Available online at http://www.journalijdr.com

IJDR

International Journal of
DEVELOPMENT RESEARCH

ISSN: 2230-9926

International Journal of Development Research
Vol. 07, Issue, 01, pp.11177-11180, January, 2017

Full Length Research Article

EAVESDROPPING ATTACK PROBLEM THREAT IN CYBER NETWORK SECURITY AND WIRELESS SENSOR NETWORK

***Umesh Sehgal, A.P. and Kamaljeet Singh, A.P**

GNA University, India

ARTICLE INFO

Article History:

Received 17th October, 2016
Received in revised form
25th November, 2016
Accepted 19th December, 2016
Published online 30th January, 2017

Key Words:

WSN and Sensor network.

ABSTRACT

Computer Security, also known as cyber security or IT security is the protection of computer systems from the theft or damage to the hardware. The field is of growing importance due to the increasing reliance on systems and the internet in most societies. Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For programs such as carnivore and narusinsight have been used in FBI and NSA to eavesdrop on the systems. In this research critical in almost any industry which uses computers, but 100 percent accurate and dependable to protect our data. There are many different ways of hacking into computers.

1. INTRODUCTION

The eavesdropping attack is a serious security threat to a wireless sensor network since the eavesdropping attack is a prerequisite for other attacks. Conventional WSNs consist of wireless nodes equipped with omnidirectional antennas, which broadcast radio signals in all directions and are consequently prone to the eavesdropping attacks (http://dsn.sagepub.com/content/9/8/760834.full). A Physical security, the motivations for breaches of computer security vary between attackers (csrc.nist.gov/groups/SMA/ispab/documents/csa_87.txt). Some are thrill seekers; others are activists or criminals looking for financial gain. A standard part of threat modeling for any particular system is to identify what motivate an attack on that system and to be secured. In this paper, we propose a model to analyze the eavesdropping probability in both single-hop WSNs and multichip WSNs with omnidirectional antennas and directional antennas. We verify the correctness of our analytical model by conducting extensive simulations. We have found that using directional antennas in either single-hop WSNs or multichip WSNs can significantly reduce the eavesdropping probability. The reason of the improved security of WSNs with directional antennas lies in

- The smaller exposure region of a directional antenna and
- The fewer hops to route a packet due to the longer transmission range of a directional antenna. Our results have also shown that the security improvement factor heavily depends on the node density, the antenna beam width, and the signal path loss factor.

1.1 Open Security Architecture

The Open Security Architecture organization defines IT security architecture as "the design artifacts that describe how the security controls (security countermeasures) are positioned, and how they relate to the overall information technology architecture (https://en.wikipedia.org/wiki/Cyber-security_regulation). These controls serve the purpose to maintain the system's quality attributes: confidentiality, integrity, availability, accountability and assurance services". Technopedia defines security architecture as "a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible". The key attributes of security architecture are.

- The relationship of different components and how they depend on each other.
- The determination of controls based on risk assessment, good practice, finances, and legal matters.
- The standardization of controls.

****Corresponding author: Umesh Sehgal, A.P.***
GNA University, India.

Conventional WSNs typically consist of nodes equipped with omnidirectional antennas which broadcast radio signals uniformly in all directions. Only a portion of these signals can reach the destinations and most of them are lost. This property of radiating signals omnidirectional inevitably leads to *high interference* and a *short transmission range*. Both these two factors severely limit the network performance of WSNs equipped with omnidirectional antennas. We call such networks as wireless omnidirectional sensor networks (*WONs*). Compared with omnidirectional antennas, directional antennas can concentrate most of radio signals on desired directions. In other undesired directions, there are no radio signals or the weakened signals. Therefore, using directional antennas in WSNs can potentially reduce the interference [5]. Besides, the transmission range can be significantly extended compared with omnidirectional antennas. We call such networks as directional-antennas wireless sensor networks (*DAWNs*).

2. IMPLEMENTATION METHODOLOGY

Hacking is ghastly increasing concept in current time where hackers use many sophisticated techniques to steal data from network or servers. Today we are going to discuss about one of the successful hacking techniques named Eavesdropping. What could happen if a person heeds your private communication without your awareness? The term in technical perspective named 'Eavesdropping'**.**

A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response (https://www.congress.gov/bill/100th-congress/house-bill/145). These processes are based on various policies and system components, which include the following:

- User account access controls and cryptography can protect systems files and data, respectively.
- Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware- or software-based.
- Intrusion Detection System (IDS) products are designed to detect network attacks in-progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.
- "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, a complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected (fas.org/irp/crs/RL32357.pdf).
- USB dongles are typically used in software licensing schemes to unlock software capabilities, but they can also be seen as a way to prevent unauthorized access to a computer or other device's software. The dongle, or key, (https://www.congress.gov/bill/100th-congress/ house-bill/145) essentially creates a secure encrypted tunnel between the software application and the key. The principle is that an encryption scheme on the dongle, such as Advanced Encryption Standard (AES) provides a stronger measure of security, since it is harder to hack and replicate the dongle than to simply copy the native software to another machine and use it. Another security application for dongles is to use them for accessing web-based content such as cloud software or Virtual Private Networks (VPNs).In addition, a USB dongle can be configured to lock or unlock a computer (www.journals.elsevier.com/computer-law-and-security-review/)
- Trusted platform modules (TPMs) secure devices by integrating cryptographic capabilities onto access devices, through the use of microprocessors, or so-called computers-on-a-chip (Emergence-of-Cyber security-Law.pdf). TPMs used in conjunction with server-side software offer a way to detect and authenticate hardware devices, preventing unauthorized network and data access.
- Computer case intrusion detection refers to a push-button switch which is triggered when a computer case is opened (Emergence-of-Cyber security-Law.pdf). The firmware or BIOS is programmed to show an alert to the operator when the computer is booted up the next time.
- Drive locks are essentially software tools to encrypt hard drives, making them inaccessible to thieves.[83] Tools exist specifically for encrypting external drives as well.
- Disabling USB ports is a security option for preventing unauthorized and malicious access to an otherwise secure computer. Infected USB dongles connected to a network from a computer inside the firewall are considered by the magazine Network World as the most common hardware threat facing computer networks.
- Mobile-enabled access devices are growing in popularity due to the ubiquitous nature of cell phones. Built-in capabilities such as Bluetooth, the newer Bluetooth low energy (LE), Near field communication (NFC) on non-iOS devices and biometric validation such as thumb print readers, as well as QR code reader software designed for mobile devices, offer new, secure ways for mobile phones to connect to access control systems. These control systems provide computer security and can also be used for controlling access to secure buildings.

2.1. Cyber security Present market in Eavesdropping

Cyber security is a fast growing field of IT concerned with reducing organizations risk of hack or data breach. The fastest increases in demand for cyber security workers are in industries managing increasing volumes of consumer data as finance and care (Emergence-of-Cyber security-Law.pdf). The cyber security attacks in eavesdropping. Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message and videoconference or fax transmission. The term eavesdrop derives from the practice of actually standing under the eaves of a house, listening to conversations inside. In case of email, if the email communication is not encrypted with digital signature, the eavesdropper could sniff the communication. He may alter the message before recipient receives it. The recipient believes that the message is coming from the original sender and surrenders his details to the attacker. Online shopping websites or social networking sites dictate users to login to access their respective accounts. There are even many payment service providers, financial agencies involved in online payment transactions. In the absence of encryption, eavesdroppers can sniff the plain text information during the transition of details like credit or debit card (http://dsn.sagepub.com/content/9/8/760834.full). Therefore, encryption should be there, which encodes the details to save from prying eyes and eavesdropping.

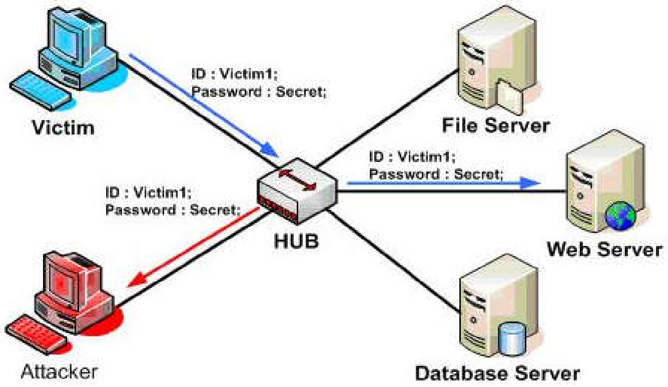

Fig. 2.1 Architecture of Eavesdropping

An attacker in search of sensitive data, catches and reads the transmitted packets from the network in the network eavesdropping attack. The captured data can be analyzed with eavesdropping tool. It is hard to detect network eavesdropping as it is a kind of passive attack (an attack that use information without affecting system resources). Network eavesdropping can be done on wired and wireless network. In a wired network, an eavesdropper has to be in touch with the wire of the network and can sniff packets using network tap (a hardware tool). While in wireless network, an unsecured wireless network attached to the computer could welcome eavesdropper to intercept or read the network packet coming from different network address with proper software tool. Eavesdropping is an unauthorized and illegal interception of a private communication. It refers to listening to the private conversions of two or more parties secretly. When an attacker listens to private communication is also referred to sniffing or snooping. Unexpectedly still major online communications take place in unsecured manner, which allows an attacker to gain access to network traffic by listening or interpreting the travelling information. Eavesdrop allows attackers to observe the network, is the major web security problem that network administrators face up in an organization. Eavesdroppers can make a successful attack in different ways, including wiretapping, email, and online chat. As the internet has expanded, people across the globe are using different web services. If all these services are not fully encrypted, then privacy of web users will be always at risk.

2.2 Security measures against Eavesdropping in cyber

- To prevent eavesdropping always use SSL protocol that makes online communication encrypted and secures the data over the internet. (https://www.cheapsslshop.com/blog/ eavesdropping-attack-a-dark-shadow-on-the-network).
- A firewall is a wise choice to protect the network traffic as it filters out the malicious or unauthorized access.
- Use Public key infrastructure that allows mutual verification. The server authenticates the user's computer before processing the transaction. The usage of PKI helps to diminish the risk of potential MITM (Man in the middle) attack.
- Network segmentation can provide ample security to the network as it restricts access to certain individuals related to network security and administration.
- The NAC (Network Access Control) used for endpoint security also defines the policy of securing a network. It ensures that the devices connected to the network are trusted.

As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data. Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying *as you* to keep the exchange going and gain more information. This attack is capable of the same damage as an application-layer attack.

3. Conclusion

Today, computer security comprises mainly "preventive" measures, like firewalls or an exit procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the Internet, and can be implemented as software running on the machine, hooking into the network stack (or, in the case of most UNIX-based operating systems such as Linux, built into the operating system kernel) to provide real time filtering and blocking. Another implementation is a so-called "physical firewall", which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet. Some organizations are turning to big data platforms, such as Apache Hadoop, to extend data accessibility and machine learning to detect advanced persistent threats. However, relatively few organizations maintain computer systems with effective detection systems, and fewer still have organized response mechanisms in place. As result, as Reuters points out: "Companies for the first time report they are losing more through electronic theft of data than physical stealing of assets". The primary obstacle to effective eradication of cybercrime could be traced to excessive reliance on firewalls and other automated "detection" systems. Yet it is basic evidence gathering by using packet capture appliances that puts criminals behind bars. Eavesdropping remains a concern for network administrator's which requires proper security measures proper security training about eavesdropping should be given to every level of any organizations.

4. REFERENCES

A MAC protocol for full exploitation of directional antennas in ad-hoc wireless networks Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '03) June 2003981072-s2.0-0242443784

Achieving maximum flow in interference-aware wireless sensor networks with smart antennas Ad Hoc Networks

2007568858962-s2.0-34248224574doi:10.1016/ j.adhoc. 2007.02.003

On the capacity improvement of Ad Hoc wireless networks using directional antennas Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '03) 2003108116doi:10.1145/ 778415.778429

On the capacity of multi-channel wireless networks using directional antennas Proceedings of the 27th IEEE

Pure directional transmission and reception algorithms in wireless Ad Hoc networks with directional antennas5 Proceedings of the IEEE International Conference on Communications (ICC '05)May 2005Seoul, Republic of Korea338633902-s2.0-24144473643doi:10. 1109/ICC.2005.1495049

Quantifying eavesdropping vulnerability in sensor networks Proceedings of the 2nd International Workshop on Data Management for Sensor Networks (DMSN '05)200539 doi: 10.1145/1080885.1080887

Transmission scheduling in Ad Hoc networks with directional antennas Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom '02) September 200248582-s2.0-0036953929

****