UNIT 1. PROBLEMS WITH COMPUTERS

Warming up

Ex.1. Discussion.

What are possible problems with computers?
Brainstorm different computer problems in small groups and make up a list of all possible computer problems. Discuss them in the class.

Mainstream

Ex.2. Learning facts.

1. Read the texts

Bug

In computer technology, a bug is a coding error in a computer program. (Here we consider a program to also include the microcode that is manufactured into a microprocessor.) The process of finding bugs before program users do is called debugging. Debugging starts after the code is first written and continues in successive stages as code is combined with other units of programming to form a software product, such as an operating system or an application. After a product is released or during public beta testing, bugs are still apt to be discovered. When this occurs, users have to either find a way to avoid using the "buggy" code or get a patch from the originators of the code.

Although bugs typically just cause annoying computer glitches, their impact can be much more serious. A Wired News article about the 10 worst software bugs in history, reported that bugs had caused major explosions, crippled space probes, and caused death. In 1982, for example a system controlling the trans-Siberian gas pipeline (allegedly implanted by the CIA) caused the largest non-nuclear explosion in history. Between 1985 and 1987, a bug in a radiation therapy device called a race condition resulted in the delivery of lethal doses of radiation, killing five people and injuring others. More recently, in 2005, Toyota recalled 160,000 cars (the Prius) because a bug caused warning lights to come on and engines to stall for no reason.

A bug is not the only kind of problem a program can have. A program can run bug-free and still be difficult to use or fail in some major objective. This kind of flaw is more difficult to test for (and often simply isn't). It is generally agreed that a well-designed program developed using a well-controlled process will result in fewer bugs per thousands of lines of code.

The term's origin has been wrongly attributed to the pioneer programmer, Grace Hopper. In 1944, Hopper, a young Naval Reserve officer, went to work on the Mark I computer at Harvard, becoming one of the first people to write programs for it. As Admiral Hopper, she later described an incident in which a technician is said to have pulled an actual bug (a moth, in fact) from between two electrical relays in the Mark II computer. In his book, The New Hacker's Dictionary, Eric Raymond reports that the moth was displayed for many years by the Navy and is now the property of the Smithsonian. Raymond also notes that Admiral Hopper was already aware of the term when she told the moth story. The term was used prior to modern computers to mean an industrial or electrical defect.

Less frequently, the term is applied to a computer hardware problem.

Glitch

In several usages in information technology, a glitch (pronounced GLIHTCH) is a sudden break in function or continuity, sometimes of a transient nature, with a varying degree of seriousness. According to Eric Raymond, author of The New Hacker's Dictionary, glitch is from the German 'glitschen,' meaning 'to slip,' via Yiddish 'glitshen,' meaning 'to slide or skid.' In different contexts, the term has different meanings.

1) In electrical service, a glitch, sometimes called a power glitch, is a momentary power failure.

2) In network service, a glitch can be any temporary loss of service in the network.

3) In a computer program, a glitch can be a bug that isn't encountered very often, resulting in a problem that sometimes goes away because next time the combination of events is different. Glitches like this are often encountered with Web browsers. (Browser glitches are often fixed by closing the browser program and then reopening it, or by restarting the operating system.) A glitch can also be an intentionally planned trap or other program device that results in exposing a user's password or in some other security breach.

4) In computer audio, a glitch is a quick temporary noise in a file that sounds like a "snap."

2. Answer the following questions paying special attention to the terms like bugs, flaws and glitches.

1. What is a bug? What do bugs cause?
2. How is the process of finding bugs called? And when is it normally started?
3. What are the steps that common users can take to solve that problem?
4. What other program problems can you name?
5. What do glitches cause? Can we call a glitch a serious problem?
6. Do you know anything about these terms' origin?

Ex. 3. Grammar and vocabulary.

1. Read the first paragraph of the text and fill in the gaps with the terms given in the box.

device	engineering	exist	imply	isolate	locating

In computers, debugging is the process of (1) … and fixing or bypassing bugs (errors) in computer program code or the (2) …of a hardware device. To debug a program or hardware (3) …is to start with a problem, (4) …the source of the problem, and then fix it. A user of a program that does not know how to fix the problem may learn enough about the problem to be able to avoid it until it is permanently fixed. When someone says they've debugged a program or "worked the bugs out" of a program, they (5) …that they fixed it so that the bugs no longer (6) ….

2. Insert articles in the second part of the text.

… debugging is … necessary process in almost any new software or hardware development process, whether … commercial product or … enterprise or personal application program. For … complex

products, … debugging is done as … result of … unit test for … smallest unit of … system, again at … component test when … parts are brought together, again at … system test when … product is used with … other existing products, and again during … customer beta test, when … users try … product out in … real world situation. Because … most computer programs and many programmed hardware devices contain …thousands of … lines of code, almost any new product is likely to contain a few bugs. Invariably, … bugs in … functions that get … most use are found and fixed first. … early version of … program that has lots of bugs is referred to as "buggy."

… debugging tools (called debuggers) help identify … coding errors at … various development stages. Some programming language packages include … facility for checking … code for … errors as it is being written.

Ex. 4. Discussion.

What can cause **all** the above-mentioned problems?
Make up a list of all possible causes of the problems in small groups and discuss them in class.

Ex. 5. Summarizing.

There are different troubles with computers. Some may be caused by force majeure, others by accident, third by ill will. Put the computer disasters into these categories and explain your answer.

Ex. 6. Listening.

At the level of enterprises most computer problems are dealt with by the IT service desk. However, the latter is in a great position to help outline the company policy and reveal hidden problems.
Listen to a part of the talk concerning this issue and answer the following questions.

1. How can a business become more effective with the help of the IT service desk?
2. Why don't IT specialists usually play a more active role in managing the business?
3. What example of such participation is given by the presenter?
4. What problems do small IT service desks often experience?

UNIT 2. COMPUTER EXPLOITS

Warming up

Ex.1. Discuss.

What do you call any software attack on a computer? Is it always malicious?

Mainstream

Ex.2. Learning facts.

Exploit

In computing, an exploit is an attack on a computer system, especially one that takes advantage of a particular vulnerability that the system offers to intruders. Used as a verb, the term refers to the act of successfully making such an attack.

Many crackers (or hackers, if you prefer that term) take pride in keeping tabs of such exploits and post their exploits (and discovered vulnerabilities) on a Web site to share with others.

Where an exploit takes advantage of a weakness in an operating system or vended application program, the owners of the system or application issue a "fix" or patch in response. Users of the system or application are responsible for obtaining the patch, which can usually be downloaded from the Web. Failure to install a patch for a given problem exposes the user to a security breach. (However, it can be difficult to keep up with all the required patches.)

Ex. 3. Grammar and vocabulary.

1. Read the first paragraph of the text and fill in the gaps with the terms given in the box. You should use some of them more than once.

exploit	exploitation	fix	notify	vulnerability

Zero-day exploit

a) A zero-day exploit is one that takes advantage of a security (1) … on the same day that the (1) … becomes generally known. Ordinarily, after someone detects that a software program contains a potential exposure to (2) … by a hacker, that person or company can (3) … the software company and sometimes the world at large so that action can be taken to repair the exposure or defend against its (2) … . Given time, the software company can repair and distribute a (4) … to users. Even if potential hackers also learn of the (1) , it may take them some time to (5) … it; meanwhile, the (4) … can hopefully become available first.

2. Insert prepositions in the second paragraph of the text.

b) … experience, however, hackers are becoming faster … exploiting a vulnerability and sometimes a hacker may be the first to discover the vulnerability. In these situations, the vulnerability and the exploit may become apparent … the same day. … the vulnerability isn't known … advance, there is no way to guard … the exploit before it happens. Companies exposed … such exploits can, however, institute

procedures … early detection of an exploit. A study released by Symantec … early 2004 found that although the number … vulnerabilities discovered was … the same in 2003 as in 2002, the time … the vulnerability and exploits based … it had narrowed. According to the infoAnarchy wiki, "14-day" groups and "7-day" groups carry out an exploit … 14 or 7 days of a product's market release. Conducting a zero-day exploit establishes crackers as members of the elite, because they must have covert industry connections to gain the inside information needed to carry out the attack.

Ex. 4. Learn and compare.

1. What prefixes can be used with **–ware** to describe applications which intend to cause some harm?
2. What is the difference between them?

Ex. 5. Discussion.

1. What have you heard about any of these:
   - *PUP*,
   - *drive-by download,*
   - *pop-up download,*
   - *cookie,*
   - *data collecting programs,*
   - *barnacle?*
   - 2. What steps can a user take to protect himself against all those in your opinion?

Ex.6 Reading.

1. What is spyware?
2. How can it get in a computer?
3. What are data collecting programs?
4. Can we call data collecting programs spyware? Why?
5. What is adware? What is the correlation between adware and spyware?

Malware

Malware (for "malicious software") is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware, programming that gathers information about a computer user without permission.

Adware

1) Generically, adware (spelled all lower case) is any software application in which advertising banners are displayed while the program is running. The authors of these applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen. The justification for adware is that it helps recover programming development cost and helps to hold down the cost for the user.

Adware has been criticized because it usually includes code that tracks a user's personal information and passes it on to third parties, without the user's authorization or knowledge. This practice has been dubbed spyware and has prompted an outcry from computer security and privacy advocates, including the Electronic Privacy Information Center.

Noted privacy software expert Steve Gibson of Gibson Research explains: "Spyware is any software (that) employs a user's Internet connection in the background (the so-called 'backchannel') without their knowledge or explicit permission. Silent background use of an Internet 'backchannel' connection must be preceded by a complete and truthful disclosure of proposed backchannel usage, followed by the receipt of explicit, informed consent for such use. Any software communicating across the Internet absent of these elements is guilty of information theft and is properly and rightfully termed: Spyware."

A number of software applications, including Ad-Aware and OptOut (by Gibson's company), are available as freeware to help computer users search for and remove suspected spyware programs.

2) AdWare is also a registered trademark that belongs to AdWare Systems, Inc. AdWare Systems builds accounting and media buying systems for the advertising industry and has no connection to pop-up advertising, spyware, or other invasive forms of online advertising.

PUP

A PUP (potentially unwanted program) is a program that may be unwanted, despite the possibility that users consented to download it. PUPs include spyware, adware, and dialers, and are often downloaded in conjunction with a program that the user wants.

The term was created by McAfee, the Internet Security company, because marketing firms objected to having their products called "spyware": in the view of such firms, all the information necessary for informed consent is included in the download agreement. It is widely recognized, however, that many if not most users fail to read a download agreement in sufficient detail to understand exactly what they are downloading.

McAfee differentiates PUPs from other types of malware, such as viruses, Trojans, and worms, which can be safely assumed to be unwanted by the user.

Drive-by download

A drive-by download is a program that is automatically downloaded to your computer, often without your consent or even your knowledge. Unlike a pop-up download, which asks for assent (albeit in a calculated manner likely to lead to a "yes"), a drive-by download is carried out invisibly to the user: it can be initiated by simply visiting a Web site or viewing an HTML e-mail message. Frequently, a drive-by download is installed along with another application. For example, a file sharing program might include downloads for a spyware program that tracks and reports user information for targeted marketing purposes, and an adware program that generates pop-up advertisements using that information. If your computer's security settings are lax, it may be possible for drive-by downloads to occur without any action on your part.

Xupiter, an Internet Explorer toolbar program, is frequently installed as a drive-by download. The program is said to replace the user's home page, change browser settings, and use redirection to take all searches to the Xupiter Web site. In some versions, the program initiates drive-by downloads of other programs. Furthermore, although it comes with an uninstall utility, Xupiter is said to be next to impossible for the average computer user to remove.

There are some arguments to be made in favor of drive-by downloads, particularly for downloads of patches or service packs that address security flaws. If these were automatically installed, instead of depending on the diligence of server administrators, computers and the

Internet in general might be safer from malicious programming such as viruses and worms. In January 2003, a worm called the SQL Slammer exploited a known buffer overflow vulnerability in Microsoft SQL 2000 server systems to cause widespread Internet outages. The attack was launched precisely six months after Microsoft released a patch for the flaw. If the patch had been installed to vulnerable systems, the attack would have had little impact.
However, although drive-by downloads for patches might address specific security flaws, they might also conflict with existing system configurations, and thus create more problems than they solve.

Pop-up download

A pop-up download (sometimes called a download pop-up) is a pop-up window that asks the user to download a program to their computer's hard drive. The window may feature a security warning, or some other type of message that is likely to lead to compliance. Often, the pop-up window has no information about the program to be downloaded, and may feature buttons for "download," "yes," or "ok" -- but none for "no" or "cancel." Faced with a pop-up download window, the user may think that the download in question is just a browser plug-in application needed for aspects of a Web site they're visiting, or that the pop-up window was generated by their own computer.

Pop-up downloads often install programs that track online behavior and report it back to a parent company (spyware) and programs that use that information to generate specific pop-up advertisements (adware). EarthLink, a popular Internet service provider (ISP) recently estimated that 40 to 50 percent of their subscribers have such applications running on their computers, usually without the owner's knowledge. Subscribers contacting the ISP to report a problem are often surprised to find that these downloads are the cause.

A less scrupulous variation of automatic installation, called a drive-by download, installs a program on a computer's hard drive without even first generating a pop-up window.

Barnacle

In a computer, a barnacle is unwanted programming, such as adware or spyware, that is downloaded and installed along with a user-requested program. Barnacles usually fall under the category of potentially unwanted programs (PUPs), a euphemistic term coined by McAfee to refer to programs that a user installs unintentionally, perhaps having unknowingly consented to their download.

The term derives from the name of a crustacean that attaches itself to whales and boats, among other things. Like its marine counterpart, the computer barnacle can be difficult to eradicate. According to PC Mechanic, barnacles often use confusing uninstall wizards. Another tactic that a barnacle may use is to require the user to fill out an online form to uninstall. Because the host system is quite likely to be clogged with spyware, there may not be sufficient resources available to allow them to do so.

Computer barnacles, like other spyware, can seriously affect computer performance. Unlike most spyware, however, they may also cause damage. Some barnacles interfere with the Winsock code that handles input/output requests for Internet applications in Windows operating systems. Winsock runs between a program (such as a browser) and the program that uses TCP/IP. Removal of this type of barnacle may corrupt Internet protocols and degrade network performance, in which case the user must reinstall the TCP/IP stack.

The term barnacle is closely related to drive-by download, which is programming downloaded without user consent and often without the user's knowledge that any download has occurred.

Cookie

A cookie is information that a Web site puts on your hard disk so that it can remember something about you at a later time. (More technically, it is information for future use that is stored by the server on the client side of a client/server communication.) Typically, a cookie records your preferences when using a particular site. Using the Web's Hypertext Transfer Protocol (HTTP), each request for a Web page is independent of all other requests. For this reason, the Web page server has no memory of what pages it has sent to a user previously or anything about your previous visits. A cookie is a mechanism that allows the server to store its own information about a user on the user's own computer. You can view the cookies that have been stored on your hard disk (although the content stored in each cookie may not make much sense to you). The location of the cookies depends on the browser. Internet Explorer stores each cookie as a separate file under a Windows subdirectory. Netscape stores all cookies in a single cookies.txt fle. Opera stores them in a single cookies.dat file.

Cookies are commonly used to rotate the banner ads that a site sends so that it doesn't keep sending the same ad as it sends you a succession of requested pages. They can also be used to customize pages for you based on your browser type or other information you may have provided the Web site. Web users must agree to let cookies be saved for them, but, in general, it helps Web sites to serve users better.

Spyware

Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet (where it is sometimes called a spybot or tracking software), spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program.

Data collecting programs that are installed with the user's knowledge are not, properly speaking, spyware, if the user fully understands what data is being collected and with whom it is being shared. However, spyware is often installed without the user's consent, as a drive-by download, or as the result of clicking some option in a deceptive pop-up window. Software designed to serve advertising, known as adware, can usually be thought of as spyware as well because it almost invariably includes components for tracking and reporting user information. However, marketing firms object to having their products called "spyware." As a result, McAfee (the Internet security company) and others now refer to such applications as "potentially unwanted programs" (PUP).

The cookie is a well-known mechanism for storing information about an Internet user on their own computer. If a Web site stores information about you in a cookie that you don't know about, the cookie can be considered a form of spyware. Spyware is part of an overall public concern about privacy on the Internet.

Many Internet users were introduced to spyware in 1999, when a popular freeware game called "Elf Bowling" came bundled with tracking software.

Ex. 7. Summarizing.

Arrange the following terms in a diagram, which would reveal correlation among them.

Malware, spyware, adware, PUP, drive-by download, pop-up download, cookie, data collecting programs, barnacle.

Ex. 8. Listening.

Flash-based malware

Listen to the first part of the recording and explain what Flash-based malware is and how it operates.
As you listen again, fill in the blanks with phrases from the recording.

1. A number of legitimate sites have become unfortunate a)_____, specifically in the form of Flash objects.

2. One of my favorites is a b) _____ which claims a user's system is infected.

3. Many of the c) _____ that have been analyzed either trigger on X number of clicks, or function by a d) _____.

4. … it … may also prove difficult for a team trying to e) _____ to perform a solid root-cause analysis of the infection, which is a key of any incident-response plan.

5. To scan ads successfully, websites need to be able f) _____ of known bad domains from which to block ads.

6. Sometimes g) _____ are used before malware is activated.

7. An attacker can take his malicious code and wrap it in a h) _____, like a Flash video.

8. Many users will install the application i) _____, perhaps believing it is required to view the content.

Listen to the second part of the recording outlining the defense strategy.
Find English equivalents to the following word combinations:

1. прибегать к услугам третьей стороны
2. убедиться
3. сообщить
4. как действует вредоносный код
5. может быть недостаточным
6. ознакомиться с
7. группа по расследованию происшествия
8. учитывая, что
9. возможности
10. несколько спорный

Rendering

Разговоры через Skype легко подслушать?

Популярная служба VoIP-телефонии Skype представляет собой легкую мишень для хакеров и открывает путь в корпоративную сеть.

Так утверждают авторы отчета из компании Network Box, специализирующейся на управляемых услугах безопасности. По их мнению, Skype может легко взломать враждебно настроенный работник, желающий устроить потайной ход в сеть своей компании.

В коротком отчете «Skype — друг или враг?» Network Box высказывает предположение, как именно может быть взломана программа. Для обнаружения лазеек Skype использует закрытый фирменный протокол, который в случае взлома становится идеальной системой для нарушения защиты коммуникаций, поддерживаемых с его помощью. Любая внедренная лазейка будет оставаться невидимой для систем безопасности компании, а когда появится возможность ее обнаружения, будет уже слишком поздно.

«Безопасность системы Skype целиком зависит от доброй воли программистов Skype и организации, эксплуатирующей серверы Skype. Не исключено, что в системе есть лазейки, позволяющие Skype — или другим — подслушивать или записывать разговоры», — говорится в отчете.

Мало того, что Skype скрывает свой протокол, она установила цикл непрерывных обновлений, который затрудняет эффективный контроль и управление. «Программа Skype способна обновляться автоматически при каждом запуске, так что параметры безопасности всей системы можно изменить без уведомления и даже без всяких видимых изменений. В случае ошибки в процессе такого обновления система может быть выведена из строя».

Указывая на случившийся на прошлой неделе двухдневный перерыв в работе службы, авторы отчета заключают, что даже компании, желающие использовать ее в резервном режиме, должны сознавать степень ненадежности этой программы по сравнению с основанными на стандартах средствах связи VoIP через VPN. Они рекомендуют также особенно тщательно проверять подлинность контактов Skype, даже если они кажутся легитимными, не применять для входа в Skype логин, используемый для доступа в какие-нибудь другие системы, и предупредить пользователей, чтобы они не указывали в своем профиле Skype компанию, в которой работают.

Сомнения по поводу безопасности Skype уже высказывались, и некоторые считают, что компания пытается решить эту проблему, выпустив бизнес-версию программы, которую будет проще контролировать и администрировать.

Skype обвиняет в аварии массовую перезагрузку компьютеров своих клиентов

Поставщик услуг интернет-телефонии Skype сообщил в понедельник, что причиной случившегося на прошлой неделе двухдневного перебоя в работе службы стал одновременный перезапуск компьютеров большого числа ее пользователей.

Миллионы пользователей загрузили рядовое обновление программного обеспечения Microsoft и перезагрузили свои машины, что привело к аварии всей одноранговой сети Skype. «Она обладает встроенной способностью к самовосстановлению, — говорится в блоге Skype, — однако это событие наложилось на неизвестную ранее ошибку в программном обеспечении, которая помешала быстрому срабатыванию функции самовосстановления. К сожалению, это привело к недоступности Skype для большинства пользователей в течение почти двух дней». Компания признает, что нарушение работы службы было «беспрецедентным по своему масштабу», но в качестве оправдания утверждает, что «сегодня очень мало ИТ- или коммуникационных сетей могут гарантировать бесперебойную работу».

В результате выхода сети из строя в четверг 220 млн клиентов Skype не смогли пользоваться дешевой интернет-телефонией. Аналитики удивлены приведенным объяснением и отмечают, что обновление программного обеспечения — относительно привычная операция, которая обычно не вызывает проблем, даже если ее одновременно выполняют 6 млн человек, — именно такое число «активных» пользователей, по оценкам компании, присутствует в ее сети в каждый момент времени. Аналитик Gartner по VoIP Стив Блад предполагает, что в данном случае при обновлении компьютеры пользователей передавали в Skype какую-то информацию, которая потребовала дополнительной обрабатывающей мощности и нагрузила сеть сильнее, чем обычно.

Skype, которая вместо централизованной коммутации вызовов использует одноранговую технологию, уверяет, что она внесла в свое ПО ряд усовершенствований, гарантирующих, что впредь пользователи будут избавлены от подобного эффекта «в маловероятном случае повторения этой последовательности событий».

Компания, которая два года назад стала подразделением eBay, позволяет пользователям компьютеров звонить друг другу бесплатно, а абонентам обычных телефонов — по относительно низким тарифам. Многие предприятия тоже начали пользоваться этой службой для снижения расходов, связанных с личными звонками сотрудников из заграничных командировок.

Магнитные «лавины» ухудшают надежность жестких дисков

Ученые обнаружили, что «лавинные» эффекты во вращающихся магнитных полях могут приводить к потере данных на жестких дисках, — и работают над изменением химического состава магнитного слоя, что должно привести к появлению более надежных устройств.

Два физика, профессор Калифорнийского университета в Санта-Круз Джошуа Дойч и сотрудник Hitachi Global Storage Technologies Андреас Бергер, обнаружили, что вращающиеся магнитные поля могут вызывать лавины, или волны, в поверхностном слое диска, и описали этот эффект в бюллетене US Physical Review Letter от 13 июля.

Когда головка чтения/записи диска записывает единицу или ноль, спин находящихся под ней атомов меняется на противоположный. Ученые установили, что это изменение происходит не сразу, а после некоторых колебаний, напоминающих прецессию земной оси. Они длятся несколько наносекунд и прекращаются, когда устанавливается новый спин атома. Однако этой прецессии спина может оказаться достаточно, чтобы повлиять на состояние соседних атомов.

В результате возникает волна лавинообразного распространения прецессии спина, которая постепенно затухает в массе материала. Пока этот эффект проявляется слабо, но по мере дальнейшего повышения плотности записи он может приводить к ненадежной работе диска. Ученые надеются уменьшить его, целенаправленно подбирая материалы с нужными магнитными свойствами.

Каждый день появляется почти 30 тыс. вредоносных веб-сайтов

В последние месяцы количество вредоносных веб-сайтов растет лавинообразно, и вместо 5000 новых сайтов в день в апреле теперь их ежедневно появляется почти 30 тыс.

Аналитическая фирма Sophos объясняет это двумя причинами. По ее мнению, хакеры все чаще переключаются с e-mail в качестве предпочтительного метода распространения вредоносного ПО на веб-сайты. Иногда они создают собственные сайты, но чаще всего взламывают легитимные сайты и помещают на них вредоносное ПО. По данным Sophos, каждый день появляется 29 700 новых инфицированных веб-сайтов, 80% которых — это взломанные легитимные сайты. В июне наиболее распространенным вредоносным ПО, заражающим веб-сайты, была программа IFrame.

IFrame размещает на веб-страницах вредоносные файлы HTML и возглавляет список Sophos десяти наиболее опасных угроз в вебе — на счету у этой программы почти две трети всех зараженных веб-страниц в мире. В июне хакеры использовали IFrame для массовой атаки на итальянские веб-сайты, в ходе которой было заражено свыше 10 тыс. веб-страниц. В числе жертв были сайты городских администраций, службы трудоустройства и туристические сайты.

«Атака IFrame в Италии должна стать тревожным сигналом для ISP во всем мире, — говорит старший консультант по безопасности Sophos Кароль Терио. — Вредоносный код, занесенный на эти сайты, обрушится на невинных серферов. Веб-сайты должны быть защищены, как Форт-Нокс, однако сегодня слишком много веб-страниц становится легкой добычей киберпреступников».

Но Терио отмечает, что есть и другая причина столь резкого скачка числа вредоносных сайтов: их просто стали лучше искать. При сканировании такого количества веб-сайтов поиск зараженных страниц представляет собой довольно трудоемкое дело. Однако чем больше исследователей этим занимается, тем лучше результат.

Тысячи веб-сайтов стали жертвами «Ограбления по-итальянски-3»

Киберпреступники организовали массовую веб-атаку, в результате которой множество легитимных веб-сайтов превратилось в послушное им оружие.

По утверждению секьюрити-фирм Trend Micro и Websense, атака началась на прошлой неделе, а к утру понедельника было заражено уже свыше 10 тыс. веб-сайтов. Более 80% инфекции пришлось на итальянские сайты, хотя впоследствии она распространилась на весь мир. Trend Micro назвала ее Italian Job 3 — по имени кинобоевика «Ограбление по-итальянски» с Майклом Кейном, римейк которого вышел в 2003 году. В основном заражены легитимные веб-сайты — не порно или азартных игр, а отелей, турбюро и т. п. Пострадали даже веб-сайты итальянских госучреждений, причем большинство зараженных веб-сайтов обслуживались одним из крупнейших в Италии сервис-провайдеров.

Все эти сайты содержат короткую строку кода HTML iFrame, которая переадресует веб-браузеры на сервер, пытающийся заразить компьютер жертвы при помощи инструмента MPack. MPack способен атаковать ПК разными способами, в зависимости от типа браузера и операционной системы. Он использует несколько известных и уже исправленных уязвимостей, так что опасен для тех, кто не обновляет свой браузер. Пострадать могут пользователи Internet Explorer, Firefox и даже Opera.

MPack устанавливает кейлоггер и программу, загружающую троян, так что злоумышленники могут шпионить за взломанными ПК и тайно исполнять на нем другие программы, превращая компьютер в собственный инструмент. Хотя приемы, используемые хакерами, не новы, атака такого масштаба выделяется своей амбициозностью и степенью координации. К расследованию инцидента подключилось ФБР США.

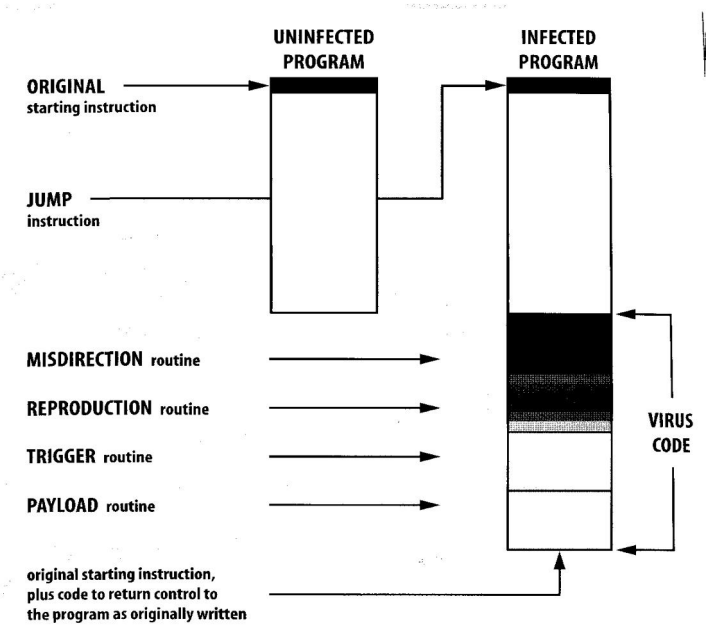
UNIT 3. VIRUSES.

Warming up

Ex. 1. Discussion.

3 Study this diagram which explains how one type of virus operates. Try to answer these questions.

1 What is the function of the Jump instruction?
2 What are the main parts of the virus code?
3 What is the last act of the virus?



(Taken from *Oxford English for Information Technology* by Eric H. Glendinning, John McEwan)

Mainstream

Ex. 2. Learning facts.

1. Read

THE ANATOMY OF A VIRUS

A biological virus is a very small, simple organism that infects living cells, known as the host, by attaching itself to them and using them to reproduce itself. This often causes harm to the host cells.

Similarly, a computer virus is a very small program routine that infects a computer system and uses its resources to reproduce itself. It often does this by patching the operating system to enable it to detect program files, such as COM or EXE files. It then copies itself into those files. This sometimes causes harm to the host computer system.

When the user runs an infected program, it is loaded into memory carrying the virus. The virus uses a common programming technique to stay resident in memory. It can then use a reproduction routine to infect other programs. This process continues until the computer is switched off.

The virus may also contain a payload that remains dormant until a trigger event activates it, such as the user pressing a particular key. The payload can have a variety of forms. It might do

something relatively harmless such as displaying a message on the monitor, screen or it might do something more destructive such as deleting files on the hard disk.
When it infects a file, the virus replaces the first instruction in the host program with a command that changes the normal execution sequence. This type of command is known as a JUMP command and causes the virus instructions to be executed before the host program. The virus then returns control to the host program which then continues with its normal sequence of instructions and is executed in the normal way.
To be a virus, a program only needs to have a reproduction routine that enables it to infect other programs. Viruses can, however, have four main parts. A misdirection routine that enables it to hide itself; a reproduction routine that allows it to copy itself to other programs; a trigger that causes the payload to be activated at a particular time or when a particular event takes place; and a payload that may be a fairly harmless joke or may be very destructive. A program that has a payload but does not have a reproduction routine is known as a Trojan.

2. Answer the questions

1 How are computer viruses like biological viruses?
2 What is the effect of a virus patching the operating system?
3 Why are some viruses designed to be loaded into memory?
4 What examples of payload does the writer provide?
5 What kind of programs do viruses often attach to?
6 Match each virus routine to its function.

Routine		Function	
1	misdirection	a	does the damage
2	reproduction	b	attaches a copy of itself to another program
3	trigger	c	hides the presence of the code
4	payload	d	decides when and how to activate the payload

7 How does a Trojan differ from a virus?
(Taken from *Oxford English for Information Technology* by Eric H. Glendinning, John McEwan)

Ex. 3. Discussion.

Discuss the following questions in the class, taking notes of the definitions.

- What is a virus?
- How is it ordinarily transmitted?
- Do they cause damages as soon as their code is executed?
- How can viruses be classified?
- What are the ways to protect a computer against a virus?
- What is the origin of the term virus?

Viruses.

In computers, a virus is a program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document. Viruses can be

transmitted as attachments to an e-mail note or in a downloaded file, or be present on a diskette or CD. The immediate source of the e-mail note, downloaded file, or diskette you've received is usually unaware that it contains a virus. Some viruses wreak [ri:k] their effect as soon as their code is executed; other viruses lie dormant until circumstances cause their code to be executed by the computer. Some viruses are benign or playful in intent and effect ("Happy Birthday, Ludwig!") and some can be quite harmful, erasing data or causing your hard disk to require reformatting. A virus that replicates itself by resending itself as an e-mail attachment or as part of a network message is known as a worm.

Generally, there are three main classes of viruses:

File infectors. Some file infector viruses attach themselves to program files, usually selected .COM or .EXE files. Some can infect any program for which execution is requested, including .SYS, .OVL, .PRG, and .MNU files. When the program is loaded, the virus is loaded as well. Other file infector viruses arrive as wholly-contained programs or scripts sent as an attachment to an e-mail note.

System or boot-record infectors. These viruses infect executable code found in certain system areas on a disk. They attach to the DOS boot sector on diskettes or the Master Boot Record on hard disks. A typical scenario (familiar to the author) is to receive a diskette from an innocent source that contains a boot disk virus. When your operating system is running, files on the diskette can be read without triggering the boot disk virus. However, if you leave the diskette in the drive, and then turn the computer off or reload the operating system, the computer will look first in your A drive, find the diskette with its boot disk virus, load it, and make it temporarily impossible to use your hard disk. (Allow several days for recovery.) This is why you should make sure you have a bootable floppy.

Macro viruses. These are among the most common viruses, and they tend to do the least damage. Macro viruses infect your Microsoft Word application and typically insert unwanted words or phrases.

The best protection against a virus is to know the origin of each program or file you load into your computer or open from your e-mail program. Since this is difficult, you can buy anti-virus software that can screen e-mail attachments and also check all of your files periodically and remove any viruses that are found. From time to time, you may get an e-mail message warning of a new virus. Unless the warning is from a source you recognize, chances are good that the warning is a virus hoax.

The computer virus, of course, gets its name from the biological virus. The word itself comes from a Latin word meaning slimy liquid or poison.

Ex.4. Listening.

Listen to the following virus definition and fill in the blanks in the summary:

It is vital for a business to understand how 1) _____ and how to prevent them 2) _____.

Viruses can be defined as computer programs created intentionally to alter the behaviour of a computer without 3) _____ or 4) _____. A virus functions in the following way: it 5) _____ placing its own code into another program. Besides it 6) _____.

Most viruses are designed to infect both 7) _____ and 8) _____ in order to damage programs, files or reformat the hard disk. Still there exist some harmless viruses which reveal themselves by 9) _____ messages. However, in this case small businesses can suffer because viruses 10) _____ used by legitimate programs and often lead to 11) _____ or even 12) _____.

Ex. 5. Discussion "Bitter experience".

Discuss your own experience and the viruses that infected your computer or the computers of your friends.

Ex.6. Learning facts.

1. E-mail virus

An e-mail virus is computer code sent to you as an e-mail note attachment which, if activated, will cause some unexpected and usually harmful effect, such as destroying certain files on your hard disk and causing the attachment to be remailed to everyone in your address book. Although not the only kind of computer virus, e-mail viruses are the best known and undoubtedly cause the greatest loss of time and money overall. The best two defenses against e-mail viruses for the individual user are (1) a policy of never opening (for example, double-clicking on) an e-mail attachment unless you know who sent it and what the attachment contains, and (2) installing and using anti-virus software to scan any attachment before you open it. (However, some e-mail viruses may be so new when your receive them that your anti-virus software may not yet be familiar with it.) Business firewall servers also attempt, but not always successfully, to filter out e-mail that may carry a virus attachment.

The Melissa virus macro virus and the ILOVEYOU virus are among the best publicized of recent e-mail viruses. Each of these also spawned copycat variations with different words in the subject line.

Microsoft has been criticized for allowing its widely-used Outlook e-mail program to be so easily exploited by virus creators. Some users indicate that other e-mail programs such as Eudora offer the user more protection.

2. Macro virus

A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it. Macro viruses tend to be surprising but relatively harmless. A typical effect is the undesired insertion of some comic text at certain points when writing a line. A macro virus is often spread as an e-mail virus. A well-known example in March, 1999 was the Melissa virus.

3. Worm

In a computer, a worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

This term is not to be confused with WORM (write once, read many).

4. Trojan horse

In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.

The term comes from Greek mythology about the Trojan War, as told in the Aeneid by Virgil and mentioned in the Odyssey by Homer. According to legend, the Greeks presented the citizens

of Troy with a large wooden horse in which they had secretly hidden their warriors. During the night, the warriors emerged from the wooden horse and overran the city.

5. Stealth virus

In computer security, a stealth virus is a computer virus that uses various mechanisms to avoid detection by antivirus software. Generally, stealth describes any approach to doing something while avoiding notice. Viruses that escape notice without being specifically designed to do so -- whether because the virus is new, or because the user hasn't updated their antivirus software -- are sometimes described as stealth viruses too. Stealth viruses are nothing new: the first known virus for PCs, Brain (reportedly created by software developers as an anti-piracy measure), was a stealth virus that infected the boot sector in storage.

Typically, when an antivirus program runs, a stealth virus hides itself in memory, and uses various tricks to also hide changes it has made to any files or boot records. The virus may maintain a copy of the original, uninfected data and monitor system activity. When the program attempts to access data that's been altered, the virus redirects it to a storage area maintaining the original, uninfected data. A good antivirus program should be able to find a stealth virus by looking for evidence in memory as well as in areas that viruses usually attack.

The term stealth virus is also used in medicine, to describe a biological virus that hides from the host immune system.

6. Hybrid virus

A hybrid virus (sometimes called a multi-part or multipartite virus) is one that combines characteristics of more than one type to infect both program files and system sectors. The virus may attack at either level and proceed to infect the other once it has established itself. Hybrid viruses can be very difficult to eradicate and, unless completely eradicated, will often reinfect the host system repeatedly.

In general, viruses fall into one of three classes: macro viruses, file infectors (also known as program infectors), and system or boot-record infectors. Macro viruses, which are fairly common and often less harmful than other types, infect a word processing application and typically insert unwanted words or phrases. A hybrid virus usually combines the approaches of the two latter types in order to maximize damage and resistance to removal. File infector viruses attack executable files on your hard drive. Each time you run the file, you unknowingly invoke the virus which, in turn, delivers its payload to your system. System or boot-record infectors infect executable code found in certain system areas on a disk, infecting the portion of your hard drive that contains the operating system instructions telling the computer how to start up. These viruses are invoked each time the computer starts.

Because getting rid of a hybrid virus can be such a difficult process, most security experts recommend prevention rather than cure, and suggest that people follow common sense security procedures; these include: running good anti-virus software and keeping virus definitions updated, practicing caution with e-mail and never opening an unexpected attachment or downloading a program from a questionable source.

Ex. 7. Grammar and vocabulary.

1. Do you know what the first wild spread virus was?
What are the oldest viruses you can remember?

2. Read the text and fill in the gaps with the words given in the box. You should use some of them more than once.

accessed	booted	copied	created	elapsed	infected
intended	passed	reported	spread	stored	uninfected

Elk Cloner

Elk Cloner was the first computer virus known to have (1) … in the wild. In 1982, Richard Skrenta, then fifteen years old, wrote the virus for the Apple II operating system, which was (2) … on floppy diskettes. When a computer (3) … from a floppy disk (4) … with Elk Cloner, the virus would start, and would subsequently copy itself to any (5) … floppy disk that was (6) …. Because computers of that time had dual floppy disk drives, and because diskettes were often (7) … around among friends, the virus was frequently (8) …. After contagion, every 50th time that a computer booted up, it would display the following text:

Elk Cloner: The program with a personality
It will get on all your disks
It will infiltrate your chips
Yes it's Cloner!
It will stick to you like glue
It will modify ram too
Send in the Cloner!

Elk Cloner was not (9) … to cause damage, but was (10) … as a practical joke. According to WorldHistory.com, the adolescent Skrenta had a penchant for modifying programs so that they stopped working after some code-specified time period had (11) …, at that point displaying some joke text that Skrenta had written. Not surprisingly, the young programmer's friends grew leery of allowing him access to their diskettes. Elk Cloner's capacity to copy itself (the major criterion of a virus) made it possible for Skrenta to continue to annoy his friends without requiring physical access. The virus is (12) … to have spread widely among his fellow students (and also to his math teacher), thus ensuring Elk Cloner's place in history.

3. Find and correct ten grammar mistakes

Virus hoax

A virus hoax is a false warning about a computer virus. Typically, the warning arrive in a e-mail note or distributed through a note in a company's internal network. This notes are usually forwarded using distribution lists and they will typical suggest that the recipient forwards the note to other distribution lists.

If you got a message about a new virus, you can check them out by go to one of the leading Web sites that keep up with viruses and virus hoaxes. If someone sends you note about a virus that you learn is a virus hoax, reply to the sender that the virus warning is a hoax.

Ex. 8. Reading and reporting.

Describe any existing virus, its code, the way it infects a program, its reproduction, trigger and payload routines.

As an example take the Chernobyl virus

Chernobyl virus

The Chernobyl virus is a computer virus with a potentially devastating payload that destroys all computer data when an infected file is executed. Since many files are executed during computer use, the virus is able to spread quickly and infect those files. The Chernobyl virus is the first virus known to have the power to damage computer hardware. The activated viral strain attempts to erase the hard drive and overwrite the system's BIOS as well.

The virus was detected as early as 1998, but its payload was first triggered April 16, 1999 - which was the 13th anniversary of the disaster at the Chernobyl nuclear reactor. Although U.S. and European computer users were affected, especially students and some businesses, most of Chernobyl's damage was wrought in Asia and the Middle East. Chernobyl actually is a variant of a virus known as CIH, the initials for the alleged author of the virus, Chen Ing-hau, a Taiwanese computer engineering student). Some CIH variants activate on the 26th day of each month, while others do their damage on April 26 or June 26.

CIH is sometimes referred to as a "space filler virus," referring to its ability to clandestinely take up file space on computers and prevent anti-virus software from running.

Users of Windows 95 and Windows 98 are more susceptible to the risk of contracting the CIH virus. It is under these programs that the virus replicates and becomes active. Users of DOS, Windows 3.x, Windows NT, Windows 2000 or Macintosh are not considered at risk.

Ex.9. Discussion

Discuss weak and strong features of anti-virus software.

Ex.10. Listening

VIRUS PROTECTOIN

1) Listen to the recording and write down the main virus protection measures. Pay special attention the ones that have not been discussed in this unit yet.

RECUPERATION FROM A VIRUS ATTACK

2) Listen to a computer security expert talking about the measures that should be taken in enterprises in case of a virus attack. Make a list of steps mentioned in the recording. Take down as many details as you can.

Rendering

Инциденты, связанные с нарушением безопасности, становятся все серьезнее

Число сообщений о взломах компьютерных сетей сокращается, между тем средняя степень тяжести последствий от них удвоилась, утверждают авторы исследования.

Исследование Ассоциации производителей вычислительной техники (CompTIA), основанное на опросе более чем тысячи ИТ-специалистов, обнаружило, что в 2006 году в 34%

организаций были случаи серьезного нарушения ИТ-безопасности — это меньше, чем в 2005 году (38%) и в 2004 году (58%). Однако среднюю степень тяжести инцидентов респонденты оценили в 4,8 балла (по десятибалльной шкале), тогда как в предыдущие годы их оценки колебались в пределах от 2,3 до 2,6 балла. Это не удивительно, учитывая количество громких взломов, таких как взлом сети TJX, когда были украдены миллионы номеров кредитных и дебитных карт.

ИТ-профессионалы сообщили о росте своих расходов на технологию безопасности, обучение и сертификацию. В 2006 году доля ассигнований на обеспечение безопасности в ИТ-бюджете компаний составила 20%, вместо 15% в 2005 и 12% в 2004 году. Более двух третей (68%) организаций выделяет какую-то часть своего ИТ-бюджета на обучение или сертификацию, тогда как год назад их было 55%. На эти цели выделяется в среднем 12% бюджета, вместо 8% в 2005 году. 78% опрошенных сказали, что теперь их руководство считает защиту информации высшим приоритетом.

«Мы достигли реального прогресса в сокращении числа инцидентов, но угрозы становятся более изощренными», — сказал операционный директор CompTIA Брайан Маккарти.

Главной угрозой для безопасности свыше половины (55%) опрошенных ИТ-профессионалов назвали шпионское ПО, за которым следует недостаточная осведомленность пользователей (54%). Почти половина считает, что вирусы и черви по-прежнему представляют опасность, а около 44% назвали главной угрозой злоупотребления авторизованных пользователей. Инциденты, вызванные ошибкой человека, произошли в 42% организаций, тогда как год назад их было 59%. В числе других проблем называют атаки через браузеры (41%), дистанционный доступ (40%), беспроводные сети (39%) и недостаточное соблюдение правил безопасности (36%).

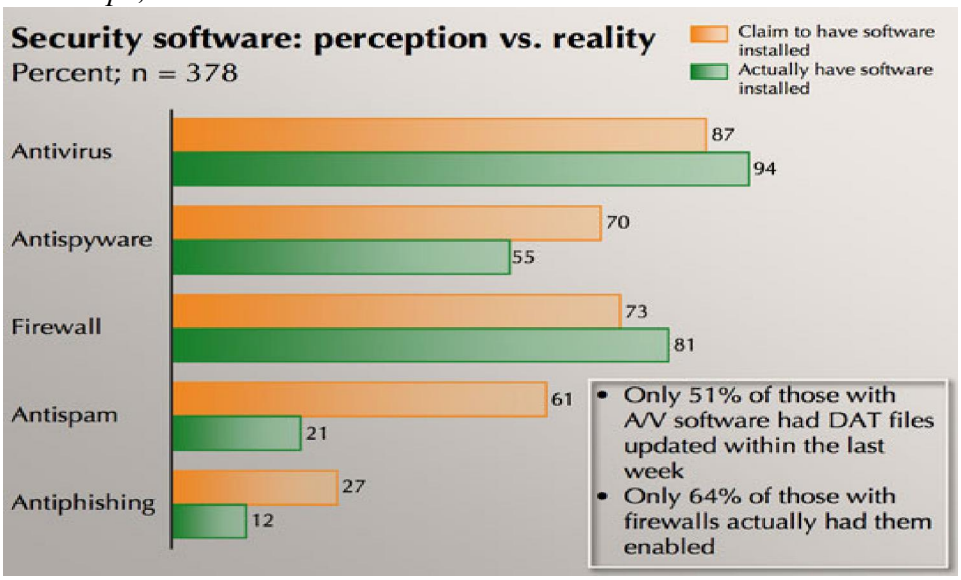
«Свыше половины всех организаций утверждает, что угрозы для безопасности, связанные с использованием карманных устройств, шпионским ПО, технологией «голос поверх IP», беспроводными сетями и удаленными/мобильными устройствами значительно усилились по сравнению с предыдущим годом», — говорится в отчете.

CompTIA отмечает, что правила безопасности и обучение могут помочь организациям не стать жертвами атак. 62% опрошенных сказали, что в их организациях составлены правила безопасности, хотя в предыдущие два года таких организаций было 47%. В 81% организаций, имеющих писаные правила безопасности, эти правила содержат сведения по защите удаленных и мобильных сотрудников.

Средняя стоимость одного взлома в 2006 году составила $369 388; среднюю экономию от проведения тренинга по ИТ-безопасности для персонала CompTIA оценивает в $352 тыс. Еще $656 тыс. организации могут сэкономить, проведя сертификацию по безопасности сотрудников своего ИТ-подразделения.

Потребители только думают, что они в кибербезопасности

2 октября, 2007



Из опубликованного в понедельник отчета следует, что хотя большинство американских потребителей считает, что их компьютеры защищены от кибератак, на самом деле они мало что делают для этого.

Как показало исследование, проведенное в США Национальным альянсом кибербезопасности (NCSA) и аналитической фирмой McAfee, 87% опрошенных потребителей считает, что на их компьютерах установлен антивирус, между тем при сканировании этих систем обнаружилось, что лишь у 52% действительно имеется обновленное за последний месяц антивирусное ПО. При этом более девяти десятых участников опроса уверены, что их компьютеры защищены от вирусов. Аналогично, 70% потребителей убеждены, что на их компьютерах установлено антишпионское ПО, но только 55% установили его на самом деле. А 61% утверждает, что у них есть защита от спама, хотя фильтры обнаружены лишь у 21%.

«У потребителей сложилось ложное чувство безопасности, — говорит вице-президент по международному маркетингу среди потребителей McAfee Бари Абдул. — То, что они говорят о защищенности своих ПК, не соответствует действительности». На 78% обследованных McAfee компьютеров не установлено то, что Абдул называет «ядром защиты» — комплект из антивируса, антишпионского ПО и межсетевого экрана. Опрос проводился по электронной почте, и 378 ответивших разрешили проверить свои компьютеры.

McAfee и NCSA, просветительская организация, в которую входят госучреждения и частные компании, представили отчет на однодневном мероприятии в Вашингтоне, посвященном началу «месячника национальной осведомленности о кибербезопасности», который проходит в октябре. На мероприятии выступили председатель Федеральной торговой комиссии США Дебора Плат Махорас и помощник секретаря по кибербезопасности и коммуникациям при Министерстве внутренней безопасности США Грег Гарсия. Оба они призвали компании сотрудничать с правительством в сфере просвещения потребителей и организаций по поводу важности киберзащиты. «Индивидуальная и корпоративная киберзащита — две стороны одной медали, — сказал Гарсия. — Одно без другого невозможно».

По словам Махорас, одна из насущных проблем, «которая меня очень тревожит», — фишинговые атаки. Она убеждена, что проблему фишинга можно было бы решить, если бы потребителям было известно о таком явлении, как «кража личности». В ходе опроса McAfee/NCSA 75% респондентов сказали, что они слышали о фишинге, но только 54% смогли точно описать это явление. 44% сказали, что на их компьютерах установлено шпионское или рекламное ПО.

Почти 90% респондентов хранят персональную информацию в своих компьютерах и в то же время пользуются онлайновыми услугами банков, совершают операции с ценными бумагами и занимаются другой подобной деятельностью.

Необходимо усилить просветительскую работу, сказал Абдул: «Чрезвычайно важно перевести этот диалог на новый уровень».

Вирус охотится на файлы MP3

3 августа, 2007

Эксперты по безопасности обнаружили вирус, который реализует заветную мечту индустрии звукозаписи: он отыскивает файлы MP3 и удаляет их из зараженного ПК.

Секьюрити-компании считают уровень риска невысоким, однако необычная вредоносная нагрузка может стать неприятным сюрпризом для меломанов. Не ясно, какими мотивами руководствовались создатели вируса. «Скорее всего, его соорудили шкодливые мальчишки, а не организованные банды, которые, как правило, ищут финансовых выгод, — прокомментировал старший консультант Sophos Грэм Клули. — Это не то, из-за чего можно лишиться сна, однако пользователи ПК, которые мало заботятся о том, чтобы минимизировать опасность заражения, получили еще один урок».

Вирус распространяется через флэш-диски USB, напоминая о временах, когда основным способом заражения компьютеров служили дискеты. Возможно, тем самым авторы вируса пытаются обойти фильтры e-mail и веб-шлюзов. Symantec, которая назвала этот вирус

W32.Deletemusic, предупреждает, что он копирует себя на все диски, имеющиеся в ПК, и создает файл автозапуска, активизирующий его при каждом обращении к диску. Вирус работает в системах Windows 2000, 95, 98, Me, NT, Server 2003, XP и Vista. Его можно заблокировать, отключив функцию Windows autorun, которая автоматически запускает программы с CD или USB-дисков.

Это не первый случай, когда вредоносные программы охотятся за музыкальными файлами. Два года назад появился червь Nopir-B, который распространялся под видом утилиты для копирования DVD. Оказавшись в машине, он отображал антипиратский плакат и пытался удалить MP3 и другие файлы. А в прошлом году объявился троян Erazer, который пошел еще дальше, удаляя не только записи MP3, но и кинофильмы.

IE и Firefox вместе создают «критическую» угрозу для безопасности

Использование Firefox в сочетании с Internet Explorer на одном и том же компьютере делает систему уязвимой, утверждают специалисты по безопасности.

Пользователи, у которых наряду с IE установлен Firefox версии 2.0 или выше, подвергаются повышенному риску. Проблемы начинаются с посещения посредством IE вредоносного сайта, который регистрирует обработчик URI (uniform resource identifier handler) "firefoxurl://" позволяющий браузеру взаимодействовать с определенными веб-ресурсами. В конечном итоге система пользователя может оказаться управляемой дистанционно.

Специалист по безопасности Тор Лархольм, обнаруживший эту проблему, и компания Symantec обвиняют главным образом IE, однако главный технолог Secunia Томас Кристенсен считает виновником Firefox 2.0. «Вообще-то виноваты оба, — прокомментировал директор Symantec Security Response Center Оливер Фридрихс. — Это два чрезвычайно сложных приложения, которые не очень хорошо сочетаются друг с другом. Каждое по отдельности может быть безопасно, а вместе — нет». Фридрихс отметил, что хотя Firefox, у которого в прошлом году вышла версия 2, становится все популярнее, на компьютерах большинства пользователей этого браузера установлен также IE, поставляемый вместе с операционной системой Windows.
Для инъекции в систему пользователя кода, исполняемого в Firefox, злоумышленник может использовать chrome-контекст — элементы интерфейса браузера, которые создают рамку вокруг отображаемых страниц. «Обработчик URI должен быть выполнен тщательнее, так как Windows не может знать, какие входные данные потенциально опасны для каждого приложения, — пояснил Кристенсен. — Например, откуда Windows может быть известно, что строка chrome опасна для Firefox?» Во избежание риска он рекомендует системным администраторам снять регистрацию обработчика URI firefoxurl или удалить его, или же изменить способ приема браузером Firefox данных chrome.

UNIT 4. BYPASS. PHISHING & PHARMING. OTHER COMPUTER CRIMES.

Warming up

Ex. 1. Discussion.

Think about the meaning of the word *bypass*. Discuss the following questions in pairs:

- What is bypass?
- What kinds of bypass do you know?

Bypass

Bypass, in general, means either to go around something by an external route rather than going through it, or the means of accomplishing that feat. In network security, a bypass is a flaw in a security system that allows an attacker to circumvent security mechanisms to get system or network access. The actual point of entry is through a mechanism (either a hardware device or program, even just a piece of code) that enables the user to access the system without going through the security clearance procedures (such as authentication) that were set up by the system administrator. A bypass may be a mechanism put in place by an attacker, a flaw in the design, or an alternate access route left in place by developers. A bypass that is purposefully put in place as a means of access for authorized users is called a back door or a trap door. A crypto bypass is a flaw that allows data to circumvent the encryption process and escape, unencrypted, as plaintext.

Mainstream

Ex. 2. Learning facts.

1. Read the text and pay attention to the terms *bypass, flaws in security systems*, *backdoors or trapdoors* and *crypto bypass.*
Explain the differences between them.

Back door

A back door is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a back door so that the program can be accessed for troubleshooting or other purposes. However, attackers often use back doors that they detect or install themselves, as part of an exploit. In some cases, a worm is designed to take advantage of a back door created by an earlier attack. For example, Nimda gained entrance through a back door left by Code Red.
Whether installed as an administrative tool or a means of attack, a back door is a security risk, because there are always crackers out there looking for any vulnerability to exploit. In her article "Who gets your trust?" security consultant Carole Fennelly uses an analogy to illustrate the situation: "Think of approaching a building with an elaborate security system that does bio scans, background checks, the works. Someone who doesn't have time to go through all that might just rig up a back exit so they can step out for a smoke -- and then hope no one finds out about it."

Ex. 3. Grammar and vocabulary.

1.Open the brackets and put the words in correct form.

Phishing

Phishing is e-mail fraud where the (1) … (*perpetrate*) sends out legitimate-looking e-mails that appear to come from well known and trustworthy Web sites in an attempt to gather (2) … (*person*) and (3) … (*finance*) information from the recipient. A phishing expedition, like the fishing expedition it's named for, is a (4) … (*speculate*) venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter the bait. Web sites that are (5) … (*frequent*) spoofed by phishers include PayPal, eBay, MSN, Yahoo, BestBuy, and America Online.

Phishers use a number of different social engineering and e-mail spoofing ploys to try to trick their victims. In one fairly typical case before the Federal Trade Commission (FTC), a 17-year-old male sent out messages (6) … (*purport*) to be from America Online that said there had been a billing problem with recipients' AOL accounts. The perpetrator's e-mail used AOL logos and contained legitimate links. If recipients clicked on the "AOL Billing Center" link, however, they were taken to a spoofed AOL Web page that asked for personal information, including credit card numbers, personal (7) … (*identify*) numbers (PINs), social security numbers, banking numbers, and passwords. This information was used for identity theft.

The FTC warns users to be suspicious of any official-looking e-mail message that asks for updates on personal or financial information and urges recipients to go (8) … (*direct*) to the organization's Web site to find out whether the request is legitimate.

2. Read the text and fill in the gaps with the terms given in the box. You should use some of them more than once.

affected	compromised	conscious	fake	fraudulent	legitimate
legitimate-looking	malicious	ominous	personal and financial		removal
scamming					

Pharming

Pharming is a(n) (1) …practice in which (2) …code is installed on a personal computer or server, misdirecting users to (3) … Web sites without their knowledge or consent. Pharming has been called "phishing without a lure."

In phishing, the perpetrator sends out (4) … e-mails, appearing to come from some of the Web's most popular sites, in an effort to obtain (5) … information from individual recipients. But in pharming, larger numbers of computer users can be victimized because it is not necessary to target individuals one by one and no (6) … action is required on the part of the victim. In one form of pharming attack, code

sent in an e-mail modifies local host files on a personal computer. The host files convert URLs into the number strings that the computer uses to access Web sites. A computer with a(n) (7) … host file will go to the (8) … Web site even if a user types in the correct Internet address or clicks on a(n) (9) … bookmark entry. Some spyware (10) … programs can correct the corruption, but it frequently recurs unless the user changes browsing habits.

A particularly (11) … pharming tactic is known as domain name system poisoning (DNS poisoning), in which the domain name system table in a server is modified so that someone who thinks they are accessing (12) … Web sites is actually directed toward fraudulent ones. In this method of pharming, individual personal computer host files need not be corrupted. Instead, the problem occurs in the DNS server, which handles thousands or millions of Internet users' requests for URLs. Victims end up at the bogus site without any visible indicator of a discrepancy. Spyware (10) … programs cannot deal with this type of pharming because nothing need be technically wrong with the end users' computers.

Once personal information such as a credit card number, bank account number, or password has been entered at a(n) (3) … Web site, criminals have the information and identity theft can be the end result.

Ex. 4. Vocabulary

Decide in your group what these kinds of computer crime are. Then match the crimes to the short descriptions which follow.

1 Salami Shaving
2 Denial of Service
3 Trojan Horse
4 Trapdoors
5 Mail bombing
6 Software Piracy
7 Piggybacking
8 Spoofing
9 Defacing
10 Hijacking

a) Leaving, within a completed program, an illicit program that allows unauthorised - and unknown - entry.
b) Using another person's identification code or using that person's files before he or she has logged off.
c) Adding concealed instructions to a computer program so that it will still work but will also perform prohibited duties. In other words, it appears to do something useful but actually does something destructive in the background.
d) Tricking a user into revealing confidential information such as an access code or a credit-card number.
e) Inundating an email address with thousands of messages, thereby slowing or even crashing the server.
f) Manipulating programs or data so that small amounts of money are deducted from a large number of transactions or accounts and accumulated elsewhere. The victims are often unaware of the crime because the amount taken from any individual is so small.
g) Unauthorised copying of a program for sale or distributing to other users.
h) Swamping a server with large numbers of requests.
i) Redirecting anyone trying to visit a certain site elsewhere.
j) Changing the information shown on another person's website.

Ex. 5. Listening.

Listen to the broadcast about a type of phishing and then answer the questions.

1) What type of phishing is described in the broadcast?

2) How does it differ from ordinary phishing?

3) What happened at West Point?

4) What does the success of this type of phishing rely upon?

5) Give a short summary about the three steps for an organization to protect itself against phishing.

Ex. 6. Discussion.

What are the main computer threats that people and organizations face nowadays?

Ex. 7. Grammar and vocabulary.

1. Choose a better synonym.

Buffer overflow

A buffer overflow **occurs/happens** when a program or process tries to **keep/store** more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a **restricted/finite** amount of data, the extra information - which has to go somewhere - can overflow into **adjacent/bordering** buffers, corrupting or overwriting the **applicable/valid** data held in them. Although it may occur **accidentally/by mistake** through programming error, buffer overflow is an increasingly common type of security attack on data **reliability/integrity**. In buffer overflow attacks, the extra data may contain codes designed to **elicit/trigger** specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or **disclose/release** confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the **vulnerability/weakness**. In July 2000, a vulnerability to buffer overflow attack was discovered in Microsoft Outlook and Outlook Express. A programming flaw made it possible for an attacker to compromise the integrity of the target computer by simply sending an e-mail message. Unlike the typical e-mail virus, users could not protect themselves by not opening **stuck/attached** files; in fact, the user did not even have to open the message to enable the attack. The programs' message header mechanisms had a **shortcoming/defect** that made it possible for senders to overflow the area with extraneous data, which allowed them to execute whatever type of code they desired on the recipient's computers. Because the process was activated as soon as the recipient downloaded the message from the server, this type of buffer overflow attack was very difficult to **protect/defend**. Microsoft has since created a patch to **get rid of/eliminate** the vulnerability.

2. Give as many synonyms as possible.

Blended threat

A blended threat is a computer network **attack** that seeks to maximize the severity of **damage** and speed of contagion by combining methods, for example using characteristics of both viruses and worms, while also taking advantage of **vulnerabilities** in computers, networks, or other physical systems. An attack using a blended approach might send a virus via an e-mail attachment, along with a Trojan horse **embedded** in an HTML file that will cause damage to the recipient computer. The Nimda, CodeRed, and Bugbear exploits were all examples of blended threats.

A blended threat typically includes:

More than one means of **propagation** -- for example, distributing a hybrid virus/worm via e-mail that will self-replicate and also **infect** a Web server, so that contagion will spread through all visitors to a particular site;

Exploitation of vulnerabilities, which may be preexisting or even caused by malware distributed as part of the attack;

The **intent** to cause real harm (rather than just causing minor computer problems for victims), for example, by launching a denial of service (DOS) attack against a target, or **delivering** a Trojan horse that will be **activated** at some later date;

Automation that enables increasing contagion without requiring user actions, such as opening attachments.

To guard against blended threats, experts **urge** network administrators to be **vigilant** about patch management, use and **maintain** good firewall products, employ server software to detect malware, and educate users about proper e-mail **handling** and online behavior.

3. Complete the sentences

Blue bomb

A "blue bomb" (also known as "WinNuke") is a technique 1)… . The "blue bomb" is actually 2)… . This condition causes the operating system to "crash" or terminate prematurely. The operating system can usually be restarted 3)… .

The blue bomb derives its name from the effect it sometimes causes on the display as the operating system is terminating – 4)… . Blue bombs are sometimes sent by multi-player game participants who are about to lose or users of Internet Relay Chat (IRC) 5)… . This is known as "nuking" someone. A commonly-used program for causing the blue bomb is WinNuke. Many Internet service providers are filtering out the packets so they don't reach users.

a) an out-of-band network packet containing information that the operating system can't process

b) a white-on-blue error screen that is commonly known as blue screen of death

c) without any permanent damage other than possible loss of unsaved data when you crashed

d) who are making a final comment

e) for causing the Windows operating system of someone you're communicating with to crash or suddenly terminate

4. Insert the words in the gaps

Bluesnarfing

a) *bluesnarfing*
b) *short-range*
c) *personal digital*
d) *high-speed*
e) *turn off*
f) *e-mail*
g) *laptop*
h) *wireless*
i) *vulnerable*
j) *legitimate*
k) *security*
l) *synchronize*

Bluesnarfing is the theft of information from a 1)… device through a Bluetooth connection. Bluetooth is a 2)… but very 3)… wireless technology for exchanging data between desktop and mobile computers, 4)… assistants (PDAs), and other devices. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information -- such as the user's calendar, contact list and 5)… and text messages -- without leaving any evidence of the attack. Other devices that use Bluetooth, such as 6)… computers, may also be 7)…, although to a lesser extent, by virtue of their more complex systems. Operating in invisible mode protects some devices, but others are vulnerable as long as Bluetooth is enabled.

According to a ZDNet UK article, attackers are exploiting a problem with some implementations of the object exchange (OBEX) protocol, which is commonly used to exchange information between wireless devices. An attacker can 8)… with the victim's device (this is known as pairing) and gain access to any information or service available to the 9)… user. The article claims that 10)… tools are widely available on the Internet, along with information about how to use them.

Adam Laurie, of A.L. Digital, discovered the vulnerability that enables bluesnarfing in November 2003, when he was testing the 11)… of Bluetooth devices. Laurie released a vulnerability disclosure notification about the problem immediately afterward. According to Laurie's bluesnarf-tracking blog, the only way to protect yourself from a bluesnarf attack is to 12)… Bluetooth on your mobile device.

5. Fit the missing sentences into the gaps (one sentence is odd).

Cache poisoning

Cache poisoning, also called domain name system (DNS) poisoning or DNS cache poisoning, is the corruption of an Internet server's domain name system table by replacing an Internet address with that of another, rogue address. 1)…… . At that point, a worm, spyware, Web browser hijacking program, or other malware can be downloaded to the user's computer from the rogue location.

Cache poisoning can be transmitted in a variety of ways, increasing the rate at which rogue programs are spread. 2)… … … . Images and banner ads within e-mail messages can also be vehicles by which users are directed to servers that have been compromised by cache poisoning. Once an end user's computer has been infected with the nefarious code, all future requests by that user's computer for the compromised URL will be redirected to the bad IP address -- even if the "victim" server resolves the problem at its site. 3)… … … .

Cache poisoning differs from another form of DNS poisoning, in which the attacker spoofs valid e-mail accounts and floods the inboxes of administrative and technical contacts. Cache poisoning is related to URL poisoning. 4)… … … .

a) One tactic is the placement of compromised URLs within spam e-mail messages having subject lines that tempt users to open the message (for example, "Serious error in your tax return").
b) In URL poisoning, also known as location poisoning, Internet user behavior is tracked by adding an identification (ID) number to the location line of the browser that can be recorded as the user visits successive pages on the site.
c) Cache poisoning is particularly dangerous when the targets are well-known and trusted sites, such as those to which browsers are pointed when automatic virus-definition updates are performed.
d) When a Web user seeks the page with that address, the request is redirected by the rogue entry in the table to a different address.
e) Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations.

6. Put the prepositions in the right places.

Caller ID spoofing

a) by
b) with
c) of
d) on
e) from
f) between
g) in
h) up
i) as
j) for

Caller ID spoofing is a service that allows a caller to masquerade 1) … someone else 2) … falsifying the number that appears 3) … the recipient's caller ID display. Just as e-mail spoofing can make it appear that a message came 4) … any e-mail address the sender chooses, caller ID spoofing can make a call appear to come from any phone number the caller wishes.

Several service providers offer caller ID spoofing, including Camophone, Spooftel, and PI Phone. To use Camophone's service, a customer pays 5) … advance for a certain number of calling minutes. To set 6) … a call, the customer opens a Web form and enters their phone number, the recipient's phone number, and the number chosen to appear on the recipient's caller display. Camophone then patches the

call through 7) … the caller and recipient phones as stipulated. Some other versions involve the caller dialing a number to access the service and then dialing the phone numbers.

Caller ID spoofing has been available for years to people 8) … a specialized digital connection to the telephone company. Collection agencies, law enforcement officials, and private investigators have used the practice, with varying degrees 9) … legality. However, the advent of VoIP (voice over Internet Protocol) service makes it simple 10) … the average person to falsify a calling number, and as Internet telephony has become more common, so has caller ID spoofing.

Frequently, caller ID spoofing is used for prank calls. For example, someone might call a friend and arrange for "The White House" to appear on the recipient's caller display. However, according to Lance James, chief technology officer (CTO) of Secure Science Corp., criminal uses of caller ID spoofing, such as identity theft, have also increased significantly.

7. Change the form of each word so that it fits the numbered space

E-mail spoofing

a) *Origin*
b) *Distribute*
c) *Solicit*
d) *Legitimate*
e) *Retaliate*
f) *Authentic*
g) *Spoof*
h) *Delete*
i) *Sense*
j) *Vary*

E-mail spoofing is the forgery of an e-mail header so that the message appears to have 1) … from someone or somewhere other than the actual source. 2) …-s of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their 3) … -s. Spoofing can be used 4) …. Classic examples of senders who might prefer to disguise the source of the e-mail include a sender reporting mistreatment by a spouse to a welfare agency or a "whistle-blower" who fears 5) … . However, spoofing anyone other than yourself is illegal in some jurisdictions.

E-mail spoofing is possible because Simple Mail Transfer Protocol (SMTP), the main protocol used in sending e-mail, does not include an 6) … mechanism. Although an SMTP service extension (specified in IETF RFC 2554) allows an SMTP client to negotiate a security level with a mail server, this precaution is not often taken. If the precaution is not taken, anyone with the requisite knowledge can connect to the

server and use it to send messages. To send 7) … e-mail, senders insert commands in headers that will alter message information. It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say. Thus, someone could send spoofed e-mail that appears to be from you with a message that you didn't write.

Although most spoofed e-mail falls into the "nuisance" category and requires little action other than 8) …, the more malicious varieties can cause serious problems and security risks. For example, spoofed e-mail may purport to be from someone in a position of authority, asking for 9) … data, such as passwords, credit card numbers, or other personal information -- any of which can be used for a 10) … of criminal purposes. The Bank of America, eBay, and Wells Fargo are among the companies recently spoofed in mass spam mailings. One type of e-mail spoofing, self-sending spam, involves messages that appear to be both to and from the recipient.

8. Fill in the gaps.

Identity theft

a) identity theft
b) Social Security
c) shoulder surfing
d) criminal record
e) false credentials
f) blank checks
g) account takeover
h) dumpster diving
i) credit applications
j) personal interaction

Identity theft is a crime in which an imposter obtains key pieces of personal information, such as 1) … or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with 2) … . In addition to running up debt, an imposter might provide false identification to police, creating a 3) … or leaving outstanding arrest warrants for the person whose identity has been stolen.

Identity theft is categorized in two ways: true name and account takeover. True name 4) … means that the thief uses personal information to open new accounts. The thief might open a new credit card account, establish cellular phone service, or open a new checking account in order to obtain 5) … . 6) … identity theft means the imposter uses personal information to gain access to the person's existing accounts. Typically, the thief will change the mailing address on an account and run up a huge bill before the person whose identity has been stolen realizes there is a problem. The Internet has made it easier for an identity thief to use the information they've stolen because transactions can be made without any 7) …

Although an identity thief might crack into a database to obtain personal information, experts say it's more likely the thief would obtain information by using old-fashioned methods. Retrieving personal

paperwork and discarded mail from trash dumpsters (8) …) is one of the easiest ways for an identity thief to get information. Another popular method to get information is 9) … - the identity thief simply stands next to someone at a public office, such the Bureau of Motor Vehicles, and watches as the person fills out personal information on a form.

To prevent identity theft, experts recommend that you regularly check your credit report with major credit bureaus, follow up with creditors if your bills do not arrive on time, destroy unsolicited 10) …, and protect yourself by not giving out any personal information in response to unsolicited e-mail.

9. Put the sentences in the right order to complete the text.

Dumpster diving

1. Dumpster diving is looking for treasure in someone else's trash.
2. …
3.
4.
5.
6.

a) Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes.

b) To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash.

c) (A dumpster is a large trash container.)

d) Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network.

e) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network.

10. Insert articles where necessary.

Shoulder surfing

1)… Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get 2)…information. Shoulder surfing is 3)… effective way to get information in 4)…crowded places because it's relatively easy to stand next to someone and watch as they fill out 5)… form, enter 6)… PIN number at an ATM machine, or use 7)… calling card at 8)… public pay phone. Shoulder surfing can also be done long distance with 9)… aid of binoculars or 10)…other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand.

11. Do the exercises

Cookie poisoning

Insert prepositions

1)… the Web, cookie poisoning is the modification 2)… a cookie (personal information 3)… a Web user's computer) 4)… an attacker to gain unauthorized information about the user 5)… purposes such as identity theft. The attacker may use the information to open new accounts or to gain access to the user's existing accounts.

Insert the terms

a) unauthorized
b) authenticate
c) cookies
d) transactions
e) hard drive
f) Web site
g) security measures
h) accessed
i) attacker
j) examine

1)… stored on your computer's 2)… maintain bits of information that allow Web sites you visit to 3)… your identity, speed up your 4)…, monitor your behavior, and personalize their presentations for you. However, cookies can also be 5)… by persons 6)… to do so. Unless 7)… are in place, an 8)… can 9)… a cookie to determine its purpose and edit it so that it helps them get user information from the 10)… that sent the cookie.

Insert the words

a) protect
b) refused
c) sent
d) validate
e) pass through
f) encrypted
g) guard
h) digital
i) means
j) tampered

To 1)… against cookie poisoning, Web sites that use them should 2)… cookies (through encryption, for example) before they are 3)… to a user's computer. Ingrian Networks' Active Application Security platform is one 4)… of securing cookies. When cookies 5)… the platform, sensitive information is 6)…. A 7)… signature is created that is used to 8)… the content in all future communications between the sender and the recipient. If the content is 9)… with, the signature will no longer match the content and will be 10)… access by the server.

12. Read the following texts about an evil twin, a directory harvest attack, and a dictionary attack. See the missing words taken out of these texts in the table and guess which attack is described in each of these texts. Choose correct titles.

A directory harvest attack (DHA)	**An evil twin**	**A dictionary attack**
directory harvest attack (DHA) harvesting	an evil twin "good twin" Evil twins evil twin	dictionary attack(s) dictionary

Text 1.

A … is a method of breaking into a password-protected computer or server by systematically entering every word in a … as a password. A … can also be used in an attempt to find the key necessary to decrypt an encrypted message or document.

… work because many computer users and businesses insist on using ordinary words as passwords. … are rarely successful against systems that employ multiple-word phrases, and unsuccessful against systems that employ random combinations of uppercase and lowercase letters mixed up with numerals. In those systems, the brute-force method of attack (in which every possible combination of characters and spaces is tried up to a certain maximum length) can sometimes be effective, although this approach can take a long time to produce results.

Vulnerability to password or decryption-key assaults can be reduced to near zero by limiting the number of attempts allowed within a given period of time, and by wisely choosing the password or key. For example, if only three attempts are allowed and then a period of 15 minutes must elapse before the next three attempts are allowed, and if the password or key is a long, meaningless jumble of letters and numerals, a system can be rendered immune to … and practically immune to brute-force attacks.

A form of … is often used by spammers. A message is sent to every e-mail address consisting of a word in the …, followed by the at symbol (@), followed by the name of a particular domain. Lists of given names (such as frank, george, judith, or donna) can produce amazing results. So can individual letters of the alphabet followed by surnames (such as csmith, jwilson, or pthomas). E-mail users can minimize their vulnerability to this type of spam by choosing usernames according to the same rules that apply to passwords and decryption keys -- long, meaningless sequences of letters interspersed with numerals.

Text 2.

A … is an attempt to determine the valid e-mail addresses associated with an e-mail server so that they can be added to a spam database.

A … can use either of two methods for … valid e-mail addresses. The first method uses a brute force approach to send a message to all possible alphanumeric combinations that could be used for the

username part of an e-mail at the server, up to and including those of length n characters (where n is some preset positive integer such as 15). The second and more selective method involves sending a message to the most likely usernames - for example, for all possible combinations of first initials followed by common surnames. In either case, the e-mail server generally returns a "Not found" reply message for all messages sent to a nonexistent address, but does not return a message for those sent to valid addresses. The … program creates a database of all the e-mail addresses at the server that were not returned during the attack.

The … approach explains how a new e-mail address can start receiving spam within days or hours after its creation. Various solutions have been developed toward repelling these attacks. Some of the most effective involve slowing down the rate at which the attack can take place, rather than attempting to filter out the entire attack. This can be done by limiting the number of e-mail messages per minute or per hour at which a server can receive messages, legitimate or otherwise. So-called spam filters, programmed to identify character and word combinations typical of spam, can also be effective, although they occasionally reject legitimate messages.

Text 3.

In security, … is a home-made wireless access point (hot spot) that masquerades as a legitimate one to gather personal or corporate information without the end-user's knowledge. It's fairly easy for an attacker to create … by simply using a laptop, a wireless card and some readily-available software. The attacker positions himself in the vicinity of a legitimate Wi-Fi access point and lets his computer discover what name and radio frequency the legitimate access point uses. He then sends out his own radio signal, using the same name.

To the end-user, the … looks like a hot spot with a very strong signal; that's because the attacker has not only used the same network name and settings as the … he is impersonating, he has also physically positioned himself near the end-user so that his signal is likely to be the strongest within range. If the end-user is tempted by the strong signal and connects manually to the … to access the Internet, or if the end-user's computer automatically chooses that connection because it is running in promiscuous mode, the … becomes the end-user's Internet access point, giving the attacker the ability to intercept sensitive data such as passwords or credit card information.

… are not a new phenomenon in wireless transmission. Historically they have been called base station clones or honeypots. What's different now is that more businesses and consumers are using wireless devices in public places and it's easier than ever for someone who doesn't have any technical expertise to create … . To protect yourself from … network connections, experts recommend that you only use public hot spots for Web browsing and refrain from shopping or banking. To protect corporate data, experts recommend that when wireless, you only connect to the Internet through a VPN and always use WEP or WPA encryption.

Ex. 8. Reporting.

You should elaborate the message to clearly deliver it to the class emphasizing the definitions and important details so that everybody could understand and take notes if necessary.

The preparation is likely to take up to 3-5 minutes of **class** time.
You should only talk for about 3 minutes.

Prepare short reports with a clear structure: introduction, main body and conclusion.

Use appropriate linking words.
You may add some details to the description you hear during or after the activity.

Make a short presentation of the topics:

1. *gray net*
2. *hijacking*
3. *browser hijacker*
4. *IP spoofing*

1. Greynet

Greynet is a term for the use of unauthorized applications on a corporate network. A greynet application is a network-based program that corporate network users download and install without permission from their company's IT department. Common examples of greynet applications include instant messaging, peer-to-peer collaboration and conferencing programs, streaming media players, and RSS readers.

Many greynet applications, such as instant messaging and collaboration programs, have legitimate business use and help boost user productivity. Other greynet applications, like peer-to-peer file and music sharing programs, pose serious security risks and can drain network resources. User-downloaded programs also can include malicious programs like spyware components for tracking and reporting information without the user's knowledge. Greynet usage by employees is thought to be a major contributor to the growth of spyware-related incidents.

All greynets, even those that benefit the end-user, can be detrimental to a company network. Because they use corporate bandwidth, the programs often have negative effects on overall network performance. They introduce security risks, including client code vulnerabilities and new avenues for attack, and can lead to data loss and property or identity theft. Greynets can be difficult to eliminate because many use encryption and port agility (the ability to dynamically send and receive traffic across any open network port), which makes them difficult to detect and block.

2. Hijacking

Hijacking is a type of network security attack in which the attacker takes control of a communication - just as an airplane hijacker takes control of a flight - between two entities and masquerades as one of them. In one type of hijacking (also known as a man in the middle attack), the perpetrator takes control of an established connection while it is in progress. The attacker intercepts messages in a public key exchange and then retransmits them, substituting their own public key for the requested one, so that the two original parties still appear to be communicating with each other directly. The attacker uses a program that appears to be the server to the client and appears to be the client to the server. This attack may be used simply to gain access to the messages, or to enable the attacker to modify them before retransmitting them.

Another form of hijacking is browser hijacking, in which a user is taken to a different site than the one the user requested. There are two different types of domain name system (DNS) hijacking. In one, the attacker gains access to DNS records on a server and modifies them so that requests for the genuine Web page will be redirected elsewhere - usually to a fake page that the attacker has created. This gives the impression to the viewer that the Web site has been compromised, when in fact, only a server has been. In February 2000, an attacker hijacked RSA Security's Web site by gaining access to a DNS server that was not controlled by RSA. By modifying DNS records, the attacker diverted requests to a spoof Web site. It appeared to users that an attacker had gained access to the actual RSA Web site data and changed it - a serious problem for a security enterprise. This type of hijacking is difficult to prevent, because administrators control only their own DNS records, and have no control over upstream DNS servers. In the second type of DNS hijack, the attacker spoofs valid e-mail accounts and floods the inboxes of the technical and administrative contacts. This type of attack can be prevented by using authentication for InterNIC records.

In another type of Web site hijack, the perpetrator simply registers a domain name similar enough to a legitimate one that users are likely to type it, either by mistaking the actual name or through a typo. This type of hijack is currently being employed to send many unwary users to a pornographic site instead of the site they requested.

3. Browser hijacker

A browser hijacker (sometimes called hijackware) is a type of malware program that alters your computer's browser settings so that you are redirected to Web sites that you had no intention of visiting. Most browser hijackers alter default home pages and search pages to those of their customers, who pay for that service because of the traffic it generates. More virulent versions often: add bookmarks for pornographic Web sites to the users' own bookmark collection; generate pornographic pop-up windows faster than the user can click them shut; and redirect users to pornographic sites when they inadvertently mistype a URL or enter a URL without the www. preface. Poorly coded browser hijackers -- which, unsurprisingly, are common -- may also slow your computer down and cause browser crashes.

Browser hijackers and the pornographic material they often leave in their wake can also be responsible for a variety of non-technical problems. Employees have lost jobs because of content and links found on their computers at work; people have been charged with possession of illegal material; and personal relationships have been severed or strained. In one case in the United States, a Russian immigrant was convicted for possession of child pornography, although he claims to have been the victim of a browser hijacker.

Like adware and spyware, a browser hijacker may be installed as part of freeware installation. In this case, the browser hijacker is probably mentioned in the user agreement -- although, obviously, not identified as a browser hijacker. The problem is that users typically either ignore the fine print or only give it a cursory reading. A browser hijacker may also be installed without user permission, as the result of an infected e-mail, a file share, or a drive-by download. To avoid contamination, experts advise users to read user agreements carefully, and to be cautious about freeware downloads and e-mail messages from unknown sources.

4. IP spoofing

IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain access to a network. Here's how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.

When IP spoofing is used to hijack a browser, a visitor who types in the URL (Uniform Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL www.loc.gov would see spoofed content created by the hijacker.

If a user interacts with dynamic content on a spoofed page, the highjacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware . The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam.

Web site administrators can minimize the danger that their IP addresses will be spoofed by implementing hierarchical or one-time passwords and data encryption/decryption techniques. Users and administrators can protect themselves and their networks by installating and implementating firewalls that block outgoing packets with source addresses that differ from the IP address of the user's computer or internal network.

Ex. 9. Listening

Listen to the description of a botnet and complete the following summary.

Botnet

A botnet (also known as a 1……) is a number of Internet computers that, although their owners are 2…… of it, have been 3…… (including spam or viruses) to other computers on the Internet. Any such computer is referred to as 4…… - in effect, a computer "robot" or 5…… that serves the wishes of some master 6…… originator. According to a report from 7……, botnets -- not spam, viruses, or worms -- currently pose the biggest 8…… to the Internet. A report from 9…… came to a similar conclusion.

Computers that are coopted to serve in this unaware army of the "walking dead" are often those whose owners fail to provide effective 10…… . A zombie or bot is often created through an Internet port that has been left open and through which a little 11…….can be left for future activation. At a certain time, the 12…… can unleash the effects of the army by sending a single command, possibly from an Internet Relay Channel (IRC) site.

The computers that form a botnet can be programmed to 13…… to a specific computer, such as a Web site that can be closed down by having to handle too much traffic – 14… … - or, in the case of spam distribution, to many computers. The motivation for a zombie master who creates a 14…… may be to cripple a competitor. The motivation for a zombie master sending spam is in the money to be made. Both of them rely on 15…… computers that can be turned into zombies.

RENDERING

Symantec хочет подорвать подпольный бизнес «кражи личности»

Специалисты компании разработали систему, которая обыскивает подпольные веб-сайты и чат-румы в поисках информации, выставленной на продажу.

Как рассказал директор Symantec Security Response по новым технологиям Оливер Фридрихс, система, называемая Dark Vision, разработана в середине 2006 года и позволяет Symantec «наблюдать за подпольной экономикой». Symantec еще не решила, будет ли она включать Dark Vision в свои семейства продуктов. «Пока это лишь прототип на ранней стадии, — пояснил Фридрихс. – Но мы видим несколько возможностей, включая возможность предупреждения потребителей, чья информация выставлена на продажу».

«Похитители личности» встречаются с подпольными покупателями информации на многочисленных веб-сайтах «кардеров», а затем договариваются о купле-продаже в чат-румах или каналах IRC. По словам Фридрихса, номер кредитной карты можно купить всего за $6, но спросом пользуется и другая информация, такая как номера социального страхования, адреса и телефоны. «Всю информацию, удостоверяющую чью-то личность, можно купить в среднем за $14-$18, — утверждает он. — На самом деле они продают ее оптом».

Dark Vision выводит графическое представление данных, «нарытых» на этих веб-сайтах и в IRC, с точным указанием расположения сервера кардера и сути переговоров. Так как большую часть информации о кредитных картах кардеры предлагают тайно — и за деньги, — Dark Vision обнаруживает лишь небольшую часть украденных данных, как правило, регистрируя только примеры данных, выложенных в форумах, для проверки легитимности продавца.

За первые три месяца тестирования Dark Vision обнаружила около 800 краденных номеров кредитных карт. Тем не менее, этот инструмент, по мнению Фридрихса, может оказаться полезным для эмитентов кредитных карт или компаний, которые ищут ранние признаки утечки информации, и, возможно, будет использоваться глобальной службой безопасности Symantec.

Symantec — не первая компания, попытавшаяся использовать подобную информацию в коммерческих целях. Небольшая фирма из Малибу (штат Калифорния) CardCops уже идет в этом направлении, вылавливая в интернете компрометирующие данные и сообщая о них предпринимателям, властям и потребителям.

Согласно прошлогодним оценкам Министерства юстиции США, от «кражи личности» страдают миллионы потребителей в год, а сумма ущерба составляет примерно $6,4 млрд.

Итальянская полиция ликвидировала банду фишеров

В ходе операции Phish & Chip итальянская полиция арестовала 26 членов предполагаемой международной преступной организации.

Guardia di Finanza задержала 18 граждан Италии и восемь выходцев из Восточной Европы, которые грабили клиентов государственной почтовой службы Poste Italiane, пользующихся онлайновыми банковскими услугами.

«Нужно приветствовать успехи итальянских властей, пресекающих преступные действия подобного рода, — говорится в заявлении старшего консультанта Sophos Грэма Клули. — Интернет-преступники могут скрываться при помощи технологии, и полиции часто приходится распутывать сложную паутину. Фишинг «и кража личности» — это глобальные проблемы, и государства должны теснее сотрудничать друг с другом, чтобы привлекать киберпреступников к суду. Эти аресты подчеркивают все более организованную природу международных банд охотников за персональными данными, и очень много фишеров еще продолжают безнаказанно орудовать».

Согласно полицейскому бюллетеню, группой руководил 22-летний хакер, который признался, что они рассылали сообщения e-mail от имени Poste Italiane. Эти сообщения направляли жертвы на зарубежные серверы, копировавшие веб-сайты реальных банков, после чего их счета опустошались хакерами при помощи перехваченных логинов. Деньги переводились на карты Postepay, которые члены банды нелегально активизировали.

Полиция сообщает, что руководитель группы был консультантом по обработке данных и помогал итальянским компаниям предотвращать мошенничество с кредитными картами.

Уязвимость Gmail позволяет красть сообщения

Учетные записи Google Gmail легко взломать с тем, чтобы переадресовывать любые старые – и новые – сообщения на собственный адрес злоумышленника, утверждает известный охотник за багами.

Уязвимость Gmail, относящаяся к категории «межсайтовой подмены запроса» (cross-site request forgery - CSRF), обнаружил британский охотник за багами Петко Петков (Petko Petkov), который уже прославился громкими находками. За последние две недели Петков обнародовал информацию о серьезных пробелах в защите Apple QuickTime, Microsoft Windows Media Player и Adobe Portable Document Format (PDF).

Не раскрывая деталей, Петков утверждает, что злоумышленники могут использовать в своих целях функцию фильтра Gmail. Жертва, зарегистрировавшись в Gmail, должна посетить вредоносный веб-сайт, который, применяет по отношению к одному из интерфейсов прикладных программ Gmail специальную HTML-команду (Петков называет ее multipart/form-date POST), после чего вводит в список фильтров пользователя вредоносный фильтр.

Петков поместил на сайт Gnucitizen.org серию скриншотов, иллюстрирующих одну возможную атаку. «В этом примере злоумышленник создает фильтр, который просто находит сообщения с вложениями и пересылает их по указанному им адресу, — поясняет Петков. — Имейте в виду, что даже если Google устранит первоначальную уязвимость, фильтр будет пересылать сообщения до тех пор, пока остается в списке».

В комментарии к постингу Петкова в качестве способа профилактики предлагается расширение для Firefox, способное заблокировать эксплойты бага Gmail. Джорджио Маоне, автор популярного расширения NoScript, утверждает, что оно блокирует атаки CSRF. (NoScript блокирует любые сценарии JavaScript, Java и другой исполняемый контент с тех сайтов, которым пользователь не доверяет.)

Как и в случае с багом в формате файлов Adobe PDF, который Петков обнародовал на прошлой неделе, он защищает свое решение опубликовать информацию об уязвимости Gmail без предварительного уведомления Google. Правда, его объяснение кажется несколько туманным: «Допустим, это один из моих социальных экспериментов», — пишет Петков.

Главный технолог WhiteHat Security Inc. Джереми Гроссман называет баг Gmail «особенно пугающим». В своем блоге он объясняет: «Учетные записи веб-почты гораздо ценнее банковских счетов, так как открывают доступ ко многим другим онлайновым учетным записям (блоги, банковские услуги, шопинг и т.п.). Эксплуатировать такие уязвимости легко, безопасно и очень мудро».

Петков добавляет к этому собственные два цента: «В век, когда все данные находятся в одном облаке, злоумышленникам нет смысла взламывать ваш компьютер. Гораздо проще установить один из таких шпионящих фильтров-лазеек. Game over! Они не контролируют вашу машину, зато они контролируют вас, а это гораздо выгоднее».

27 сентября, 2007

В документах PDF обнаружена серьезная уязвимость

Британский охотник за багами, недавно обнаруживший две критические ошибки в популярных форматах медиафайлов, утверждает, что уязвимость в вездесущем формате файлов Adobe PDF можно использовать для получения контроля над системами Windows XP.

В четверг специалист по безопасности Петко Петков, неделю назад сообщивший о неисправленной ошибке в Apple QuickTime, а во вторник — об аналогичном критическом баге в Microsoft Windows Media Player, заявил, что Adobe Acrobat Reader тоже содержит серьезную уязвимость.

Петков утверждает, что уязвимость PDF не идет ни в какое сравнение с багами в медиафайлах. «Документы Adobe Acrobat/Reader PDF можно использовать для взлома Windows-систем, — утверждает он в своем блоге за пятницу. — Полного взлома!!! Незаметно и без спроса!!! Все, что для этого нужно, — открыть документ PDF или посетить содержащую его веб-страницу».

В случаях с QuickTime и Windows Media Player Петков привел примеры кода эксплойтов. На сей раз он решил этого не делать. «Проблема слишком серьезна, учитывая тот факт, что документы PDF составляют основу современного бизнеса, — пишет Петков. — К тому же Adobe может понадобиться время для исправления своего фирменного продукта, поэтому я не могу публиковать никакие POCs [proof-of-concepts]. Можете поверить мне на слово. POCs будут, как только появится обновление».

Несмотря на отсутствие доказательств, Symantec готова поверить Петкову. «Хотя в данный момент эти заявления подтвердить нельзя, этот исследователь уже выявил несколько уязвимостей, и ему, по всей видимости, можно доверять», — пишет компания в предупреждении для клиентов своей службы оповещения об угрозах DeepSight.

«Мой совет вам – не открывать никакие файлы PDF (ни локально, ни дистанционно)», — говорит Петков. По его словам, он проверил на тестах и убедился, что уязвимость присутствует в последней версии Acrobat Reader 8.1, и ее можно эксплуатировать на ПК с Windows XP SP2.

Это не первый баг, обнаруженный в популярном формате файлов Adobe PDF или программах для создания и отображения таких файлов. Например, в январе Adobe обновила Reader и Acrobat на версию 8.0, чтобы исключить уязвимость типа cross-site scripting. *24 сентября, 2007*

«Глупые» ошибки в Oracle 11g

Последняя версия флагманской базы данных Oracle защищена лучше предыдущих, однако ошибки программистов оставили в ней уязвимости, которые злоумышленники могут использовать для кражи данных.

«В 11g Oracle достигла большого прогресса, но я обнаружил некоторые уязвимости, которые являются следствием глупых ошибок программирования, — сказал Александр Корнбрюст, управляющий директор Red Database Security GmbH, в интервью на конференции Hack In The Box (HITB) Security Conference 2007, в Куала-Лумпур (Малайзия). — Oracle следует провести ликбез среди своих программистов, чтобы они не оставляли таких простых уязвимостей».

Корнбрюст помогает крупным компаниям проверять безопасность своих баз данных Oracle. Исследовав ПО, он обнаружил уязвимости типа SQL injection, которые позволяют злоумышленникам исполнять вредоносный код. Он нашел также способ обойти средства контроля в 11g и других версиях СУБД, что может свести на нет усилия компании по гарантированному соблюдению нормативных требований.

На HITB, которая продлится до 6 сентября, Корнбрюст расскажет о некоторых уязвимостях Oracle, но не раскроет своего метода обхода средств контроля до тех пор, пока Oracle не решит эту проблему. Некоторые уязвимости, которые обнаружил Корнбрюст, отражают архитектурные

проблемы СУБД Oracle. На конференции он планирует продемонстрировать, как такие проблемы позволяют злоумышленникам обходить новейшие средства защиты Oracle, включая Oracle Database Vault и Oracle Audit Vault.

Ввиду критической роли, которую СУБД Oracle играют в бизнесе крупных компаний, а также широкого спектра платформ, поддерживаемых этим ПО, расходы и время, необходимые для устранения уязвимостей, могут достигать колоссальных размеров. Корнбрюст привел в пример немецкую компанию, в которой 8000 баз данных Oracle. Для установки одного исправления ей может потребоваться 32 тыс. часов работы, по четыре часа на базу данных. Это выливается в 60 штатных администраторов — без учета трудозатрат на тестирование исправлений на каждой БД.

Для каждой устраняемой уязвимости Oracle приходится разрабатывать заплатку на каждую поддерживаемую версию своей базы данных для каждой аппаратной платформы и операционной системы. В результате для устранения одной уязвимости выпускается около ста отдельных патчей.

Виртуализация — не гарантия безопасности

Одним из преимуществ виртуализации считалась безопасность, однако согласно недавнему исследованию, это уже не так.

Новое вредоносное ПО способно определять, что оно работает внутри виртуальной машины, и в зависимости от этого менять свое поведение. «Скрыть существование ВМ принципиально невозможно», утверждают авторы отчета в ответ на высказываемые некоторыми разработчиками технологии виртуализации и средств безопасности надежды на создание необнаруживаемых ВМ.

Документ, называемый «Совместимость и прозрачность не одно и то же: мифы и реальность обнаружения механизмов управления виртуальными машинами», опубликован поставщикам ПО виртуализации VMware и XenSource совместно с учеными из Стэнфордского и Карнеги-Меллонского университетов. В нем обсуждается возможность использования виртуальных машин (ВМ) в качестве способа перехвата атак руткитов — так называемого хонипотинга — а также для обнаружения червей. Надежды на это опирались на неспособность обычного вредоносного ПО распознать, что оно атакует не реальную, физическую машину.

Авторы отмечают, что «по аналогичным причинам поставщики антивирусов стараются оправдать использование ими ВМ для идентификации новых эксплойтов. Другие предлагают использование виртуализации для агрессии в форме руткитов на базе ВМ в надежде на то, что прозрачность механизмов управления ВМ (VMM) скроет их присутствие и создаст идеальную платформу для атак… Мы считаем, что требуемая для этих целей прозрачность недостижима ни сегодня, ни в будущем».

Согласно отчету, проблема заключается в том, что эти разрабатываемые средства защиты отталкиваются от предположения, будто если все технические характеристики совпадают с реальной машиной, то ПО не может обнаружить, что находится в виртуальной среде. Однако существуют важные признаки, которые выдают присутствие ВМ. «Виртуальная реализация этой архитектуры существенно отличается от физических реализаций… Логические различия состоят в семантических особенностях интерфейсов реальной и виртуальной аппаратуры. Большинство современных методов обнаружения VMM используют особенности интерфейса виртуального ЦП VMM, такого как VMware Player или Microsoft VirtualPC, который нарушает архитектуру x86».

Для подавляющего большинства программ эти и другие различия не имеют значения, поэтому VMM не пытаются скрыть их. Но программы могут обнаруживать различия в ЦП, запоминающих устройствах и драйверах устройств, главным образом потому, что разработчики VMM больше сосредоточены на совместимости и производительности, чем на возможности обнаружения или безопасности в целом.

В результате, заключают авторы, «простота создания новых методов обнаружения предполагает, что обеспечить полную прозрачность VMM практически невозможно».

1 августа, 2007

Symantec хочет подорвать подпольный бизнес «кражи личности»

Специалисты компании разработали систему, которая обыскивает подпольные веб-сайты и чат-румы в поисках информации, выставленной на продажу.

Как рассказал директор Symantec Security Response по новым технологиям Оливер Фридрихс, система, называемая Dark Vision, разработана в середине 2006 года и позволяет Symantec «наблюдать за подпольной экономикой». Symantec еще не решила, будет ли она включать Dark Vision в свои семейства продуктов. «Пока это лишь прототип на ранней стадии, — пояснил Фридрихс. – Но мы видим несколько возможностей, включая возможность предупреждения потребителей, чья информация выставлена на продажу».

«Похитители личности» встречаются с подпольными покупателями информации на многочисленных веб-сайтах «кардеров», а затем договариваются о купле-продаже в чат-румах или каналах IRC. По словам Фридрихса, номер кредитной карты можно купить всего за $6, но спросом пользуется и другая информация, такая как номера социального страхования, адреса и телефоны. «Всю информацию, удостоверяющую чью-то личность, можно купить в среднем за $14-$18, — утверждает он. — На самом деле они продают ее оптом».

Dark Vision выводит графическое представление данных, «нарытых» на этих веб-сайтах и в IRC, с точным указанием расположения сервера кардера и сути переговоров. Так как большую часть информации о кредитных картах кардеры предлагают тайно — и за деньги, — Dark Vision обнаруживает лишь небольшую часть украденных данных, как правило, регистрируя только примеры данных, выложенных в форумах, для проверки легитимности продавца.

За первые три месяца тестирования Dark Vision обнаружила около 800 краденных номеров кредитных карт. Тем не менее, этот инструмент, по мнению Фридрихса, может оказаться полезным для эмитентов кредитных карт или компаний, которые ищут ранние признаки утечки информации, и, возможно, будет использоваться глобальной службой безопасности Symantec.

Symantec — не первая компания, попытавшаяся использовать подобную информацию в коммерческих целях. Небольшая фирма из Малибу (штат Калифорния) CardCops уже идет в этом направлении, вылавливая в интернете компрометирующие данные и сообщая о них предпринимателям, властям и потребителям.

Согласно прошлогодним оценкам Министерства юстиции США, от «кражи личности» страдают миллионы потребителей в год, а сумма ущерба составляет примерно $6,4 млрд.
31 июля, 2007

Symantec представила стратегию Consumer Identity

Компания надеется включиться в бизнес аутентификации потребителей в онлайне, объем которого к 2011 году предположительно составит $1,1 млрд.

В среду, на конференции DEMO 07, Symantec продемонстрировала новый клиент для удостоверения личности, основной компонент своей инициативы Security 2.0. Программа, которая находится в стадии разработки, будет называться Norton Identity Client и станет первым шагом по реализации рассчитанного на 1-2 года проекта, который должен связать сервисы с программным обеспечением, а потребителей — с предприятиями. Symantec сравнивает свой клиент с международными водительскими правами — он будет служить удостоверением личности покупателя для продавцов.

Программа содержит и инструменты для покупателей, позволяющие, например, получать сведения о репутации сайта, включая время регистрации домена, или об использовании сайтом известного цифрового сертификата фишеров и генерировать одноразовые адреса e-mail для потенциально «спамящих» веб-сайтов.

Norton Identity Client будет независимым от протокола. Symantec планирует поддерживать и систему хранения цифровых удостоверений личности Microsoft CardSpace, и среду

аутентификации open-source OpenID. Клиент будет поддерживать также одноразовые пароли с использованием специального устройства USB, которые начинают практиковать некоторые банки и брокерские фирмы и которые уже в этом году начнут применяться для дебетных и кредитных карт в США.

Чтобы дать старт своему клиенту аутентификации, Symantec воспользуется системой Norton Account, которая хранит ключи потребительских программных продуктов на серверах компании на тот случай, если эти продукты придется переустанавливать. Symantec утверждает, что в этой системе зарегистрированы свыше половины пользователей ее продуктов семейства Norton.

Однако пока неизвестно, как именно Norton Identity Client будет распространяться среди потребителей. Возможно, что он будет продаваться отдельно, как Norton Confidential, или же будет встроен в другие потребительские пакеты Symantec, такие как Norton Internet Security.

«Мы хотим, чтобы с помощью Norton Identity Client потребители обрели уверенность при онлайновых операциях, а предприятия смогли сосредоточиться не на аутентификации, а на своем основном бизнесе», — рассказал архитектор ПО Symantec Брайан Хернаки.

1 февраля, 2007

UNIT 5. PIRACY. COPYRIGHT.

Warming up

Ex.1. Discussion

What is piracy in the general English?
What is piracy in computing?
What types of piracy in computing do you know?
What derivatives of the word 'piracy' do you know?
What is copyright?

Mainstream

Ex.2. Reading. Learning facts.

piracy

Software piracy is the illegal copying, distribution, or use of software. It is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries. According to the Business Software Alliance (BSA), about 36% of all software in current use is stolen. Software piracy causes significant lost revenue for publishers, which in turn results in higher prices for the consumer.

When you purchase a commercial software package, an end user license agreement (EULA) is included to protect that software program from copyright infringement. Typically, the license states that you can install the original copy of software you bought on one computer and that you can make a backup copy in case the original is lost or damaged. You agree to the licensing agreement when you open the software package (this is called a shrink wrap license), when you open the envelope that contains the software disks, or when you install the software.

Software piracy applies mainly to full-function commercial software. The time-limited or function-restricted versions of commercial software called shareware are less likely to be pirated since they are freely available. Similarly, freeware, a type of software that is copyrighted but freely distributed at no charge, also offers little incentive for piracy.

Types of software piracy include:

Softlifting: Borrowing and installing a copy of a software application from a colleague.

Client-server overuse: Installing more copies of the software than you have licenses for.

Hard-disk loading: Installing and selling unauthorized copies of software on refurbished or new computers.

Counterfeiting: Duplicating and selling copyrighted programs.

Online piracy: Typically involves downloading illegal software from peer-to-peer network, Internet auction or blog. (In the past, the only place to download software was from a bulletin board system and these were limited to local areas because of long distance charges while online.)

Ex.3. Discussion

What is your opinion of software piracy?
Moral aspects of piracy.

Rendering

Сеть прошла мимо

Госдума защитила интеллектуальную собственность повсюду, кроме Интернета
ДМИТРИЙ МИГУНОВ

Фирму, систематически занимающуюся кражей интеллектуальной собственности, с 2008 года могут ликвидировать. Такая норма содержится в четвертой части Гражданского кодекса РФ, принятой Госдумой вчера во втором чтении. До Интернета, в котором с защитой авторских прав положение хуже некуда, у депутатов руки пока не дошли.

Законопроект определяет исчерпывающий перечень видов интеллектуальной деятельности, подлежащих правовой охране: произведения науки, литературы и искусства, ноу-хау и промышленные образцы, программы для ЭВМ, базы данных и топологии интегральных схем, фирменные наименования и средства индивидуализации. Закрепляется исключительное право автора на произведение – в течение всей его жизни и 70 лет после смерти – с возможностью перехода права к другим лицам только на основании договора.

Как рассказал «Новым Известиям» член комитета Госдумы по конституционному, гражданскому и уголовному законодательству Петр Шелищ, одним из ключевых нововведений закона становится повышение ответственности за нарушение исключительных авторских прав. «В случае неоднократного или особо грубого нарушения ответственное за это юридическое лицо может быть ликвидировано по решению суда, – отметил депутат. – При этом оборудование, использованное для кражи собственности, должно быть уничтожено за счет его владельца».

Интересно, что совсем недавно, в сентябре, поправки, направленные на ужесточение санкций против «пиратов», были внесены и в Уголовный кодекс. Их преступления были отнесены к категории «тяжких» и стали караться максимальным сроком лишения свободы на 6 лет. По словам г-на Шелища, граница между административным и уголовным преследованиями по факту нарушения авторских прав пролегает по стоимости произведенного контрафакта – 2 тыс. долларов. Те, кто накопировал, скажем, дисков с ПО на большую сумму, рискует увидеть небо в клетку.

Изменения в Гражданском кодексе коснулись и творческих работников. Хотя, по словам председателя того же комитета Госдумы Павла Крашенинникова, исключительные авторские права переданы от разработчиков к продюсерам, последние будут обязаны выплачивать вознаграждение непосредственным изобретателям или творцам. Сумма будет определяться трудовым контрактом. Впрочем, в законе присутствует и ряд ограничений для обладателей прав. Так, не будет зарегистрирован и защищен товарный знак, вводящий потребителя в заблуждение относительно товара или его производителя или противоречащий общественным интересам, принципам морали и гуманности. Еще одним достаточно любопытным новшеством закона стала возможность авторов потребовать свои права назад, если они выкуплены, но не используются текущим обладателем.

Ожидалось, что поправки коснутся и такой скандальной с точки зрения интеллектуальной собственности сферы, как Интернет. Однако перед вторым чтением из списка объектов, защищенных авторским правом, доменные имена в Сети были исключены. Как рассказал «НИ» г-н Крашенинников, этот вопрос «будет рассмотрен в ближайшее время». Эксперты считают, что на сегодняшний день торопиться с этим не стоит, поскольку опыта практики у государственных органов в этой сфере нет. Но, несмотря на исключение доменной главы, одобренный вариант текста законопроекта все равно содержит понятие «домен». В частности, регистрация товарного знака запрещается, если схожее название уже зарегистрировано в качестве доменного имени.

Доменные имена остались на заборе

Депутаты защитили интеллектуальную собственность

Вчера Госдума приняла во втором чтении проект четвертой части Гражданского кодекса (ГК), которая полностью посвящена защите прав на результаты интеллектуальной деятельности. Напомним, что законопроект был подготовлен президентской администрацией и внесен в Думу в июле 2006 года. Суть: все действующие ныне специальные законы в сфере интеллектуальной собственности, такие как закон «Об авторском праве и смежных правах», «О товарных знаках,

знаках обслуживания и наименованиях мест происхождения товаров» и другие, отменяются и заменяются кодексом.
Споры о том, нужен или нет России "интеллектуальный" кодекс как таковой, не утихают до сих пор. Как и споры о содержании этого документа. Заметим, что число поправок, представленных ко второму чтению законопроекта, перевалило за тысячу.
Больше всего нареканий специалистов вызвала глава проекта четвертой части ГК, определяющая правила защиты доменных имен в сети интернет. В частности, в ней речь шла о признании объектом авторских прав (со всеми вытекающими отсюда последствиями) доменных имен в Рунете.
О том, что доменным именам вообще не место в ГК, заявляли многие эксперты. Специалисты говорили о том, что практики подобного контроля за доменными именами не существует нигде в мире. Законодательное же регулирование Рунета приведет, по мнению экспертов, либо к бесконечным спорам и конфликтам, либо к массовому переходу владельцев доменов в другие зоны обслуживания, чего закон не запрещает.
Депутаты с этими доводами в итоге согласились. По словам председателя думского комитета по гражданскому, уголовному арбитражному и процессуальному законодательству Павла Крашенинникова, ко второму чтению из четвертой части Гражданского кодекса была исключена глава, посвященная законодательному регулированию доменных имен. В итоге других серьезных поправок депутаты в президентский законопроект внести так и не рискнули.
Напомним: принятый вчера документ определяет перечень видов интеллектуальной деятельности, подлежащих правовой охране. К ним, в частности, относятся произведения науки, литературы и искусства, секреты производства, изобретения, промышленные образцы и полезные модели, селекционные достижения, фирменное наименование, программы для ЭВМ, содержание баз данных.
Сохранились в кодексе и репрессивные меры в отношении «пиратов». Так, за грубое нарушение исключительных авторских прав у нарушителя будет конфисковываться оборудование, устройства и материалы. Депутаты лишь уточнили ко второму чтению, что конфискованные "оборудование, устройства и материалы" будут уничтожаться "за счет нарушителя". Кроме того, если "изготовление, распространение, иное использование, а также импорт или хранение материальных носителей приводят к нарушению исключительного права, то такие материальные носители считаются контрафактными и по решению суда подлежат изъятию из оборота и уничтожению".
Впрочем, у некоторых парламентариев президентский законопроект все-таки вызвал сомнения. Первый зампредседателя комитета Госдумы по образованию и науке Олег Смолин заявил, что считает "верхом паразитизма" введение института публикаторов. "Вот представьте, что кто-то из вас пошел в архив и нашел там неизданное произведение Пушкина. Как только вы его издали, вы приобретаете как публикатор все права на доходы от использования этого произведения. Ни Пушкин, ни его наследники, а именно вы как публикатор", - возмущался депутат. По его словам, в России существует масса архивных материалов, которые до сих пор не рассекречены, а значит, тот, кто будет их рассекречивать, и станет "новым интеллектуальным миллиардером".
Принятый во втором чтении законопроект по-прежнему вызывает опасения и у экспертов. По словам председателя совета директоров концерна «Союз» Александра Менна, до сих пор не определено ведомство, которое будет отвечать за подготовку необходимых подзаконных актов. "Существует опасность, что в результате в отношении интеллектуальной собственности мы попадем в информационный вакуум", - пояснил он. В результате, по мнению Александра Менна, старые законы действовать перестанут, а новый так и не начнет.

UNIT 6. SPAM.

Warming up

Ex.1. Discussion.
What is spam?
Do you know the ways spammers collect e-mail addresses?
How many spam letters do you receive every day?
Have you ever responded to a spam letter?

Mainstream

Ex.2. Listening.
What is the origin of the word 'spam'?
What types of unsolicited mail are described in the podcast? How do they differ from each other?
What problems does spam create for businesses?

Find the English equivalents to the Russian words and phrases:

принятый повсеместно
адреса, найденные в интернете
неновый, неоригинальный
предшествовать
список рассылки
вездесущий, повсеместный
широко распространенный, преобладающий
автоматически нажать на ссылки
обходить антивирусные программы
список друзей (контактов)
приноровиться
бессмысленный и абсолютно бесполезный
вероятность мошенничества
обращаться к проблеме (решать проблему)

Write definitions for the four types of unsolicited messages described in the podcast.

Ex.3.
fill the gaps

appear build called decode designed devised gather generate harvest led modified outlaw pass prevent recover reported unsolicited write

spambot

A spambot is a program 1) _____to collect, or 2) _____, e-mail addresses from the Internet in order to 3) _____ mailing lists for sending 4) _____e-mail, also known as spam. A spambot can 5) _____ e-mail addresses from Web sites, newsgroups, special-interest group (SIG) postings, and chat-room conversations. Because e-mail addresses have a distinctive format, spambots are easy to 6) _____.
A number of legislators in the U.S. are 7) _____ to be devising laws that would 8) _____ the spambot. A number of programs and approaches have been 9) _____ to foil spambots. One such technique is known as munging, in which an e-mail address is deliberately 10) _____ so that a human reader can 11) _____ it but a spambot cannot. This has 12) _____ to the

evolution of sophisticated spambots that can 13) _____ e-mail addresses from character strings that 14) _____ to be munged.
The term spambot is sometimes used in reference to a program 1) _____ to 15) _____ spam from reaching the subscribers of an Internet service provider (ISP). Such programs are more often 16) _____ e-mail blockers or filters. Occasionally, such a blocker may inadvertently 15) _____ a legitimate e-mail message from reaching a subscriber. This can be prevented by allowing each subscriber to 17) _____a whitelist, or a list of specific e-mail addresses the blocker should let 18) _____.

Ex.4
fill the gaps

antenna	**default**	**legitimately**	**unprotected**
authorized	**equipped**	**perpetrators**	**variation**
broadcast	**extends**	**required**	**volumes**
configuring	**insecure**	**source**	**vulnerable**

drive-by spamming

Drive-by spamming is a(n) _____of drive-by hacking in which the _____ gain access to a vulnerable wireless local area network (WLAN) and use that access to send huge _____of spam. Using the drive-by method allows spammers to save themselves the considerable bandwidth costs _____to send that many messages _____, and makes it very difficult for anyone to trace the spam back to its _____.
A drive-by spamming incident starts with war driving: driving around seeking _____ networks, using a computer with a wireless Ethernet card and some kind of a(n) _____. A wireless LAN's range often _____beyond the building housing it, and the network may _____ identifying information that makes access simple. Once the attacker finds a(n) _____ e-mail (SMTP) port, the attacker can send e-mail as easily as someone inside the building. To the mail server, the messages appear to have come from a(n) _____ network user.
According to a report in Geek News, 60-80% of wireless LANS are _____ to a drive-by attack, mostly because administrators fail to change the _____ settings for network access points (devices that serve as base stations in a wireless network) when _____ the network.

Ex.5
fill the gaps with phrases
(a) **a munged e-mail address, and can easily and unmistakably deduce the true e-mail address**
(b) **a response to a particular correspondence is desired**
(c) **the presence of the @ symbol**
(d) **an e-mail address in order to send a confirmation**
(e) **in this respect**
(f) **information so it is no longer accurate**
(g) **legitimate addresses belonging to third parties**
(h) **spambots to scour the Internet for e-mail addresses**
(i) **Web-based programs that build e-mail lists for spamming purposes**
(j) **Web sites, e-mail correspondence, chat rooms, and postings to newsgroups and special interest groups (SIGs)**

munging

Munging (pronounced (MUHN-jing or MUHN-ging) is the deliberate alteration of an e-mail address online with the intent of making the address unusable for 1) _____. People who transmit unsolicited e-mail advertisements, called spam, often use programs called 2) _____. Such addresses are easily recognized because of their unique format, and because of 3) _____.

When munging is done, it should be in such a way that a person reading the document (as opposed to a program scanning it) can easily tell that it is 4) _____. Here are four examples of the munging of stangib@reno.com:
stangib at reno dot com
s-t-a-n-g-i-b-at-r-e-n-o-d-o-t-c-o-m
stangibNOSPAM@reno.com
My username is stangib, and the domain name is reno dot com.
Munged e-mail addresses can be useful in 5) _____**.** However, some experts advise against the practice because it may violate the Terms of Service (TOS) of the subscriber's Internet service provider (ISP). Munging should not be used if 6) _____**.** For example, when making an online purchase, the seller typically asks for 7) _____**.** If the address is munged, the confirmation will not reach the purchaser.
It is important that munged e-mail addresses not be mistaken for 8) _____**.** If an innocent person, corporation, or institution is harmed as a result of a munged e-mail address, civil or criminal action could result. Fake usernames or domain names are particularly dangerous 9) _____**.**
The term munging probably derives from the acronym mung (pronounced just as it looks), which stands for "mash until no good." It may also derive from the hackers' slang term munge (pronounced MUHNJ), which means "to alter 10) _____**."**

Ex.6
Decide what word is missing. The first letter is provided for help as well as the number of letters in the word. (There may be plural or verb forms)

self-sending spam

Self-sending spam is **u - - - - - - - - - -** e-mail that looks like you sent it to yourself: your name **a - - - - - -** on the "from" line as well as the "to" line. For example, Benjamin Googol might **r - - - - - -** a message addressed to "bengoogol@yourisp.net" that **p - - - - - - -** to be from "bengoogol@superfantasticdeals.com." In some cases (especially if you use one of the most common e-mail **s - - - - - - -**, such as Hotmail or Yahoo) a message may appear to be sent from your exact e-mail address.
Self-sending spam is one version of e-mail **s - - - - - - -** (disguising a message's "from" address so that it appears to be from someone other than the actual sender). The sender manually constructs a message header with their chosen information in it. E-mail **s - - - - - - -** is often sometimes used **l - - - - - - - - - -**, for example, by someone **s - - - - - - -** their own address to manage their e-mail. However, **s - - - - - - -** anyone other than yourself is illegal.
Senders **r - - -** upon two factors - curiosity and a positive emotional response - that make the **r - - - - - - - -** more likely to open or even respond to a message that seems to be from someone with their name. A recent study at McMaster University found that people respond more positively to e-mail messages sent (at least apparently) from people with names similar or **i - - - - - - - -** to their own. Researchers, who sent out thousands of **r - - - - - - -** for simple information, found that the response rate was over 10 per cent higher for messages sent using the exact name of the **r - - - - - - - -** as the sender. Even if only one name matched that of the **r - - - - - - - -**, the response rate was higher than for messages from someone with a different first and last name. However, as people receive more of these messages and the **n - - - - - -** wears off, it is unlikely that self-sending spam will continue to **e - - - - -** any positive response.

Ex.7
fill in the prepositions

splog

A splog (spam blog) is a fake blog created solely to promote affiliated Web sites, **…** the intent of skewing search results and artificially boosting traffic. Some splogs are written like long-winded ads **…** the Web

sites they promote; others have no original content, featuring either nonsense or content stolen **…** authentic Web sites. Splogs include huge numbers of links **…** the Web sites **…** question to fool Web crawlers (programs that search the Web **…** sites to index). The sploggers associate popular search keywords **…** their pages so that the splog links turn up **…** blog search results and are sent out as search subscription notifications through e-mail and RSS feeds.
Splogs have existed almost as long as blogs have, as enterprising spammers quickly realized the new medium's potential **…** exploitation. However, the attacks have become more common as attackers' methods have become more sophisticated. Automated attacks have caused what many in the industry referred **…** as a "turning point" for splog. **…** late October of 2005, a splogger used Google's blog-creation tool, Blogger, **…** conjunction **…** the BlogSpot hosting service to create what Tim Bray, of Sun Microsystems, called a "splogsplosion": hundreds, or even thousands of splogs turning up **…** search results and clogging RSS readers and e-mail inboxes.
Here's how this attack was conducted: The splogger ran a search **…** blog search engines **…** popular keywords. Among those selected were the names of two prominent bloggers, Chris Pirillo and Dave Winer. Next, using a bot to automate the process, the splogger created tens of thousands of splogs, listing the selected keywords and publishing text taken directly **…** Pirillo's and Winer's own sites, along **…** the commercial links. People searching **…** the legitimate bloggers' sites and people **…** search subscriptions for RSS feeds found their results filled **…** splog links.
… response to the attack and the media outcry **…** its wake, Google published a list of some 13,000 splog sub-domains. The company also implemented a type of Turing Test known as a CAPTCHA, forcing any entity creating a blog to prove satisfactorily that it is, **…** fact, a human and not a computer program.

Ex.8
fill in the articles

SMS spam

SMS spam (sometimes called cell phone spam) is any junk message delivered to ... mobile phone as ... text messaging through ... Short Message Service (SMS). ... practice is fairly new to ... North America, but has been common in ... Japan for ... years. In 2001-2002, ... systems at ... DoCoMo, ... country's major service provider, were overcome by ... volume of SMS spam, causing ... users' screens to freeze and spreading programs that caused ... phones to dial ... emergency numbers.
According to some experts, … other parts of … world should brace themselves for … similar deluge. … others, however, point to … several reasons why SMS spam is not likely to become as prevalent in … North America and … Europe as it is in … Japan. For … one thing, … text messaging itself is much more popular in … Japan. … Forrester Research reported that 80% of … Japanese mobile users use … text messaging, in … contrast to just 17% in … United States. Furthermore, it costs … sender about $0.08-0.12 to send … each text message -- not prohibitive for … most users, but too costly to make … mass mailings of … spammer profitable.

UNIT 7. PEOPLE IN SECURITY

warming up

Ex.1 Discussion
What terms to call people involved in computing do you know? Which of them can be related to the security aspect of IT?

Mainstream

Ex.2. Reading and discussing.
Which of people described below act legally and which illegally?
Find correlations with:
hackers – crackers
black hat – white hat – grey hat
Arrange the terms denoting people in security in a scheme to show correlations among them.

hacker

Hacker is a term used by some to mean "a clever programmer" and by others, especially journalists or their editors, to mean "someone who tries to break into computer systems."
1) Eric Raymond, compiler of The New Hacker's Dictionary, defines a hacker as a clever programmer. A "good hack" is a clever solution to a programming problem and "hacking" is the act of doing it. Raymond lists five possible characteristics that qualify one as a hacker, which we paraphrase here:
A person who enjoys learning details of a programming language or system
A person who enjoys actually doing the programming rather than just theorizing about it
A person capable of appreciating someone else's hacking
A person who picks up programming quickly
A person who is an expert at a particular programming language or system, as in "Unix hacker"
Raymond deprecates the use of this term for someone who attempts to crack someone else's system or otherwise uses programming or expert knowledge to act maliciously. He prefers the term cracker for this meaning.
2) Journalists or their editors almost universally use hacker to mean someone who attempts to break into computer systems. Typically, this kind of hacker would be a proficient programmer or engineer with sufficient technical knowledge to understand the weak points in a security system.

cracker

A cracker is someone who breaks into someone else's computer system, often on a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there. Some breaking-and-entering has been done ostensibly to point out weaknesses in a site's security system.
The term "cracker" is not to be confused with "hacker". Hackers generally deplore cracking. However, as Eric Raymond, compiler of The New Hacker's Dictionary notes, some journalists ascribe break-ins to "hackers."
A classic story of the tracking down of a cracker on the Internet who was breaking into U.S. military and other computers is told in Clifford Stoll's The Cuckoo's Egg.

black hat

Black hat is used to describe a hacker (or, if you prefer, cracker) who breaks into a computer system or network with malicious intent. Unlike a white hat hacker, the black hat hacker takes advantage of the break-in, perhaps destroying files or stealing data for some future purpose. The black hat hacker may also

make the exploit known to other hackers and/or the public without notifying the victim. This gives others the opportunity to exploit the vulnerability before the organization is able to secure it.
The term comes from old Western movies, where heros often wore white hats and the "bad guys" wore black hats.

white hat

White hat describes a hacker (or, if you prefer, cracker) who identifies a security weakness in a computer system or network but, instead of taking malicious advantage of it, exposes the weakness in a way that will allow the system's owners to fix the breach before it is can be taken advantage by others (such as black hat hackers.) Methods of telling the owners about it range from a simple phone call through sending an e-mail note to a Webmaster or administrator all the way to leaving an electronic "calling card" in the system that makes it obvious that security has been breached.
While white hat hacking is a hobby for some, others provide their services for a fee. Thus, a white hat hacker may work as a consultant or be a permanent employee on a company's payroll. A good many white hat hackers are former black hat hackers.
The term comes from old Western movies, where heros often wore white hats and the "bad guys" wore black hats.

gray hat

Gray hat describes a cracker (or, if you prefer, hacker) who exploits a security weakness in a computer system or product in order to bring the weakness to the attention of the owners. Unlike a black hat, a gray hat acts without malicious intent. The goal of a gray hat is to improve system and network security. However, by publicizing a vulnerability, the gray hat may give other crackers the opportunity to exploit it. This differs from the white hat who alerts system owners and vendors of a vulnerability without actually exploiting it in public.

ethical hacker

An ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. To test a security system, ethical hackers use the same methods as their less principled counterparts, but report problems instead of taking advantage of them. Ethical hacking is also known as penetration testing, intrusion testing, and red teaming. An ethical hacker is sometimes called a white hat, a term that comes from old Western movies, where the "good guy" wore a white hat and the "bad guy" wore a black hat.
One of the first examples of ethical hackers at work was in the 1970s, when the United States government used groups of experts called red teams to hack its own computer systems. According to Ed Skoudis, Vice President of Security Strategy for Predictive Systems' Global Integrity consulting practice, ethical hacking has continued to grow in an otherwise lackluster IT industry, and is becoming increasingly common outside the government and technology sectors where it began. Many large companies, such as IBM, maintain employee teams of ethical hackers.
In a similar but distinct category, a hacktivist is more of a vigilante: detecting, sometimes reporting (and sometimes exploiting) security vulnerabilities as a form of social activism.

hacktivism

Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose. The individual who performs an act of hacktivism is said to be a hacktivist.
A hacktivist uses the same tools and techniques as a hacker, but does so in order to disrupt services and bring attention to a political or social cause. For example, one might leave a highly visible message on the home page of a Web site that gets a lot of traffic or which embodies a point-of-view that is being opposed. Or one might launch a denial-of-service attack to disrupt traffic to a particular site.
A recent demonstration of hacktivism followed the death of a Chinese airman when his jet fighter collided with a U.S. surveillance plane in April 2001. Chinese and American hacktivists from both countries hacked Web sites and used them as "blackboards" for their statements.

Whether hacktivism is a crime may be debated. Opponents argue that hacktivism causes damage in a forum where there is already ample opportunity for nondisruptive free speech. Others insist that such an act is the equivalent of a protest and is therefore protected as a form of free speech.

insider threat

An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, or agency. The term can also apply to an outside person who poses as an employee or officer by obtaining false credentials. The cracker obtains access to the computer systems or networks of the enterprise, and then conducts activities intended to cause harm to the enterprise.
Insider threats are often disgruntled employees or ex-employees who believe that the business, institution, or agency has "done them wrong" and feel justified in gaining revenge. The malicious activity usually occurs in four steps or phases. First, the cracker gains entry to the system or network. Secondly, the cracker investigates the nature of the system or network in order to learn where the vulnerable points are and where the most damage can be caused with the least effort. Thirdly, the cracker sets up a workstation from which the nefarious activity can be conducted. Finally, the actual destructive activity takes place.
The damage caused by an insider threat can take many forms, including the introduction of viruses, worms, or Trojan horses; the theft of information or corporate secrets; the theft of money; the corruption or deletion of data; the altering of data to produce inconvenience or false criminal evidence; and the theft of the identities of specific individuals in the enterprise. Protection against the insider threat involves measures similar to those recommended for Internet users, such as the use of multiple spyware scanning programs, anti-virus programs, firewalls, and a rigorous data backup and archiving routine.

script kiddy

Script kiddy (sometimes spelled kiddie) is a derogative term, originated by the more sophisticated crackers of computer security systems, for the more immature, but unfortunately often just as dangerous exploiter of security lapses on the Internet. The typical script kiddy uses existing and frequently well-known and easy-to-find techniques and programs or scripts to search for and exploit weaknesses in other computers on the Internet - often randomly and with little regard or perhaps even understanding of the potentially harmful consequences. Hackers view script kiddies with alarm and contempt since they do nothing to advance the "art" of hacking but sometimes unleashing the wrath of authority on the entire hacker community.
While a hacker will take pride in the quality of an attack - leaving no trace of an intrusion, for example - a script kiddy may aim at quantity, seeing the number of attacks that can be mounted as a way to obtain attention and notoriety. Script kiddies are sometimes portrayed in media as bored, lonely teenagers seeking recognition from their peers.

packet monkey

On the Internet, a packet monkey is someone (see cracker, hacker, and script kiddy) who intentionally inundates a Web site or network with data packets, resulting in a denial-of-service situation for users of the attacked site or network. Packet monkeys typically use tools created and made available on the Internet by hackers.
According to one writer's distinction, a packet monkey, unlike a script kiddy, leaves no clues as to who is making the exploit, making the identity of a packet monkey more difficult to trace. In addition, a denial-of-service attack can be launched on a wider scale than attacks performed by script kiddies, making them more difficult to investigate.
Hackers look down on packet monkeys and often describe them as "bottom feeders." Because a packet monkey uses tools created by others, the packet monkey has little understanding of the harm that may be caused. Typically, packet monkey exploits are random and without any purpose other than the thrill of making an effect.