Chapter 2
Security Analysis of Information Technology

Madhusudan Singh

Abstract As we know security is always important challenges in technology. In cyberworld is full of lack of security. We need to protect our cyber worlds in real time. This article has described basics of security, security impact and provide and an overview on security areas and their vulnerable places in our cyber world such as Computer security, Network Security, and Cyber security. These security features must not be limited to protecting confidential information, but also needs to address safety critical systems such as brake, accelerator or steering etc.

Keywords Security · Cyber security intelligent vehicle · Autonomous vehicles · Information security

2.1 Introduction

Security is protected the assets of the system from malicious vulnerability and mitigate their impact on the system. The assets can be possible any object or entity or system of any organization or organization itself. Any assets can be exploited by attacker/hacker for their own benefits due existing vulnerability in the system. The attackers/hackers exploit the system with the help of system vulnerability and, it has made possible to illegally access the system or modify any asset of the system. The malicious users (Attacker/Hacker/Unauthorized) can find a single week point as individual or as group in a system or framework and targeting that single to harm or damage or illegally access the whole system information or that system itself [1]. In Fig. 2.1, we can see the security requires in every area, digital (e.g., Internet), physical (e.g., vehicle), and non-physical (e.g., Wireless environment).

The security resources are itself very important assets of any system that should be protect the system against malicious threats and attacks. The environment of

M. Singh (✉)
School of Technology Studies, Endicott College of International Studies, Woosong University, Daejeon, Republic of Korea
e-mail: msingh@wsu.ac.kr

M. Singh, *Information Security of Intelligent Vehicles Communication*,
Studies in Computational Intelligence 978,
https://doi.org/10.1007/978-981-16-2217-5_2

Fig. 2.1 Overview of security

the system and environment are impact each other such as if security assets are environment friendly then it has added on for system environment and vice versa.

The rest of the chapter is organized as follows. Section 2.2 discussed the concept of security; Sect. 2.3 gives the overview of computer security with the network security. Section 2.4 presents vulnerabilities and attacks in computer/IT Security. Section 2.5 describe the details of security goals and final Sect. 2.6 has conclude security details.

2.2 Security Conceptual

There are certain conceptual definitions of security which comes across now and then, whenever security is referred in different security areas [2]. Figure 2.2 has shown the different way of security concept.

- ***Security Objective***: A statement stating high level organization's security goals and business security needs to achieve.
- ***Constraint***: A restriction that provide hindrance so that the security objectives can be achieved.
- ***Security Mechanism***: A mechanism that detects, prevent, and mitigate the harm done by an attack.
- ***Threats***: A harm or danger or potential loss to the assets.
- ***Vulnerability***: A fault, flaw or weakness which can be exploited by a threat.

Fig. 2.2 Security conceptual

- ***Defense in Depth***: An absolute range of multiple layers of security protection measures for the overall security of the system.
- ***Risk***: An event that could compromise the critical assets of the system.
- ***Policy***: Security rules which put constraints on the users of the system to abide by these rules for the protection of the system.
- ***Countermeasure***: Security measures used to mitigate threats to achieve the security objective.
- ***Assurance***: A confident declaration that the security mechanism will meet the expectation.
- ***Resilience***: The potential ability to retrieve swiftly from harm, attacks, and threats.

2.3 Overview of Computer Security

The computer security ensure that peripherals of computer system are protected from outsider and achieved the tried protection features which are CIA (Confidentiality, Integrity, Availability). A computer has basic components which are hardware, software, firmware, and data which are termed as the main assets in any computer system.

2.3.1 Computer Protection

There are malicious users, intruders and hackers who hack, steal, and modify your personal and critical assets. Assets can be any important data, information, bank money or anything which is important to you. We can protect our assets by following simple but very useful steps. In Fig. 2.3, we can see ways of the computer security.

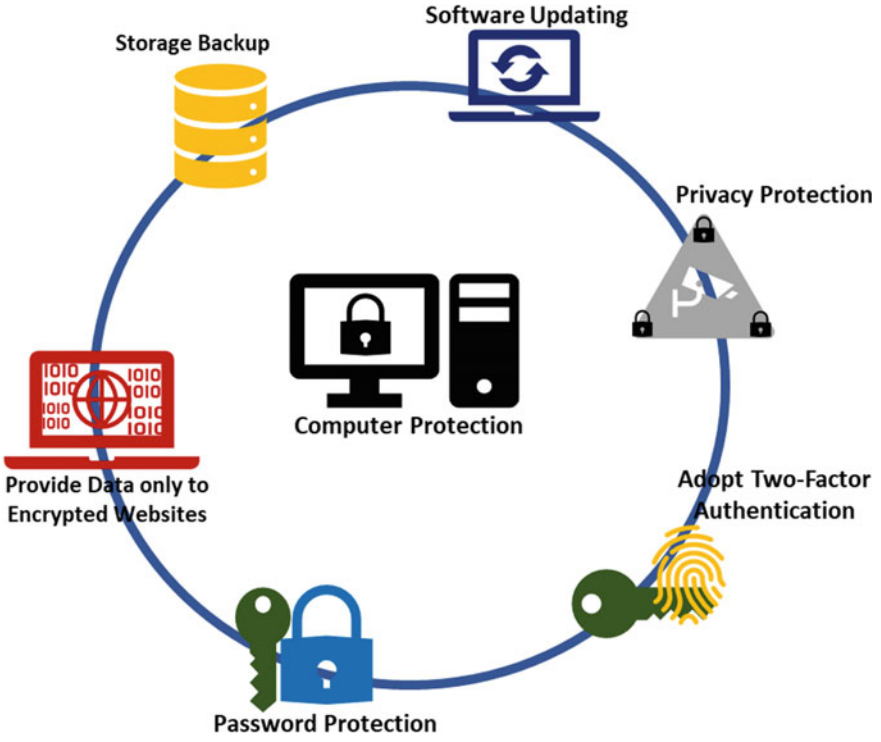

Fig. 2.3 Ways of computer protection

They are described as follows:

- **Software Updating**

Systems software's, Application software's and programming software's should be refreshed routinely, particularly the internet browsers that are utilized for associating the Internet on the grounds that doing so can shield them from more up to date and lately developed attacks and threats that infected your software's and in the long run your PC. It is imperative to introduce great observing applications, which can identify the infectious virus and alleviate the issues it caused.

Software Updating

- **Privacy Protection**

It is not wise to trust any email, webpage, phone call or message and share your private information. There are many spams and phishing activities which steal, and hack your important assets, such as your important card numbers, bank account, and security numbers and passwords. Be aware and know of such witty scammers as they act very trustworthy and reliable.

Privacy Protection

- **Password Protection**

We may have come across such login sites which do not accept an only alphabet, or only numbers or only alpha numeric or only special character passwords. They accept your password which has numbers, alphabets, and special characters all together. This combined password is termed to be very strong and not easy to guess or hack.

Password Protection

Below are mentioned some ways to make your passwords strong enough to keep them safe from hackers.

- Try to form long passwords combining numbers, alphabets, and special characters, not less than 10 characters. You may also use Capital letters and small letters together.
- Try not to make obvious passwords which resemble your name, date of birth, dates or ordered numbers, instead try something unique combination of numbers, alphabets, and special characters.
- Try not to use similar password for many of your accounts. If your password is stolen, then all your accounts are at risk.
- Don't ever share your passwords by texting, emailing or via voice.
- If you are liable to forget your password, then be cautious to keep your written password safely out of reach of everyone.

- **Adopt Two-Factor Authentication**

As the name suggests Two Factor Authentication utilizes two factors for authenticating your identity. One factor is your password, and the other factor may be a simple code sent to your mobile phone registered with your account or any random alphabet or number generated by an application [3]. So, even if your password is compromised, the second factor can be saving your account from hacking.

- **Provide Data Only to Encrypted Websites**

During internet shopping, use only encrypted websites. These sites will encrypt the personal information in your computer before sending it to the website's server. The websites which use encryption use Hyper Text Transfer Protocol Secure (HTTPS) before the web address [4]. This is different from the commonly used HTTP as it uses an additional S which stands for secure.

- **Storage Backup**

Never re-lie on single storage of your important files. Always make a backup of your important files to other storage mediums. Even if your computer is compromised, you can still have access to your files via alternate storage [5].

2.3.2 Overview of Network Security

Network security is a vast topic and is an area of specialization to the Information Technology (IT). Internet users are getting aware of the importance of Security and its role. In the recent years a huge number of internet users are exploring security associated websites. The Banking applications ask to install security plugins or programs before any transaction of money. The security certifications have gain popularity. Biometric security measures such as fingerprint and retina identification which were once read only in science fictions have become very common and adopted by a lot of gadgets for secure authentication. Although, the awareness and importance of security has increased, still many organizations when developing a technology or a gadget; give a secondary thought to security after development being the primary [6]. They don't have a well sought out plan for security from the very initial phase of elicitation of requirements and planning. Computer security ranges from protecting

Fig. 2.4 Network security overview

the hardware, software and the information broken into bits. Figure 2.4 has shown the overview of network security.

Next, we describe the vulnerabilities in the network and the importance of network security and later, we will discuss the methods to overcome them.

- **Wired and Wireless Physical Networks**

In a wired network, as the names suggests that computers are connected through wires; wire can be copper wire, twisted pair or fiber optic. Wired networks work on the principles of Ethernet protocol. Computers are first connected to wires or the Unshielded Twisted Pair (UTP) cables, which in turn are connected to multiple switches and which further are connected to the router for internet connectivity. In Fig. 2.5 has represents the wired network.

In Fig. 2.6 has shown the wireless network.

In contrast the wireless network as the name suggests, the computers are not connected with wire instead they are connected to access points via radio transmissions [6]. Further, the access points are connected via cables to switch/router for internet connectivity.

Although both wired and wireless networks are used in organizations the wireless networks are more popular than wired networks because of the factor of mobility. Advantage of wireless networks is that multiple devices can be used remotely and can share files and resources remotely. Wireless networks increase accessibility and ease of use.

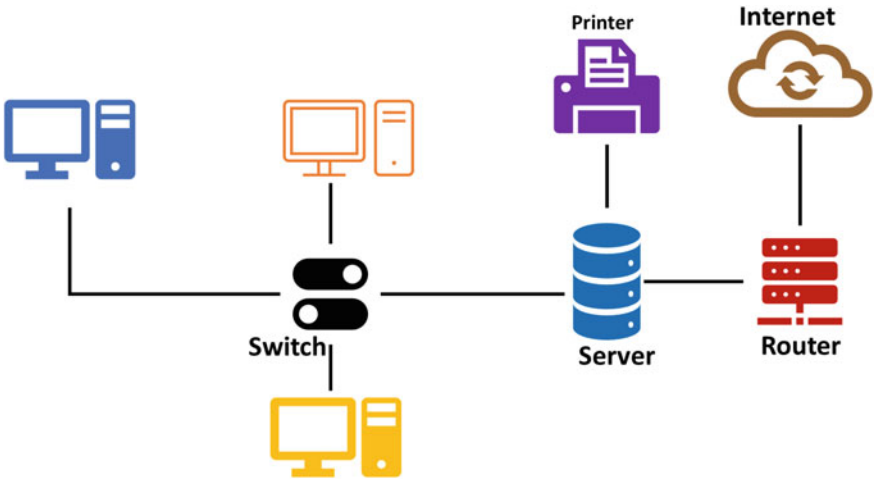

Fig. 2.5 Wired network

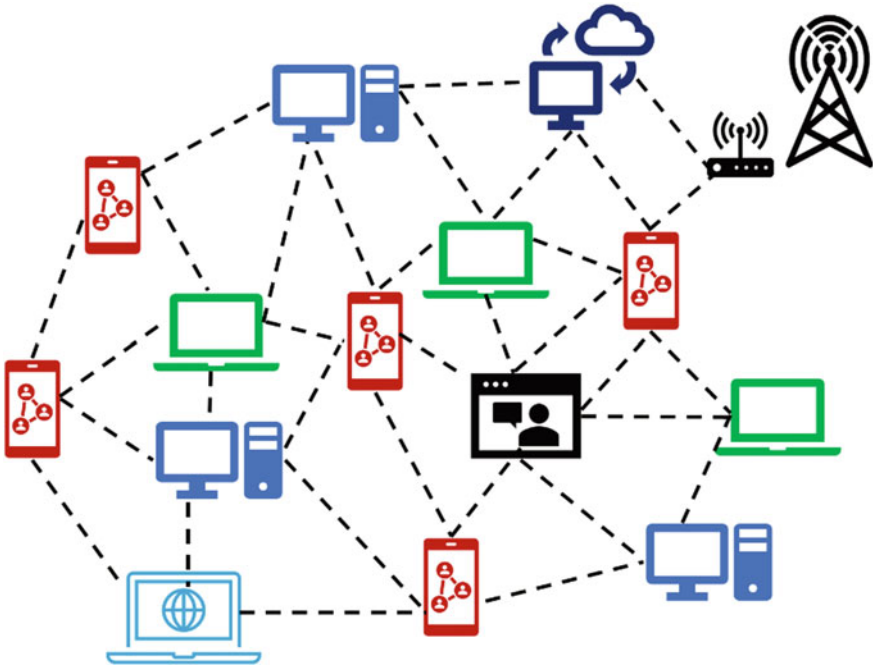

Fig. 2.6 Wireless networks

2.4 Vulnerabilities and Attacks

If we talk about vulnerabilities and attacks in terms of wired and wireless networks, then attacker can be easily attack on wireless networks due it's unsecure switch port and to attack on switch port attackers doesn't require any essential physical connection for device [7]. The most common vulnerability in wired and wireless networks is accessing the network unauthorized way. At below, we can find some other vulnerabilities that can place after unauthorized.

- Attackers' attacks during the data transmission in the networks and sniffing the data packet.
- Attackers can transmit the bogus information in the network and overloaded with unauthentic data.
- Attacker placed himself between receiver and sender nodes within the network and the MAC addresses of authentic hosts are spoofed to capture data and induce Man-in-the-middle attack.

Therefore, we cannot take security as non-essential elements in networks. Security is very important elements for the system, and we must be think beginning of any system designing and implementation to remove vulnerabilities from the network.

2.5 Security Goals

It is essential to have successful primitives to guarantee the security of the nodes in a vehicular network. All in all, tending to the security of any system requires the accompanying security administrations: confidentiality, integrity assurance, availability, authentication, and non-repudiation. The automobile system also requires having these security services in order to provide safe and appropriate operation of the system. Figure 2.7 shows the security goals.

As shown in Fig. 2.7 security goals are discussed below:

2.5.1 Confidentiality

A confidentiality mechanism guarantees the secrecy of the transmitted information by guaranteeing that the message isn't unveiled to an unapproved client/user. Confidentiality can be accomplished by utilizing cryptographic primitives that gives encryption/decryption functionalities. These type of cryptographic primitives transforms the message in such a way that only legitimate nodes (e.g., sender and receiver) can comprehend the actual meaning of the message while it seems meaningless to the other nodes.

Fig. 2.7 Security goals

2.5.2 Integrity Assurance

Integrity assurance (often also referred as data integrity) of a message provides the receiver with an assurance that the data has not been modified during transmission. Data integrity affirmation can be accomplished by utilizing a Message Authentication Code (MAC) tag. Note that this system doesn't keep an assailant from altering the message, rather it gives the collector an intend to identify unapproved alteration of the message.

2.5.3 Availability

Availability ensures information assets such as session key and applications are accessible by the authorized users. Cryptographic techniques cannot provide availability. Rather availability can be ensured by having proper backups, redundant units/paths etc.

2.5.4 User Authentication

User authentication is the process of verifying something to be true. Particularly a system needs to verify the ID, location, and property of the sender. In general authentication is the mechanism that verifies the claimed identity of a user. This guarantees the received message is really from the sender who he/she is professing to be. Cryptographic procedures, for example, the digital signature can be utilized to give client/user verification. These are systems where one party (sender) can sign the message utilizing a digital signature, while the other party (collector) can confirm the message is really from the authorized sender or not.

2.5.5 Non-repudiation

Non-repudiation ensures that the network entities (sender and receiver) cannot falsely deny a prior communication.

2.5.6 Network Security Goals

As discussed so far, we realize that there are huge weakness in the any network even data transmission within network does not reliable it's vulnerable with attacks. Firstly,

Fig. 2.8 Network security goals

attacker transmits an enormously data in network and based on that data it's acquiring the communication channel and accessing the real transmits data and misused the network data. Figure 2.8 has represents the security goals of the networks.

The network security provides the security for the entire network and end to end connectivity. It does not target to secure the end devices only.

Network security has numerous secondary goals, for example, reliability, usability, integrity, and wellbeing of data and the network [8]. The essential goal of system security is the groups of three Security which are Confidentiality, Integrity, and Availability as shown in Fig. 2.8.

- ***Confidentiality***: The point is to secure the critical assets (information) from unapproved clients in confidentiality. The confidentiality for security guarantees that the critical elements are open just to approved clients.
- ***Integrity***: This aims to ensure that the data is not modified or tampered by unauthorized users during its transmission in the network.
- ***Availability***: The aim of availability to assure that availability of resources and data are available, whenever it requested by the legal and authorized users.

2.6 Summary

We studied at the beginning of this chapter that Security is the protection of critical assets of the system. There are some common terms such as Cybersecurity, IT Security, Network Security, and Computer Security. All their aim is protection of computer systems, their hardware, software, and their data from damage, harm or attack from unauthorized users. The cybersecurity is extending and emerging essential part of every level in the technology such as supercomputer to smallest communication device or technology.

Acknowledgements This research was funded by Woosong University Academic Research in 2021.

References

1. A. Alshnoul, Information systems security measures and countermeasures: protecting organizational assets from malicious attacks. Commun. IBIMA **2010**, 1–9. Article ID 486878 (2010). IBIMA Publishing
2. B.B. Naik, D. Singh, A.B. Samaddar, H.-J. Lee, Security attacks on information-centric networking for healthcare system, in *19th International Conference on Advanced Communication Technology (ICACT)*, South Korea, 19–22 Feb 2017, pp. 436–441
3. J. Browning, *White Paper: Protecting Your Assets: Information Security in the Teradata Database* (TERDATA, US, 2015)
4. R. Zhuang, A.G. Bardas, S.A. DeLoach, X. Ou, A theory of cyber attacks, in *Proceedings if the Second ACM Workshop on Moving Target Defense (MTD-15)* (2015)
5. N. Ahmad, M.K. Habib, Analysis of network security threats and vulnerabilities by development & implementation of a security network monitoring solution, Master thesis, Department of Telecommunication, Blekinge Institute of Technology, Sweden, 2016
6. M. Singh, S.-G. Lee, W.K. Tan, J.H. Lam, Throughput analysis of wireless mesh network testbed, in *International Conference on Convergence and Hybrid Information Technology (ICHIT-2011)*. CCIS, vol. 206, Daejeon, Korea (2011), pp. 54–61. https://doi.org/10.1007/978-3-642-24106-2_8
7. J. Thomas, Tutorials, Omnisecu, Primary Goals of Network Security-Confidentiality, Integrity and Availability (2017), https://www.omnisecu.com/ccna-security/primary-goals-of-network-security.php
8. M. Singh, Secure ID-based routing data communication in IoT. EAI Endorsed Trans. Internet Things **18**(6) (2018). ISSN 2424-1399. https://doi.org/10.4108/eai.15-1-2018.153566