Goals and Different Types of Security Attacks in Networks

Dr. K. Kiran Kumar, N. Anusha, B. Anusha

Department of CSE, Chalapathi Institute of Engineering & Technology, Guntur

Abstract - The Computer network innovation is growing quickly, and the advancement of web innovation is all the more rapidly, individuals more mindful of the significance of the system security. System security is principle issue of figuring on the grounds that numerous kinds of assaults are expanding step by step. In versatile specially appointed system the hubs are autonomous. Ensuring PC and system security are basic issues. This paper introduces the objectives of system security and distinctive sorts of assaults in organize security layer.

Keywords: Technology, internet, security, confidentiality, availability.

I. INTRODUCTION

An assault can be dynamic or detached A "dynamic assault" endeavors to adjust assets or influence their operation.so it bargains trustworthiness or accessibility. An "inactive assault" framework[1] endeavors to learn or make utilization of data from the framework however does not influence framework resources.so it bargains secrecy. The significant objectives of system security are classification, Integrity, Availability. In this paper we are principally focused on the distinctive sorts of security assaults in arrange layer.

Goals of Network Security: The goals of network security are

- Confidentiality
- Integrity
- Availability

Confidentiality: Secrecy is generally proportionate to security. Measures attempted to guarantee classification are intended to keep touchy data from contacting the wrong individuals, while ensuring that the perfect individuals can in truth get it.

Integrity: It includes keeping up the consistency, precision, and dependability of information over its whole life cycle. Information must not be changed in travel, and steps must be taken to guarantee that information can't be modified by unapproved individuals (for instance, in a break of secrecy).

Availability: It includes keeping up the consistency, precision, and dependability of information over its whole life cycle. Information must not be changed in travel, and steps must be taken to guarantee that information[2] can't be modified by unapproved individuals (for instance, in a break of secrecy).

II. LITERATURE SURVEY

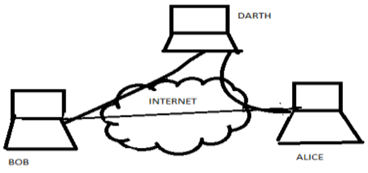
As already discussed in introduction, research on these vampire attacks is not adequate and the problems are not yet defined, evaluated, or mitigated in a comprehensive manner at the routing layer [11]. As we know that these vampire attacks are meant for resource depletion i.e., power exhaustion of the nodes batteries. These types of attacks obstruct nodes from incoming into a less power cycle, which is a result of which the batteries will not sleep and will drain really quick compared to normal situations. And the recent research works on the “denial-of-sleep attacks” only judges the attacks that generally happen at the MAC layer. Part from increasing the efficiency of underlying the routing protocols and MAC or switching away from source routing, effective mitigation[3] measures were not proposed in most of the works.

Different Types of Network Security Attacks are shown below

a) Internal Attacks: An inner assault happens when an individual or a gathering inside an association looks to disturb tasks or adventure authoritative resources. Much of the time, the aggressor utilizes a lot of assets[4], apparatuses and ability to dispatch an advanced PC assault and possibly evacuate any proof of that assault.

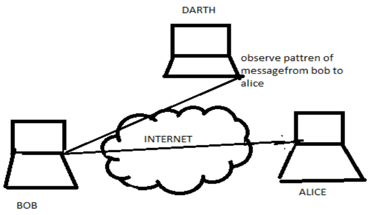
b) External Attacks: Outer assaults are done by hubs that don't have a place with the system. It causes blockage sends false steering data or causes sends false directing data or causes inaccessibility of administrations. These sorts of assaults endeavor to cause clog in the system, disavowal of administrations and promoting incorrectly steering External assaults[5] keep the system from typical correspondence and delivering extra overhead to the system. Outer assaults can arrange into two classes like dynamic and detached assaults

c) Passive Attack:



A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target. Passive attacks include active reconnaissance and passive reconnaissance.

d) Active Attacks:



An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target. Types of active attacks: In a masquerade attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges

e) Eavesdropping Attack: By and large, the lion's share of system interchanges happen in an unsecured arrangement, which permits an assailant who has accessed information ways in your system to "tune in" or decipher (read) the movement. At the point when an assailant is listening stealthily on your interchanges, it is alluded to as sniffing or snooping[6]. The capacity of a meddler to screen the system is for the most part the greatest security issue that directors look in a venture. Without solid encryption benefits that depend on cryptography, your information can be perused by others as it crosses the system.

f) Data Modification: After an aggressor has perused your information, the following legitimate advance is to adjust it. An assailant can change the information in the bundle without the learning of the sender or collector. Regardless of whether you don't require privacy for all correspondences, you don't need any of your messages to be changed in travel. For instance, in the event that you are trading buy demands, you don't need the things, sums, or charging data to be altered[7].

g) Identity Spoofing: (IP Address Spoofing) most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet. After gaining access to the network[8] with a valid IP address, the attacker can modify, reroute, or delete your data. The attacker can also conduct other types of attacks, as described in the following sections.

h) Password-Based Attacks: A common denominator of most operating system and network security plans is password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password. Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user. When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time. After gaining access to your network with a valid account.

i) Denial-of-Service Attack: Unlike a password-based attack, the denial-of-service attack prevents normal use of your computer or network by valid users. After gaining access to your network, the attacker can do any of the following

- Randomize the consideration of your inward Information Systems staff with the goal that they don't see the interruption instantly, which enables the aggressor to make more assaults amid the preoccupation.Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.

j) Man-in-the-Middle Attack: 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 aggressor can re-highway an information trade. At the point when PCs are imparting at low levels of the system layer, the PCs won't not have the capacity to decide with whom they are trading information. Man-in-the-center assaults resemble somebody accepting your character keeping in mind the end goal to peruse your message. The individual on the opposite end may trust it is you on the grounds that the assailant may be currently answering as you to keep the trade going and acquire data. This assault is equipped for an indistinguishable harm from an application-layer assault, depicted later in this area[9].

k) Compromised-Key Attack: A key is a mystery code or number important to decipher secured data. In spite of the fact that acquiring a key is a troublesome and asset serious process for an aggressor, it is conceivable. After an assailant acquires a key, that key is alluded to as a traded off key. An assailant utilizes the bargained key to access a secured correspondence without the sender or collector monitoring the assault. With the traded off key[10], the assailant can unscramble or change information, and endeavor to utilize the bargained key to process extra keys, which may permit the aggressor access to other secured interchanges.

l) Sniffer Attack: A *sniffer* is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted *and* the attacker does not have access to the key.

m) Application-Layer Attack: An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:

- Read, add, delete, or modify your data or operating system.
- Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.
- Introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or to corrupt your systems and network.
- Abnormally terminate your data applications or operating systems.

III. PROPOSED APPROACH

1) **Network Creation Module**: We have created the network with source, sink and six nodes named A, B, C, D, E, F. Each node is having a unique identification number and topology discovery is done at transmission time. Transmission of data is possible based upon the malicious nodes and honest nodes. If any malicious node is present in our network nodes then it will chooses the longest path or loops. We need to the fix the malicious node in the network otherwise it will corrupts the entire network nodes to be deployed and cannot control their positions.

2) Carousel attack Module: In this attack, malicious node composes the packets with purposely by introducing the routed loops. This is called as a carousel attack and it forwards the packets in the path form in the below figure. In these attacks, same node occurs so many times while routing the packet in the network. Mainly this attack is used to raise the length of the route.

3) **Stretch Attack Module:** In case of stretch attack, the adversary itself creates long paths by mainly traversing each and every node in the network. It increases the packet path lengths and it is shown in the figure. In a randomly generated topology, Carousel attack increases the energy consumption by a factor of 4, stretch attacks increments the usage of energy and it depends upon the malevolent node.

4) **Energy Level Identification Module:** In this module, we show the energy levels for each and every node to demonstrate the vampire attack affect. Here, node is permanently stops working once the bandwidth of the node are exhausted. Nodes can be recharged by active cycles. During frequent charging cases, power exhausting attacks are more dangerous if the adversary consumes more power rather than the nodes can recharge. Vampire attacks many honest nodes if the sending packet constitutes amplification.

5) **Secured Transmission Module:** In this module, we protect the nodes bandwidth and network from vampire attacks by sending the secured transmission. In this secured transmission data travels in the honest node and mitigates the vampire attack during the packet forwarding phase.

5) **Privacy Enhancing Technologies (PET) implementation** Privacy-Enhancing Technologies [9] is a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system.

6) **Disclosure containment for anonymous users** Social privacy provided using username and pass word provided by the each user (check profile details in developed applications) present in the network advancement. Verify each user details if that particular user was present or not in the online social network where the condition was checked by all the users if they are accessed services or not. Intruder detection was verified by the user name and password of each user, if that particular was present or not in his friends list. If user was not present in the processing online social networks then find his/her mail id as an intruder with specified foundation of online social security. Social independence security also verified by all the users present in the social security in data sharing process which was organized by the all the users present in the online social networks. If users were not interest to take updates from source of the application of social networks then he/she was also have permissions to stop their updates in presented application.

7) **Surveillance Results** When the others who are not friends for me are accessing my profile then by the intruder detection i get the message that includes how many times, what data is browsed for how much time in a day display on my wall. Depending on this surveillance report proper action can be taken if that particular person is a intruder[14].

IV. DISCUSSION

Who has the assurance to formulate what makes a security problem in network? Nowadays the social networks turn desegregated into unremarkable life, users incline to take them as a given, and are probably to describe on how they make do with the given intention. This farther restrains what can be disclosed through user studies. For example, a study that asks users to severely enlist in the values and ideologies implanted into a particular social network design, or to suppose radical design choices, may overtake participants and fail to furnish results.

How is the privacy problem in social networks enunciated? In security, one dispute prevarications in ascertaining the appropriate mechanisms through which social network users can bed is closed to complex and unintelligible privacy consequences. This may endue users to find their emplacements on matters that do not appear to directly affect them. How to behavior studies that surface the user view on abstract risks and impairments remains however an open question.

What is the background of the security problem? In the social privacy view, the privacy problems are consociated with boundary talks and decision making. Both expressions are pertained with willing actions, i.e., designated disclosures and interactions. Accordingly, user studies are more potential to arouse interests with respect to explicitly shared information than with respect to implicitly generated d information. In demarcation, PETs research is mainly pertained with ensuring privateness of data to unauthorized parties. Here, any information, explicit or implicit, that can be tapped to learn something about the users is of interest.

V. CONCLUSION

Computer Network security endeavors to guarantee the privacy, honesty, and accessibility of registering frameworks and their parts. Three primary parts of a registering framework are liable to assaults: equipment, programming, and information. In this paper we display security objectives and a portion of the security assaults. In next paper we will show the relief systems for these assaults.

REFERENCES

[1] William Stallings "CRYPTOGRAPHY AND NETWORK SECURITY" 4th Edition, (Pearson Education/PHI).

[2] Behrouz A.Forouzen ,"Cryptography & Network Security", TMH.

[3] Kaufman, Perlman, Speciner , "NETWORK SECURITY", 2nd Edition, (PHI / Eastern Economy Edition)

[4] Trappe & Washington, "Introduction to Cryptography with Coding Theory", 2/e, Pearson.

[5] I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom, 2004.

[6] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

[7] T. Aura, "Dos-Resistant Authentication with Client Puzzles," Proc. Int'l Workshop Security Protocols, 2001.

[8] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.

[9] D. Bernstein and P. Schwabe, "New AES Software Speed Records," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), 2008.

[10] D.J. Bernstein, "Syn Cookies," http://cr.yp.to/syncookies.html, 1996.

[11] I.F. Blaked, G. Seroussi, and N.P. Smart, Elliptic Curves in Cryptography, vol. 265. Cambridge Univ. , 1999.

[12] J.W. Bos, D.A. Osvik, and D. Stefan, "Fast Implementations of AES on Various Platforms," Cryptology ePrint Archive, Report 2009/ 501, http://eprint.iacr.org, 2009.

[13] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[14] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.