Exercises
Introduction to Computer Security

Computer Security

Exercise 1

Consider the following scenario: *A small manufacturing company, one of the most important producers of a specialized musical instrument, is hit by a ransomware attack (i.e., infected by malware with the sole purpose to encrypt all the files in the infected computer until the victim pays a ransom to the attacker). The ransomware is able to quickly propagate to all the computers in use by the company.*

1. What are the <u>two most important Threat/Risk</u> in this scenario? Name and describe each of them, specifying the <u>asset</u> at risk and list one or two possible <u>countermeasures</u>.

Threat/Risk 1 Description:

Asset at risk:

Countermeasure:

Threat/Risk 2 Description:

Asset at risk:

Countermeasure:

Threat/Risk 1 Description: *Loss of business-critical data (e.g., key intellectual property) so that the company is not able to produce the (specialized) goods anymore*

Asset at risk: *Business-critical data*

Countermeasure: *Backups*

Threat/Risk 2 Description: *Loss of production time due to the downtime incurred to restore the infected computers and systems. During this time the factory must me kept shut off, bringing a substantial economic damage.*

Asset at risk: *company's production*

Countermeasure: *redundant systems, isolated systems, procedures for a fast disaster recovery, …*

2. What is (or are) the possible threat agent(s) according to what you answered in (1.)?

2. What is (or are) the possible threat agent(s) according to what you answered in (1.)?

The most likely threat agent is a cybercriminal motivated by the fact that the victim will pay a ransom, due to the value of the assets at risk. Another possible threat agent is a competitor who wants to damage the company's ability to carry on business or to cause monetary loss. If the victim is listed on the stock market a threat agent could be a malicious trader willing to capitalize on stock loss.

Exercise 2

Consider a self-driving and Internet-connected vehicle (e.g., self-driving car), such as the ones currently being developed, being used in a taxi service scenario:

1. [3 points] What are the three most valuable assets at risk in this scenario?

Consider a self-driving and Internet-connected vehicle (e.g., self-driving car), such as the ones currently being developed, being used in a taxi service scenario:

1. [3 points] What are the three most valuable assets at risk in this scenario?

- people inside the car
- people outside the car
- car

Consider a self-driving and Internet-connected vehicle (e.g., self-driving car), such as the ones currently being developed, being used in a taxi service scenario:

2. [2 points] Suggest at least two potential attack surfaces on the vehicles.

Consider a self-driving and Internet-connected vehicle (e.g., self-driving car), such as the ones currently being developed, being used in a taxi service scenario:

2. [2 points] Suggest at least two potential attack surfaces on the vehicles.

- CAN bus via diagnostic port
- Remote interface to car

Consider a self-driving and Internet-connected vehicle (e.g., self-driving car), such as the ones currently being developed, being used in a taxi service scenario:

3. [2 points] Suggest, in a rough order of prevalence (i.e., frequency) the two most likely potential digital attacks against such vehicles and their operating companies.

Consider a self-driving and Internet-connected vehicle (e.g., self-driving car), such as the ones currently being developed, being used in a taxi service scenario:

3. [2 points] Suggest, in a rough order of prevalence (i.e., frequency) the two most likely potential digital attacks against such vehicles and their operating companies.

- Local: an attacker inside the car can manipulate the packet transiting on the CAN bus via diagnostic port and take control of the car
- Remote: an attacker could manipulate the communication between car and the backend, potentially drive the car somewhere else

Exercise 3

An Internet-connected “smart speaker”, featuring a voice-controlled intelligent virtual assistant (think about a device similar to Amazon Echo, Google Home, or Jarvis), is installed inside a house.

The speaker is *connected to a wireless network*, and *linked to a cloud service account* (e.g., the owner’s Google/Amazon/iCloud/… account). The device is *always listening for a particular keyword* (e.g., “*OK, Google!*”). As soon as the keyword is detected, it records a short audio clip, which is uploaded to a cloud speech recognition service. Then, the device performs the action requested in the recognized command.

The available actions allow to *search particular pieces of information on the Internet* (e.g., providing weather or traffic information), or to *interact with the owner’s cloud account* (e.g., making and accessing to-do lists stored in the cloud, playing music from a streaming service). Furthermore, the device can act as a *“home automation hub” controlling “smart” devices* via voice commands. Thus, the device supports commands to turn on and off the house lights, open the front door, control the heating, and so on.

1. What are the three most valuable assets at risk in this scenario?

1. What are the three most valuable assets at risk in this scenario?

1) *Personal information (musical preferences, location - e.g., from weather requests, ...)*
2) *Owners' voice (recorded commands and the possibility of recording unwanted conversation given that the device sports an always-listening microphone)*
3) *The actual house (remotely-controlled door)*
4) *The device vendor reputation*

2. Suggest at least two potential attack surfaces of this “smart speaker”.

2. Suggest at least two potential attack surfaces of this "smart speaker".

1) *The voice command interface*
2) *Cloud backend (exploit \ data breaches)*
3) *Local network*
4) *Physical access*

3. Suggest, in a rough order of prevalence (i.e., frequency) the two most likely potential digital attacks in this scenario.

3. Suggest, in a rough order of prevalence (i.e., frequency) the two most likely potential digital attacks in this scenario.

1) *Compromise the cloud vendor to access all the recordings, user data, …, and, according to the implementation, gain control of the house.*
2) *Malicious voice commands: performed by a physical person or even by a recording, e.g., a malicious TV advertisement or a malware that plays a command so that it's picked up by the virtual assistant*
3) *Device gets compromised from the local network to access information, or to snoop on the user*

Exercise 4

“SmartCar” is a new device that you can plug into your car to keep track of your driving habits and patterns—as well as your car’s location—directly from your smartphone.

All modern automobiles are equipped with an internal wired network that connects together all the electronic control units (e.g., engine controller, dashboard, parking sensors). This network is used to exchange commands and data, including safety-related ones (e.g., data for the ABS, setpoint of the cruise control). This network is based on the standard known as CAN (controller area network): all messages are broadcast to all control units connected to the network, are not encrypted, and their sender is not authenticated. In order to gather information about how the vehicle is driven, “SmartCar” must be physically connected to the car’s internal CAN network, where it actively exchanges messages with the car’s control units in order to gather the required data.

Furthermore, to display real-time data, “SmartCar” is connected via Bluetooth to the vehicle owner’s smartphone, and sends information about the vehicle’s location to a remote server over a cellular network (3G\4G), so that the vehicle’s owner can constantly track its movements—for instance to remotely locate the vehicle in case of theft.
Consider the following scenario: a vehicle owner installs “SmartCar” in their car.

1. What are the three most valuable assets at risk in this scenario?

1. What are the three most valuable assets at risk in this scenario?

1) *Life/Health of the people inside and around the car*
2) *Owner's private driving data*
3) *The device vendor reputation / car manufacturer reputation*
4) *The vehicle itself*
5) *Smartphone*

2. Suggest at least two potential attack surfaces of SmartCar.

2. Suggest at least two potential attack surfaces of SmartCar.

1) *The smartphone application*
2) *The company’s backend*
3) *Physical Access to the vehicle*
4) *Bluetooth/cellular network*

3. Suggest two potential digital attacks in this scenario.

3. Suggest two potential digital attacks in this scenario.

1) *Compromise the company's backend to retrieve all user data… and according to implementation, endanger driver safety by reflashing device and send data inside network*
2) *Physically compromise device to then send commands to the vehicle from remote*
3) *Compromise the application to retrieve data on different users / gather live data on one user*

Exercise 5

Consider object tracking devices such as the one developed by Apple or Tile. They are hardware devices designed to act as object finders, which help people find personal objects (e.g., keys, bags, apparel, small electronic devices, and vehicles).

Consider the following infrastructure implementation:

A user can use an app installed on smartphones to help locate the item if it is lost. In particular, to locate lost items, they use a crowdsourced network of devices: approximately billions of devices worldwide that detect and anonymously report emitted Bluetooth Low Energy 4.0 radio technology signals. If the tracking device is reported as lost and comes within range of any smartphone running the tracking app, the nearby user's app will send the item's owner an anonymous update of the lost item's location.

Each tracking device comes with a built-in speaker, which can be triggered by the user through the app to play a sound to aid in locating items at close range.

The tracking devices usually also have a "Find My Phone" feature, which can be used to produce a sound on the user's paired smartphone when the user presses a button on the device. Tracking devices usually have built-in batteries with a battery life of about one year that can be easily replaced.

[1 point] 1. What are the main assets at risk in such a scenario? Suggest at least two assets.

Asset	Motivation

[1 point] 1. What are the main assets at risk in such a scenario? Suggest at least two assets.

1. Personal information and location data: As users rely on these tracking devices to locate lost items, they may also be sharing personal information and location data with the tracking device's infrastructure and operating companies, as well as other users in the crowdsourced network. This data could be at risk if a security breach occurs or if the data is mishandled by the company.
2. Physical assets: The physical assets that the tracking devices are being used to locate, such as keys, bags, apparel, small electronic devices, and vehicles, are also at risk if lost or stolen. The tracking devices may help users locate these assets, but they do not provide any protection against their loss or theft.
3. Network and infrastructure: The tracking devices rely on a network of smartphones and a centralized infrastructure to locate lost items, which could be at risk if it is compromised by a cyber attack or other security breaches.
4. Business reputation: If the tracking device infrastructure and operating companies fail to protect users' personal information and location data, or if there are issues with the device's performance, it could lead to negative publicity and damage the company's reputation.

[1 point] 2. Suggest, in rough order of prevalence (i.e., frequency), the most likely potential security threats against such infrastructure and their operating companies.

Threats
1) **Motivation:**
2) **Motivation:**

[1 point] 2. Suggest, in rough order of prevalence (i.e., frequency), the most likely potential security threats against such infrastructure and their operating companies.

1. Privacy concerns: As the tracking devices use a crowdsourced network to locate lost items, there could be concerns about users' privacy as their location data is being shared anonymously with other users.
2. Security breaches: These tracking devices rely on a network of smartphones and a centralized infrastructure, a security breach in the system could potentially expose the personal information and location data of users.
3. Physical tampering and theft: The tracking devices themselves could be tampered with or stolen, potentially exposing personal information and location data, or rendering the device useless.
4. Malware and cyber attacks: The tracking devices infrastructure and operating companies may be targeted by malware or cyber attacks, which could compromise personal information and location data, as well as disrupt the service.
5. Denial of service: The infrastructure and operating companies may be targeted by a denial of service attack, which could disrupt the service and prevent users from being able to locate lost items.

[1 point] 3. Suggest, in rough order of prevalence (i.e., frequency), the most likely potential security threat agents against such infrastructure and their operating companies.

Threats Agents
1) **Motivation:**
2) **Motivation:**

[1 point] 3. Suggest, in rough order of prevalence (i.e., frequency), the most likely potential security threat agents against such infrastructure and their operating companies.

1. Hackers and cybercriminals: These may include individuals or groups that use various techniques to gain unauthorized access to the tracking device's network and infrastructure and steal or misuse the personal information and location data of users.
2. Insider threats: These may include current or former employees of the tracking device companies who have access to sensitive information and could misuse it for personal gain or to disrupt the service.
3. State-sponsored actors: These may include nation-states or agents targeting the tracking device companies for political or strategic reasons.
4. Competitors: These may include other companies that operate in the same space and may try to gain an advantage by stealing proprietary technology or information.

[1 point] 4. Suggest, in rough order of prevalence (i.e., frequency), the most likely potential security solutions that can be deployed to counter the threats and threat agents identified in the previous questions.

[1 point] 4. Suggest, in rough order of prevalence (i.e., frequency), the most likely potential security solutions that can be deployed to counter the threats and threat agents identified in the previous questions.

1. Encryption: Encrypting personal information and location data, both in transit and at rest, can help protect it from unauthorized access and misuse.
2. Multi-factor authentication: Implementing multi-factor authentication, such as using a password and a biometric factor, can ensure that only authorized users can access personal information and location data.

The End