DNS Reflection Attacks

Joe Abley <jabley@ca.afilias.info>

AfNOG, Nairobi, May 2006

Denial of Service Attacks

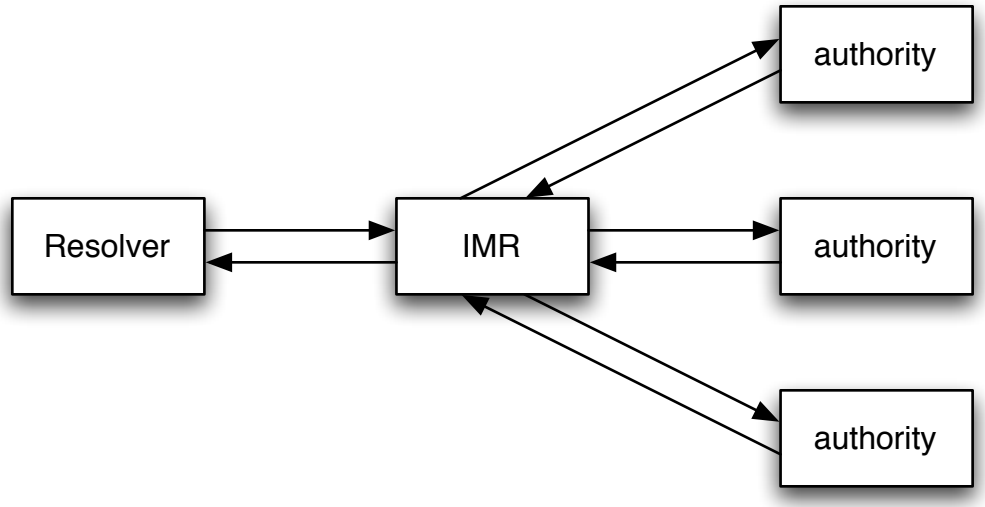
- Attacks which interfere with normal Internet services, making them unusable
- Usually take the form of high volumes of queries or other traffic which overloads networks or servers
- Many attacks today are motivated by money

DNS Infrastructure

- The DNS is an essential component of Internet infrastructure
  - authority servers
  - intermediate-mode resolvers (caches)
  - resolvers (clients)

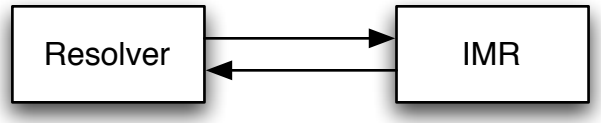
Normal Operation

- Resolvers send small queries, and receive back (usually) fairly small replies
- The IMR contains a cache, so authority servers are consulted relatively infrequently



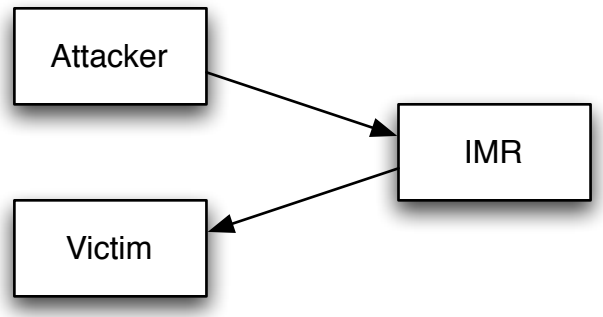
Normal Operation

- Frequently-requested answers are cached
- The lifetime of cached answers is controlled by TTL parameters, which originate from the authority servers



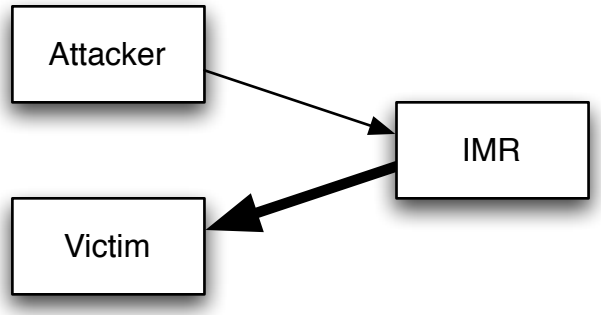
Source-Spoofed Query

- By sending a request from a spoofed source address, an attacker can cause a response to be sent to a third party
- The victim would normally discard the answer, since it doesn't correspond to any outstanding request



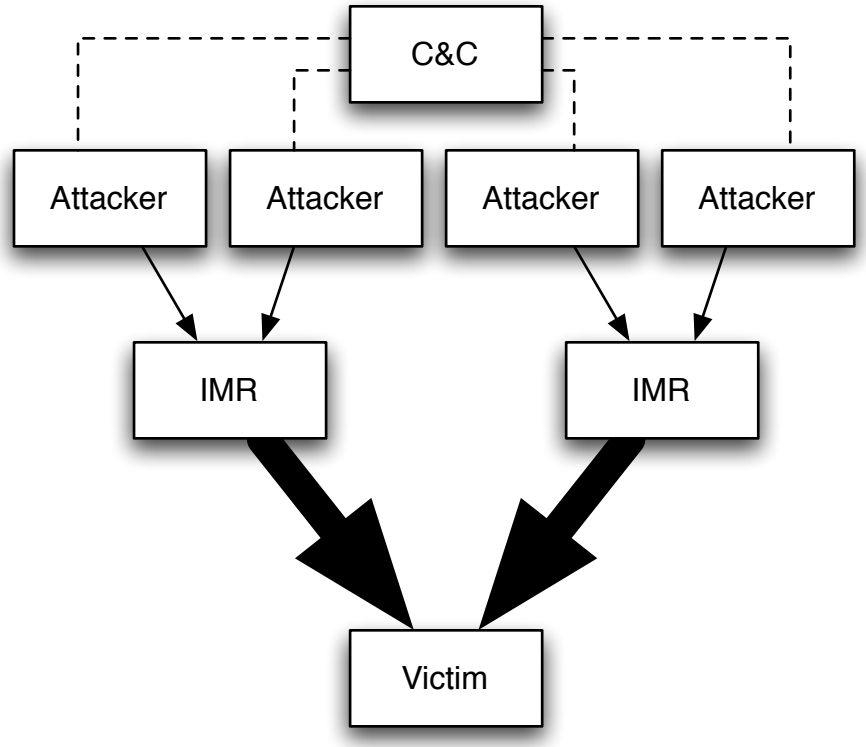
Amplification

- Attacker spoofs request with an answer which is larger than the question
- Victim receives more bits than the attacker sends
- 60x amplification is possible with the right questions and answers



Distributed Amplification

- If many attackers can be made to spoof requests at once, the victim can be quickly overwhelmed
- Thousands of IMRs can be used simultaneously
- Botnets of over 50,000 attackers have been documented



An Internet-Wide Problem

- Much African content is hosted outside Africa, effectively reducing the number of attack targets within the continent
  - much, but not all
  - local content is growing
  - clients are targets, too
- You don't need much bandwidth to launch an attack at someone else, somewhere else

Attack Impact

- Individual hosts can be brought to their knees
- Upstream networks can be clogged with traffic to the extent that routers and links are overwhelmed
- Attacks can last for a long time

Tracking Attacks

- From the victim's perspective, the traffic is coming from a very large number of different sources (the abused IMRs)
- From the IMRs' perspective, the traffic is coming from a very large number of different sources too (the bots)
- The bots are generally compromised machines run by naïve end-users

Attack Mitigation

- Making the traffic stop is hard (many, many people to contact)
- Distinguishing bad traffic from good traffic is often possible, but blocking it can be difficult (large ACLs which need frequent revision)
- Blocking DNS replies altogether may not be useful (collateral damage)

How is this Possible?

- What do the attackers need in order for their attacks to succeed?
  - source of large RRsets on authority servers
  - IMRs which will perform recursive lookups for everybody
  - established botnets
  - bots which are able to spoof requests from victim source addresses

Large RRsets

- In some attacks, throwaway domains are primed with large records
- Other times, vulnerable authority servers are compromised and the records are inserted
  - removing delegations or RRsets can stop the attacks growing (but cached records remain cached)

Naturally-Large RRsets

- Existing, production RRsets may be more difficult to remove from the DNS
  - smaller amplification, but greater persistence

AOL.COM IN MX?

```
;; QUESTION SECTION:
;aol.com.                       IN      MX

;; ANSWER SECTION:
aol.com.                3600    IN      MX      15 mailin-01.mx.aol.com.
aol.com.                3600    IN      MX      15 mailin-02.mx.aol.com.
aol.com.                3600    IN      MX      15 mailin-03.mx.aol.com.
aol.com.                3600    IN      MX      15 mailin-04.mx.aol.com.

;; AUTHORITY SECTION:
aol.com.                3600    IN      NS      dns-01.ns.aol.com.
aol.com.                3600    IN      NS      dns-02.ns.aol.com.
aol.com.                3600    IN      NS      dns-06.ns.aol.com.
aol.com.                3600    IN      NS      dns-07.ns.aol.com.

;; ADDITIONAL SECTION:
mailin-01.mx.aol.com.   300     IN      A       64.12.137.249
mailin-01.mx.aol.com.   300     IN      A       205.188.156.185
mailin-01.mx.aol.com.   300     IN      A       205.188.158.121
mailin-02.mx.aol.com.   300     IN      A       64.12.138.185
mailin-02.mx.aol.com.   300     IN      A       205.188.155.89
mailin-02.mx.aol.com.   300     IN      A       205.188.157.25
mailin-03.mx.aol.com.   300     IN      A       64.12.138.57
mailin-03.mx.aol.com.   300     IN      A       64.12.138.120
mailin-03.mx.aol.com.   300     IN      A       205.188.157.217
mailin-03.mx.aol.com.   300     IN      A       205.188.159.57
mailin-04.mx.aol.com.   300     IN      A       64.12.138.89
mailin-04.mx.aol.com.   300     IN      A       64.12.138.152
mailin-04.mx.aol.com.   300     IN      A       205.188.156.249
mailin-04.mx.aol.com.   300     IN      A       205.188.159.217

;; Query time: 900 msec
;; SERVER: 196.200.222.1#53(196.200.222.1)
;; WHEN: Sun May 14 11:46:12 2006
;; MSG SIZE  rcvd: 443
```

Open IMRs

- Many IMRs will happily perform recursive queries for anybody on the Internet
  - useful for debugging DNS problems
  - useful for supporting roaming users
- Many open IMRs can be restricted to serve a more limited subset of the Internet without impacting service

If all IMRs were closed...

- ... there would still authority servers to abuse
  - authority servers are necessarily open
  - amplification is still possible (e.g. via referrals to the root servers)
  - modifying this behaviour has the potential to impact all IMRs, which might destabilise the DNS

Eradication of Botnets

- Botnets are generally managed through a loosely-coordinated game of whack-a-mole
- There will be bots as long as there are software defects on end-user machines which can be exploited
  - i.e. there will always be bots

Bot Chasing

- The NSP-SEC community spends a lot of time every day chasing and closing down botnets
- This neither prevention nor cure, but it's arguably better than doing nothing
- https://puck.nether.net/mailman/listinfo/nsp-security

What's left?

- The fundamental requirement for this attack to succeed is for attacking hosts to be able to source packets from a victim's IP address
  - "source spoofing"
  - this is not a new vulnerability
  - other attacks which don't involve the DNS also exploit the ability to spoof

RFC 2827/BCP 38

Network Working Group
Request for Comments: 2827
Obsoletes: 2267
BCP: 38
Category: Best Current Practice

P. Ferguson
Cisco Systems, Inc.
D. Senie
Amaranth Networks Inc.

May 2000

Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

One-Slide BCP38 Summary

- **Drop packets if the source address isn't genuine**

Cost-Benefit Analysis

- The short-term cost-benefit equation for BCP 38 deployment does not favour deployment
  - deployment costs money
  - deployment earns no additional revenue
  - deployment helps the competition!

Longer-Term

- Non-Deployment of BCP 38 hurts the Internet
  - without a functional Internet, we are all looking for new jobs
- The cost of dealing with attacks is high
  - encouraging other people to do the right thing will save us money, eventually

Predictions

- ISPs will refuse to peer with people who don't don't do BCP 38
- Content providers will refuse to buy service from ISPs who don't do BCP 38
  - note: you can start making this prediction true right now!

How Can I Help?

- If you have a choice of Internet access suppliers, give your business to companies who are doing the right thing
  - *especially* if you are a government or educational institution
  - increases the cost of not deploying BCP38 for ISPs

How Can I Help?

- Be tidy at the edge of your network
  - don't let outbound packets with foreign source addresses escape
  - if you can distinguish good from bad, don't let inbound packets with bad source addresses in

If you are an ISP

- **Do not let your customers spoof their source addresses!**
- Remember we need technical measures, not commercial or legal ones
  - customers with infected machines don't know what their machines are doing

Cost of BCP38

- For a very large network with multi-homed customers, the cost of deploying BCP38 can be non-trivial
- For smaller networks with mainly single-homed customers, the cost is much lower
  - many African ISPs fall into the second category

Toolbag

- Unicast RPF (loose-mode, strict-mode)
- Manually-maintained access-lists
- RADIUS anti-spoofing filters
- AfNOG 2006 BCP38 workshop (see instructors for details, materials)

Questions?