1 Exercise 2.23: Translate into English

1.1 Проблема незахищеності комп’ютера стає все більш складною через складність програмного забезпечення, а також через те, що зломлювачі завжди відкривають нові вразливі місця.

The problem of computer insecurity becomes more challenging due to software complexity and the fact that intruders constantly discover new vulnerabilities.

1.2 Перевірка достовірності здійснюється, аби пересвідчитися, що ця інформація є коректною і не суперечить здоровому глузду.

Sanity checking is done to ensure that the information is valid and does not contradict common sense.

1.3 Виявлення зломлювача є дуже непростою задачею, оскільки дуже складно відрізнити його від легального користувача.

Detecting an intruder is a very hard problem, since it’s extremely difficult to distinguish them from legitimate users.

1.4 Викравши ідентифікаційну інформацію легального користувача, зломлювач може здійснювати атаки на інші комп’ютерні системи, приховуючи своє справжнє місцеперебування.

By stealing a legitimate user’s identity, an intruder is able to attack other computer systems while hiding their true location.

1.5 Ті, хто прагнуть поліпшити захист, вдосконалюють засоби захисту, тоді як ті, хто прагнуть його обійти, використовують як помилки проектування, так і помилки реалізації з тим, щоби чинити перешкоди політиці захисту системи.

Those seeking to improve the security improve the defensive measures, while those trying to circumvent it use design flaws and implementation bugs to violate the security policy.

1.6 Отримавши контроль над вашим комп'ютером, зломлювач може читати вашу електронну пошту, фінансові звіти, спричиняти відмову прикладних програм, перешкоджати нормальній роботі програми, або ж завдати шкоди вашому комп'ютеру, переформатувавши ваш жорсткий диск або змінивши дані.

After gaining control of your computer an intruder can read your emails, financial statements, prevent normal operation of applications or damage your computer by formatting your hard drive or changing your data.

1.7 Атака типу переповнення динамічно розподілюваної області може мати місце внаслідок виділення для буфера пам'яті некоректного розміру.

Heap overflow attacks can take place due to allocating a memory buffer of incorrect size.

1.8 Звичайні користувачі не завжди уважно перевіряють вхідні дані, що надходять з сумнівних джерел.

Ordinary users don't always carefully check the input that comes from untrustworthy sources.

1.9 Неуважне або неналежне користування засобами керування доступом буває причиною виникнення вразливих місць, що їх може використати зломлювач для отримання доступу до системи.

Careless or improper use of access control tools leads to vulnerabilities that an intruder can exploit to gain access to a system.

1.10 Ви, можливо, не вважаєте своє спілкування надсекретним, але зломлювача може не цікавити ваша ідентифікаційна інформація — ваш комп'ютер йому потрібен для здійснення атак на інші комп'ютерні системи.

Perhaps you don't consider your communications "top secret", but an intruder may not be interested in your account information, they might need your computer to attack other computer systems.

1.11 Якщо для належного функціонування програми необхідним є правильний порядок виконання, зломлювач може скористатися цією ситуацією і втрутитися у послідовність операцій або ввести зловмисний код.

If proper functioning of a program requires the correct execution order, an intruder may use this situation to interfere with the sequence of operations or insert malicious code.

1.12 Для посилення безпеки використовують різні методи: застосування паролів, смарт-карт, біометричне сканування, але найслабшою ланкою в системі засобів захисту є сама людина.

Different methods are used to improve security such as passwords, smart-cards and biometric scans, however the weakest link in the chain of security measures is the person themselves.