A Survey on System Attack Models

V.P. Ajay

Abstract--- *Managing Networks have become quite a task in the current scenario, due to many external challenges and threats to the security and integrity of our systems. The perfectly balanced solutions meant for providing ease of management and the actual implementation in real time are being given from many parts of the research community. The basic requirements which have been found to be vital for all types of sensor networks are protection of stored / transmitted information and the adaptability of systems to all new technologies. Though the technological developments of the sensor networks can be accommodated well enough with equal development of devices and framed standards, it is found to be difficult to cater to the needs of security requirements of sensor networks, both individually and as a whole.*

The growth of networks seems to have achieved great speed, in terms of both sizes and their importance. This shows us how important it is to weed out all security threats as well as to always stay ahead of all new attacks. Attacks may be of different levels from simple loss of information to shut down of the entire network permanently. Though it is impractical to have practical knowledge on all the types of attacks possible, it is however, possible to have a thorough theoretical knowledge of the same. This makes sure that it will be easier to form better solutions to prevent and eradicate the attacks through simple integration of inbuilt mechanisms.

Keywords--- *Active Attacks, Analytic Attacks, Network Attacks, Passive Attacks*

I. INTRODUCTION

WITHthe advent of high end technologies and better hardware solutions, attacks needed more time and higher end devices connected to high performance computers for even making an effort at attacking a network in earlier days. However, with more sophistication of computers, knowledge and better utilization of resources, attacks have become frequent and greatly potent.

Such advancements in the types of attacks have pushed us to rely more on our level of knowledge and so, we need frequent updates of the same to stay ahead of attackers at all times. The current terminologies include certain terms like hackers, black hat, white hat, spammer, cracker, phisher, phreaker and listener. Furthermore, the different forms of attacks may be classified into the following (table 1), based on the attackers' techniques and the domains used. They can also be divided into many sub categories, based on the network layers, cryptographic details, stealth level and network standards and by their nature of operation (active / passive).

Table 1: Classification of Attacks

S.No	Term	Explanation
1.	Hackers	Attempts unauthorized access
2.	Black Hat	Breaks into the networks without prior permission
3.	White Hat	Breaks into the network with prior permission
4.	Spammer	Sends unwanted messages / overloads server
5.	Cracker	Form of Black Hat
6.	Phisher	Makes us to divulge secure information by using "trick" emails
7.	Phreaker	Causes a network to perform a function which is not allowed
8.	Listener	Continuously listens to the network transmissions and prepares for thievery

II. CLASSIFICATIONS FOR ATTACKS

A. Layered Attacks

Attacks may be of different forms when seen inside each of the network layers.[9] This is because the signals of radio frequency are very easily disrupted, interrupted and , if needed.

Some of the commonly seen attack structures in the layers may be given as follows;

Table 2: Network Layers – Attack types

LAYER	ATTACKS FOUND
Physical Layer	Overhearing, Intercepting, signal disruption
Data Link Layer	Disrupt MAC layer, weakening of the WEP, Monitor and analysis of Traffic
Network Layer	Black-holes, Resource wastage, Worm-hole, Positioning attacks, overloading
Transport Layer	Sync overloading, Session duplication
Application Layer	Corrupts vital data, Repetition of data
Other Layers	Masquerading, session replay, DoS, Middle "man" attack

Many attacks are seen in all the layer levels of the network model and their inherent attack types may be tabulated as above.

V.P. Ajay, Department of Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India, E-mail: brittoajay@rediffmail.com

B. *Active / Passive Attacks*

These attacks are classified based on their ability to disrupt the communication links between systems.

Passive attacks are the ones which steal data exchanged in the network without disrupting the communication link in any way.

Active attacks are quite the opposite where they first disrupt the link and then utilize its full potential to completely get involved in data theft.

Some of the main types of such attacks may be tabulated as follows; (Table 3 & 4)

Table 3: Passive Attacks

PASSIVE ATTACKS	
ATTACKS	EXPLANATION
Traffic analysis	Intercepts data and scrutinizes the same
Monitoring traffic	Monitors data flow and tries to guess the access codes
Listening / Eavesdropping	Listens to data traffic and steals them

Table 4: Active Attacks

ACTIVE ATTACKS	
ATTACKS	EXPLANATION
DoS (Denial of Service)	Makes resources scarce for actual users
Replay Attacks (Middle Man Attack)	Stores session details and uses it for repeated accessing of information
Attacks – Internal / External	External – Attacks from nodes in other networks Internal – Attacks from nodes in nodes of the same network
Jamming / Access modification	Prevents actual user from accessing the network

C. *Cryptographic Attacks*

Cryptography can either be used for protection of the network or to make it difficult for the authorized user to use his own systems [6] [9]. This form of attack concept has many types;

Table 5: Cryptography Attacks

CRYPTOGRAPHIC ATTACKS	EXAMPLES
DSA – Digital Signature Attacks	Digital Signature, ElGamal Signature, RSA Signature, DSS
Pseudorandom Numbering Attacks	Timestamp variation, Nonce, Vector initialization
Collision Attacks	MD5, HAVAL-128, SHA-0, MD4

III. List of Main Attacks and their Explanation

1. MAC Layer Attack

Disrupts the cooperation of protocols with one another and thereby, controls the radio channel as a whole.

2. Disruption on Back-Off Mechanism and DCF (Distributed Coordinated Function)

Selfish nodes will disrupt the working modes of MAC protocols.

3. Corrupting the System

Includes or removes bits from the present transmission in order to activate DoS [6] attacks later on.

4. Disruption of Network Vector of Allocation or NVA (sometimes NAV)

Prevents RTS and CTS signals from being transmitted / received to aid in the current transmissions.

5. Network Congestion

It is also an attack which will prevent the allocation of resources by occupying them indefinitely.

6. Routing Information Table Attack

Causes the routing table to overflow and prevents periodical updating of routes.

7. Rush Attack

Tunneling of data packets from two malicious users to a single location using the same time period.

8. Positioning Attack

Malicious nodes gather information of other nodes and then disclose them to other unauthorized nodes.

9. Consumption of Resources

Attempts to deplete all resources by false requests and forwarding techniques.

10. Poisoning of Cache Attack

Corrupts the route table by adding unwanted route details to the actual node information.

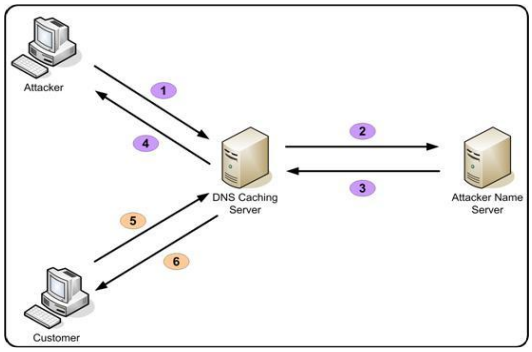

Figure 1: Poisoned Cache

11. Route Maintenance Attack

Transmits bogus control messages and gains outside control of the routing capability of the network.

12. Data Forwarding Attacks

Performs modification of forwarded packets (complete / partial) or simply drops them to cause routing and transmission confusion.

13. Selective Forwarding Attacks

Forwards selective packets alone, irrespective of routing table intentionally [1] [12].

14. Route Discovery Attacks

Bypasses the routing standards of a network and causes route overload.

15. Selective Routing Attacks

Modification of routing table itself by deletion, addition and switching the nodes in the list.

16. Signature Attacks

Though digital signatures of the RSA algorithm is genuine and effective, it is easy to generate a similar digital signature with blind try methods.

17. Wormhole Attack

Tunneling of packets down to a different location and prevents new route discovery [10].

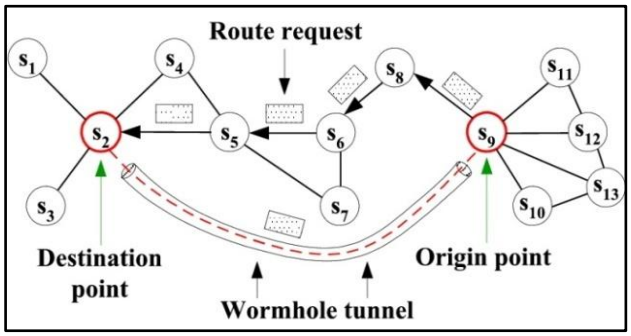

Figure 2: Wormhole Attack

18. Traffic Analysis and Tracking Problems

Nodes will gain information of the entire traffic and will change the log to suit the malicious node's needs.

19. Flood SYN Attacks

It is a DoS attack that creates huge numbers of open connections and floods the buffer with these information [2][4][5].

20. Session Theft

Since a session needs authentication only at the beginning of the connection, it is possible for the malicious node to copy the credentials right at the startup and then use it to utilize the resources later on.

21. Code Attacks

Programs meant for corrupting all functionalities of the network.

22. Repudiating Attacks

Denies communication between nodes, in whole or in part.

23. Denial of Service

Signal disruption can be made at all the layers and thereby disrupt normal communications.

24. Impersonation Attacks

Nodes utilizing resources of the network by impersonating the other nodes.

25. Middle Man Attack

A third node obtains information of the transmission between two nodes by listening in or by masquerading as each of the nodes.

26. Pseudorandom Attacks

Time stamps of the packets may be altered to accommodate the generation of session key from the altered time stamp and a random number.

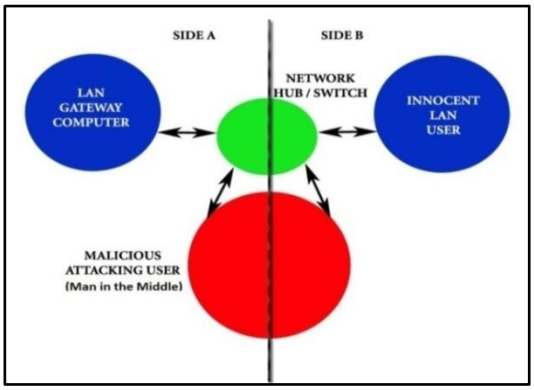

Figure 3: Man in the Middle

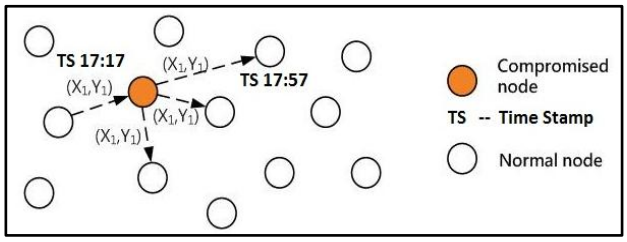

Figure 4: Pseudorandom Attacks

27. Hash Attacks

Attacks meant to find similar messages containing the same hash function, from which other authentication details are obtained.

28. Defective Key Management

By utilizing host key information log, the key management schemes can be manipulated in such a way that the attackers can gain control of the facilities like storage, generation, updating and authentication service of keys.

29. Rate Monitoring Attack

Malicious node in the network would use the fact that the nodes near to the base station would transmit and forward more packets than the other nodes to gain control of the amount of traffic found within that part of the network.

30. Time Difference Attack

Nodes can generate certain parameters on their own, which is then forwarded onto the other nodes to get reports from them.

IV. CONCLUSION

Though it is necessary for all to know about the ways in which our data may be protected from an attack, it is best to know more of the ways in which an attack may actually be performed; better understanding of levels in which an attacker thinks will also be an added advantage. Such knowledge will be useful in monitoring, detecting and protecting the systems and all network components from internal and external attacks and intrusions [3]. This survey is a step towards the formation

of a compendium of attack types, from which better surveys and rigorous protective schemes may be framed. In addition to the discussion of basic factors needed to classify attacks, different types of attacks which are possible were also included here. The possibility of missing an attack in our practical considerations will be remote, if proper surveys are carried out in this regard.

V. FUTURE DIRECTIONS

Other trivial forms of attacks can also be included in this survey. Also, this survey may further be extended to include the ways of combating such attacks.

REFERENCES

[1] Bin Xiao, Bo Yu, and Chuanshan Gao. Chemas, "Identify suspect nodes in selective forwarding attacks", Journal of Parallel Distributed Computations, Vol. 67(11): Pp. 1218–1230, 2007.
[2] Danny McPherson, "BGP Security Techniques", APRICOT, 2005.
[3] Mouratidis. H, Giorgini. P, Manson. G, "Using Security Attack Scenarios to Analyse Security during Information Systems Design", Proceedings of the International Conference on Enterprise Information Systems, Porto-Portugal, Pp. 10-17, 2004.
[4] Taka Mizuguchi, Tomoya Yoshida, "BGP Route Hijacking", APRICOT, 2007.
[5] Su-Chiu Yang, "Flow-based Flooding Detection System", APRICOT, 2004.
[6] Ray Hunt, "Network Security: The Principles of Threats, Attacks and Intrusions", part1 and part 2, APRICOT, 2004.
[7] Ehab Al-Shaer, "Network Security Attacks I:DDOS", DePaul University, 2007.
[8] Markus Schumacher, Eduardo Fernandez Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad, "Security Patterns- Integrating Security and System Engineering", John Wiley & Sons, Ltd., 2006.
[9] William Stallings, "Cryptography and Network Security Principles and Practices", Fourth Edition, Prentice Hall, 2005.
[10] Y.C.Hu, A.Perrig, and D.B.Johnson "Packet leashes: a defense against wormhole attacks in wireless networks", INFOCOM 2003. 22nd Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, 2003.
[11] Hemanta Kumar Kalita and Avijit Kar "Wireless sensor network security analysis", International Journal of Next-Generation Networks, 2009.
[12] Bo Yu and Bin Xiao. "Detecting selective forwarding attacks in wireless sensor networks" Parallel and Distributed Processing Symposium, IPDPS 2006. 20th International, Pp. 8, 2006.

V.P. Ajay received his B.E from Anna University Chennai in the year 2008 and has shown interest in many add-on studies in the field of Networks and Communication Systems. Currently, he is in the final year of his Master's degree in Communication Systems from Anna University Coimbatore. He has presented many of his ideas, in national and international level conferences and technical symposiums. He also has two International Journal contributions to his credits. He has served as a Research and Development Engineer and a Research article writer for over a period of two years. His research interests are in the domain of wireless networks, wireless communication techniques, switching techniques, security protocols and intelligent systems.