Security implications of Network Address Translators (NATs)

(draft-gont-behave-nat-security)

Fernando Gont
UTN/FRH

Pyda Srisuresh
EMC Corporation

76th IETF meeting, November 8-13, 2009
Hiroshima, Japan

Overview

- Includes a number of requirements leading to a security-wise NAT implementations.
- Additionally includes requirements that allow the operation of security mechanisms through NATs.
- Initial version submitted in late 2008, and presented at the IETF 73 meeting (Minneapolis).
- Last revision: draft-gont-behave-nat-security-03
  - Document has been restructured
  - Lots of edits
  - Explicity states the requirements as “REQ-n”

Resilience to Denial of Service Attacks

- The document provides advice for leading with DoS attacks.
- Currently, it only addresses fragmentation

  "REQ-1: A NAT device capable of forwarding out-of-order IP fragments MUST take measures to protect itself against well-known IP fragment based attacks."

Port reservation

- The document discusses issues that may arise when running applications on the NAT itself.

"REQ-2: When a NAT device supports local applications on the device, it is RECOMMENDED that the NAT device reserves specific ports for local use, different from NAT use, so there is no overlap of ports between local use and NAT use. Doing this will ensure there is no possibility of cross session contamination between NAT sessions and local sessions."

P2P communications

- Describes issues that may arise as a result of TCP/UDP hole punching

"REQ-3: Applications attempting to establish peer-to-peer communication across NAT devices using TCP/UDP hole punching technique SHOULD employ relevant authentication mechanism to connect to their peers."

- May remove this one (as a "REQ"), and just leave it as "information".

Secure transport for end-hosts

- Aims at enabling the operation of security-related protocols through the NAT

  "REQ-4: A NAT device MUST permit the traversal of NAT compliant security protocols. Specifically, a NAT device MUST do the following.

  a. A NAT device MUST NOT block traffic directed to or coming from UDP port numbers 500 and 4500.

  b. A NAT device MUST NOT block traffic directed to or coming from TCP/UDP port number 443.

  c. A NAT device MUST NOT include an ALG that treats IKE packets or SSL/TLS packets differently than any other TCP/UDP packet."

Implications of protocol header fields

- From the external realm, packets originated in the external real look as comming from the same system.
- Thus, hosts in the external realm expect in those packets the same properties as if they had been sent from a single system.
- **Failure to comply with these requirements may introduce NEW (i.e., previously inexistent) INTEROPERABILITY problems.**

IP Identification

- The tuple (SrcIP, DstIP, Protocol, IP ID) is not reused to quickly, or else there's else the reassembled packet may be corrupted.

"REQ-5: NATs MUST ensure that a tuple (SrcIP, DstIP, Protocol, IP ID) is not reused while there are still packets in the network with that tuple. Additionally, they SHOULD generate the IP Identification values such that they are not trivially predictable."

TCP SEQ number and ACK number

- BSD-derived sytems (and others) recycle TCPs in the TIME-WAIT state if the ISNs are monotonically-increassing across connections.
- If a NAT does not ensure monotonically-increasing ISNs, connections through the NAT that would have otherwise succeeded might FAIL

  "REQ-6: A NAT MAY rewrite the TCP Sequence Number of packets forwarded to the external realm, such that all connection requests from to a TCP endpoint in the external realm result in monotonically-increasing Initial Sequence Numbers (ISNs). The ISN generator SHOULD select Initial Sequence Numbers such that it is difficult for an off-path attacker to predict the ISNs of future connections. If the NAT rewrites the Sequence Number of packets forwarded to the external realm, it MUST also rewrite the TCP Acknowledgement Number of packets being forwarded into the internal realm."

TCP timestamps

- Same rationale as for rewriting the TCP Sequence Number and the TCP Acknowledgement number.

"REQ-7: A NAT MAY rewrite the TCP timestamps option(TSval) of packets forwarded to the external realm, such that all connection requests from to a specific TCP endpoint in the external realm result in monotonically-increasing timestamps. The timestamps generator SHOULD be such such that it makes it difficult for an off-path attacker to predict the timestamps of future connections. If the NAT rewrites the TCP timestamp of packets forwarded to the external realm, it MUST also rewrite the TCP timestamp echo (TSecr) of packets forwarded from the external realm into the internal realm."

Moving forward

- Any feeback will be appreciated
- TODO:
  - Address a number of other DoS attacks, as suggested off-list by Reinaldo Penno
  - Fix the missing REQ for the TCP Source Port

Should this I-D be adopted as a BEHAVE WG item?