RIPE "IP Anti-Spoofing" Task Force

Daniel Karrenberg

Document ID: ripe-379
Date: 16 May 2006

---

1. Introduction

IP source address spoofing is the practice of originating IP datagrams with source addresses other than those assigned to the host of origin. In simple words, the host pretends to be some other host.

This can be exploited in various ways, most notably to execute Denial of Service (DoS) amplification attacks that cause an amplifier host to send traffic to the spoofed address.

There are many recommendations to prevent IP spoofing by ingress filtering, e.g. checking source addresses of IP datagrams close to the network edge.

Most equipment vendors support ingress filtering in some form.

Yet recently, significant DoS amplification attacks have happened that would be impossible without spoofing.

This demonstrates that ingress filtering is definitely not deployed sufficiently. Unfortunately, there are no direct benefits to an Internet Service provider (ISP) that deploys ingress filtering. Also, there is a widely held belief that ingress filtering only helps when it is universally deployed.

At RIPE 52 in Istanbul, RIPE established a task force that promotes deployment of ingress filtering at the network edge by raising awareness and provide indirect incentives for deployment.

---

2. Charter

This task force shall

- raise awareness about this issue among network operators,
- inform about operational methods to implement ingress filtering,
- collect and channel requirements to equipment vendors where appropriate,

and

- seek ways to provide incentives and benefits to operators that do implement ingress filtering.

The task force shall have completed its task when

- network operators cannot reasonably claim not to be aware of the issue,
- information about ways to deploy ingress filtering are readily available

and

- any incentives that it may have devised have become available.

The task force shall be disbanded when these tasks have been completed or when there is consensus within RIPE that completion of the tasks is no longer realistic.

---

3. Time-Line

RIPE 52: BoF and Establishment of Task Force
Quickly draft and publish a RIPE recommendation citing existing work.
Compile How-To with (pointers to) vendor documentation and operational experience reports.
Establish liaison with MIT ANA Spoofer Project and promote their tools.
Analyse Spoofer data for the RIPE region.

RIPE 53: Published "RIPE Recommendation on Ingress Filtering".
Published first edition of "Ingress Filtering How-To".
Collect any critical requirements to be communicated to equipment vendors.
First analysis of Spoofer data.
Discuss possible incentive schemes.
Revise and extend How-To.
Devise possible incentive schemes like a "Source Address Clean" network logo, suitable RIPE Database attributes ...

RIPE 54: Published second edition of "IP Source Address Filtering How-To".
Further analysis of Spoofer data for the RIPE region.
Launch of any incentive scheme.
Implement incentive scheme.
Monitor progress and effectiveness.

RIPE 55: Evaluation and Disbanding of Task Force.

---

4. Contacts

The task force mailing list is <spoofing-tf@ripe.net>.

The web interface for subscriptions and the archive are at http://www.ripe.net/mailman/listinfo/spoofing-tf .

The task force is co-chaired by Nina Hjorth Bargisen (NINA1-RIPE) and Daniel Karrenberg (DK58).

A web page detailing current activities will be set up.

---

5. References

RFC2827 aka BCP38
Network Ingress Filtering:
Defeating Denial of Service Attacks which employ IP Source Address Spoofing
http://www.ietf.org/rfc/rfc2827.txt

SSAC004
Securing the Edge
http://www.icann.org/committees/security/sac004.txt

SSAC008
DNS Distributed Denial of Service (DDoS) Attacks
http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf

ripe-66
RIPE Task Forces
ftp://ftp.ripe.net/ripe/docs/ripe-066.txt

MIT Spoofer Project
http://spoofer.csail.mit.edu/

RFC3024 - Reverse Tunneling for Mobile IP, revised
ftp://ftp.rfc-editor.org/in-notes/rfc3024.txt