NETWORK SECURITY ATTACKS AND AVOIDANCE TECHNIQUES: A SURVEY

Kalyan Kumar Dasari[1], Dr.E.Srinivasa Reddy[2]

1Research scholar, Department of Computer Science & Engineering, Acharya Nagarjuna University, AP, India, dkkumar123@gmail.com
2 Professors, Department of Computer Science & Engineering, Acharya Nagarjuna University, AP, India, edara_67@yahoo.com.

Abstract

Network security has become more significant to personal computer users, public and private organizations, research & development organization and the military. With the arrival of the internet, security became a major roll and the history of security allows a enhanced understanding of the appearance of security technology. Due to rapid need of computer's in business and other organizations many networks has been constructed. In today scenario attacks on computer networks has drastically increased. Networks are very much needed but they are very prone to attacks because of security breaches and vulnerabilities in traditional establishments. There are many types of attacks which can be penetrated in our networks or edge devices. In this paper we would examine different types of attacks and avoidance techniques to secure our network.

Keywords: *Network Security Attacks; Security Avoidance techniques; Challenges*

---------- *** ----------

1. INTRODUCTION

The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. Based on this research, the future of network security is forecasted. New trends that are emerging will also be considered to understand.

1.1. Network security:

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a well-developed process that is based on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development.

When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, and decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message.
When developing a secure network, the following need to be considered:

- **Access** – authorized users are provided the means to communicate to and from a particular network.
- **Confidentiality** – Information in the network remains private.
- **Authentication** – Ensure the users of the network are who they say they are.

- **Integrity** – Ensure the message has not been modified in transit.
- **Non-repudiation** – Ensure the user does not refute that he used the network.

1.2. Differentiate Data Security and Network Security:

Data security is the aspect of security that allows a client's data to be transformed into unintelligible data for transmission. Even if this unintelligible data is intercepted, a key is needed to decode the message. This method of security is effective to a certain degree. Strong cryptography in the past can be easily broken today. Cryptographic methods have to continue to advance due to the advancement of the hackers as well.

When transferring cipher text over a network, it is helpful to have a secure network. This will allow for the cipher text to be protected, so that it is less likely for many people to even attempt to break the code. A secure network will also prevent someone from inserting unauthorized messages into the network. Therefore, hard ciphers are needed as well as attack-hard networks.

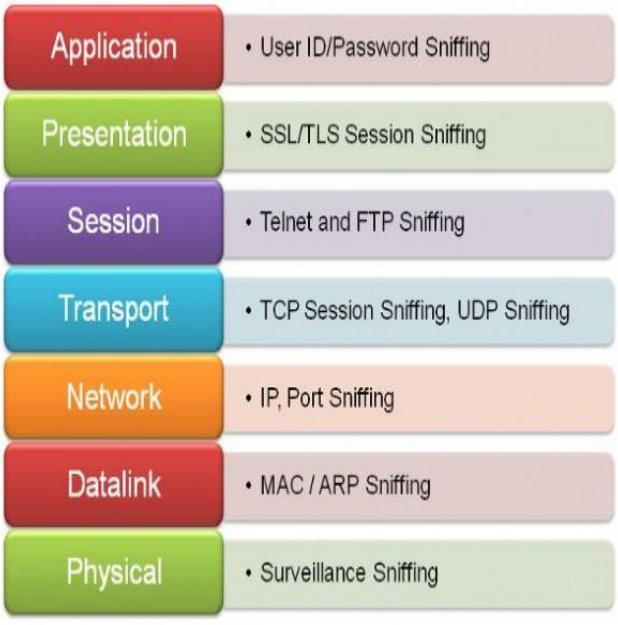

Fig 1.1: Based on the OSI model, data security and network

1.3. Security has a different security function.

The association of network security and data security to the OSI model is shown in Figure 1. It can be seen that the cryptography occurs at the application layer; therefore the application writers are aware of its existence. The user can possibly choose different methods of data security. Network security is mostly contained within the physical layer. Layers above the physical layers are also used to accomplish the network security required. Authentication is performed on a layer above the physical layer. Network security in the physical layer requires failure detection, attack detection mechanisms, and intelligent Countermeasure strategies.

2. SECURITY SERVICES FOR THE NETWORKS

2.1. Data Confidentiality:

Confidentiality is the ability to hide messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security.

2.2. Data Authentication:

Authentication ensures the reliability of the message by identifying its source. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject extra fake packets. Data authentication verifies the identity of the senders and receivers. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys.

2.3. Data Integrity:

Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed.
Even if the network has confidentiality measures, there is still a possibility that the data integrity has been compromised by alterations. The integrity of the network will be in trouble when:

- A malicious node present in the network injects fake information.
- Unbalanced conditions due to wireless channel cause damage or loss of data.

2.4.Data Availability:

Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network. Thus availability is of primary importance for maintaining an operational network. Finally data availability provides data to authorized persons at any time when they required.

2.5.Data Freshness:

Even if confidentiality and data integrity are assured, there is a need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. To solve this problem a nonce, or another time related counter, can be added into the packet to ensure data Freshness.

2.6.Self-Organization:

A wireless sensor network is a typically an ad hoc network, which requires every sensor node be self-determining and flexible enough to be self-organizing and self-remedial according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security.

2.7.Time management:

Most sensor network applications rely on some form of time synchronization. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications.

2.8.Secure Localization:

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pin point the location of a fault. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals.

3. ATTACKS ON NETWORKS

Without security measures and controls in place, your data might be subjected to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself. Your networks and data are vulnerable to any of the following types of attacks if you do not have a security plan in place.

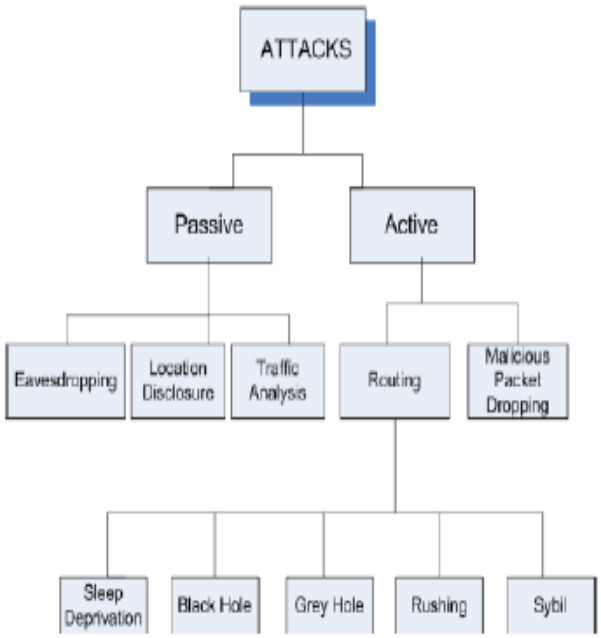

Fig 3.1: Basic types of attacks.

3.1. Eavesdropping:

Interception of communications by an unauthorized party is called eavesdropping. Passive eavesdropping is when the person only secretly listens to the networked messages. On the other hand, active eavesdropping is when the intruder listens and inserts something into the communication stream. This can lead to the messages being distorted. Sensitive information can be stolen this way.

3.2.Viruses:

Viruses are self-replication programs that use files to infect and propagate. Once a file is opened, the virus will activate within the system.

3.3. Worms:

A worm is similar to a virus because they both are self-replicating, but the worm does not require a file to allow it to propagate. There are two main types of worms, mass-mailing worms and network aware worms. Mass mailing worms use email as a means to infect other computers. Network-aware worms are a major problem for the Internet. A network-aware worm selects a target and once the worm accesses the target host, it can infect it by means of a Trojan or otherwise.

3.4. Trojans:

Trojans appear to be benign programs to the user, but will actually have some malicious purpose. Trojans usually carry some payload such as a virus.

3.5. Phishing:

Phishing is an attempt to obtain confidential information from an individual, group, or Organization. Phishes trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information.

3.6. IP Spoofing Attacks:

The address of a trusted computer in order to gain access to other computers. The identity of the intruder is hidden by different means making detection and prevention difficult. With the current IP protocol technology, IP spoofed packets cannot be eliminated.

3.7. Denial of Service:

Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service.

3.8. Node Subversion:

Capture of a node may reveal its information including disclosure of cryptographic keys and thus compromise the whole sensor network. A particular sensor might be captured, and information (key) stored on it might be obtained by an adversary.

3.9. Node Malfunction:

A malfunctioning node will generate inaccurate data that could expose the integrity of sensor network especially if it is a data-aggregating node such as a cluster leader.

3.10. Node Outage:

Node outage is the situation that occurs when a node stops its function. In the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the effects of node outages by providing an alternate route.

3.11. Physical Attacks:

Sensor networks typically operate in hostile outdoor environments. In such environments, the small form factor of the sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks, i.e., threats due to physical node destructions. Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.

3.12. Message Corruption:

Any modification of the content of a message by an attacker compromises its integrity.

3.13. False Node:

A false node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false data or prevents the passage of true data. Insertion of malicious node is one of the most dangerous attacks that can occur. Malicious code injected in the network could spread to all nodes, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary.

3.14. Node Replication Attacks:

Conceptually, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the node ID of an existing sensor node. A node replicated in this approach can severely disrupt sensor network's performance. Packets can be corrupted or even misrouted. This can result in a disconnected network, false

sensor readings, etc. If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor nodes. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether.

3.15. Passive Information Gathering:

An adversary with powerful resources can collect information from the sensor networks if it is not encrypted. An intruder with an appropriately powerful receiver indwells- designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques needs to be used. This section explained about the attacks and their classification that widely happens on wireless sensor networks. The next section discusses about the security mechanisms that are used to handle the attacks.

4. SECURITY MECHANISMS

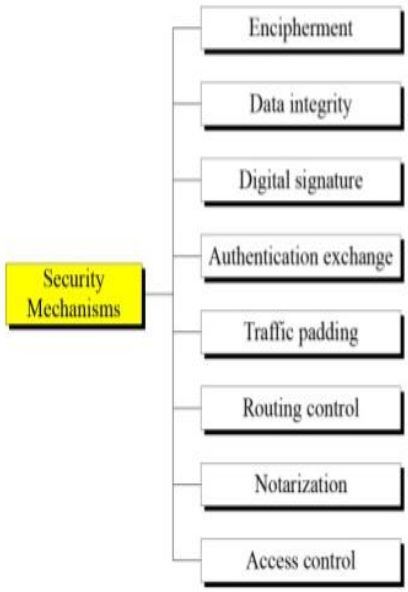

Fig 4.1: Types of Security Mechanisms

4.1. Encipherment:

Encipherment mechanisms are used either to protect the confidentiality of data units or traffic flow information or to support or complement other security mechanisms. The cryptographic techniques that are used for encipherment.

4.2. Data integrity mechanisms:

This type of mechanisms are used to protect the integrity of either single data units and fields within these data units or sequences of data units and fields within these sequences of data units. Note that data integrity mechanisms, in general, do not protect against replay attacks that work by recording and replaying previously sent valid messages. Also, protecting the integrity of a sequence of data units and fields within these data units generally requires some form of explicit ordering, such as sequence numbering, time-stamping, or cryptographic chaining.

4.3. Digital signature mechanisms:

Digital signature mechanisms are used to provide an electronic analog of handwritten signatures for electronic documents. Like handwritten signatures, digital signatures must not be forgeable; a recipient must be able to verify it, and the signer must not be able to repudiate it later. But unlike handwritten signatures, digital signatures incorporate the data (or the hash of the data) that are signed. Different data therefore result in different signatures even if the signatory is unchanged. Again, we postpone the discussion of digital signatures mechanisms.

4.4. Authentication exchange mechanisms:

These mechanisms are used to verify the claimed identities of principals. In accordance with ITU-T recommendation X.509 , we use the term strong to refer to an authentication exchange mechanism that uses cryptographic techniques to protect the messages that are exchanged, and weak to refer to an authentication exchange mechanism that does not do so. In general, weak authentication exchange mechanisms are vulnerable to passive wiretapping and replay attacks.

4.5. Traffic padding mechanisms:

Traffic padding mechanisms are used to protect against traffic analysis attacks. Traffic padding refers to the generation of spurious instances of communication, spurious data units, and spurious data within data units. The aim is not to reveal if data that are being transmitted actually represent and encode information. Consequently, traffic padding mechanisms can

only be effective if they are protected by some sort of a data confidentiality service.

4.6. Routing control mechanisms:

It can be used to choose either dynamically or by prearrangement specific routes for data transmission. Communicating systems may, on detection of persistent passive or active attacks, wish to instruct the network service provider to establish a connection via a different route. Similarly, data carrying certain security labels may be forbidden by a security policy to pass through certain networks or links.

4.7. Notarization mechanisms:

It can be used to assure certain properties of the data communicated between two or more entities, such as its integrity, origin, time, or destination. The assurance is provided by a trusted third party (TTP) in a testifiable manner.

4.8. Access control mechanisms:

It is used the authenticated identities of principals, information about these principals, or capabilities to determine and enforce access rights. If a principal attempts to use an unauthorized resource or an authorized resource with an improper type of access, the access control function rejects the attempt and may additionally report the incident for the purposes of generating an alarm and recording it as part of a security audit trail.

5. CONCLUSION

Network security is an important field that is increasingly gaining attention as the internet expands. The security threats and internet protocol were analyzed to determine the necessary security technology. The security technology is mostly software based, but many common hardware devices are used. The current development in network security is not very impressive. This paper summarizes the attacks and their classifications in wireless sensor networks and also an attempt has been made to explore the security mechanism widely used to handle those attacks. This survey will hopefully motivate future researchers to come up with smarter and more robust security mechanisms and make their network safer.

REFERENCES

[1]. John Paul Walters, Zhengqiang Liang, Weisong Shi, VipinChaudhary, “Wireless Sensor Network Security: A Survey”, Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006.

[2]. TahirNaeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, year 2009.

[3]. Adrian Perrig, John Stankovic, David Wagner, “Security in Wireless Sensor Networks” Communications of the ACM,Page53-57, year 2004.

[4]. Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously, "*Computer*, vol.31, no.9, pp.24-28, Sep 1998.

[5]. IanF. Akykildiz, Weilian Su, ogeshSankarasubramaniam, and ErdalCayirci, “A Survey on Sensor Networks”, IEEE Communication Magazine, year 2002.

[6]. Chris Karlof, David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, AdHoc Networks (elsevier), Page: 299-302, year 2003.

[7]. Pathan, A.S.K.; Hyung-Woo Lee; ChoongSeon Hong, “Security in wireless sensor networks: issues and challenges” Advanced Communication Technology (ICACT), Page(s):6, year 2006.

[8]. Al-Sakib Khan Pathan, Hyung-Woo Lee, ChoongSeon Hong, “Security in Wireless Sensor Networks: Issues and Challenges**”,** International conference on Advanced Computing Technologies**,** Page1043-1045, year 2006.

[9]. Zia, T.; Zomaya, A., “Security Issues in Wireless Sensor Networks”, Systems and Networks Communications (ICSNC) Page(s):40 – 40, year 2006

ABOUT THE AUTHOR:

1 **Mr. Kalyan Kumar Dasari** is research scholar, department of computer science & engineering, Acharya Nagarjuna University. dkkumar123@gmail.com.

2 **Dr. E. Srinivasa** Reddy is working as a professor in the department of computer science & engineering, at Acharya Nagarjuna University. edara_67@yahoo.com