Filtering of ICMP error messages

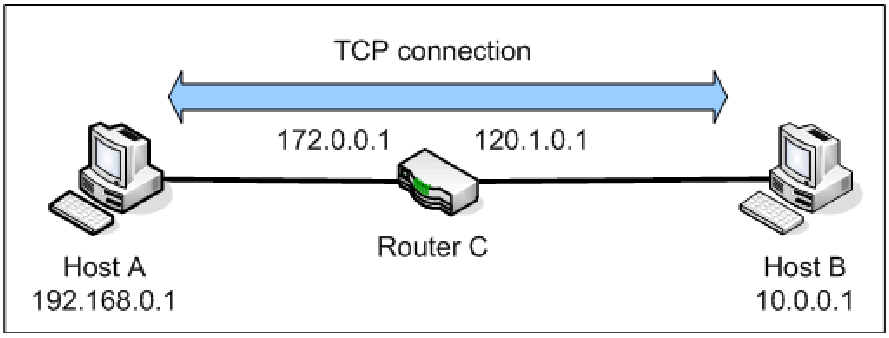
Fernando Gont <fernando@gont.com.ar>
web: http://www.gont.com.ar

Abstract

This document describes the ingress and egress filtering of ICMP error messages. This document came up as an informal explanation (via e-mail) of some of the issues described in the internet-draft “ICMP attacks against TCP” [Gont]. Given that there seems to be some misunderstanding on the filtering of ICMP error messages, that aforementioned informal explanation is herein made publicly available, together with some companion graphics.

1. Problem statement

Let's say that a TCP connection is established between host A (192.168.0.1) and host B (10.0.0.1).



Let's say that a packet sent from Host A to Host B elicits a (legitimate) ICMP error message. Let's say that some intermediate router, Router C (172.0.0.1) detects the error. The contents of the ICMP error message will be:

- Source IP: 172.0.0.1 (on of Router C's IP addresses)
- Destination IP: 192.168.0.1 (that of Host A)
- Innermost packet's source IP address: 192.168.0.1 (that of Host A, as contained in the packet that elicited the error)
- Innermost packet's destination IP address: 10.0.0.1 (that of Host B, for the same reasons)

So, the IP addresses of the innermost packet must be those contained in the IP packet that elicited the ICMP error message. The outermost source IP address must be that of the router that sends the ICMP error message, and the outermost destination IP address must be the IP address of the system that is supposed to get the error.

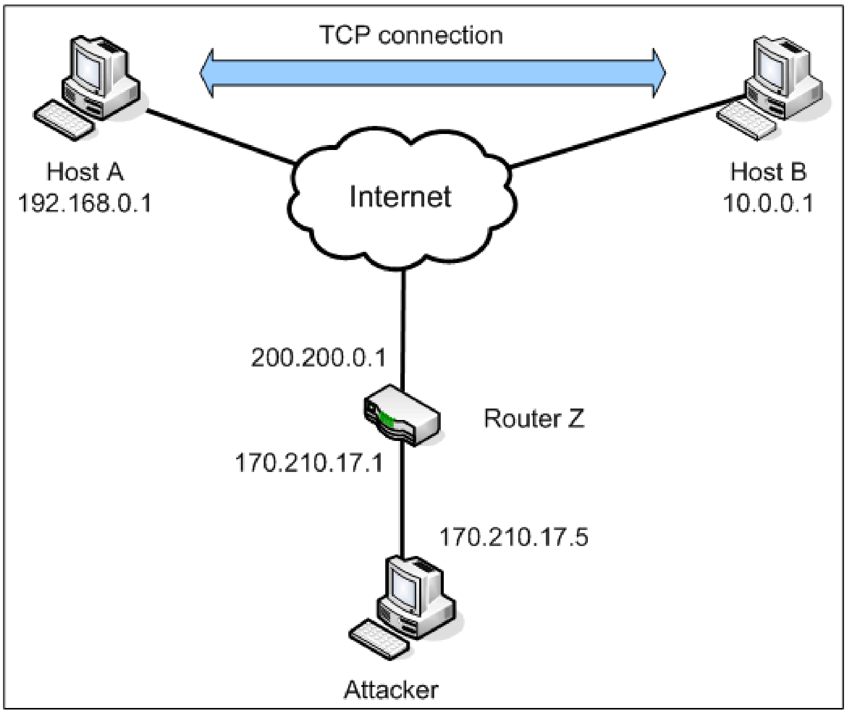
Now, let's suppose that an attacker wants to attack a TCP connection by means of any of the attacks discussed in the "ICMP attacks against TCP" internet-draft [Gont]. In principle, he won't need to spoof the source IP address of the outermost packet (as the ICMP error message could have been elicited by any intermediate router, and the attacked system cannot know the IP addresses of every intermediate router). The destination IP address of the outermost packet will be, of course, that of the target system.

Till this point, we can see that "traditional" ingress/egress filtering (based on the IP addresses of the "outermost" packet) will not help at all, as the attacker does not need to spoof them.

But the attacker does need to forge the IP addresses in the innermost packet, as they must be the ones that correspond to the TCP connection to be attacked.

2. ICMP attacks against TCP

Consider the following scenario:



Host A has established a TCP connection with Host B. Let's suppose that the Attacker wants to perform an ICMP attack. The contents of the ICMP packet would be as follows:

- Outermost packet
  - Source IP address: 170.210.17.5 (He doesn't need to spoof the source address, as he can "pretend" to be an intermmediate router)
  - Destination IP address: 192.168.0.1 (assuming the target is Host A)

- Innermost packet
  - Source IP address: 192.168.0.1 (as the ICMP error message is supposed to have been elicited by one of Host A's packets)
  - Destination IP address: 10.0.0.1 (the other endpoint of the TCP connection).

Now, let's "analyze" this packet from the point of view of Router Z. The source IP address of the outermost packet is "170.210.17.5". There's nothing wrong with that. That host belongs to the network Router Z is connecting to the Internet. The destination IP address of the outermost packet is "192.168.0.1". Again, nothing wrong with this: a host in the local network is sending a packet to some host in the Internet.

However, neither the source IP address of the innermost packet nor the destination IP address of the innermost packet contain an IP address that belongs to the 170.210.17.0/24 network. So, the packet that is supposed to have elicited the ICMP error message could have never been there!

3. Filtering of ICMP error messages

3.1 Packets received on the internal interface

In the case of packets that Router Z received on its interface on the local network (LOCAL_NETWORK), and is supposed to send to the Internet (INTERNET):

- Source IP address of outermost packet: LOCAL_NETWORK (170.210.17.0/24)
- Destination IP address of the innermost packet: INTERNET (i.e., IP != 170.210.17.0/24)
- Source IP address of the innermost packet: INTERNET (i.e., IP != 170.210.17.0/24, in our case)
- Destination IP address of the innermost packet: LOCAL_NETWORK (170.210.17.0/24)

3.2 Packets received on the external interface

In the case of packets that Router Z received on the "external network interface", and is supposed to send to the local network:

- Source IP address of outermost packet: INTERNET (i.e., IP != 170.210.17.0/24, in our case)
- Destination IP address of the innermost packet: LOCAL_NETWORK (i.e., 170.210.17.0/24, in our case)
- Source IP address of the innermost packet: LOCAL_NETWORK
- Destination IP address of the innermost packet: INTERNET

Furthermore, the source IP address of the innermost packet can be required to be the same as the destination IP address of the outermost IP packet.

(You cannot require the destination IP address of the innermost packet to be the same as the source IP address of the outermost packet, as this will only be true for ICMP error messages generated by end-systems).

Note that this check should be performed in intermediate systems, as a kind of "advanced" ingress/egress packet filtering. If this check were enforced by all internet routers, then you could only perform ICMP attacks against TCP connections that have one endpoint in your own network.

4. References

[Gont] Gont, F. “ICMP attacks against TCP”, IETF internet-draft (work in progress). Available at: http://www.gont.com.ar/drafts/icmp-attacks-against-tcp.html