especially the present popular network, security problem is emphasized by at all levels of sectors and industries especially the area of intranet security. Network security is a huge and complex dynamic system, hardware equipments provide basic security for the network, but a system which continues to improve can find a kind of dynamic equilibrium only with the help of network security audit system by doing real-time audit and effective evaluation to the system which has been established and discovering the potential safety hazard in time. These problems will become hot spots for future security research in building a solid and reliable network security audit system.

Computer network security audit is a very complex and extensive research subject, as an indispensable part in integrity security framework, it is a complement for a firewall system and a intrusion detection system. It involves a wide range of knowledge. With the complexity of computer operating system and network communication technology increasing, the complexity of network security audit is also increasing. How to improve network security audit system performance of various technologies and how to build a strong network security audit system need to further constantly explore and research.

12.1 Translate the following word combinations.

1) backbone switches
2) thinking ability
3) virus infection mechanism
4) serious threaten
5) internal personnel’s
6) the audit profundity
7) effective utilization
8) intranet security

9) dynamic equilibrium
10) real-time audit
11) intrusion detection system

12.2 Answer the following questions.
1) What is the main forces in Audit system?
2) What does Audit involve?
3) Why do the auditor should understand the operating system of Audit?
4) What do you know about structure of security Audit?
5) Explain what data security is?

12.3 Read and Learn the following definitions.

Confidential/sensitive information is information which demands protection.
Access to information is acquaintance with information, its processing (copying in particular), updating, deleting.

Access subject is a person or process, whose actions are regulated by the rules of access differentiation.

Rules of access differentiation (security policy) is a set of rules regulating the rights of access subjects to access objects.

Unauthorized access to information is access to information which breaks rules of access differentiation with the use of regular means provided by means of computer facilities or automated systems.

12.4 Read the following word combinations and translate.

Информационная безопасность / Аутентичность информации / Безопасность / Безопасность сети / Достоверность информации / Доступность информации / Защита информации / Защищенность информационной системы / Злоумышленник / Контроль доступа / Конфиденциальная информация / Нарушение безопасности информации / Политика информационной безопасности / Программа преимущественного права на защиту личной информации / Система обеспечения безопасности / Угроза безопасности / Хакер / Целостность данных / Чувствительная информация.

Text 13
Read and translate the text

Cyber Security

Prior to HTML, browsers, and the WWW, computer interconnections were localized and limited. Since the early 1990s, web technologies have made it easy for everyone to access and post content on the Internet. Before long, there were thousands, then hundreds of thousands, and soon tens of millions of computers, all connected together via the Internet. As noted by Robert Metcalfe, and as later codified in what became known as "Metcalfe's Law", the value of a network goes

up as the square of the number of users. Regardless of whether we accept his exact quantification of the value, there is no question that a few interconnected computers are more valuable than the same computers not being interconnected, and that many (or all) computers being interconnected has much more value than only a portion of them.

This is the situation today: essentially all desktop, notebook, net book and tablet computers are interconnected via the Internet, and the same is true for the majority of cell phones. Additionally, even a significant portion of embedded computers are being connected via the Internet, as well as most industrial control and monitoring computers. Suffice it to say that, if the trend continues, and the evidence is very strong that it will, most computers, mobile devices, and even embedded systems either are or soon will be connected via the Internet.

While this has dramatic advantages for a free and open society, there has always been an element of society that would attempt to take advantage of this openness in ways that are damaging to other computers, users, the data, or to society as a whole. The need to protect our computers, users, data, and society, from this type of abuse, is the field of information assurance and security.

Guarding our information.

Most businesses today would recognize the need to follow the most economical path to maximum profit. Frequently an organization's profit margins form the primary indicators as to their success. Even government agencies must admit to being somewhat cost-driven. With the recent economic downturn and increased competition to stay one foot ahead, businesses may be tempted to consider security as an afterthought, rather than an integral part of their business models and practices. In this Chapter we will look at some of the devastating implications of this error and why every genre of organization must place security at the forefront of business planning and practice.

Consider the owner of an expensive luxury vehicle who, each day outside his workplace, leaves his doors unlocked, with the keys in the ignition. The foolhardiness of the owner is apparent, and some readers may go so far as to suggest he would deserve to have his vehicle stolen. Yet in our modern information-driven organizations, corporations and agencies that depend on their information and data in their day-to-day operations often omit security entirely from consideration. At best it is an afterthought, akin to putting a 'do not steal' sign on the aforementioned vehicle and hoping this will deter all potential criminals.

Visualizing the cyber-landscape.

The first step in better understanding cyber-attacks is to become aware of how intricately connected information systems and technology have become. A system should not be thought of as a series of devices connected by wires, but rather a combination of people, technology and networks that function within defined parameters to achieve a specified objective. As organizations begin to view their systems from this perspective, it becomes obvious why few technical measures, even if expensive and state-of-the-art, may be ineffective in ensuring their protection from a cyber-attack.

13.1 Translate the following words and word combinations.

1) Information assurance
2) Economic downturn
3) Cyber attacks
4) Tablet computers
5) Embedded computers
7) Luxury vehicle
8) Economical path
9) Devastating implications
10) Day-to-day operations

13.2 Match the following words and word combinations.

1) To protect from	exact quantification
2) To have	via the internet
3) To become	foot ahead
4) To follow	do not steal'
5) To take	the door unlocked
6) To leave	an advantage of openness
7) To put a sign	an economic path
8) To stay	aware of something
9) To connect	luxury vehicle
10) To accept	cyber attack

13.3 Give the antonyms to the following words.

Connect, easy, together, strong, frequently, limited, advantage, lock, expensive, known, maximum, increase, primary, valuable, effective, true, codify, obvious, recent.

13.4 Read the following word combinations and translate.

Безопасность - состояние защищённости жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Различают:

- социальную безопасность: правовую, интеллектуальную, духовно-культурную; - экономическую безопасность: финансовую, хозяйственную, технологическую; - территориальную безопасность: экологическую, сырьевую, жизненную.

Безопасность сети - меры, предохраняющие информационную сеть: - от несанкционированного доступа;

- от случайного или преднамеренного вмешательства в нормальные действия; - или от попыток разрушения ее компонентов.

Безопасность информационной сети включает защиту оборудования, программного обеспечения, данных и персонала.

Text 14

Read and translate the text

Intrusion Detection and Prevention in High Speed Network

With the rapid development and comprehensive application of network technology, network security problems gradually appear serious- Traditional firewall technologies can't provide sufficient security protection against various attacks and intrusions, while intrusion detection systems (IDS) are faced with compromise between false alarms and false positives. In this chapter, we investigate intrusion detection and intrusion prevention in high speed network, introduce related technology and our research results.

1. The information system and system security.

Information system is an integrated set of components for collecting, storing, processing, and communicating information. Information systems are more than just computer programs. Though information and communications technologies are playing an increasing role in meeting organizations' information needs, an information system is a much more general concept. It refers to the wider systems of people, data and activities, both computer- based and manual that effectively gather, process, store and disseminate organizations' information. Of course, system security is essential for information system. In another words, security is the most reliable foundation for information system.

2. The actual condition of information system security.

With the development of Internet, the world economy has been deeply communed together. The nation is just like a huge network computer, and computer network has been the foundation and life vein of a nation's economy. As the entire society increasingly relies on network infrastructures, network security also changes for the worse seriously. It is very difficult for traditional security policies or mechanisms (such as authentication, cryptography and firewall) to prevent network attacks. The whole society needs new technology to solve those problems.

The openness of the system network, the security hole of the network protocol, the defects of the software...Those drawbacks make the network security worse than worse. According to the recently research and report, people found the details and data of network attack easily. The high occurrence probability makes the problem urgent.

Cases are known, the network security is the most reliable foundation for network applications. Even7 country, for commercial or military purposes, spared a lot to study network security. Research on this issue.

Although there are various measures to protect safety, they are not the keys to all kinds of attack. For instance:

1) Network infrastructures, network security of software safety is impossible.

2) Encryption technology itself has some problems, and those shortcomings may lead to key logger activities. Moreover, people may misunderstand the arithmetic.

3) The security hole of the network protocol.

4) The contradiction between the availability and the safety is always one of those contradictions running through the long developing process of computer technology.

5) The complex security system is usually difficult to configure. The blander of wrong configuration will leave some hidden danger.

6) The system log and the audit have massive data. They need automatic mode to work with that information.

7) Staff members may abuse the safety system.

14.1 Translate the following words and word combinations.

1) intrusion detection
2) prevention in high speed network
3) sufficient security protection
4) firewall technologies
5) hidden danger
6) network infrastructures
7) network security
8) reliable foundation.
9) the actual condition
10) network protocol

14.2 Answer the following questions.

1) What is the information system?
2) Why do Traditional firewall technologies can't provide sufficient security protection against various attacks?
3) What new technology do the society need to protect the network security ?
4) Why is it very difficult to prevent network attacks?
5) What measures should we take to solve network security problems?

14.3 Translate the following derivative groups.

Detect, detector, detection, detective. Measure, measurement, measurable.

Inform, information, informational, informative, informal, informally.

Apply, application, applicable. Rely, reliable, reliably. Collect, collection, collective, collectively. Probable, probability. probably.

14.5 Read the following word combinations and translate.

Политика информационной безопасности - совокупность правил, определяющих и ограничивающих виды деятельности объектов и участников, системы информационной безопасности.

Программа преимущественного права на защиту личной информации - набор стандартов и технологических спецификаций для коммерческих веб-сайтов и браузеров. Программа обеспечивает пользователям возможность автоматического контроля информации, которую они оставляют на сайте.

Text 15
Read and translate the text

Information systems

An information system is specifically designed to operate on information, i.e., information is the flow variable in the system. In general, systems are designed for a purpose and have the following operational properties:

1) Consume (ingest).
2) Process (convert).
3) Produce (output).
4) Control signaling (regulate operations).
5) Store (hold).

*A system can be defined as a combination of hardware, software, infrastructure, and trained personnel operating to achieve specified mission obj***e**ctives. This definition of system includes both the communications technology and information that is employed in addition to the way in which people interact with the technology.

Modem information systems increasingly rely on globally sourced ICT components and services**.** The variety and abundance in the marketplace is driven by the rapid decline in cost and the rapid increase in performance advancements. As supply is able to meet the demand for low cost and more functions, today's information systems are increasingly complex in nature.

Trusted information systems.

One foundation for building trusted information systems is systems assurance. Systems assurance is defined as the justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed.

Challenges in Building Trusted Information Systems. Inserted as part of the system at any time during the life cycle (NDIA, 200S). The ideal scenario where no exploitable vulnerabilities exist is unrealistic. Therefore, active risk management must be performed to reduce the probability and impact of vulnerabilities to tolerable levels of risks.

Confidence establishes trustworthiness and tolerable residual risk. Trust in any information system is really the result of the methods employed to assure confidence in the system, both in its functions and protection of the information it holds and the results it produces.

Trust & risk.

Trust and risk are closely related. Trust can be described as the willingness to take risk. Trust can be defined in terms of willingness to assume risk, intention in terms of willingness to assume risk, intention to make oneself vulnerable, acceptance of risk, and readiness to assume risk.

15.1 Translate the following words and word combinations.

1) Information systems
2) Specified mission objectives
3) Trusted Information Systems
4) Modem information systems
5) Tolerable residual risk.
6) Exploitable vulnerability
7) Systems assurance
8) Control signaling
9) To assume risk
10) Justified confidence.

15.2 Give the synonyms to the following words.

Consume, purpose, achieve, variable, increase, perform, rapid, willingness, define, assume, trust, store, mission, interact, complex, demand, method.

15.3 Answer the following questions.

1) What is the trusted information systems?
2) Indicate the main idea of factual information systems.
3) Name a number of common qualities of information systems.
4) Formulate the terms of databases and data management systems.
5) Explain the meaning of the word "secrecy/confidentiality".
6) How is data independence defined?

15.4 Write the definitions to the following words.

Hardware, software, risk, trust, store, intention, rely on, supply, abundance, challenge, cost, modem, output.

15.5 Read the following sentences and translate.

Информационная система общего пользования – информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Информационная угроза – реальная или нереальная (мнимая, сфальсифицированная) априорная опасность, содержанием которой являются различного рода информация или ее комбинации, которые могут быть использованы против того или иного социального объекта с целью изменения его интересов, потребностей, ориентаций в соответствии с целями субъекта информации.

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах

(библиотеках, архивах, фондах, банках данных, других информационных системах.

Информационный риск – пограничное состояние между информационной угрозой и реальным действием по ее применению.

Text 16
Read and translate the text

The motivation of cyber attack

In the last few years, studies have highlighted the vulnerability of critical infrastructure to cyber-attack. Nuclear plants, electric smart-grids, gas pipelines, traffic management systems, prison systems, and water distribution facilities have all been identified as at risk from a cyber-attack. Fortunately at the time of this publication, actual attacks like these remain the subject of academic discussion. Many security analysts fear this situation will be short-lived.

It should be clear by now that there is no such thing as an uninteresting target for cyber attackers. We know that certain industries and organizations may be targeted more persistently and receive more attacks than others, but should realize that every system and organization is at risk. Understanding the motivation an attacker may have to attack our systems can help us to be more prepared for the eventuality of an attack.

In summary, the motivation for cyber-attacks may include:

1) Intellectual property theft.
2) Serviced isruption.
3) Financial gain.
4) Equipment damage.
5) Critical infrastructure control sabotage.
6) Political reasons.
7) Personal entertainment.

In the next section, we shall see how recent cyber-attacks are being targeted to realize these objectives and describe their potential impact to information systems and organizations.

The actors that typically have these motivations can be categorized as: organized groups; loosely-organized groups; and lone wolves. These categories are points in a continuum.

An example of an organized group would be the espionage organization of a nation (such as the CIA); an example of a criminal organized group would be the Russian Business Network. These groups are typically highly organized, they pursue specific objectives, and they are well funded.

More recently, there has been a surge in the category of loosely-bound groups with varying motivations. Some of the best-known of these groups include Lulzsec and Anonymous. Collectively these groups are responsible for dozens of the highest-profile attacks in recent times (Wikipedia, 2012). Indeed, many of the

aforementioned attacks against Sony came from one of these groups (Security Curmudgeon, 2011). Their targets range from governments, to corporations, to religious institutions (to date having hacked the Vatican twice). Self-labeled as part of the 'Antisec' movement, they encourage other groups to join their cause and represent a politically and geographically diverse group of individuals with skills ranging from basic script kiddie, to more advanced exploitations. Recently, a new group known as The Consortium (BBC News Technology, 2012) claimed affiliation with Anonymous in a hack against a pornography website resulting in the loss of subscriber information. While some may argue that these groups have political motives, it appears that they seek organizations with a low-security profile to public ally embarrass at every opportunity.

A lone wolf or solo hacker, often incorrectly stereotyped as a basement-dwelling spotty teenager, can in some instances pose an equal threat. An example of the lone wolf includes the case of the Scottish systems administrator, Gary McKinnon, and is perhaps one of the more famous of these. Driven by self-curiosity he hacked into multiple US government agencies before being apprehended (Boyd, 200S). Such hackers are greatly assisted by organizations or individuals that provide tools for creating malware.

16.1 Translate the following word combinations.

1) vulnerability of critical infrastructure
2) electric smart-grids,
3) gas pipelines,
4) traffic management systems,
5) water distribution facilities
6) intellectual property theft
7) an uninteresting target
8) basic script kiddie
9) loosely-organized groups
10) financial gain

16.2 Give antonyms to the following words.

Fortunately, shot-lined, interesting, certain understand, personal, loose, encourage, known, appear.

16.3 Read the following sentences and translate.

Атака типа DOS (сокр. от Denial of Service - "отказ в обслуживании") - это внешняя атака на узлы сети предприятия, отвечающие за ее безопасную и эффективную работу (файловые, почтовые сервера). Злоумышленники организуют массированную отправку пакетов данных на эти узлы, чтобы вызвать их перегрузку и, в итоге, на какое-то время вывести их из строя. Это, как правило, влечёт за собой нарушения в бизнес-процессах компании-жертвы, потерю клиентов, ущерб репутации и т. п.

16.4 Make sentences with the following word combinations.

1) To suffer from cyber attack
2) To understand the motivation of cyber attack
1) To have loosely-organized groups
3) To describe potential impact
4) To peruse specific objectives
5) To seek organizations with low security profile
6) To provide tools for creating malware

Text 17

Read and translate the text

Cyber-attack types

In a sample study of 50 organizations conducted in 2011, researchers found that on average a successful cyber-attack occurs over than 70 times per year, or on average, 1.4 times per week. This represents an increase of 44% from 2010. If this growth continues, fifteen years from now organizations will be responding to a successful attack every 30 minutes .

The exact type of attack can vary in type and sophistication. Fortunately, many of these attacks are fairly simple in nature. Automated vulnerability probes along with known and recognizable self-propagating malware (worms) form the bulk of attack attempts. These are generally easy to detect and prevent using standard off-the-shelf firewalls, and intrusion protection/detection systems. The primary danger in these attacks is the noise they generate, which can make it difficult to locate the more serious threats. In excess, however, they can constitute a Denial of Service (DOS), or Distributed Denial of Service attack (DDOS), leading to a much more serious degradation of service, unpredictable behavior and even complete loss of service. Although relatively infrequent, DOS and DDOS attacks are one of the most costly types of attack.

Another type of cyber attack against infrastructure is stealing Internet access. An example of this type of security compromise is the case of Ryan Harris, the owner of TCXISO. His company produces products that enable users to steal Internet service .

One very successful form of attack today focuses on exploiting vulnerabilities in websites and web applications. These attacks pose the greatest danger to most organizations due to the relative simplicity with which they may be attempted and with the immense volumes of valuable information that can be stolen if successful. Many websites are connected to backend databases, which not only contain information that may be of interest to criminals, but provide an entry point into the organization's internal network. The latter form of attacks are known as pivoting attacks and enable the attacker to pivot from a principal entry point to attack other systems deeper in an organizations infrastructure. Pivoting attacks are a severe form

of web-based attacks as they allow attackers to completely bypass perimeter security controls at the network edge.

Web attacks involve the attacker identifying a potential vulnerability in a web system. There are several types of vulnerabilities that allow for different forms of attacks. The most common of these are cross-site scripting (XSS) and SQL injection.

Cross-site scripting allows an attacker to plant malicious code in an organization's website and from there attack clients visiting a company's site, stealing passwords, subverting network traffic, and monitoring communications. In many instances, XSS attacks enable attackers to leverage further vulnerabilities in client web browsers to install malicious software on the visitor. Thus unknowingly a visitor of an infected site can become themselves infected, and in some instances, part of a group of infected computers known as a botnet. This form of client infection is known as a drive-by-download and is one of the principal ways attackers gain control of systems. Controlled systems can be used for a variety of purposes including sending unsolicited e-mails (SPAM), targeted cyber-attacks against organizations, and DOS attacks. Using a victim's system to attack another victim is known as an indirect attack and can be done with relative anonymity.

The vulnerability to these type of attacks can be easily reduced by careful website programmers who include checks to validate the length of user-entered information, and remove any illegal characters. Failing to do this introduces a significant probability that the site is vulnerable to both cross-site scripting and SQL injection attacks.

An SQL injection permits the attacker to access and manipulate a backend database, revealing customer records, intellectual property and even opening routes deeper into the organization's network. Most experts agree that SQL injection attacks were used in most of the 21 independent successful attacks against Sony that occurred between 21 April and 7 July 2011 (Security Curmudgeon, 2011). Targeted attacks of this nature currently form the majority of successful cyber-attacks and are the most cost-effective for attackers.

17.1 Translate the following words and word combinations.

1) A successful cyber-attack
2) Automated vulnerability probes
3) Denial of Service (DOS)
4) Controlled systems
5) User-entered information
6) Malicious software
7) An SQL injection
8) Cross-site scripting
9) Degradation of service,
10) Unpredictable behavior.

17.2 Answer the following questions.

1)What types of cyber attacks do you know?
2)What does Cross-site scripting allow?
3) How many cyber attacks are occurred per year and per week?
4) What do web attacks involve?
5) What does SQL injection mean?

17.3 Read and learn the following definitions.

CHAP - Challenge Handshake Authentication Protocol.
PAP -Password Authentication Protocol.
Denial of service (DOS) -is a condition in which a part (or parts) of the network becomes inaccessible.
SMTP- (Simple Mail Transport Protocol).
POP- (Post Office Protocol).
IMAP- (Internet Mail Access Protocol).
MIME - is the abbreviation of Multipurpose Internet Mail Extensions.
MBR - Master Boot Records.
TSR - Terminate and Stay Resident.
NDS - Netware Directory Services.
ON- Organizational Units.
PVN -Private Virtual Network.
NAT- Network Address Translation.

17.4 Read the following sentences and translate.

Компьютерные вирусы. Отдельная категория электронных методов воздействия - компьютерные вирусы и другие вредоносные программы. Они представляют собой реальную опасность для современного бизнеса, широко использующего компьютерные сети, интернет и электронную почту. Проникновение вируса на узлы корпоративной сети может привести к нарушению их функционирования, потерям рабочего времени, утрате данных, краже конфиденциальной информации и даже прямым хищениям финансовых средств. Вирусная программа, проникшая в корпоративную сеть, может предоставить злоумышленникам частичный или полный контроль над деятельностью.

Список литературы

1. Andrew S. Tanenbaum, Jorrit N. Herder, Herbert Bos “Can We Make Operating Systems Reliable and Secure?”. - Computer - Innovative Technology for Computing Professionals, May 2006.

2. Longman Dictionary of Contemporary English. 2001.

3. Чепурова В.М., Гришина Г.А., “Обучение чтению литературы на английском языке по специальностям” «Комплексное обеспечение информационной безопасности автоматизированных систем» и «Компьютерная безопасность» МГТУ им. Н.Э. Баумана, 2010.

4. Baimukhamedov M.F., “Information systems”. - Алматы, 2013.

5. Christos Kalloniatis, “Security Enhanced Applications for Information Systems”. - Oxford 2012.

Содержание

Сводный план 2014г., поз. 274

Ахетова Гульзайнаб Сапаровна
Иманкулова Жанетта Ералина

ПРОФЕССИОНАЛЬНО-ОРИЕНТИРОВАННЫЙ АНГЛИЙСКИЙ ЯЗЫК

Security of Information Systems

Методичекие указания для студентов специальности 5В100200

Редактор Н.М.Голева.
Специалист по стандартизации Н.К. Молдабекова.

Подписано в печать_____ Формат 60х84 1/16

Тираж 50 экз. Бумага типографская № 1

Объем 2,8 уч. – изд. л. Заказ_____. Цена 1400 тг.

Копировально-множительное бюро
некоммерческого акционерного общества

«Алматинский университет энергетики и связи»

050013, Алматы, Байтурсынова, 126.