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.**

Integrity failures can make data completely useless. If the integrity of a system could not be ensured, its expected behavior cannot be relied on.

If data is compromised, a company would have to assess the impact of that compromise. If it has an impact on e.g. employees, company brand, company reputation, business affairs or technical development, actions and control must be achieved to ensure the safety of the business operations.

Damages are financial loss, Market share, technical advantages.

1. **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.**

If a design document is lost, the company would have to rethink the production of that design due to its leak. If the whole idea is compromised, the company would have to put down the design completely. If the market is still available and production may be fast, the design document would have to be recreated.

If an encryption key or user data is compromised, the company would have to change the security of those entities.

Such losses of data would hurt a company’s budget in terms of cost and time, it may compromise the security of its product users or employees.

1. **Describe a situation in which you have experienced harm as a consequence of a 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?**

A profile on a fantasy management floorball competition based on our own team and scores was performed 7 years ago. A profile associated with a player’s name, age, image, and scores were uploaded. Yet today, this profile was not accessible from the admin account or the players account to be deleted.

1. **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.**

An example is the amount of software used in todays automobiles. It requires all range of microcontrollers along with engine control unit, infotainment, and control systems. This makes automobiles in general more prone to vulnerabilities and effective control of such.

Another example is the expensive hardware integrated and mounted on automobiles which must be protected from theft.

Automobile industry have had less experience in cybersecurity compared to the computer science fields and thus, there has been a lack in security awareness embedded into the development lifecycle.

Dealing with security patching.

1. **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?**

Use of a version control system. Push update whenever a change is final. This will control against accidental software deletion against changes made before current edit.

1. **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?**

I (the admin) can change operating systems data and install programs. None of these actions can be performed remotely.

1. **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?**

The program can be patched. The data can be encrypted so even though the data is stolen, it would not be retrievable for the perpetrator.

1. **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?**

Interception of data can compromise someone’s confidentiality. Interruption of data flow can compromise availability of that data. Modification or fabrication of data can compromise the integrity of that data.

1. **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?**

Attempting to break in shall not be illegal since that would put criminals into an empty room with their target. We shall not exclude hobby hackers, white-hats or professional research teams to perform security or authorization attempts.

1. **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.**

Confidentiality with short timeliness:

* A weekly email can have a timeliness of just a day or less.
* An upcoming event plan can have a timeliness of just a day or less.

Confidentiality with long timeliness:

* Marketing or product plans
* Medical records
* Tax returns

1. **Do you currently use any computer security control measures? If so, what? Against what attacks are you trying to protect?**

Windows defender – To avoid attacks on the operating system and attacks on applications.

Windows firewall – To avoid attacks from the network.

Network Modem/router – To avoid attacks on the network.

Addblocker – To avoid popup site, fishing, and imitation.

VPN – To avoid IP tracking.

TOR – To avoid networking tracking.

Duckduckgo – To prevent search engines to track my activity and history.

Incognito/private browser mode – Avoid sites from getting personal information.

Knowledge – To visit only trusted sited on the internet.

1. **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?**

Absolute denial of service is a critical harm when the user is in an emergency and must perform a certain operation on that computer.

10 % slower computation than usual may become a serious problem when the user application is safety critical.

If many unauthorized people are accessing the same system, depending on the system design, it may delegate resources to those users resulting in a potential 10 % denial of service to legitimate users.

1. **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”?**

A software is of high quality when all aspects of quality is covered. This includes security IF, there is a requirement that the application must be secure (that is if the application can be used to cause any harm). If a system is insecure, the system obviously has some requirement of being secure and the security is thus of lower quality affecting the overall quality of the software.

1. **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?**

A vulnerability is a fault which may be used to cause a failure. Not every fault is a vulnerability, nor the opposite. Even though it is likely that a vulnerability is a fault, there might be external factors creating a vulnerability. A vulnerability can potentially lead to a failure of functionality or usage overall.

1. **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?**

An attacker could have the motive to make the website insignificant to redirect traffic to another website. Another motive could be to spread confusion among the public. A third motive would be to track traffic or display adds to make a financial benefit.

They may want to put down the site. They might want to modify the site. They might want to fabric the site. They might want to surveillance the traffic.

1. **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?**

A competitor who want an advantage in sales. An activists who interest are not inline with the companies. A government secret service, if the site is used to steal user and payment credentials and information.

They might cause financial loss, time loss etc.

The attackers may use e.g. denial of service. Loading the product system to much making an interruption long enough to making an impact on the sales, reputations and customers.

The attackers may use a fishing email, imitating the interface of the web interface, stealing customer information.

Attackers may use other malware to steal customer or company information.

1. **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?**

Government supported hackers, criminal networks, political organizations. They may want to change the outcome of the election by flipping the tabulate votes.

They might use vulnerabilities in social networks, creating fake profiles spreading misinformation and propaganda.

1. **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?**

Government/regime supported hackers, technical competitors, someone who wants to cause harm or blackmail for money.