Implement anti-spoofing to prevent DNS Amplification Attack

MAEMURA ‘maem’ Akinori
maem@maem.org
for
MATSUZAKI ‘maz’ Yoshinobu
maz@iij.ad.jp
ip spoofing

creation of IP packets with source addresses other than those assigned to that host
Malicious uses with IP spoofing

• impersonation
  – session hijack or reset
• hiding
  – flooding attack
• reflection
  – ip reflected attack
impersonation

sender

ip spoofed packet

coll src: partner
dst: victim

partner

victim

Oh, my partner connected to me. I'll serve him.
hiding

sender

ip spoofed packet

src: random
dst: victim

Oh what a DOS attack, who are they? I will pay them back later…

victim
reflection

sender

ip spoofed packet

src: victim
dst: reflector

reflector

reply packet

src: reflector
dst: victim

victim

Ooops, a lot of replies without any request...
ip reflected attacks

• smurf attacks
  – icmp echo (ping)
  – ip spoofing(reflection) + amplification (multiple replies)

• dns amplification attacks
  – dns query
  – ip spoofing(reflection) + amplification (bigger reply / multiple replies)
amplification

1. multiple replies

2. bigger reply
DNS amplification attack

IP spoofed DNS queries

Attacker

DNS replies

victim
solutions for ip reflected attacks

- **Prevent IP spoofing**
- **Disable open amplifiers**

**diagram:**
- Attacker
- IP spoofed packets
- Open amplifier
- Replication
- Victim

- Prevent IP spoofing
- Disable open amplifiers
two solutions

• disable amplification
  – disable ‘directed-broadcast’, ‘open dns server’
    • Actually we need to accept dns queries for resolution of our own zone.
    • But we can limit recursive query to limited area that server need to serve.

• prevent ip spoofing!!
  – source address validation
  – BCP38 & BCP84
Source Address Validation

• Check the source ip address of incoming ip packets close to the network edge
  – BCP84/RFC3704
    • updating BCP38/RFC2827
    • It is important for ISPs to implement ingress filtering to prevent spoofed addresses being used, both to curtail DoS attacks and to make them more traceable, and to protect their own infrastructure.
How to configure the checking

• ACL
  – packet filter

• uRPF check
  – uRPF: Unicast Reverse Path Forwarding
  – using ‘routing table’
  – look-up the return path for the source ip address
cisco ACL example

ISP Edge Router

point-to-point 10.0.0.0/30

customer network 192.168.0.0/24

ip access-list extended fromCUSTOMER
permit ip 192.168.0.0 0.0.255.255 any
permit ip 10.0.0.0 0.0.0.3 any
deny ip any any
!
interface Gigabitethernet0/0
ip access-group fromCUSTOMER in
!
juniper ACL example

```
; firewall family inet {
  filter from CUSTOMER {
    term CUSTOMER {
      from source-address {
        192.168.0.0/16;
        10.0.0.0/30;
      }
      then accept;
    }
    term Default {
      then discard;
    }
  }
}
[edit interface ge-0/0/0 unit 0 family inet]
filter {
  input from CUSTOMER;
}"
```
cisco uRPF example

ISP Edge Router

interface Gigabitethernet0/0
ip verify unicast source reachable-via rx

customer network
192.168.0.0/24

point-to-point
10.0.0.0/30
juniper uRPF example

ISP Edge Router

point-to-point
10.0.0.0/30

customer network
192.168.0.0/24

[edit interface ge-0/0/0 unit 0 family inet]
rpf-check;