Traffic Diversion Attacks

Eitan Menahem
IBM, Cyber Security Center of Excellence
17 PUBLICATIONS **204** CITATIONS
SEE PROFILE

Yuval Elovici
Ben-Gurion University of the Negev
323 PUBLICATIONS **4,542** CITATIONS
SEE PROFILE

Degrading the Network's Quality of Service via Traffic Diversion Attacks

Eitan Menahem[1], Gabi Nakibly[2], and Yuval Elovici[1]

[1] Ben-Gurion University,
Telekom Innovation Laboratories
Information System Engineering Department
Be'er Sheva, 84105, Israel
[2] Rafael – Advanced Defense Systems Ltd., Haifa, Israel
{eitanme,elovici}@bgu.ac.il,gabin@rafael.co.il

Abstract. Currently, there are two ways for an attacker to harm the QoS of a network. The first way is to change the routes the normal production traffic takes. The second way to harm the QoS of a network is to induce extra production traffic that would normally not have been generated. The traffic diversion attacks are considered more subtle and harder to detect. There are various ways for an attacker to implement such attacks. In this short paper we present four such attacks: two OSPF based and two DNS based attacks.

Keywords: Traffic Diversion, Network Attacks, OSPF Attacks, DNS Attacks

1 Introduction

Currently, there are two ways for an attacker to harm the QoS of a network. The first way is to change the routes the normal production traffic takes. This way, the attacker may direct traffic through a narrow link or lengthen its route in order to increase the delay and the packet-loss the traffic experiences. The second way to harm the QoS of a network is to induce extra production traffic that would normally not have been generated. One example of this is a reflected SYN attack in which the attacker sends many spoofed SYN packets to various end hosts who respond with SYN-ACK packets. In this example, the extra traffic is induced by the attacker itself (SYN packets), as well as the victim end hosts (SYN-ACK packets). By inducing a high volume of traffic an attacker may exhaust the bandwidth of one or more links in the network. Traffic diversion attacks are considered more subtle and harder to detect. There are various ways for an attacker to implement such attacks. In the following section we describe four variants of such attack.

2 Attack Scenarios

In general, there are two ways for an attacker to harm the QoS of a network. The first way is to change the routes the normal production traffic takes. This way, the attacker may direct traffic through a narrow link or lengthen its route in order to increase the delay and the packet-loss the traffic experiences. The second way to harm the QoS of a network is to induce extra production traffic that would normally not have been generated. One example of this is a reflected SYN attack in which the attacker sends many spoofed SYN packets to various end hosts who respond with SYN-ACK packets. In this example, the extra traffic is induced by the attacker itself (SYN packets), as well as the victim end hosts (SYN-ACK packets). By inducing a high volume of traffic an attacker may exhaust the bandwidth of one or more links in the network.

The first attack type is considered more subtle and harder to detect. There are various ways for an attacker to implement such attacks. For example, he may advertise false routing advertisements in order to change the routing tables, he may poison a DNS cache in order to change the destination IP address of the traffic; or he may launch any application-specific impersonation attack in order to divert traffic to a false end host. From the network's point of view, all such attacks have a similar effect, namely, traffic diversion.

The current paper, describes two OSPF and two DNS poisoning attack variants. These attacks are *currently* the most flexible and powerful way to achieve traffic diversion.

The OSPF routing protocol [1] is the most popular intra-domain routing protocol on the Internet. This protocol works by having each router periodically advertise its links to its immediate neighbors. In this way, every router has a complete view of the domain's topology. The routing table is calculated based on this view. The attacks we generated sent spoofed advertisements on behalf of victim routers, while giving other routers a false view of the domain's topology. This altered the routing process in the domain.

2.1 Semi-Disconnecting Attack

The adversary generates a false view of the domain's topology at some routers by sending spoofed OSPF advertisements (LSA) on behalf of a victim router. The spoofed LSA announces only a fraction of the victim's available interfaces. This will logically disconnect the victim's complementary interfaces so that traffic can still pass or be routed through him, though only on the logically connected interfaces. Hence, the victim's is partially "disconnected". An example of this attack, where two out of four of the victim's links are disconnected is demonstrated in Figure 1.

2.2 Link Weight Distortion Attack

In this attack the adversary modifies the weight of a network link (and thus also the routing scheme) by sending spoofed OSPF advertisements to two routers that are connected via a "victim" link. The attack affects the cost of the interfaces that connect the two routers connected through the 'victim' links. The network routing may therefore be affected and become skewed and sub-optimal. Normally, such attack is very hard to detect manually, as all the network's components

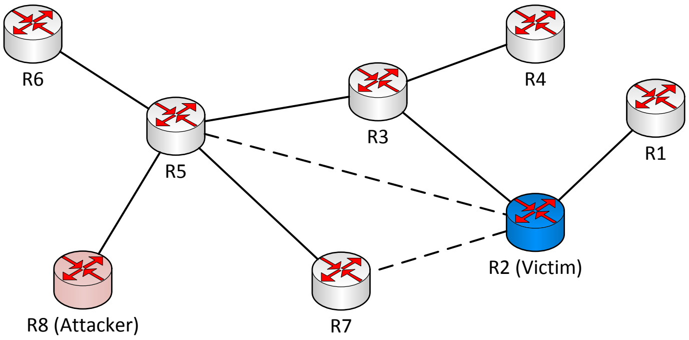

Fig. 1. An example of the "semi-disconnecting" attack. Two of the victim router's links ($R2 \leftrightarrow R5$ and $R2 \leftrightarrow R7$) become disconnected while the rest remain operative.

should still function normally during the attack. An example of the 'link weight distortion' attack is demonstrated in Figure 2.

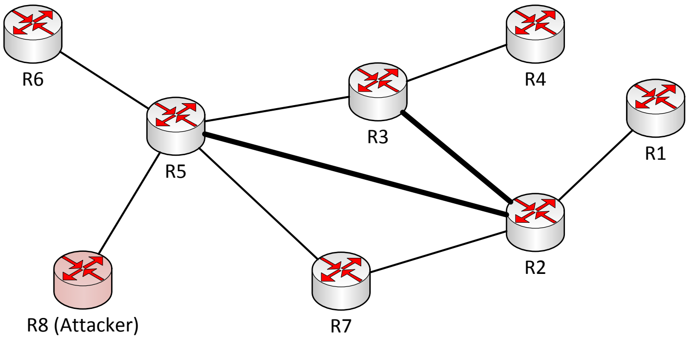

Fig. 2. An example of the link weight distortion attack. Here, the weights of two link ($R2 \leftrightarrow R5$ and $R2 \leftrightarrow R3$) were altered.

2.3 DNS Cache Poisoning

The adversary, in this attack, poisons a fraction of the victim(s) DNS cache table. This attack results with a partially invalid or malicious mappings between symbolic names (URL) and IP addresses. Specifically, in this study we simulated a condition in which the attacker replaces a portion of the original IPs in the victim's DNS table entries with his own IP. The attacker uses a unique destination port in each DNS entry he poisons. On receiving an attack related traffic, the attacker forward it to its original destination, by resolving its destination port. As a result, as exemplified in Figure 3, some of the network's traffic becomes reverted. In this way, the network's endpoint computers receive the service they require, albeit with a reduced QoS.

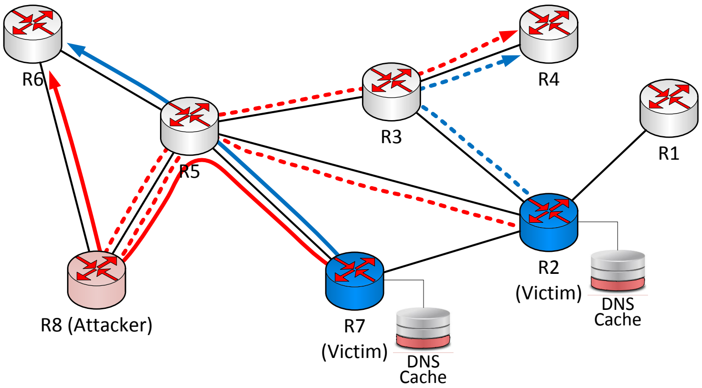

Fig. 3. An example of the DNS cache poisoning attack, where the cache of two routers, $R2$ and $R7$ were poisoned. The solid and the broken lines indicate the routes between $R7$ to $R6$ and $R2$ to $R4$ respectively. The blue lines indicate the optimal routes, and the red lines indicate the routes that the packet would take due to the attack.

2.4 Authoritative DNS Server Poisoning

The attack simulates a scenario where an adversary had either poisoned the DNS cache by compromising an Authoritative DNS server or by forging a response to a recursive DNS query sent by a resolver to an authoritative server. Similar to the DNS cache attack, each poisoned entry at the Authoritative DNS server will contain the IP of the attacker This attack results with a fraction of the traffic made by every node in the network routed to the attacker, instead of to the correct destination. Upon receiving diverted traffic, the attacker will reroute it to the original destination, in order to preserve the network's routing functionality.

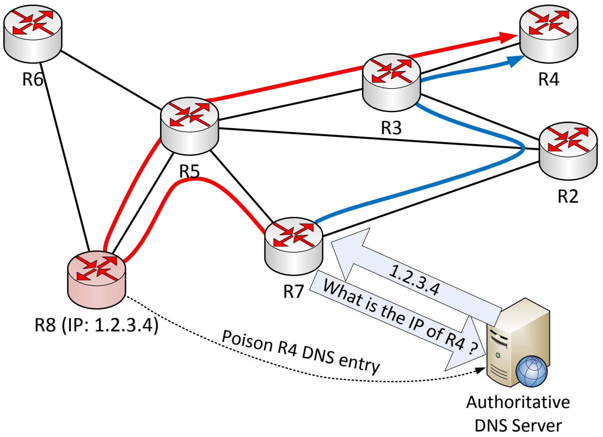

Fig. 4. An example of the authoritative DNS server poisoning attack, in which the affect of a single poisoned Authoritative DNS server entry is illustrated.

References

1. J. Moy. OSPF version 2. IETF RFC 2328, Apr. 1998.