Course book – Exercises

## 1.8

1. **Distinguish between vulnerability, threat, and control**

Threat is a set of circumstances which can cause harm.

Vulnerability is a weakness that could be exploited to cause harm.

Control is a measure that prevents threats from exercising vulnerabilities.

1. **List three kinds of harm company might experience from theft of computer equipment**

Financial loss – They would have to pay for new computer equipment.

Asset loss – They would have to come up with e.g. new design documents of their system product.

Asset loss – If a product, cooperation, or marketing idea were stolen, they would have to compensate for that by making sure to track competitors and maintain customers.

1. **List at least three kinds of harm company could experience from electronic espionage or unauthorized viewing of confidential company materials.**

Financial loss – Loss in market shares if a competitor is introducing the idea

Financial loss – If a competitor get hand on a asset which has been expensive to develop and go straight to production.

Asset loss – If the given stolen information can be used to seduce employers or customers of competitor.

1. **List at least three kinds of damage a company could suffer when the integrity of a program or company data is compromised.**
2. **List at least three kinds of harm a company could encounter from loss of service, that is, failure of availability. List the product or capability to which access is lost, and explain how this loss hurts the company.**
3. **Describe a situation in which you have experienced harm as a consequence ofa failure of computer security. Was the failure malicious or not? Did the attack target you specifically or was it general and you were the unfortunate victim?**
4. **Describe two examples of vulnerabilities in automobiles for which auto manufacturers have instituted controls. Tell why you think these controls are effective, somewhat effective, or ineffective.**
5. **One control against accidental software deletion is to save all old versions of a program. Of course, this control is prohibitively expensive in terms of cost of storage. Suggest a less costly control against accidental software deletion. Is your control effective against all possible causes of software deletion? If not, what threats does it not cover?**
6. **On your personal computer, who can install programs? Who can change operating system data? Who can replace portions of the operating system? Can any of these actions be performed remotely?**
7. **Suppose a program to print paychecks secretly leaks a list of names of employees earning more than a certain amount each month. What controls could be instituted to limit the vulnerability of this leakage?**
8. **Preserving confidentiality, integrity, and availability of data is a restatement of the concern over interruption, interception, modification, and fabrication. How do the first three concepts relate to the last four? That is, is any of the four equivalent to one or more of the three? Is one of the three encompassed by one or more of the four?**
9. **Do you think attempting to break in to (that is, obtain access to or use of) a computing system without authorization should be illegal? Why or why not?**
10. **Describe an example (other than the ones mentioned in this chapter) of data whose confidentiality has a short timeliness, say, a day or less. Describe an example of data whose confidentiality has a timeliness of more than a year.**
11. **Do you currently use any computer security control measures? If so, what? Against what attacks are you trying to protect?**
12. **Describe an example in which absolute denial of service to a user (that is, the user gets no response from the computer) is a serious problem to that user. Describe another example where 10 percent denial of service to a user (that is, the user’s computation progresses, but at a rate 10 percent slower than normal) is a serious problem to that user. Could access by unauthorized people to a computing system result in a 10 percent denial of service to the legitimate users? How?**
13. **When you say that software is of high quality, what do you mean? How does security fit in your definition of quality? For example, can an application be insecure and still be “good”?**
14. **Developers often think of software quality in terms of faults and failures. Faults are problems (for example, loops that never terminate or misplaced commas in statements) that developers can see by looking at the code. Failures are problems, such as a system crash or the invocation of the wrong function, that are visible to the user. Thus, faults can exist in programs but never become failures, because the conditions under which a fault becomes a failure are never reached. How do software vulnerabilities fit into this scheme of faults and failures? Is every fault a vulnerability? Is every vulnerability a fault?**
15. **Consider a program to display on your website your city’s current time and temperature. Who might want to attack your program? What types of harm might they want to cause? What kinds of vulnerabilities might they exploit to cause harm?**
16. **Consider a program that allows consumers to order products from the web. Who might want to attack the program? What types of harm might they want to cause? What kinds of vulnerabilities might they exploit to cause harm?**
17. **Consider a program to accept and tabulate votes in an election. Who might want to attack the program? What types of harm might they want to cause? What kinds of vulnerabilities might they exploit to cause harm?**
18. **Consider a program that allows a surgeon in one city to assist in an operation on a patient in another city via an Internet connection. Who might want to attack the program? What types of harm might they want to cause? What kinds of**

**vulnerabilities might they exploit to cause harm?**