International Journal of Engineering & Technology, 7 (2.33) (2018) 279-282

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Attacker standard for secure routing protocols

Ms. Divya [1] *, Dr. R. Gobinath [2]

[1] Research Scholar, Department of Computer Science, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Pallavaram, Chennai, Assistant Professor, Department of Computer Science, Prince Shri Venkateshwara Arts and Science College Chennai
[2] Assistant Professor, Department of Computer Science, VISTAS, Pallavaram, Chennai
**Corresponding author E-mail: iamgobinathmca@gmail.com*

Abstract

The secured routing protocol expresses an underlying elementary unit confide in information interchanging system. Miserably, presently no anatomy remains to supports in the layout and inquiry of secured routing protocols. This work investigates the structured approaches of secured routing and the interrelating attacker standards to contribute a structure for modeling prime protocols. Based on this anatomy, it is detected that the powerful attacks are targeting the data in the control plane. In this paper the strength of attackers are classified with respect to the locations under its direct control.

Keywords: *Network; network security; routing and routing protocol.*

1. Introduction

The computer network allows nodes to share resources which are called as digital telecommunications. In computer networks, data is exchange between computing devices by connecting the nodes (data links).The guided media such as wires or optic cables, or unguided media such as Wi-Fi are used to establish the data links. The network node is the device that originate route and terminate the data. Personal computers, phones, servers and networking hardware are some host that includes the nodes. Two devices can exchange information, whether or not they have a direct connection between them.

The Attackers repeatedly exhibited in their ability to harm and exploit the routing systems. The wireless mobile network has also introduced the significant challenges of security. It is designed in such a way that the connections between routers are relatively stable; communication is increasingly performed among mobile devices. Such environments are characterized by frequent changes with routing by resource constraints and unpredictable network connectivity.

The objective of an attacker can be well-heeled and varied in the distributed routing system relation: the familiarity, possibility, and integrity of information transmitted in packets either directly or indirectly(the information is passed and refined in the network) are some targets of an attacker. An attacker may attack the authority information in the routing protocol relation to make the other quantities act in random manner.

The traffic deviation is a significant target of an attacker through a geological area, where the packet movement arrangements can be monitored and blocked at any time. In high-performance and latency-critical networks, the cryptographic operations are very expensive to achieve. Therefore the integrity of route is assured by the routing protocol.

In the modern networking standards such as Software-Defined Networking, the routing system and routing attacks are poorly cited still today. To categorize the probable attacks on routing protocols the occurrence of prime standards are taken as a scope in the secured routing system.

The taxonomy of the routing system, possible aspect and vulnerabilities directing on routing protocol attackers are some of the configured view expansions indicated in this work. Forwarding, topology, transport, and identity resolution are the primary functions offered in the routing system corruption. Based on this corruption, attacksand division of attackers are established and developed respectively.

2. Routing

Recruiting a route between networks or across multiple networks is one of the routing technique. Circuit-switched networks, such as the public switched telephone network (PSTN) and computer networks such as the Internet also implements the routing technology. Routing focuses network packets from their source toward their target by individual packet promoting mechanisms.

The network packets passed from one network interface to another addressed network is known as Packet forwarding. The network hardware devices such as routers, bridges, gateways, firewalls and switches are considered as the moderate nodes. Packet transmission and routing implementation is also achieved even in General-purpose computers without any special hardware. Packet forwarding by routing tables manages a transcript of routes to different network targets are regularly focused by the routing system. For valuable routing, composing routing tables from router's storage area is very significant. Only single network path is almost used by greater routing algorithms. Numerous alternative routes utilization is facilitated by Multipath routing techniques.

With bridging the network addresses are structured and the similar addresses are implied by proximity within the network. A single routing table entry under structured address represents the route to a group of devices. In enormous networks, the structured addressing (routing) is exceeded by the unstructured addressing (bridging). In the Internet the routing is said to be the effective form of addressing.

For the purpose of our taxonomy, we identify some routing service components: (1) network transport service, (2) network topology service and (3) data forwarding and routing. Additionally, a routing service routinely combines with external services and resources. Constructing a perfect anatomy of attacks across routing needs various cooperation's and inferences.

3. Resource and external service routing

Hardware: Various hardware peripherals such as routers, links, SDN controllers, etc. are used in the routing system implementation. Rather than hardware errors the protocols and logics of routing system are focused to delight the peripheral entity as hardware.
Identity resolution: The identity management of routing systems relation is the most essential part of node identity resolution. With identity resolution logic the routing service is cooperated which grants the identity resolving of any node. Identity resolution is delighted as a peripheral service, yet we introduced it in our analysis.

3.1. Transport service

Connection-oriented services and reliable data delivery services are contributed by the network transport protocol layer. The top of network layer is occupied by the transport layer. Transport services and network services are contributed by TCP and IP in the internet protocol series. For file transfers and mission-critical applications, the transport layer protocol guarantees the delivery which is accommodated as the significant feature of routing. TCP protocol utilizes IP protocol, where the reliability services are enumerated at the rate of overhead and minimized performance. Between source and destination the virtual connection is installed as the function by the routing services. To create the connection with the destination the handshaking facility is used by the sender during session inauguration. During the session, a conversation is involved between source and destination where the data flow is managed to avoid the receiver from overflowing and the receipt of TCP segments are approved. A communication session of routing system is as follows:

1) Network Connection is established (virtual circuit).
2) Session parameters are negotiated.
3) Reliable data delivery and data transfer management.
4) Termination of Network Connection.

The services provided by transport protocols are as follows;
Establishment of connection setup and multiplexing services.

i) Network Flow control service.
ii) Congestion control and slow start services.
iii) Reliable management services.
iv) Avoiding Congestion service.
v) Multiplexing service

Establishment of connection setup and multiplexing services: Before the sender starts transmitting data packets it must first associate the receiver to establish the connection first, and then the data transmission is begun which is employed as the three way handshake. Multiple connections with multiple devices are created simultaneously by the single system. This feature is known as multiplexing.
Flow control mechanisms: The sender is prevented from overflowing the receiver with much data, while slow start and congestion control are used to deflect network traffic. Therefore due to overwhelming the receiver lost packets and those packets must be retransferred which increases the network traffic and minimizes system performance.
Congestion control and slow start: The sender starts transmitting packets slowly after the link has been created. The transmission picks up the measure if the congestion is not poor. This situation is known as "slow start". If the network gets busy then the, congestion manages the mechanism which helps the sender to scale back.
Reliability services: The dropped packets are retransmitted by the reliability services. The sender is approved by the positive acknowledgement that the receiver received a packet. To identify the lost packets, the packets are reassembled in order by allocating sequence number for each packet. The corrupted packets are encountered by error checking techniques.
Congestion avoidance: Congestion control can manage traffic jam entry into a telecommunications network to avoid oversubscription of any of the communication capabilities of the intermediate nodes and networks and resource decreasing steps such as decreasing the rate of transmitting packets. For example, automatic repeat requests may keep the network in a crowded state; this position can be neglected by enumerating congestion avoidance to the flow control, including slow-start. This maintains the bandwidth utilization at a low level while the transmission begins or after packet retransmission.
Multiplexing: Ports can accommodate many endpoints on a specific node. Computer operations will listen for message on their own ports, which permits the utilization of many network services simultaneously. It is a portion of the transport layer in the TCP/IP model and the session layer in the OSI model.

3.2. Topology service

Contributing a partial view on the network topology, information about connectivity and adequacy of communication such as packet bandwidth, packet delay and packet reliability are the major objectives of a topology service. Through the utilization of control messages, the topology service is executed and broadcasted by the transport service. Control messages can be either altered by the nodes or the nodes can admit prime control messages. An outlook of the network can be accessed by the information obtained either from direct neighbors or from other nodes through multi-hop communication.
The topology service also consists of neighbor discovery. Information used by the topology service is reserved in a probably distributed database where the knowledge about neighbors, network topology, and the network path metrics are controlled. The network topology services are built upon the transport service of the network

3.3. Data forwarding

The Network Layer in the Open Systems Interconnection (OSI) model is answerable for packet forwarding. The forwarding model unicasting elaborate a packet relayed from source to its destination. Broadcasting involves a packet to be redundant and transmits on multiple links on the network. Broadcast packets are not transmitted all over a network, but only to devices in a broadcast domain.

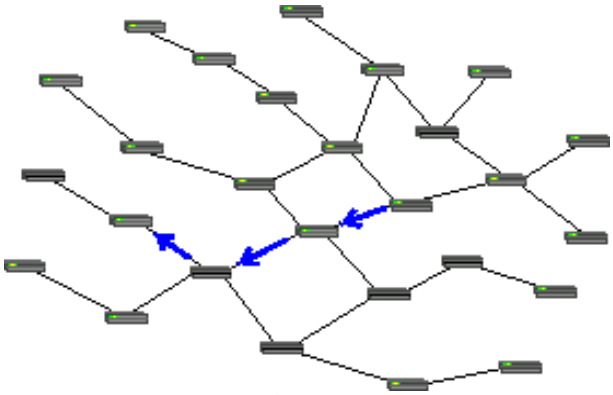

Fig. 1: Overview of Unicast Data Forwarding.

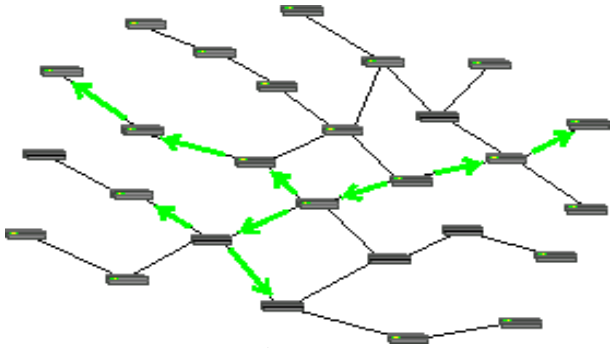

Fig.2: Overview of Multicast Data Forwarding.

At nodes where many links extending outwards are available, the choice for forwarding an available packet desires a decision making process. Since forwarding decision must be obtained for all packets obtained by a node. The transmission of data from one node of a network to another node is known as Node-to-node data transfer, which is organized by the physical layer and data link layer of the OSI model.

4. Network security attacks

Some basic network security attacks are-

- Eavesdropping attacks
- Logon abuse attacks
- Spoofing
- Intrusion attacks
- Hijacking attacks
- Denial-of-service (DoS) attacks

An attack can be either active or passive. An active attacks pursuits to modify system resources or affect their operation. A passive attack pursuits to determine or uses the information from the system without affecting system resources. An attack can be carried by an internal or external organization. An "inside attack" is an attack admitted by an individual inside the security perimeter. An "outside attack" is admitted by an unauthorized or illegitimate user of the system.

4.1. High level security and privacy attack goals

The security goals can be broken by an attacker. The attributes of an attack are as follows;

- Availability: These attacks incorporate to avoid forwarding data to nodes, attacks which separate the nodes and attacks. Thus the performance of the routing service is reduced.
- Authenticity: These attacks consist of nodes representing other nodes in neighbour discovery and maintenance protocols.
- Integrity: Attacks that adjust the advantage of the forwarded data or state information. For example, in current Internet, messages of the BGP protocol are often proliferated in an unsecure manner, which attackers might accomplish.
- Confidentiality: These types of attacks adjust the familiarity of transmitted data or packet state information. For instance, an attacker may decide to learn about traffic connected by other inhabitants.
- Anonymity: Attacks that adjust anonymity and region privacy.

4.2. Attacker goals and capabilities

The basic actions performed by attackers are as follows:

i) Manipulating information: An attacker may employ control or data information transmitted in packets. For example, it can publish wrong communication measures or BGP routes.

ii) Eavesdropping communication: An attacker may hack or record sensitive information transmitted in packets, or detects traffic patterns.

iii) Data forwarding attacks: An attacker can drop, delay, or divert links.

iv) Identification related attacks: An attacker can imitate another entity.

4.3. Route computation service

Attacks on the route computation service include:

i) Packet drop: An attacker can misuse the routing system availability without forwarding packets.

ii) Incorrect Forwarding: An attacker can disregard the confidentiality of traffic by forwarding packets to the wrong ports. For example, attackers can retreat information.

iii) Change header fields: The packet information can be modified by the attacker during transmitting the packet. For example, by altering the network tags, information can be retreat by the attacker, again disregarding confidentiality.

iv) Route computation: An attackers who can consequence the routing algorithm, can extremely disregard the possibility and confidentiality of the routing service.

5. Conclusion

The taxonomy discussion for secure routing protocols is initiated in this paper, which is considered as the underexplored field of research. This discussion brings an attention to address the security issues which is outlined in this work. However, some modifications were introduced in this work in order to attain these goals which require a constant process.

References

[1] Netis routers leave wide open backdoor. Http: //blog.trendmicro.com/trendlabs-security-intelligence/ netis-routers-leave-wide-open-backdoor/, 2014.

[2] H. Ballani, P. Francis, and X. Zhang.A study of prefix hijacking and interception in the internet. In Proc. ACM SIGCOMM, pages 265–276, 2007.

[3] A. Barbir, S. Murphy, and Y. Yang.Generic threats to routing protocols. Request for Comments 4593, 2006.

[4] K. Butler, T. Farley, P. McDaniel, and J. Rexford.A survey of bgp security issues and solutions. Proceedings of the IEEE, 98(1):100–122, 2010.

[5] H. Chan, D. Dash, A. Perrig, and H. Zhang.Modeling adoptability of secure BGP protocols.In Proc. ACM SIGCOMM, Sept. 2006.

[6] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer. Castor: Scalable Secure Routing for Ad Hoc Networks. In IEEE INFOCOM, pages 1–9, San Diego, CA, USA, March 2010.

[7] S. Goldberg, M. Schapira, P. Hummon, and J. Rexford. How secure are secure interdomain routing protocols. In Proc. ACM SIGCOMM, 2010.

[8] Y.-C. Hu and A. Perrig.A survey of secure wireless ad hoc routing. IEEE Security and Privacy, 2(3):28–39, May 2004.

[9] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. Wireless Networks, 11(1):21–38, 2005.

[10] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2–3):293–315, Sept. 2003.

[11] F. Lindner. Cisco ios router exploitation.Black Hat USA, 2009.

[12] R. Lychev, S. Goldberg, and M. Schapira.BGP security in partial deployment.is the juice worth the squeeze? In Proc. ACM SIGCOMM, 2013.

[13] D. Montgomery and S. Murphy. Toward secure routing infrastructures. Security Privacy, IEEE, 4(5):84–87, 2006.

[14] P. Papadimitratos and Z. Haas. Secure Routing for Mobile Ad Hoc Networks. In SCS CNDS, pages 193–204, San Antonio, TX, USA, January 2002.

[15] P. Papadimitratos, Z. Haas, and J. Hubaux.How to Specify and How to Prove Correctness of Secure Routing Protocols for MA-NET.In IEEE-CS Third International Conference on BroadBand-Communcations, Networks, and Systems, 2006.
[16] P. Papadimitratos and Z. J. Haas. Secure Data Communication in Mobile Ad Hoc Networks. IEEE Journal on Selected Areas in Communications, 24(2):343–356, February 2006.
[17] D. Pei, L. Zhang, and D. Massey. A framework for resilient internet routing protocols. IEEE Network, 18(2):5–12, Apr. 2004.
[18] M. Poturalski, P. Papadimitratos, and J. P. Hubaux.Formal Analysis of Secure Neighbor Discovery in Wireless Networks. IEEE Trans. on Dependable and Secure Computing, 10(6):355–367, Nov 2013.
[19] B. Snyder. Snowden: The nsa planted backdoors in cisco products. InfoWorld, 2014.