

Professional Practices

2021

Major Project

**Information Security Risks in IT Profession**

**Information Security Risks in IT Profession**

***Self-Introduction:***

**ABDUL RAFEH** student of Sindh Madressatul Islam University from Karachi, Pakistan. Bachelors in computer science in progress. Research interest is Information Security Risks in IT Profession.

**Abstract:** Now a days we are living in “Information world”. Information is current in everywhere. Information is so necessary for us. If we favor to dealing with and doing any work, we constantly prefer to up-dated ourselves according to the cutting-edge and up to date information. If we are in training world or commercial enterprise world or any different kind of working world, then we all choose the required statistics in a much less losing time and the 2nd thing of required information is its “Security”. Security consists of private information, employer secrets, economic data, laptop equipment, and objects of country wide safety are positioned at threat if suited protection processes are not followed. Evaluating a hazard appetite aided in prioritizing and finding out ideal risks. From the analysis, it used to be deduced that human being posed the biggest Information security hazard through intentional/ accidental human error for this Information protection attention may be a primary device in overcoming these errors.

***Keywords:*** Security threats, security tools, security techniques.

**Introduction:** Today, information technology is used as a base to support the company's business strategy, improve service quality and business processes. In use, information technology will bring risks. Management of risk are things that need attention. Management of risks can reduce the risk of such as business processes that are not optimal, financial losses, declining reputation of the company, or the destruction of the company's business. To reduce damage to the information systems of the company's business process, there should be a risk management assessment. Security in general is the quality or state of being Secure, that is, to be free from harm. In a more operational sense, security is also taken steps to ensure the security of the country, people, things of value, etc. Therefore, the objective of security is to build protection against the enemies of those who would do damage, intentional or otherwise. Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure. The information security performs four important functions for an organization which is enables the safe operation of application implemented on the organization’s Information Technology (IT) systems, protect the data the organizations collects and use, safeguards the technology assets in use at the organization and lastly is protect the organization’s ability to function. The information security also enables the safe operation of application implemented on the organization’s Information Technology (IT) systems.

This is because to protect the data, the organization will have applied or install the appropriate software that will secure the data such as antivirus and others protected applications. So, information security is very important in an organization to protect the applications that implemented in organizations and protect the data store in computer as well. Besides protect the data, the application installed also need to be protect because it can contribute to information lost or damages.

To protect data, there are several methods of security protection that can be implemented.

* Software Firewall
* Smartcard Security
* Biometric Security
* Data backups
* Data encryption

There are several methods of physically protecting computer equipment:

* Use cable locks with equipment.
* Keep telecommunication rooms locked.
* Fit equipment with security screws.
* Use security cages around equipment.
* Label and install sensors, such as Radio Frequency Identification (RFID) tags, on equipment.
* Install physical alarms triggered by motion-detection sensors.
* Use webcams with motion-detection and surveillance software.

**METHODOLOGY:**

Potential threats to computer security:

* Internal Threats

Employees can cause a malicious threat or an accidental threat.

* External Threats

Outside users can attack in an unstructured or structured way.

Types of attacks to computer security:

* Physical

Theft, damage, or destruction to computer equipment.

* Data

Removal, corruption, denial of access, unauthorized access, or theft of information.

Spyware - distributed without user intervention or knowledge, monitors activity on the computer. Phishing - attacker pretends to represent a legitimate organization and asks for verification

of victim’s information such as password or username

Network security risks

The main security risk in today's network is:

* Availability
* Integrity
* Confidentiality
* Authenticity
* Non-repudiation

**Availability:**

Availability is essential to information security, because for any such system to satisfy its purpose, the information on it must be available as needed by any authorized personnel. There is a need for the computer systems that store the information, the safety controls that are employed to guard it, and the communication channels that access it to function in the correct manner. Availability systems make certain that they are available all the time, stopping disruptions to information service from the likes of power outages, system upgrades, or hardware failures.

**Integrity:**

The ability of data not to be modified without undergoing detection is what defines integrity in the information systems world. Integrity is regarded as being violated when any message is actively modified when it is still in transit. In the information security systems world, integrity is closely linked with data confidentiality. Most of the time, information security systems offer message integrity along with a guarantee that transmitted data remains confidential.

**Confidentiality:**

The definition of confidentiality is ensuring that no unauthorized people or systems ever get a hold of information that is not meant for them.

Violations of information systems confidentiality can take the shape and form of many things. As an example, just the act of permitting a person to look at the computer screen while you are showing data that is confidential may already rise to a breach of confidentiality. If a computing device that holds sensitive information about a company’s clients or employees is unlawfully taken and then resold, that is another case of a confidentiality violation; because of all these easy ways in which confidentiality can be breached, it must be made a high priority in companies alike.

**Authenticity:**

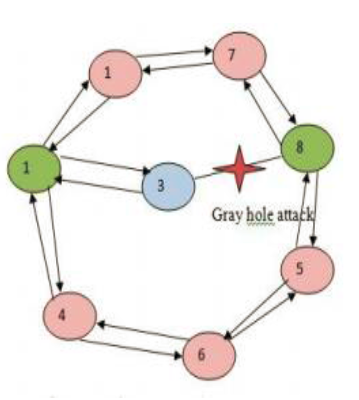
Authenticity is an integral component of information security. In the field of information security, as well as in the fields of e-Business and computing, it is of great importance to ensure the genuineness of physical or electronic documents, communications, transactions, and data. Such authenticity helps to reduce instances of fraud by way of misrepresentation. For further authenticity purposes, it is also important to verify that all parties in a transaction are who they really claim to be.

**Non-repudiation:**

The legal definition of non-repudiation is the implication of one party’s intent to satisfy their duties to a contract. Furthermore, it is also the implication that one party in a transaction is not allowed to deny having received a transaction, nor, conversely, is the other party permitted to deny having sent the transaction. E-commerce is the business of buying and selling services or products across electronic systems like the Internet. E-commerce is an example of an industry that utilizes technology like encryptions and digital signatures to establish non-repudiation in a transaction.

**Threats on each security risks with examples.**

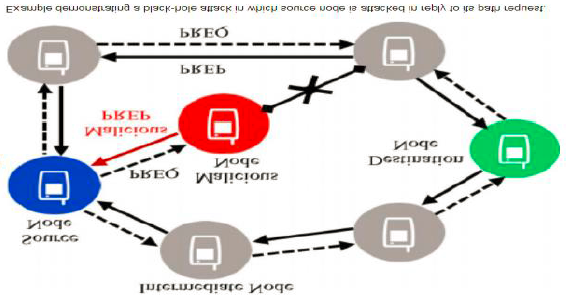
**THREATS ON AVAILABILITY:**

* Gray hole attack and black hole attack
* D2D Communication attack
* Flooding attack
* Jamming attack
* Coalition & Platooning Attack

**Example of Grey hole attack:**

Gray-hole is an attackthat can switch from behaving genuine to sinkhole. Because it can act as normal node switch over to malicious node it becomes too typical to identify the state whether it us normal node or malicious node. It mostly damages the mesh networks.

**Example of Black hole attack:**

In networking, black holes refer to places in the networkwhere incoming or outgoing traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient.

This is called routing attack which harms the whole network.

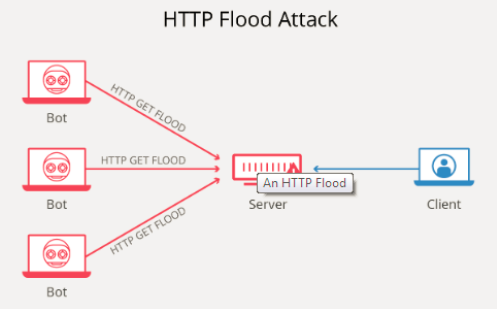
**D2D Communication Attack:**

Device-to-device (D2D) communications can effectively offload the traffic of cellular system in a distributed way. However, during the data forwarding process, malicious D2D users can intermittently discard data of other users, which seriously affects the data forwarding efficiency.

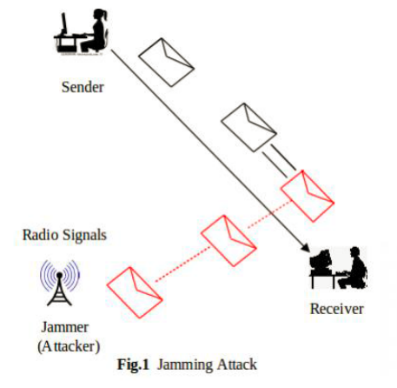
D2D users communicate directly with cellular-assigned links, which allows attackers sneak into the server or user applications, steal personal data and violate user privacy. Due to the nature of radio broadcast, attackers may launch denial of service, man in the middle, free rides, impersonate attack and other kinds of attacks during the data transmission process. In particular, some malicious users may discard the data received from other users, which results in communication failures.

Therefore, a malicious forwarding-behavior-aware D2D link selection mechanism is proposed to analyze the trust relationship among users, prevent malicious users from disrupting the network and attacking users in the network, choose the most credible relay user, reduce the corresponding risk and increase the data delivery rate.

**Flooding Attack:**

Flooding is a Denial of Service (DoS) attack that is designed to bring a network or service down by flooding it with large amounts of traffic. Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the hosts memory buffer. Once this buffer is full no further connections can be made, and the result is a Denial of Service.

An HTTP flood attack is a type of volumetric distributed denial-of-service (DDoS) attack designed to overwhelm a targeted server with HTTP requests. Once the target has been saturated with requests and is unable to respond to normal traffic, denial-of-service will occur for additional requests from actual users.



**Jamming Attack:**

Jamming attacks are a subset of denial of service (DoS) attacks in which malicious nodes block legitimate communication by causing intentional interference in networks.

**Coalition and Platooning attack:**

Data is transferring continuously so the attack jams the packet which was sending and the packet will not reach towards its destination.

**THREATS ON NON-REPUDIATION:**

**Threat #1 DOS Error & DDOS Error**

**Security Solutions**

* Monitoring the packets to save your server from the entrance of the counterfeit packets.
* Timely upgrading of the security patches on your host’s operating system.
* Beware of running of your server very close to the last level of the capacity.

**Threat #2 Unauthorized Access**

**Security Solutions**

* Enforce strong authentication strategies.
* Keeping usernames and passwords secret from the unreliable sources.
* Not providing unnecessary access to any user or even to any employee.

**Threat #3 Eavesdropping**

**Security Solutions**

* Entertaining encryption strategy will secure you a way out from eavesdropping. Using encryption measures like digital certificates (SSL certificates) will definitely lessen the risk of eavesdropping attacks.
* Apply network segmentation which will prevent eavesdropping as well as other network attacks.
* Employing Network Access Control enhances the security of your network by checking the authenticity of every device before establishing any connection.

**Threat #4 IP Spoofing**

**Security Solutions**

* Filtering of packets entering into the network is one of the methods of preventing Spoofing. In
* other hand, filtering of incoming and outgoing traffic should also be implemented.
* ACLs helps prevent Spoofing by not allowing falsified IP addresses to enter.
* Accreditation to encryption should be provided in order to allow only trusted hosts to communicate with.
* SSL certificates should be used to reduce the risk of spoofing at a greater extent.

**Threat #5 GPS spoofing Attack:**

* Install GNSS antennas in areas where they are not visible to the public, or set up barriers such as plastic fencing that would hide their location without interfering with signals.
* Ideally, the antenna location should have a clear view of the sky, but buildings or other structures block signals from the ground and other nearby public locations.
* Blocking antennas can help protect against interference and jamming, and reduce the danger of spoofing signals.
* Rubidium or Cesium clocks can serve as backup timing systems and inertial sensors can help determine position until GPS reception is restored.

**Recovering Tools or Software to Recover Attack**

**Cryptographic System:**

Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.

**Firewall:**

The firewall is a typical border control mechanism or perimeter defense. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside.

A firewall is the front-line defense mechanism against intruders to enter in the system. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. The most widely sold solution to the problems of Internet security is the firewall. This is a machine that stands between a local network and the Internet, and filters out traffic that might be harmful. The idea of a "solution in a box" has great appeal to many organizations, and is now so widely accepted that it’s seen as an essential part of corporate due diligence. Firewalls come in basically three flavors, depending on whether they filter at the IP packet level, at the TCP session level, or at the application level.

**Cloud Cracker:**

Cloud Cracker is the online password cracking tool for cracking WPA protected Wi-Fi networks. This tool can also be used to crack different password hashes. Just upload the handshake file, enter the network name and start the tool. This tool has a huge dictionary of around 300 million words to perform attacks.

**Comm View for Wi-Fi:**

Comm View for Wi-Fi is another popular wireless monitor and packet analyzer tool. It comes with an easy-to-understand GUI. It works fine with 802.11 a/b/g/n/ac networks. It captures every packet and displays useful information as a list. You can get useful information like access points, stations, signal strength, network connections and protocol distribution. Captured packets can be decrypted by user-defined WEP or WPA keys. This tool is basically for Wi-Fi network admins, security professionals, and home users who want to monitor their Wi-Fi traffic and programmers working on software for wireless networks.

**CONCLUSION:**

The foremost threats faced with the aid of these assets are human mistakes from staffs, SQL injections, records breaches, fraud, cross-site scripting, data theft, social engineering and energy

interruptions which are responsible for the most prominent facts security dangers in the employer. Appropriate enterprise-widespread administrative, technical and bodily controls have been employed to prevent, detect, mitigate and decrease the exploitation of vulnerabilities detected with the belongings. One essential challenge of this file is the scope of belongings used. It is very uncommon to have an organization with only 5 key belongings. We strongly propose that ISM practitioner’s paintings hand in hand with all stakeholders to ensure accurate facts for all belongings and their vulnerabilities are obtained. However, it ought to be noted that from this document, one ought to be capable of observe systematically the processes and technicalities undertaken in making ready a records security hazard evaluation and management report. Irrespective of the selection of organization for this record, the same ideas used in this document observe globally to all industry sectors. In this company record, a qualitative approach became used to evaluate the dangers. However, other firms would choose to adopt extra quantitative methods which use tough metrics, such as pounds or dollars. It will be common to find other terms like publicity factors, single loss expectancy, the annual price of occurrences, annualized loss expectancy and total cost of possession that all become getting used to address the same problem of dangers management. On combining with Risk Analysis, the Total Cost of Ownership and Return on Investment calculations must factor into right budgeting.

**Reference:**

* <https://www.researchgate.net/publication/331859493_Information_System_Security_Human_Aspects>
* <https://www.sciencedirect.com/science/article/pii/S1876610212005760>
* <https://www.sciencedirect.com/science/article/pii/S1877050918314558>
* <https://www.researchgate.net/publication/244989198_Information_Technology_Risk_Management_The_case_of_the_International_Islamic_University_Malaysia>