1 Exercise 2.28: Translate into English

1.1 Незахищеність комп’ютера — це поняття, зміст якого полягає в тому, що комп’ютерна система завжди вразлива до атак і що це породжує постійну боротьбу між тими, хто прагнуть поліпшити захист і тими, хто прагнуть його обійти.

Computer insecurity is the concept that a computer system is always vulnerable to attack, and that this fact creates a constant battle between those looking to improve security and those looking to circumvent security.

1.2 Комп’ютерна інформація все частіше стає об’єктом атак хакерів або кібер-терористів, котрі прагнуть доступу до комп’ютерних систем або їх руйнації.

Computerized information is increasingly the target of computer hackers or cyber-terrorists that seek access to or destruction of computer systems.

1.3 Ми використовуємо комп’ютери для всього: від банківських операцій та інвестування до покупок і спілкування з іншими через електронну пошту або чат-програми.

We use computers for everything from banking and investing to shopping and communicating with others through e-mail or chat programs.

1.4 Хоча ви, може, й не вважаєте свої інформаційні матеріали надсекретними, вам, мабуть, не хочеться, щоби сторонні особи читали вашу електронну пошту, використовували ваш комп’ютер для атак на інші системи, відправляли електронною поштою з вашого комп’ютера підроблені повідомлення або вивчали особисту інформацію, що зберігається на вашому комп’ютері.

Although you may not consider your communications “top secret“, you probably do not want strangers reading your e-mail, using your computer to attack other systems, sending forged e-mail from your computer or examining personal information stored on your computer (such as financial statements).

1.5 Однією з цілей визначення периметру безпеки системи є відрізними зломлювачів від легальних користувачів.

One of the purposes of defining a system's security perimeter is to distinguish intruders from legitimate users.

1.6 Зломлювач — це особа, яка перетинає периметр безпеки системи без дозволу.

An intruder is an individual who crosses a system's security perimeter without authorization.

1.7 Оскільки зломлювач може отримати доступ до системи, викравши ідентифікаційну інформацію легального користувача, виявлення такого зломлювача є складною задачею.

Since an intruder may gain access to a system by stealing a legitimate user's identity, detecting such intruders is a hard problem.

1.8 Зломлювачів може не цікавити ваша ідентифікаційна інформація. Часто вони хочуть отримати контроль над вашим комп'ютером, щоби здійснювати атаки на інші комп'ютерні системи.

Intruders may not care about your identity. Often they want to gain control of your computer so they can use it to launch attacks on other computer systems.

1.9 Контроль над вашим комп'ютером дає можливість зломлювачам приховувати своє справжнє місцеперебування.

Having control of your computer gives the intruders the ability to hide their true location.

1.10 Навіть якщо ви підключили комп'ютер до Інтернету лише для того, аби грати у нові ігри або відправляти електронною поштою повідомлення рідним і друзям, ваш комп"ютер може бути об'єктом атаки.

Even if you have a computer connected to the Internet only to play the latest games or to send e-mail to friends and family, your computer may be a target.

1.11 Зломлювачі можуть мати можливість спостерігати за всіма вашими операціями на комп'ютері або завдавати шкоди вашому комп'ютеру, переформатувавши ваш жорсткий диск або змінивши дані.

Intruders may be able to watch all your actions on the computer, or cause damage to your computer by reformatting your hard drive or changing your data.

1.12 Також, деякі прикладні програми мають параметри за замовчуванням, які дозволяють іншим користувачам отримувати доступ до вашого комп'ютера, якщо ви не зміните ці параметри, щоби бути більш захищеним.

Also, some software applications have default settings that allow other users to access your computer unless you change the settings to be more secure.

1.13 Прикладами є чат-програми, які дозволяють стороннім суб'єктам виконувати команди на вашому комп'ютері, або веб-браузери, які можуть дозволити комусь розмістити на вашому комп'ютері шкідливі програми, котрі запускаються, коли ви натискаєте на них.

Examples include chat programs that let outsiders execute commands on your computer or web browsers that could allow someone to place harmful programs on your computer that run when you click on them.

1.14 Існує багато способів атакувати цільову систему. Цього можна досягти, використовуючи відомі вразливі місця у програмному забезпеченні або скориставшись погано сконфігурованою політикою безпеки.

There exist numerous ways to attack a target system. It could be achieved by exploiting known vulnerabilities in software or taking advantage of a badly configured security policy.

1.15 Уразливе місце — це пробоїна або слабке місце у прикладній програмі, що може бути помилкою проектування або реалізації, яку можна використати, щоби чинити перешкоди політиці захисту системи.

A vulnerability is a hole or a weakness in the application, which can be a design flaw or an implementation bug, that could be exploited to violate the system's security policy.

1.16 Більшість уразливих місць системи захисту програмного забезпечення належить до однієї з невеликої групи категорій: переповнення буфера; неперевірений вхід; стан перегонів; проблеми, пов'язані з контролем за доступом; слабкі місця в практиці аутентифікації, авторизації або криптографії.

Most software security vulnerabilites fall into one of a small set of categories: buffer overflows, unvalidated input, race conditions, access control problems, weaknesses in authentication, authorization or cryptographic practices.

1.17 Переповнення буфера виникає, коли прикладна програма намагається записувати дані після закінчення або до початку буфера.

A buffer overflow occurs when an application attempts to write data past thte end or past the beginning of a buffer.

1.18 Переповнення буфера може спричинити відмову прикладних програм, розкрити дані і може надати вектор атаки для подальшого розширення привілеїв.

Buffer overflows can cause applications to crash, can compromise data, and can provide an attack vector for further privilege escalation.

1.19 Як загальне правило, слід перевіряти всю вхідну інформацію, що її отримала ваша програма, аби пересвідчитися, що ця інформація є коректною.

As a general rule, you should check all input received by your program to make sure that the data is reasonable.

1.20 Для цього ви повинні уважно перевірити ваші вхідні дані. Цей процес є загальновідомий як перевірка входу або перевірка достовірності.

To do so, you must check your input data carefully. This process is commonly known as input validation or sanity checking.

1.21 Всяка вхідна інформація, що її ваша програма отримала з ненадійного джерела, є потенційним об'єктом для атаки.

Any input received by your program from an untrusted source is a potential target for attack.

1.22 Стан перегонів існує, коли зміни у порядку двох або більше подій може спричинити зміну у поведінці.

A race condition exists when changes to the order of two or more events can cause a change in behavior.

1.23 Це є вадою, якщо для належного функціонування програми необхідним є правильний порядок виконання.

If the correct order of execution is required for the proper functioning of the program, this is a bug.

1.24 Якщо зломлювач може скористатися цією ситуацією, щоби ввести зловмисний код, змінити ім'я файла або якимось іншим чином перешкоджати нормальній роботі програми, стан перегонів є вразливим місцем системи захисту.

If an attacker can take advantage of the situation to insert malicious code, change a filename or otherwise interfere with the normal operation of the program, the race condition is a security vulnerability.

1.25 Зломлювачі можуть інколи скористатися невеликими часовими проміжками в обробці коду для того, щоби втрутитися у послідовність операцій, що вони потім використовують у своїх цілях.

Attackers can sometimes take advantage of small time gaps in the processing of code to interfere with the sequence of operations, which they then exploit.

1.26 Контроль за доступом — це процес керування тим, кому що дозволено робити.

Access control is the process of controlling who is allowed to do what.

1.27 Деякі механізми контролю за доступом здійснюються операційною системою, деякі — окремою прикладною програмою або сервером, деякі — послугою, котра використовується.

Some access control mechanisms are enforced by the operation system, some by the individual application or server, some by a service in use.