Computer Security
Exercises

Christian Rossi

Academic Year 2023-2024

Abstract

The course topics are:

- Introduction to information security.
- A short introduction to cryptography.
- Authentication.
- Authorization and access control.
- Software vulnerabilities.
- Secure networking architectures.
- Malicious software.

Contents

CHAPTER 1

Exercise session I

1.1 Exercise one

A small manufacturing company, known for being one of the most important producers of a specialized musical instrument, falls victim to a ransomware attack. This attack, initiated by malware designed to encrypt all files on the infected computer until a ransom is paid to the attacker, quickly spreads to all computers in use by the company.

1. Identify and describe the two most critical threats/risks in this scenario, including the at-risk asset and suggesting one or two possible countermeasures for each
2. Identify the possible threat agents based on the risks identified in point one.

Solution

1. The two most critical threats/risks in this scenario are:
    - Loss of business-critical data: this involves the potential loss of vital data such as key intellectual property, which could hinder the company's ability to continue producing its specialized goods.
        - Asset at risk: business-critical data.
        - Countermeasure: implement regular backups of all important data to ensure data recovery in case of an attack.
    - Loss of production time: the ransomware attack could result in significant downtime required to restore infected computers and systems, leading to a halt in production.
        - Asset at risk: company's production capabilities.
        - Countermeasure: implement redundant systems, isolate critical systems, and establish procedures for rapid disaster recovery to minimize downtime and economic losses.
2. The possible threat agents in this scenario are:
    - Cybercriminals: motivated by the potential for ransom payments, cybercriminals deploy ransomware attacks to extort money from victims.

- Competitors: a competitor may seek to damage the company's business operations or cause financial harm by disrupting production through a ransomware attack.
- Malicious traders: if the victim company is publicly listed, a malicious trader may exploit the resulting stock market decline caused by the ransomware attack for personal gain.

1.2 Exercise two

Consider a scenario involving a self-driving, internet-connected vehicle operating within a taxi service context:

1. Identify the three most valuable assets at risk in this scenario.
2. Suggest at least two potential attack surfaces on the vehicles.
3. Provide, in rough order of prevalence, the two most likely potential digital attacks against such vehicles and their operating companies.

Solution

1. The valuable assets at risk are: passengers inside the car, pedestrians and other individuals outside the car, and the vehicle itself.
2. Potential attack surfaces include:
   - The Controller Area Network (CAN) bus via the diagnostic port, which may be vulnerable to manipulation.
   - The remote interface to the car, which could be exploited if not properly secured.
3. Likely potential digital attacks include:
   - Local attack: an attacker inside the car may manipulate the packets transmitted on the CAN bus via the diagnostic port to gain control of the vehicle.
   - Remote attack: an attacker could manipulate communication between the car and the backend systems, potentially diverting the car to a different location or disrupting its normal operation.

1.3 Exercise three

Consider an Internet-connected smart speaker equipped with a voice-controlled intelligent virtual assistant, installed within a residence. The speaker is linked to a wireless network and connected to a cloud service account. It operates by continuously monitoring for a specific keyword. Upon detection of the keyword, the device records a brief audio clip, which is then uploaded to a cloud-based speech recognition service. Subsequently, the device executes the requested action as per the recognized command. These actions may include searching for specific information on the internet or interacting with the owner's cloud account. Additionally, the device functions as a home automation hub, allowing voice commands to control various smart devices such as lights, door locks, heating systems, and more.

1. Identify the most valuable assets at risk in this scenario.
2. Suggest at least two potential attack surfaces of this smart speaker.
3. Provide, in rough order of prevalence, the most likely potential digital attacks in this scenario.

Solution

1. The most valuable assets at risk in this scenario include:
   - Personal information such as musical preferences and location.
   - Owners' voice, which is recorded for commands and has the potential to capture unintended conversations due to the device's always-listening microphone.
   - The security of the actual house, particularly with the possibility of remotely controlling the door.
   - The reputation of the device vendor.
2. The potential attack surfaces of this smart speaker encompass:
   - The voice command interface.
   - The cloud backend, susceptible to exploits or data breaches.
   - The local network.
   - Physical access to the device.
3. The most likely potential digital attacks in this scenario involve:
   - Compromising the cloud vendor to access recordings, user data, and potentially gain control of the house.
   - Malicious voice commands issued by a physical person or via a recording, such as a deceptive TV advertisement or malware playing a command to exploit the virtual assistant.
   - Compromising the device from the local network to access information or monitor the user.

1.4 Exercise four

Consider the SmartCar device, a new plug-in device designed to monitor driving habits, patterns, and the location of a car via a smartphone application. All modern cars are equipped with an internal wired network that connects together all the electronic control units. This network is used to exchange commands and data, including safety-related ones. 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 or 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. Identify the most valuable assets at risk in this scenario.
2. Suggest at least two potential attack surfaces of the SmartCar device.
3. Suggest potential digital attacks in this scenario.

Solution

1. The most valuable assets at risk in this scenario include:
    - Life/Health of individuals: safety of people inside and around the car is paramount.
    - Owner's private driving data: confidential driving habits and patterns.
    - Device vendor/car manufacturer reputation: reputation of the device vendor and car manufacturer.
    - Vehicle: physical integrity and functionality of the vehicle.
    - Smartphone: security and privacy of the owner's smartphone.
2. Potential attack surfaces of this smart speaker:
    - Smartphone application: vulnerabilities in the application used to interact with the device.
    - Company's backend: weaknesses in the backend infrastructure and services.
    - Physical access to the vehicle: unauthorized access to the vehicle's physical components.
    - Bluetooth/cellular network: vulnerabilities in the communication channels used by the device.
3. The most likely potential digital attacks in this scenario are:
    - Compromise of company's backend: attackers may breach the company's backend to access user data and compromise safety by re-flashing the device or sending unauthorized data within the network.
    - Physical compromise of device: attackers could physically compromise the device to send remote commands to the vehicle.
    - Compromise of application: attackers may target the application to access user data or gather real-time data on specific users.

1.5 Exercise five

Consider object tracking devices, such as those developed by Apple or Tile, designed to assist in locating personal items like keys, bags, and electronic devices. These devices utilize a smartphone app and a crowdsourced network of devices emitting Bluetooth Low Energy 4.0

signals for location tracking. If reported as lost and detected by nearby smartphones running the tracking app, the device's location is anonymously updated for the owner. The devices also include features such as a built-in speaker for close-range sound alerts and a "Find My Phone" function to locate paired smartphones. They typically have a battery life of about one year, with easily replaceable batteries.

1. Identify the main assets at risk in this scenario. Suggest at least two assets.
2. Provide, in rough order of prevalence, the most likely potential security threats against such infrastructure and their operating companies.
3. Suggest, in rough order of prevalence, the most likely potential security threat agents against such infrastructure and their operating companies.
4. Recommend, in rough order of prevalence, potential security solutions to counter the identified threats and threat agents.

Solution

1. The primary assets at risk in this scenario include:
    - Personal information and location data: users rely on tracking devices to locate lost items, potentially sharing personal information and location data with the device's infrastructure and operating companies, as well as other users in the crowdsourced network. This data could be vulnerable to security breaches or mishandling by the company.
    - Physical assets: the tangible items being tracked, such as keys, bags, apparel, small electronic devices, and vehicles, are also at risk if lost or stolen, despite the assistance of tracking devices.
    - Network and infrastructure: the tracking devices depend on a network of smartphones and a centralized infrastructure for locating lost items, which could be compromised by cyberattacks or other security breaches.
    - Business reputation: failure to protect users' personal information and location data, or performance issues with the tracking devices, could lead to negative publicity and damage the company's reputation.
2. The most likely potential security threats against such infrastructure and their operating companies include:
    - Privacy concerns: users may have concerns about privacy as their location data is shared anonymously with other users via the crowdsourced network.
    - Security breaches: the infrastructure and operating companies could be vulnerable to security breaches, exposing personal information and location data of users.
    - Physical tampering and theft: tracking devices themselves could be tampered with or stolen, compromising personal information and location data.
    - Malware and cyberattacks: infrastructure and operating companies may face attacks that compromise personal information and location data, disrupting services.

- Denial of service: infrastructure and operating companies may be targeted with denial-of-service attacks, disrupting the service and preventing users from locating lost items.

3. The most likely potential security threat agents against such infrastructure and their operating companies include:

   - Hackers and cybercriminals: individuals or groups may attempt to gain unauthorized access to the network and infrastructure to steal or misuse personal information and location data.
   - Insider threats: current or former employees with access to sensitive information may misuse it for personal gain or to disrupt the service.
   - State-sponsored actors: nation-states or agents may target the companies for political or strategic reasons.
   - Competitors: other companies in the same industry may seek to gain an advantage by stealing proprietary technology or information.

4. The most likely potential security solutions to counter these threats and threat agents include:

   - Encryption: encrypting personal information and location data in transit and at rest can protect it from unauthorized access.
   - Multifactor authentication: implementing multifactor authentication, such as using passwords and biometric factors, can ensure only authorized users access personal information and location data.

CHAPTER 2

Exercise session II

2.1 Exercise one

Translate the given C code into assembly x86.

```
if (c == 0)
    a = b;
else
    a = -b;
```

Assume b is stored in EBX, c is stored in ECX, and a is stored in EAX.

Solution

The equivalent assembly code for the C program is as follows:

```
    mov edx, 0
    cmp ecx, edx
    jne ELSE
    mov eax, ebx
    jmp ENDIF
ELSE:
    mov eax, 0
    sub eax, ebx
ENDIF:
    nop
```

2.2 Exercise two

Translate the given C code into assembly x86.

```
a = 0;
for(i = 0; i < 10; i++)
    a += i;
```

Assume a is stored in EAX.

Solution

The equivalent assembly code for the C program is as follows:

```
    mov eax, 0
    mov ebx, 0
    mov ecx, 10
LOOP:
    cmp ebx, ecx
    jge END
    add eax, ebx
    inc ebx
    jmp LOOP
END:
    nop
```

CHAPTER 3

Exercise session III

3.1 Exercise one

Consider a data protection mechanism which encrypts an entire hard disk, block by block, by means of AES in Counter (CTR) mode, employing a 128 bit key. The system administrator, following a new directive which mandates keys to be at least 256 bits long, implements the following compatibility measure: it encrypts the volume again, with the same 128 bit key and counter. Argue on whether the method provides a security margin which is larger, smaller or the same with respect to the original encryption scheme.

1. Describe an alternative measure to comply with the directory, other than decrypting and re-encrypting the entire volume.

2. Considering the aforementioned scenario, is it possible to claim that the information on the disk cannot be tampered with in a meaningful way, given that all the information on disk is fully encrypted? Either support the claim or disprove it providing a practical example and a solution to prevent tampering.

Solution

1. The compatibility measure is actually decrypting the volume, as applying twice the AES-CTR encryption function with the same key and counter adds via xor the same pseudorandom pad to the ciphertext. The security margin is clearly lower than before: it's non-existent. Encrypting with AES-CTR and a different 128 bit key actually solves the decryption issue, and provides 256 bits of equivalent security (under the largely believed assumption that AES is not a group).

2. Encrypting data with AES in counter mode does not provide any protection against tampering. Indeed, an attacker could modify the ciphertext at her own will, knowing that a bit flip in the ciphertext will result in a bit flip in the plaintext, in the same position. Adding a message authentication code (MAC) to the data (e.g., disk-block-wise) prevents tampering altogether.

3.2 Exercise two

Consider the following authentication system. Each legitimate user generates a key pair for an asymmetric encryption scheme, and uploads on the server which should be authenticating her the corresponding public key. To get authenticated, the user draws a random string r, decrypts it with her own private key obtaining a string s, and sends the pair (r, s) to the server over a confidential and integrity preserving channel. The server encrypts s with the user's public key and checks if the result matches r, in which case it authenticates the user.

1. Argue on whether this system is providing proper authentication, either justifying why it is secure, or showing an attack and proposing a working countermeasure. To this end, consider an attacker which comes into possession of a user's public key k_{pub}.

2. Consider the following password-based authentication mechanism: you mandate that the user inputs six words, uniformly randomly drawn from an English dictionary (containing 2^{14} words). Whilst your users have been trained to randomly pick the words, you want to put up an extra layer of defenses, locking an account after some number n of failed attempts. Consider the following scenario: one user every eight picks two words from the dictionary at random, and repeats them three times. What is the value of n capping the probability of a successful sequence of n guesses to at most one in a billion? Justify your answer. Describe a simple check upon password enrollment/renewal, which is more effective than the guessing cap, and quantify its effectiveness.

Solution

1. The authentication system can be broken in the following way. The attacker picks a random string s', encrypts it with k_{pub} obtaining r', and sends (r', s') to the server. Switching the asymmetric primitive from an encryption to a signature scheme fixes the problem, as an attacker would need to randomly guess a valid signature string which can be verified with the user's public key.

2. Notice that the system does not prevent an attacker from trying to guess the passwords of multiple accounts simultaneously: the accounts will be locked only when the failed attempts against a single account are more than n. As a consequence, we can assume that the attacker will always be hitting at least an account of a user with poor password policies. This results in a single guess succeeding with probability $(2^{-14})^2 = 2^{-28}$, which is already higher than our target ($\sim 2^{-30}$). No cap can improve this. A simple check upon password enrollment is to test that at least a subset of the words composing the password are different. While this reduces the possible passwords, it does so by a negligible amount. As an example consider testing that at least four words are different: this reduces the number of potential passwords from 2^{84} to $2^{84-(2^{14}+20\cdot 2^{28}+30\cdot 2^{42})} < 2^{84-(32\cdot 2^{42})} = 2^{84-(2^{47})}$, which is still way larger than 2^{83}, thus definitely large enough.