The Greenhouse Effect Attack

Pietro Marchetta Valerio Persico Antonio Pescapé
University of Napoli “Federico II”, Italy
{pietro.marchetta, valerio.persico, pescape}@unina.it

Introduction

IP option-based applications

Powerful Internet measurement techniques

✓ Accurate RTT dissection	[PAM14]
✓ Alias resolution	[CoNEXT13]
✓ Hidden router detection and locationing	[GIS13]
✓ Third-party addresss detection	[SIGCOMM12]
✓ Classic routing violation detection	[IMC12]
✓ Reverse Traceroute	[NSDI10]
✓ …	

We use IP options to perform network attacks!

ICMP Flooding Attack

- The attacker overwhelms the victim with ICMP Echo Request packets
- The victim is forced to generate ICMP Echo Reply packets
- The victim consumes CPU cycles and both incoming and outgoing bandwidth.

Greenhouse Effect Attack (GEA)

- Evolution of ICMP flooding attack
- The victim handles *double* the incoming packets of the ICMP flooding attack
- Network routers are used as unaware yet effective attackers.

GEA

Basic Idea

The attacker (*the Sun*) issues a single IP Timestamp option-equipped ICMP Echo request (*a sunbeam*) towards the victim device (*the Earth*); the solicited ICMP Echo Reply is blocked along the reverse path by a network router (*a greenhouse gas*) and another packet, an ICMP Parameter Problem (*the re-radiation*), is sent back to the victim.

Background

GEA exploits IP Timestamp Option and ICMP Parameter Problem packets.

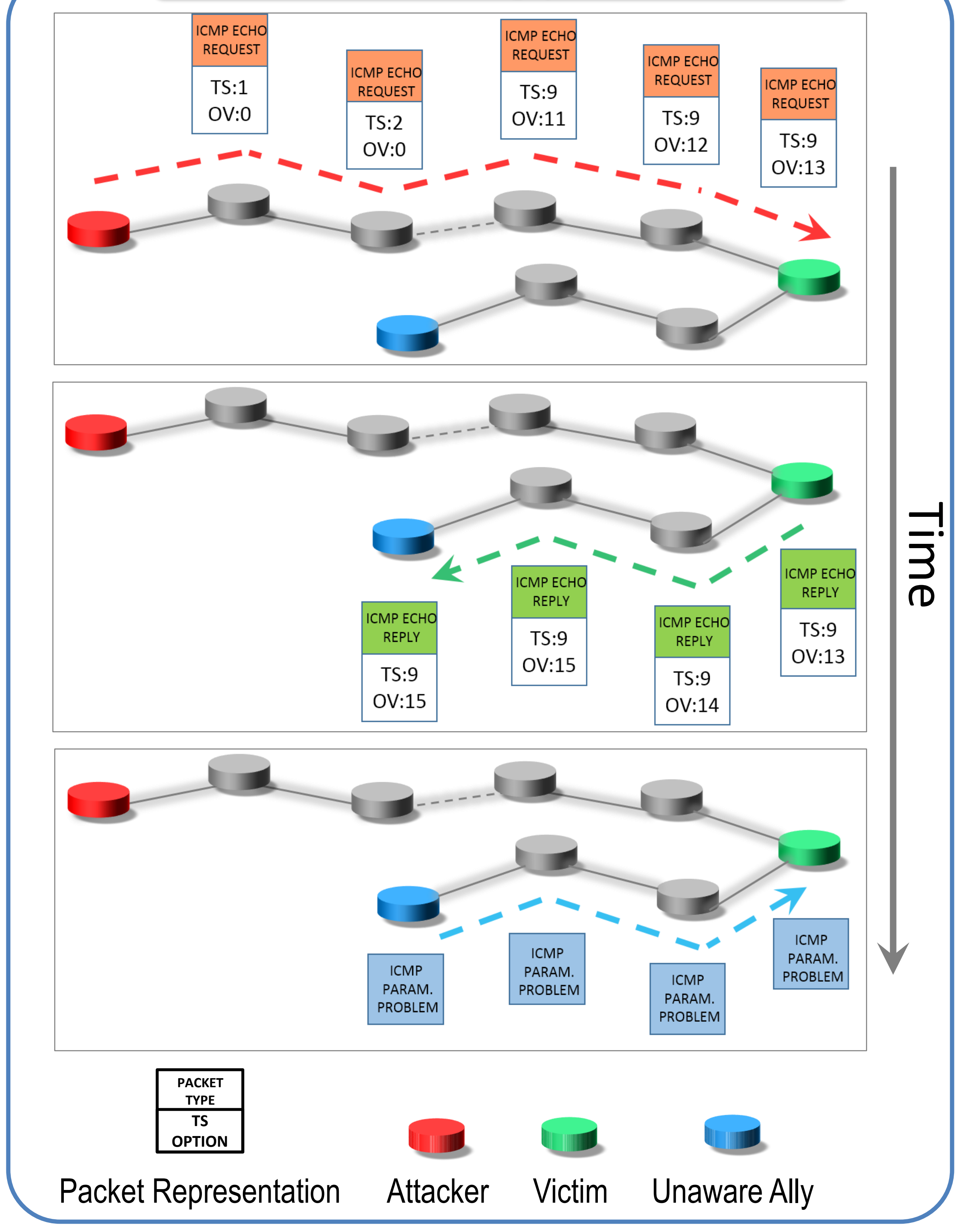
✓ **ICMP Parameter Problem**
Generated when an incoming packet must be discarded and no other ICMP message covers the detected problem.

✓ **IP Timestamp Option**
Each traversed router is requested to

- insert a timestamp into the option data if enough space is available
- increment by one the overflow field, otherwise
- if the overflow field counts itself in overflow, the packet is dropped and an ICMP Parameter Problem message is sent back to the source.

A TS option-equipped packet triggers an ICMP Parameter Problem after having traversed 24 routers managing the option.

Attacking phase



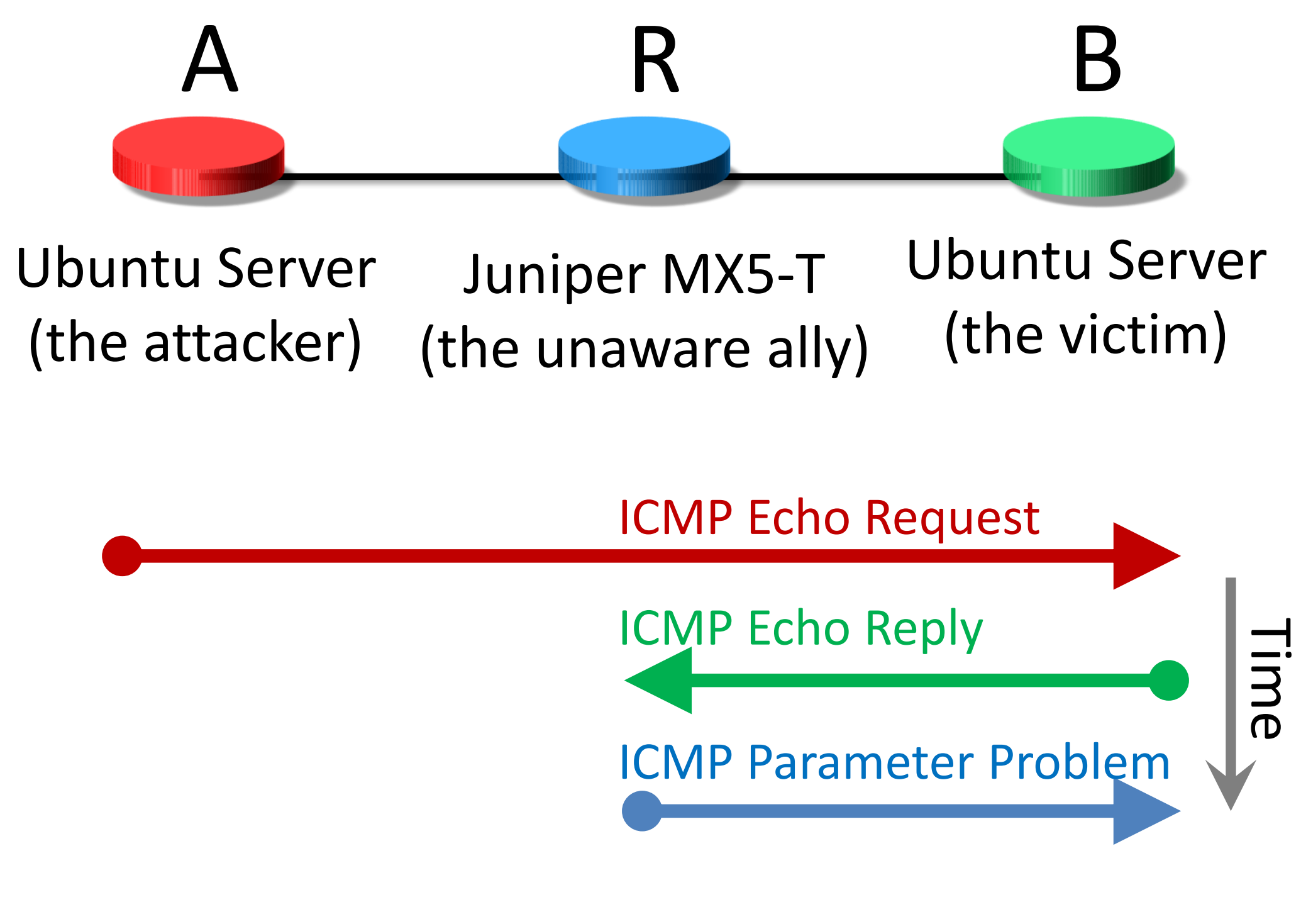
Proposed approach

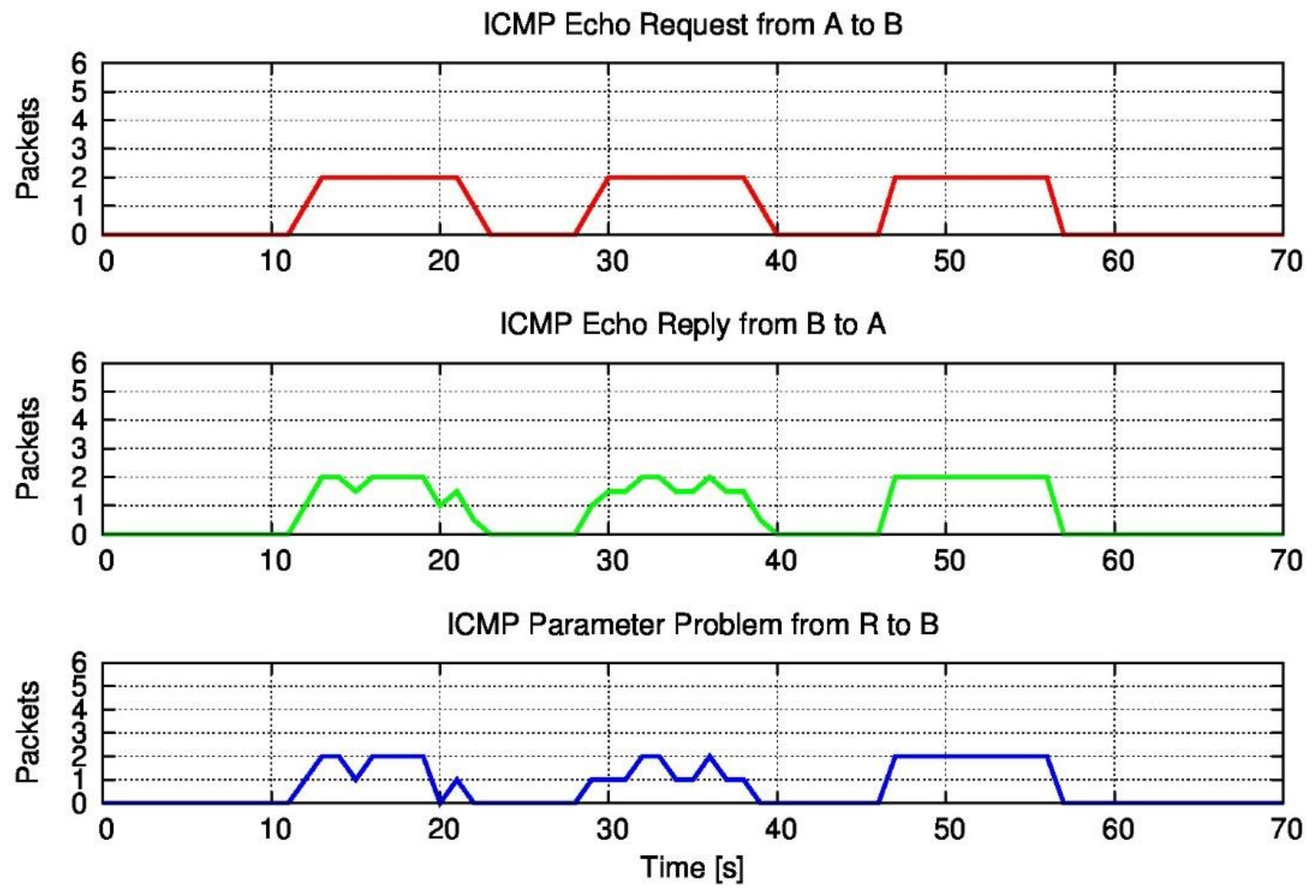
GEA induces a router on the reverse path to (i) drop the ICMP Echo Reply packet, and (ii) generate an ICMP Parameter Problem hitting again the victim.

- **Preliminary phase:** the attacker estimates the number of devices managing the TS option along the reverse path, from the victim back to the attacker.
- **Attacking phase:** the attacker sends a purposely crafted TS-equipped ICMP Echo Request to the victim such that a router along the reverse path (i.e., an *unaware ally*) generates a Parameter Problem message and hits the victim for the second time.

Preliminary results

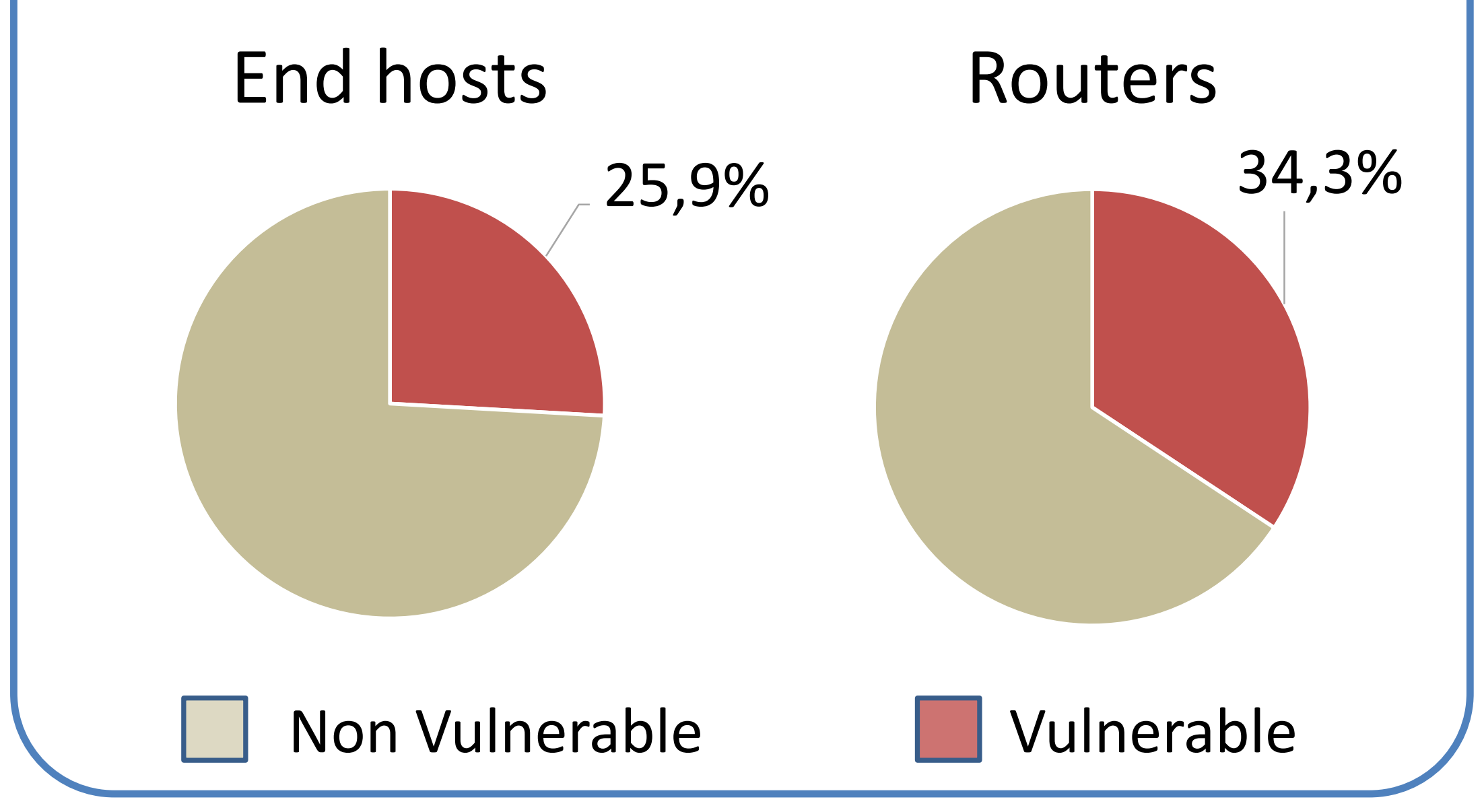
Controlled testbed





Vulnerable targets

Any device replicating the IP Timestamp option inside the ICMP Echo Reply message.



References
[PAM14] P. Marchetta, A. Botta, E. Katz-Bassett, and A. Pescape´, “Dissecting Round Trip Time on the Slow Path Using a One-Packet Approach,” in PAM, 2014.
[CoNEXT13] P. Marchetta, V. Persico, and A. Pescape`, “Pythia: Yet another active probing technique for alias resolution” in ACM CoNEXT, 2013.
[GIS13] P. Marchetta and A. Pescape`, “DRAGO: Detecting, Quantifying and Locating Hidden Routers in Traceroute IP Paths” in IEEE Global Internet Symposium, 2013.
[SIGCOMM12] P. Marchetta, W. de Donato, A. Pescapè “Detecting Third-party Addresses in Traceroute IP Paths” in ACM SIGCOMM, 2012.
[IMC12] T. Flach, E. Katz-Bassett, and R. Govindan. “Quantifying violations of destination-based forwarding on the Internet” in ACM SIGCOMM IMC, 2012.
[NSDI10] E. Katz-Bassett et al., “Reverse traceroute,” in USENIX NSDI, vol. 10, 2010, pp. 219–234.

This work is partially funded by the MIUR projects:
PLATINO (PON01_01007), SMART HEALTH (PON04a2_C), S2MOVE (PON04a3_00058) and SIRIO (PON01 02425).