Attacking Routers by Packet Misrouting

K. H. YEUNG and W. K. FUNG
Teletraffics and Networking Laboratory
Department of Electronic Engineering
City University of Hong Kong
Tat Chee Avenue
HONG KONG

Abstract: - Malicious misrouting of packets is a kind of packet mistreatment attack. In such attack a malicious router misroute packets so that triangle routing is formed. This kind of attacks is very difficult to detect, and the problem is considered as an open problem. In this paper, how this kind of attacks can be launched by router configurations is discussed. The aim of this discussion is to show that when a router is compromised, it is easy to launch packet mistreatment attacks to a network. With skilful configurations, the paper shows that attacks can be scheduled at specific time intervals. This makes the attacks very difficult to be detected, especially when the network is large. In conclusion, the paper clearly states that the problem of packet mistreatment attack must be addressed by the researchers of the field

Key-Words: - Network Infrastructure Security, Malicious Misrouting, Packet Mistreatment, Triangle Routing, Router Attacks

1 Introduction

It is widely accepted that network security is very important in the success management of computer networks. This awareness is partly due to the attacks to many high profile web sites such as Amazon and Yahoo [1]. Due to the success of these attacks, network administrators are finding ways to improve the security of their networks. Vendors are also providing solutions which could help in this aspect. So far the attention on network security is mainly paid on securing the corporate information and servers only. Less research work has been done on securing the network infrastructure itself. This includes the protection on network infrastructure equipment such as routers and switches. With the growing fear of cyber terrorism, researchers start to think of all possible means of attacks including those aimed at the network infrastructure.

A very good discussion on Internet infrastructure security is given in [2] with taxonomy of security attacks being provided. The taxonomy describes four types of infrastructure attacks, and packet mistreatment is one of them. In packet mistreatment, either a link attack or a router attack can be launched by a malicious router. To launch a link attack, a malicious router can interrupt, modify/fabricate, or replicate data packets. Mistreating packets in these ways can cause network congestion and throughput lowering, and can also be used to launch DoS attacks. Solutions to link attacks include the WATCHERS project [3], the use of packet dropping profiles and intrusion detection [4], and the use of IPSec [5].

In addition to link attacks, router attacks can also be launched by a malicious router if it deliberately misroutes packets. Instead of forwarding packets that follows the best path, packets are misrouted maliciously to a wrong direction. This results in an intractable problem of triangle routing as illustrated in Figure 1. In the figure, all links have a default cost of 64 (i.e. the cost for T1 links) except the link connecting routers *R2* and *R*3 together. When a packet sourced from Net-1 is sent to Net-2, the shortest path should be *R3-R1-R2-R4*. This is the expected path in normal packet forwarding. If *R2* is a malicious router, however, it may mishandle the packet by sending the packet out to its link FastEthernet0/0 (i.e. send the packet to *R3)*. In that case a routing loop is formed and the packet will circulate until its TTL value expires. When substantial number of such packets are circulated in the loop, it may overload the routers and cause network congestion. The problem becomes even more intractable if the router only misroutes packets selectively (says only for selected networks or hosts at random time intervals), or if the number of routers involved in the routing loop is large.

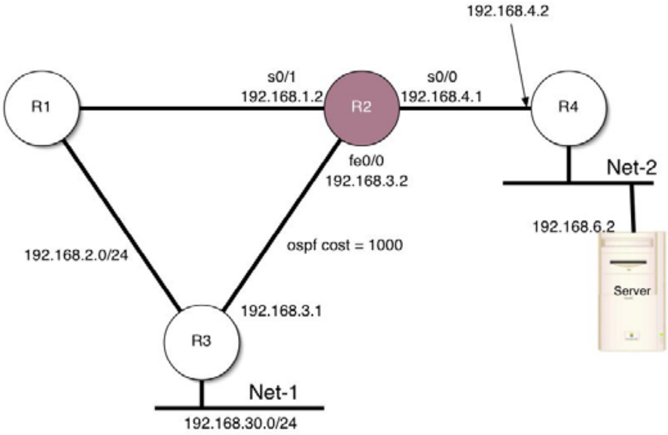

Figure.1 The network under study

Currently the only two solutions (that the authors of this paper aware of) to this problem are discussed in [3] and [6]. The problem is indirectly discussed in [3] when the problem of link attacks is addressed. To solve the problem, each router has to keep the routing tables of its neighbouring routers. Misroute counters are also set up in each router to count the misrouted packets sent from the neighbouring routers. When a counter exceeds a certain threshold, an alarm is sent. Another simpler solution is proposed in [6]. The method described is to discard all packets that are sent and received by the same router interface. However, this simple method can only prevent a naive router attack. As mention in [2], it remains an open problem to detect and prevent more sophisticated router attacks. The authors of this paper are currently working on possible solutions to this problem.

Despite of the efforts on solving the problem of packet misrouting, no research work on how to create the problem is aware of in the literature. To fill this missed effort, this paper discusses the methods to create the problem by router configurations. Due to their large market share, Cisco routers are considered in our discussions. But the methods discussed should also apply to all other router platforms and implementations (e.g. Juniper and Bay). The purpose of our discussions is to show that the problem of packet misrouting is serious and should not be overlooked by network administrators.

2 Router Attacks by Misrouting Packets

In this section, we discuss how packets can be misrouted by router configurations. We assume that a router has already been compromised, and the configuration file of the router can be modified freely. Please refer to [7,8] on how to exploit a router. We first discuss how static routes can be used for packet misrouting attacks. We then discuss more sophisticated attacks by using Access Control Lists (ACLs).

2.1 Static Routes

To see why setting up static routes can launch router attacks, refer back to our earlier discussion on Figure 1. Suppose we have a server on Net-2 with IP address 192.168.6.2. Note that *R*2 is the compromised router. Under normal condition *R*2 will forward packets destined to 192.168.6.2 to R4. But if we set up a static route (in *R*2) which forwards all these packets to *R*3, a routing loop for the address 192.168.6.2 is created. Figure 2 shows the configuration of *R*2 with the static route setting being highlighted. Note that this static route is *not* redistributed to the OSPF routing process in *R*2. This means that other routers will not know about this static route in *R*2 (see Figure 3 for the routing table of *R*3).

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router2
!
enable secret 5
$1$foQK$0OgJk/3BMv6FUOA.g1F3q1
!
!
!
!
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!
!
!
process-max-time 200
!
interface FastEthernet0/0
 ip address 192.168.3.2 255.255.255.0
 no ip directed-broadcast
 ip ospf cost 1000
!
interface Serial0/0
 ip address 192.168.4.1 255.255.255.0
 no ip directed-broadcast
!
interface Serial0/1
 ip address 192.168.1.2 255.255.255.0
 no ip directed-broadcast
!
router ospf 10
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.4.0 0.0.0.255 area 0
!
ip classless
ip route 192.168.6.2 255.255.255.255
192.168.3.1
no ip http server
!
!
line con 0
 password 3star
 login
 transport input none
line aux 0
line vty 0 4
 password 3star
 login
!
!
no scheduler allocate
end
```

Figure 2 Static route setting to launch a packet misrouting attack.

The reason why only one IP address is used (instead of the whole Net-2 subnet) in the static route is that it makes the network administrator difficult to aware of the attack. Since when the administrator tries to ping other workstations on Net-2, it will work. Of course the hacker can set up multiple static routes on multiple IP addresses in order to put a much heavier load to the network.

2.2 Access Control Lists

It is easier for the network administrator to detect an attack if packet misrouting occurs at all time. If the misrouting appears to be happening at random, the administrator may misinterpret an attack as a network congestion problem. This sidetracks the administrator and makes the attack to be more successful. To launch such random attacks, time

```
Router3#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

C    192.168.30.0/24 is directly connected, Ethernet1
O    192.168.4.0/24 [110/192] via 192.168.2.1, 03:20:50, Serial0
O    192.168.6.0/24 [110/193] via 192.168.2.1, 03:20:50, Serial0
O    192.168.1.0/24 [110/128] via 192.168.2.1, 03:20:51, Serial0
C    192.168.2.0/24 is directly connected, Serial0
C    192.168.3.0/24 is directly connected, Ethernet0
```

Figure 3 Routing table of R3: the static route being set in R2 does not appear in R3's routing table.

based access lists can be used. Time based access lists are ACLs that only apply at specified times. A good discussion on ACLs and time based ACLs can be found in [9]. Figure 4 shows the configuration of the malicious router (*R*2 in Figure 1) using a time based access list.

```
.
.
.

ip route 192.168.6.0 255.255.255.0
192.168.3.1
ip route 192.168.6.0 255.255.255.0
192.168.4.2

access-list 101 deny   ip 192.168.30.0
0.0.0.255 192.168.6.0 0.0.0.255
time-range block-ip

access-list 101 permit ip any any
access-list 102 permit ip any any
time-range block-ip

time-range block-ip
 absolute start 20:45 18 June 2003 end
21:00 18 July 2003
 periodic Wednesday 20:45 to 21:00
.
.
.
interface Serial0/0
 ip access-group 101 out

interface FastEthernet0/0
 ip access-group 102 out
.
.
.
```

Figure 4 Time based access lists can launch an attack at a specified time.

In the configuration shown in Figure 4, two static routes have been set: the first one points to the wrong direction (192.168.3.1) and the second one to the correct one (192.168.4.2). By using two access control lists (101 and 102), we can control the packet flows, sourced from 192.168.30.0 and destined to 192.168.6.0, under different time intervals. Access list 101 is applied on the link connecting R4, and the list 102 is applied on the link connecting R3. The attack is scheduled at 20:45 to 21:00 on every Wednesday starting from June 18, 2003 to July 18, 2003. Since one attack only last for 15 minutes, it becomes extremely difficult for the administrator of the network to find out what is actually happening. This is particularly true if the network is large (e.g. there are fifty routers in the network and each router has a configuration file with hundreds of lines). Note that we can also modify the access lists to launch attacks for specific services only (e.g. WWW or SMTP). This further complicates the process in detecting the attacks.

Figure 5 shows the results when the network is not under attacked. As observed from Figure 5 (a), the first statement of access list 101 is inactive. Only the operation specified by the second statement will

```
Router2#sh clock
20:35:45.395 UTC Tue Jul 8 2003
Router2#sh access-list

Extended IP access list 101
   deny ip 192.168.30.0 0.0.0.255 192.168.6.0 0.0.0.255 time-range
(inactive) (440 matches)
   permit ip any any (4032 matches)
Extended IP access list 102
   permit ip any any time-range block-ip (inactive) (16987 matches)
```

(a) Results on packet matching in R2.

```
C:\>tracert 192.168.6.2

Tracing route to 192.168.6.2 over a maximum of 30 hops

  1     2 ms     2 ms     2 ms  192.168.30.1
  2    25 ms    26 ms    26 ms  192.168.2.1
  3    25 ms    25 ms    25 ms  192.168.1.2
  4    50 ms    50 ms    50 ms  192.168.4.2
  5    59 ms    59 ms    59 ms  192.168.6.2

Trace complete.
```

(b) Trace route from 192.168.30.0.

Figure 5 Experimental results – network is not under attacked.

```
Router2#sh clock
20:50:49.271 UTC Tue Jul 8 2003

Router2#sh access-list

Extended IP access list 101
   deny ip 192.168.30.0 0.0.0.255 192.168.6.0 0.0.0.255 time-range block-ip (active) (440
matches)
   permit ip any any (4116 matches)
Extended IP access list 102
   Permit ip any any time-range block-ip (active) (17005 matches)
```

(a) Results of packet matching in R2.

```
C:\>ping -t 192.168.6.2

Pinging 192.168.6.2 with 32 bytes of data:

Reply from 192.168.2.1: TTL expired in transit.
Reply from 192.168.2.1: TTL expired in transit.
Reply from 192.168.2.1: TTL expired in transit.
Reply from 192.168.2.1: TTL expired in transit.
Reply from 192.168.2.1: TTL expired in transit.
Reply from 192.168.2.1: TTL expired in transit.
Reply from 192.168.2.1: TTL expired in transit.
Reply from 192.168.2.1: TTL expired in transit.
Reply from 192.168.2.1: TTL expired in transit.
Reply from 192.168.2.1: TTL expired in transit.
Reply from 192.168.2.1: TTL expired in transit.
Reply from 192.168.2.1: TTL expired in transit.
Reply from 192.168.2.1: TTL expired in transit.
```

(b) Trace route from 192.168.30.0.

Figure 6 Experimental results – the network is under attacked.

be performed (i.e. to permit the forwarding of all ip packets) This also means that all packets sourced from 192.168.30.0 and destined to 192.168.6.0 will be forwarded to *R*4 as normal. From the figure it is also observed that the only statement in access list 102 is inactive. Since the implicit last statement of all access lists is to deny all packet forwarding, packets sourced from 192.168.30.0 and destined to

192.168.6.0 will therefore *not* allow to be forwarded out to the FastEthernet0/0 interface (i.e. not forward to *R*3). When tracing the route from 192.168.30.0 to 192.168.6.2, we observed that the response is normal (see Figure 5(b)).

Figure 6 shows the results when the network is under attacked. As observed, packets sourced from 192.168.30.0 and destined to 192.168.6.0 are not allowed to flow to R4. Instead, they are forwarded to R3. This forces the packets to circulate in the loop until their TTL values expire (see Figure 6 (b)).

3 Conclusion

In this paper methods to launch router attacks have been discussed. The objective of the discussion is to show that when a router is compromised, it can easily be used to launch router attacks. The discussion so far is only on OSPF routing protocol. We believe, however, similar techniques can be used in other routing protocols. The aim of this paper is to make the researchers of the field aware of the importance of the problem, i.e. network attacks by packet mistreatment. It is our hope that after the publication of this present work, more research work on the problem will be triggered.

References:

[1] K. J. Houle and G. M. Weaver, "Trends in Denial of Service Attack Technology," CERT Advisory, v1.0, October 2001.

[2] Anirban Chakrabarti and G. Manimaran, “Internet Infrastructure Security: A Taxonomy,” *IEEE Network*, November/December 2002, pp.13-21.

[3] K. A. Bradley *et al.*, “Detecting Disruptive Routers: A Distributed Network Monitoring Approach,” *Symp. Security Privacy*, May 1998, pp.115-124.

[4] X. Zhang *et al.*, “Malicious Packet Dropping: How It Might Impact the TCP Performance and How We Can Detect It,” *Symp. Security Privacy*, May 1998, pp.263-272.

[5] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol,” RFC 2401, November 1998.

[6] Cisco-DOS Cisco White Papers, “Strategies to Protect against Distributed Denial of Service Attacks (DDoS),” February 2000.

[7] Mark Wolfgang, "Exploiting Cisco Routers (Part One)," www.securityfocus.com/infocus/1734.

[8] Mark Wolfgang, "Exploiting Cisco Routers (Part Two)," www.securityfocus.com/infocus/1749.

[9] Gil Held and Kent Hundley, *Cisco Access Lists*, McGraw-Hill, 2000.