ATTACKS ON CRYPTOGRAPHIC SERVICES: A SURVEY

[1]Architha H , [2]Akshay R, [3]Shunmuga Priya S
[3]Assistant Professor
[1,2,3]Sri Krishna College of Engineering and technology
[1]archithaharinath@gmail.com,[2]akshayravindran96@gmail.com, [3]shunmugapriyas@skcet.ac.in

Abstract:

This paper presents a survey on various attacks on network and segregates those attacks based on their ability to compromise the cryptographic services such as confidentiality, availability, non repudiation, integrity. Common attacks are known to everyone but for what purpose the attacks are done is dealt with this paper.

Index terms: Cryptography,network Security, Confidentiality, Integrity, Availability, Authentication, Non-Repudiation.

I. INTRODUCTION TO ATTACKS ON CRYPTOGRAPHIC SERVICES

Cryptography is the study of secure communication of data in the presence of third party adversaries. Cryptography is the science that deals with safeguarding an information. In networks the conversion of a plaintext to a ciphertext is called as cryptography. When a message is sent using cryptography it is encrypted and is represented in another form. The process of misrepresenting the data by means of an algorithm is termed as encryption. The message is called as plaintext and the encrypted message is called as the ciphertext .Ciphertext belies the plaintext such that it is confounding to the cryptanalyst. A cryptanalyst is the one who tries to extract the original data from the ciphertext. The process of extracting the information from the encrypted form is called as cryptanalysis. There are two types of cryptography based on the key used for encryption and decryption. namely symmetric and asymmetric cryptography If the same key is used in the sender and receiver end then it is symmetric and if the keys are different it is termed as asymmetric. There are 4 cryptographic services namely confidentiality integrity availability and non repudiation. These four also called as security goals. Sensitive data must be protected from disclosure in transit.The cryptanalyst may try to extradite the data from the ciphertext or he might try to confound the data. There are various attacks that extradite the information or impasses the transaction of the message and provide hindrances to the integrity of the information. An attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. In this paper we are providing a taxonomy of the existing attacks based on their attempt to compromise the security goals.

In Section II the cryptographic services and the attacks on them is looked upon. In Section II the conclusion is discussed followed by references.

II. CRYPTOGRAPHIC SERVICES AND ATTACKS ON THEM

2.1.Confidentiality:

Data confidentiality is the important constraint of the network security. Confidentiality means protecting the data from disclosure to the unauthorized external environment. It also means that data being transferred via the network can never be viewed by the unauthorized user unless they are authenticated by the authenticated nodes. If confidentiality is not maintained the sensitive information can be used to harm

the network. Data encryption techniques are used to give protection to the network.

2.1.1 Attacks on Confidentiality:

The various attacks that affects the confidentiality of data and which impinge the information are.

2.1Routing table poisoning:

Routing table poisoning is one of the routing attacks. Compromised nodes in the network send malicious updates or modify the original packets sent to the uncompromised nodes[14]. It can cause confusion in the network,or even makes some parts of network inaccessible. Confidentiality of the system is thus corrupted by making the node data being viewed and damaged by other nodes.

2.1Sybil attack:

A single node gets duplication and send to various location. The main area on which the attacks is done is fault tolerance schemes such as distributed storage,multipath routing and topology maintenance[13]. Multiple identities are present that causes chaos in the system. In this attack the confidentiality is violated because without the data or nodes being transferred.

2.1.2Node subversion:

Node subversion means taking the node into control and accessing all the information the adversary wants. When a node is compromised and taken into control the cryptographic key used and the node can be easily taken into control[15]. So automatically the contents confidentiality is corrupted because the data gets exposed to the malicious environment.

2.1.3Physical attack:

The attack in which the hardware components is directly attacked and access all the details in the hacked device[20]. Confidentiality is corrupted because the device is in adversary control and the data is exposed.

2.1.4Hello flood attack:

In this type of attack a malicious node outside the network comes and compromises one of the node in another network gains trust for it. The compromised node gives some messages to the malicious node and asks it to transfer it to the destination[19]. The malicious node gains access and reads the data in it confidentiality is disturbed for that network.

2.1.5 Passive information gathering:

If the network via which the data is sent is not encrypted the data stream which is passed through that network can be easily accessed by the adversary with forte skills. The requisite for accessing data from the network are an powerful antenna and receiver[9]. When the data streams are accessed the location of the nodes can be easily accessed through those packets and all the important data can be accessed that can be used in a malice way to other receivers and network.

2.2 Integrity:

Integrity of information adverts to safeguarding the information from being modified by unauthorized parties. Integrity involves perpetuating the consistency, accuracy, and trustworthiness of data over its entire life cycle. Information is no longer reliable or accurate. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people. High encryption techniques are used to give protection from malicious nodes or adversaries. This could be the modification of a file, or the change in the configuration to a system. Integrity is one of the most important constraint in the network security. The data is being transferred through the network only

because of the reason that the data being transferred is secured and will never gets changed. If the integrity constraint of the system is destroyed the network become malicious.

2.2.1 Attacks on networks integrity:

Even though system is with encryption technology some attacks occur that destroy the integrity of the system. These are as follows.

2.2.2 Colluding mis-relay attack:

This attack is caused by multiple nodes in partnership by causing collision in the nodes being transferred. It can modify or destroy the packets in the network this disrupting the normal functioning of the system[9]. This attack is done without any loopholes for detection purpose. Normal methods such as pathrater and watchdog cannot be used.

The packets or data in the system is being destroyed so the integrity constraint of the network is violated.

2.2.3Device tampering attacks:

Wireless AD hoc network are fragile, compact and has to be handled very carefully .

They can be damaged or stolen easily. Whenever the message is been transferred an authentication process has to be done by the receiving node which can never be done by the packets[17]. This attacks prevent authentication by causing looping and fabrication because of no packet can do this authentication. As there is no centralized administrator attacks can easily occur. Due to continuous looping and fabrication the packets sent are never received and can be destroyed or altered based on attackers need. This destroys the integrity of the system.

2.2.4 Gray hole attack:

This compromises the message by selectively forwarding certain packets based on probability statistics which might alter the message , the whole intended message by the user will not be received and the information vary which will result in ambiguity[$a]. Thus the gray hole compromises the integrity of the network.

2.2.5 Packet dropping:

In malicious intermediate node is the complete reason for this attack. Direct interruption to the messages is done by constant dropping of the packets by the harmful nodes during the route discovery process[4]. The packets can be dropped altogether, selective or periodical basis.The packets are dropped by the authenticated nodes thus creating a malicious network.

2.2.6 Camouflage:

This attack occurs when an false node is inserted or existing node is compromised and then the it acts as an friendly node thus attracting the packets being transferred and misroute them causing malfunctioning in the system[10]. Camouflage is attracting the packets in the system thus prevents in forwarding of the packets to the original destination.

2.2.7 Node replication attack:

This attack is just causing the replication of the nodes being transferred in the network. Replication is done by copying the id of the existing node the replicate the node and then insert it in the network[3]. This causes a malicious network. If the attacker gains the system cryptographic keys the entire packets being transferred can be replicated and then causing disruption in the connection. Replication of node is done which alters the data being transferred thus violates the network's integrity.

2.2.8 False node:

False node attack is the most dangerous attack that inserts a duplicate

node into the network and inserts malicious code into it by adversary. This node when placed into the system floods all the node in the network with malicious code thus destroys the entire network security[5]. Additional fake nodes destroy the normal system in which data is being transferred.

2.2.9 Message corruption:

Any modification of the message in the network causes disruption in the network thus destroying the integrity of the network[3].

2.2.10 Node malfunction:

Node malfunction destroys the integrity of the network by generating inappropriate data that can expose the details of the network and the data transferred[10]. It can alter the data being transferred and violates the integrity.

2.2.11 Selective forwarding:

An infected node will destroy or remove only the selected packets. In any network in which data is been transferred it is seen that the intermediate node actively forward the received packets. But this constraint is violated by compromising the nodes and stopping the process. The transferring process takes place via another network[4] .

The node being transferred is stopped by the trustworthy intermediate nodes thus causing the violation in the network integrity.

2.2.12 Fabrication:

In this type of attack instead of altering the original packets in the network malicious node in the network will include malicious packet in the network of their own. It causes sleep deprivation attacks by introducing many packets into the system thus destroying the entire network[20]. It is not caused by malicious nodes alone it can even be caused by the nodes being compromised. Since the data in the nodes are modified and extra nodes are added integrity is destroyed.

2.2.13 Modification:

In this type of attack adversaries make some modification to the existing nodes in the network. Ad hoc networks are free to move and fragile it can even be affected by some malicious nodes and packet[19]. This cause complete disruption in the network and can be identified only after the message is delivered. If the data is modified in the network automatically the integrity is violated.

2.2.14 Impersonation:

Impersonation is otherwise also known as spoofing attack. In this attack the compromised node pretends to be as the original node of the network. As a result of this network loops and misleads in networks occur[18]. The data may reach some other node or the existing data can be altered and sent to the receiver. Thus violating the integrity constraint.

2.3 Authentication:

Authentication means having recognised access to the node data, encryption techniques used, node trust etc. only the authorised users can access information. Unauthorised users cannot have access to information. Authentication of who is going to access the data is important because without that property is being checked unauthorised user without possessing the node it can access the node data and interfere in the operation of the network operation.

2.3.1 Attacks on Authentication:

Various attacks that violates the property of authentication and does disclosure of data are.

2.3.2 Passive attack:

Passive attacks are those type of attacks in which the normal operation is not affected and the data in the network line is unaltered and the data is only snooped[14]. The confidentiality constraint is violated. Since the operation of the network is unaffected the attack can never be identified easily. To avoid these types of attacks the only way is to improve

2.3.3 Eavesdropping:

It is one of the main attack that violates the authentication property. The unauthorised member gains access to the network and gets all the information about node values, encryption techniques used, data passed, private key[$a]. If all these private information is exposed the network will become useless to transfer data. Hence authenticity property has to be maintained.

2.4 Non repudiation:

Nonrepudiation is a method of guaranteeing message transmission between parties via digital signature or encryption. It the constraint that sends a confirmation to the sender that receiver has received the message. But in originality the receiver has never received the packet sent and it was a fake confirmation sign to the sender. This attack completely violates the security of the network because the sender will think that the message has reached but the message has been eavesdropped and it can be used in many ways. So the network becomes completely unsafe and it will not be known that message has been eavesdropped and prevented from sending until someone notifies the sender.

2.4.1 Attacks on Nonrepudiation :

Limitable attacks confound the repudiation of a message they are as follows.

2.4.2 Link spoofing attack:

The name link spoofing itself tells that the links between the nodes in the network has been faked by some malicious nodes creating new routes to some other nodes causing failure of transmission to the original receiver[7]. But the sender gets notified or updated that the receiver received the node. And all the data will be eavesdropped by the malicious node violating the network security.

2.4.3 Session hijacking attack:

As the communications layers are protected only until session setup this attack hijacks the session to be carried out. This attack spoofs the ip address of the victim then the receiver information is known and denial of service is done to the receiver but the sender never knows about it[16]. The attacker acts as the sender and performs the attack on other nodes.

2.5Availability:

Availability is one more main constraint of network security. Availability means the sent information should reach the correct person at the right person without any delay. If the message is not delivered properly there is no use of transferring the information. So availability should be maintained whenever the data is being transferred. Before the data usage or need gets over for the receiver it should reach the receiver without any alteration or malicious information. Various attacks that destroy the availability of the information are:

2.5.1 Attacks on Availability:

Various attacks that destroy the availability of the information and make the packets unavailable are

2.5.2 Neighbour attack:

This attack violates the availability constraint because the intermediate node that transfers the packet makes a copy of id

of packet and then forwards the packet to some other node[12]. It sends the data two hops to the next node. The fake receiver gets the data than the original receiver.

2.5.3 Jamming attack:

In this type of attack an interference is caused so that the data will reach the destination in wireless communication systems[3]. Interference can cause either denial of packets or repetition of legitimate packets to the destination. This can be achieved through jammer that causes denial of messages. As this attack causes denial of service so it violates availability.

2.5.4 Resource consumption attack:

This is also called as sleep deprivation attack.It mitigates the resources used by the network gradually diminishing it and by forwarding selected packets the integrity of the message is compromised[6]. And the attacker might also try to waste the battery power which leads in the disruption of Availability.

2.5.5 Route cache poisoning:

This is done on on demanding routing protocols such as AODV protocols. This attack compromises certain nodes in the system making it inaccessible which makes availability constraint unavailable[15].

2.5.6 Rushing attack:

An adversary node which receives a Route Request packet from the source node floods the packet quickly through the network which makes the original nodes think that the message has been received already and discards the packet which in turn affects the availability of the message BEING TRANSMITTED[6].

2.5.7 Denial of service:

Denial of service attack happens when attacker sends large amount of junk packets which uses handsome amount of resources into the network[$a]. It introduces wireless channel contention and network contention in MANET. The other types of DOS attacks are routing table overflow attack and sleep deprivation attack. The attacker tries to create routes to non-existent nodes in routing table overflow attack. Sleep deprivation attack aims to consume the batteries of a victim node.

2.5.8 Flooding attack:

The attacker causes depletion of network resources in a flooding attack. The resources maybe bandwidth, battery power of nodes etc. When an attacker sends large quantities of Read request to a destination node which does not exist in the network, no reply is given to the Read requests(RREQ'S)[7]. Therefore the requests flood the entire network causing depletion of resources and denial of service to take place. Flooding attack shows the unavailability of resources and nodes in the network.

2.5.9 Jelly-fish:

When data packets are sent the attacker intrudes the data packets and withhold them for some time for no apparent reason[$o]. Hence there occurs a delay in receiving data packets and the performance of real time applications are affected. The availability of data packets are disturbed for a period of time.

2.5.10 Sleep deprivation torture:

Ad hoc networks are susceptible to this type of attacks. The services of certain nodes are used repeatedly so they do not go to power preserving state,this results in depletion of resources that are limited in quantity[8]. It is known to cause harm to networks of limited resources. The

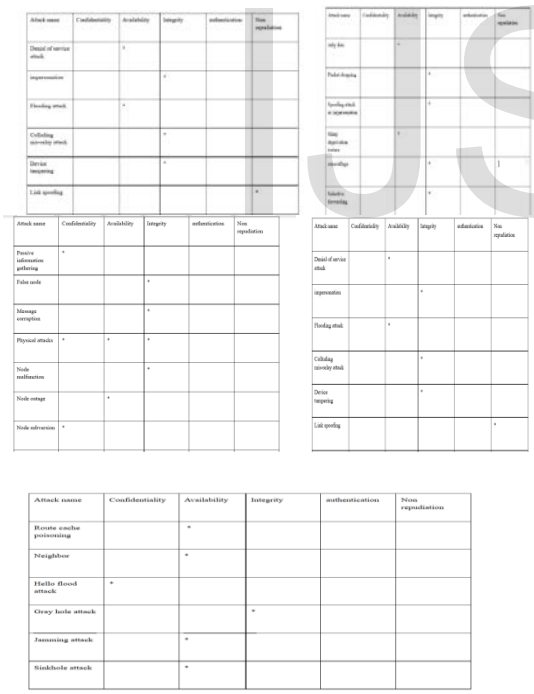
availability of resources is affected hence availability constraint is violated.

2.5.11 Sinkhole:

Sinkhole attack is the attraction of attack to a specific node. The attackers aim is to attract all attention of a network to a particular node thus inhibiting other nodes from gaining resources. The availability of resources for other nodes are affected .

2.5.12 Node outage:

As the name suggests it is the outage of nodes in a network i.e the node stops functioning[9]. For the network to be free of devastating effects the network sensor protocol should be strong enough to diminish the effects caused by node outage. The functions are unavailable so availability constraint in affected.



Attack name	Confidentiality	Availability	Integrity	authentication	Non repudiation
Route cache poisoning		*			
Neighbor		*			
Hello flood attack	*				
Gray hole attack			*		
Jamming attack		*			
Sinkhole attack		*			

FIG 1 : DENOTING THE ATTACKS ON CRYPTOGRAPHIC SERVICES.

III CONCLUSION

Thus the survey of different attacks on the cryptographic services has been tabularized to give a basic compromising cryptographic services.

IV REFERENCES

[1]Routing Attacks in Wireless Sensor Networks: A Survey, Deepali Virmani#1, Ankita Soni*2, Shringarica Chandel*2, Manas Hemrajani*2 Bhagwan Parshuram Institute of Technology, India

[2]Network Security and Types of Attacks in Network
Mohan V. Pawar , Anuradha J Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, Maharashtra, India 2
School of Computing Science and Engineering, VIT University, Vellore, Tamil Nadu, India

[3]Classification of Internet Security Attacks Khaleel Ahmad, Shikha Verma, Nitesh Kumar and Jayant Shekhar
CSE/IT Dept. S.I.T.E., Swami Vivekananda Subharti University Meerut, Uttar Pradesh, India

[4]SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS: A SURVEY Vinh Hoa LA, Ana CAVALLI Department of Software and Networks Telecom SudParis, 9 rue Charles Fourier 91011 EVRY, France.

[5]Classification of Attacks in Wireless Sensor Networks Mohamed-Lamine Messai Doctoral school in computer science, university of Bejaia, Algeria Networks & Distributed Systems Laboratory, UFAS, Setif, Algeria

[6]Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey
Amitav Mukherjee, Member, IEEE, S. Ali A. Fakoorian, Student Member, IEEE, Jing Huang, Member, IEEE, and A. Lee Swindlehurst, Fellow, IEEE

[7]A Survey on Cryptography using Optimization algorithms in WSNs Swapna

B. Sasi, and N. Sivanandam Department of CSE, Karpagam University, Coimbatore, India; swapna@jecc.ac.in Department of CSE, Jyothi Engineering College, Thrissur, Kerala, India Department of CSE, Karpagam College of Engineering, Coimbatore, India

[8]Comparative Analysis of Cryptography Cipher Techniques Laukendra Singh, Rahul Johari Department of Computer Engineering, USICT, GGSIP University New Delhi, India

[9]A Survey of Mobile Ad Hoc Network Attacks PRADIP M. JAWANDHIYA Research Scholar, Department of Computer Science & Engineering, Prof. Ram Meghe Institute of Technology & Research, Badnera and Assistant Professor & Head of Department, Department of Computer Science & Engineering, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, Maharashtra, India. MANGESH M. GHONGE Faculty,Department of Computer Science & Engineering, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, Maharashtra, India.DR. M.S.ALI Principal,Prof. Ram Meghe Institute of Technology & Management, Badnera, Amravati, Maharashtra, India PROF. J.S. DESHPANDE Pro-vice chancellor, Sant Gadge baba Amravati University, Amravati, Maharashtra, India

[10]A Survey Of Attacks,Security Mechanisms And Challenges in Wireless Sensor Networks
Dr. G. Padmavathi, Prof and Head, Dept. of Computer Science, Prof and Head, Dept. of Computer Science,padmavathi@gmail.com .Mrs. D. Shanmugapriya, Lecturer, Dept. of Information Technology,ds_priyaa@rediffmail.com . Avinashilingam University for Women, Coimbatore, India, ganapathi.

[11]A Survey on Network Attacks in Mobile Ad Hoc Networks. Vivek Richhariya, Ph. D Scholar, Department of Computer Science & Engineering, Praveen Kaushik Assistant Professor, Department of Computer Science & Engineering, MANIT, AISECT University, Bhopal, India

[12]A Concise Evaluation of Issues and Challenges in MANET Security K. Muthukumaran1, D. Jeyakumar2, C. U.Omkumar3 1,2,3Assistant Professor, Easwari engineering College, Chennai, India.

[13] Security Issues in Mobile Ad Hoc Networks - A Survey Wenjia Li and Anupam Joshi Department of Computer Science and Electrical Engineering University of Maryland, Baltimore Country .

[14] Security in Ad Hoc Networks Vesa Kärpijoki Helsinki University of Technology Telecommunications Software and Multimedia Laboratory Vesa.Karpijoki@hut.fi

[15] A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS. BOUNPADITH KANNHAVONG, HIDEHISA NAKAYAMA, YOSHIAKI NEMOTO, AND NEI KATO, TOHOKU UNIVERSITY ABBAS JAMALIPOUR, UNIVERSITY OF SYDNEY

[16] Security in MANET: Vulnerabilities, Attacks & Solutions Sachin Lalar Department of Computer Science & Engg., TERI, Kurukshetra

[17] ROUTING ATTACKS IN MOBILE AD HOC NETWORKS .P. Narendra Reddy1, CH. Vishnuvardhan2, V. Ramesh3 1Computer science, JNTU-A/ Sree Vidyanikethan Engineering College, Tirupati, India

[18] Comparative Analysis of Various Attacks on MANET Pooja Chahal Department of Computer Science Gaurav Kumar Tak Department of Computer

Science Anurag Singh Tomar Department of Computer Science Lovely Professional University Phagwara, India

[19] MANET: Vulnerabilities, Challenges, Attacks, Application Priyanka Goyal1, Vinti Parmar2, Rahul Rishi3 1,2 Research Scholar, Dept. of CSE, Technological Institute of Textile and Science, Bhiwani, Haryana, India goyaldrpriya2@gmail.com, vinirajput14@gmail.com 3 Research Scholar, Dept. of CSE, Technological Institute of Textile and Science, Bhiwani, Haryana, India rahulrishi@rediffmail.com

[20] Malicious attacks on ad hoc network routing protocols PO-WAH YAU, SHENGLAN HU and CHRIS J. MITCHELL Information Security Group, Royal Holloway, University of London Egham, Surrey TW20 0EX, UK {P.Yau, S.Hu, C.Mitchell}@rhul.ac.uk