SAV-based Anti-DDoS Architecture (SAV-D)

Yong Cui, Jianping Wu, **Linbo Hui**, Lei Zhang, Yannan Hu

Tsinghua University, Zhongguancun Laboratory

Mar 29, 2023

Outline

- Problem Statement
- SAV-D Design
- SAV-D Use Case
- Summary

Problem Statement

The deployment of SAV devices is an incremental process.

- Deployment ratio will remain low for time
  - 28% of IPv4 ASes (excluding NAT) and 34% of IPv6 Ases are still spoofable[1]
  - defense effectiveness will be limited by the partial deployment
- Bots migrating from SAV to non-SAV domains
  - partial deployment drives bots to be migrated from SAV to non-SAV domains[2]
  - resulting in fewer spoofed packets being blocked by SAV devices
- No direct incentives for deployers
  - may hinder the further deployment process

SAV's effectiveness under incremental deployment need to be improved.

[1] CAIDA - State of IP Spoofing. https://spoofer.caida.org/summary.php
[2] [CCS'21] Scan, Test, Execute: Adversarial Tactics in Amplification Ddos Attacks

SAV-D Design - Overview

Control Plane (SAV controllers)

- detecting DDoS with spoofing stastics collected from SAV devices
- generating filtering rules based on detection
- issuing rules to SAV and legacy devices
- maintaining IP Blocklists
- sharing threat information to victims' defense

Data Plane (SAV devices, legacy devices, victims' defense)

- SAV devices selectively allow spoofed packets pass through but record and send statistics to the controller, acting as **honeypots**
- SAV and legacy devices can receive filtering rules
- victim's defense can receive threat information

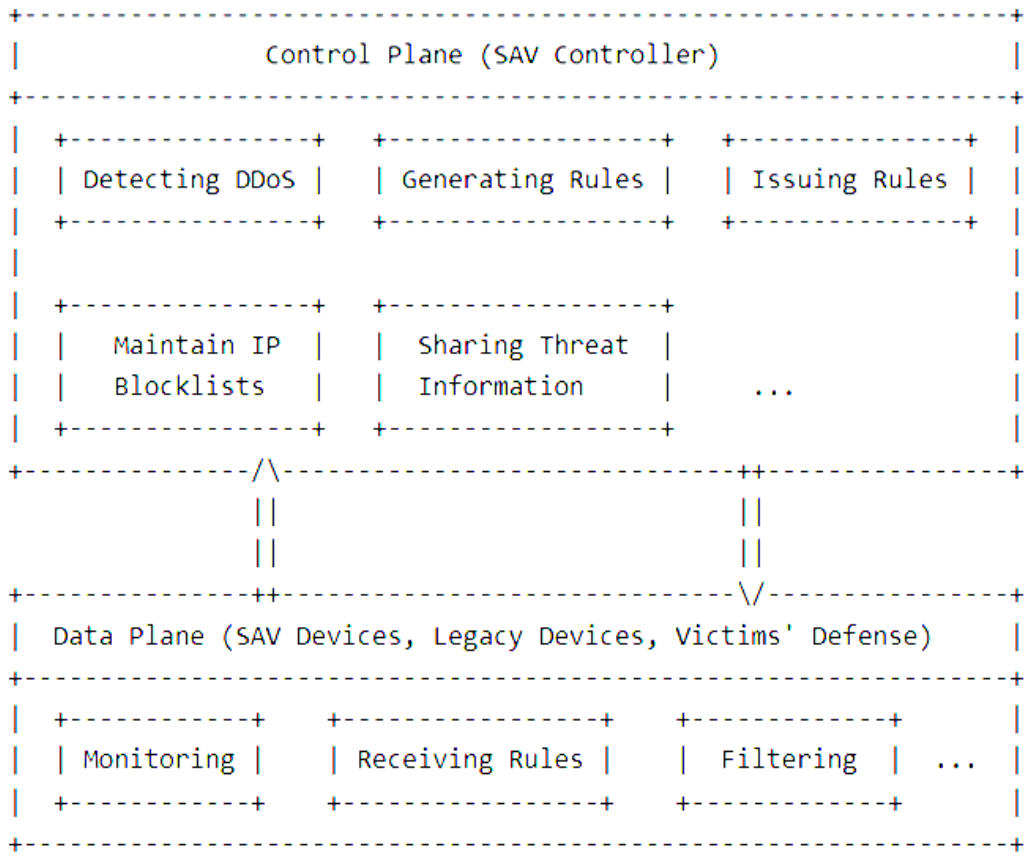


Figure 1: The SAV-based Anti-DDoS Architecture

SAV-based honeynet-like distributed defense architecture

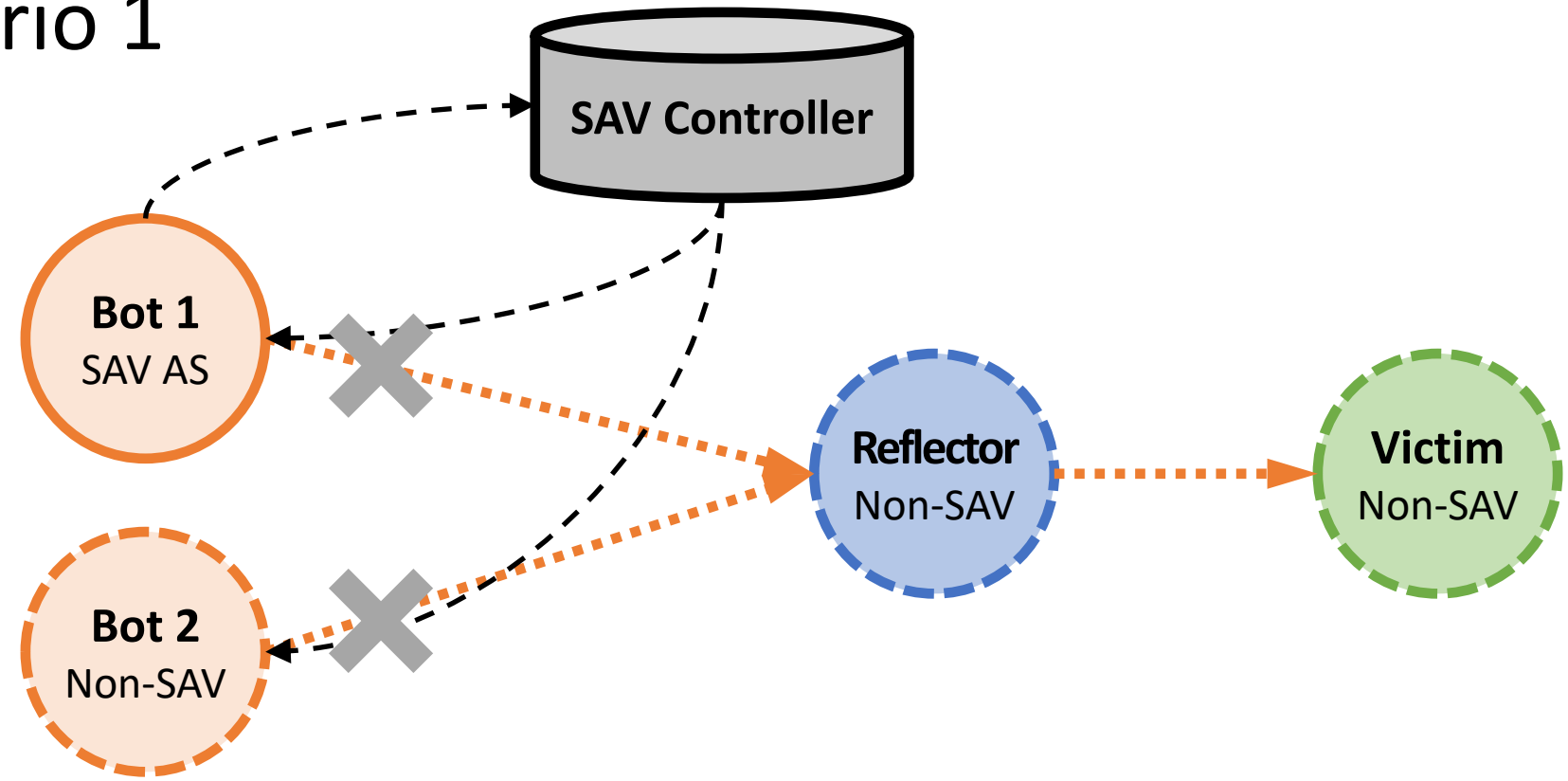
SAV-D Design - Advantages

- Achieve reliable attack detection
  - SAV devices serve as honeypots to record spoofing characteristics instead of directly blocking spoofed packets
  - can capture more threat data to support reliable attack detection
- Enable extensive defense
  - both SAV and non-SAV devices can use filtering rules to block malicious packets, including spoofed and reflected packets.
- Improve victims' defense
  - threat information can boost DDoS detection time as auxiliary signals
  - provide real-time updated IP blocklists for filtering

SAV's effectiveness can be significantly improved under incremental deployment.

SAV-D Use Case - Reflection DDoS Attack

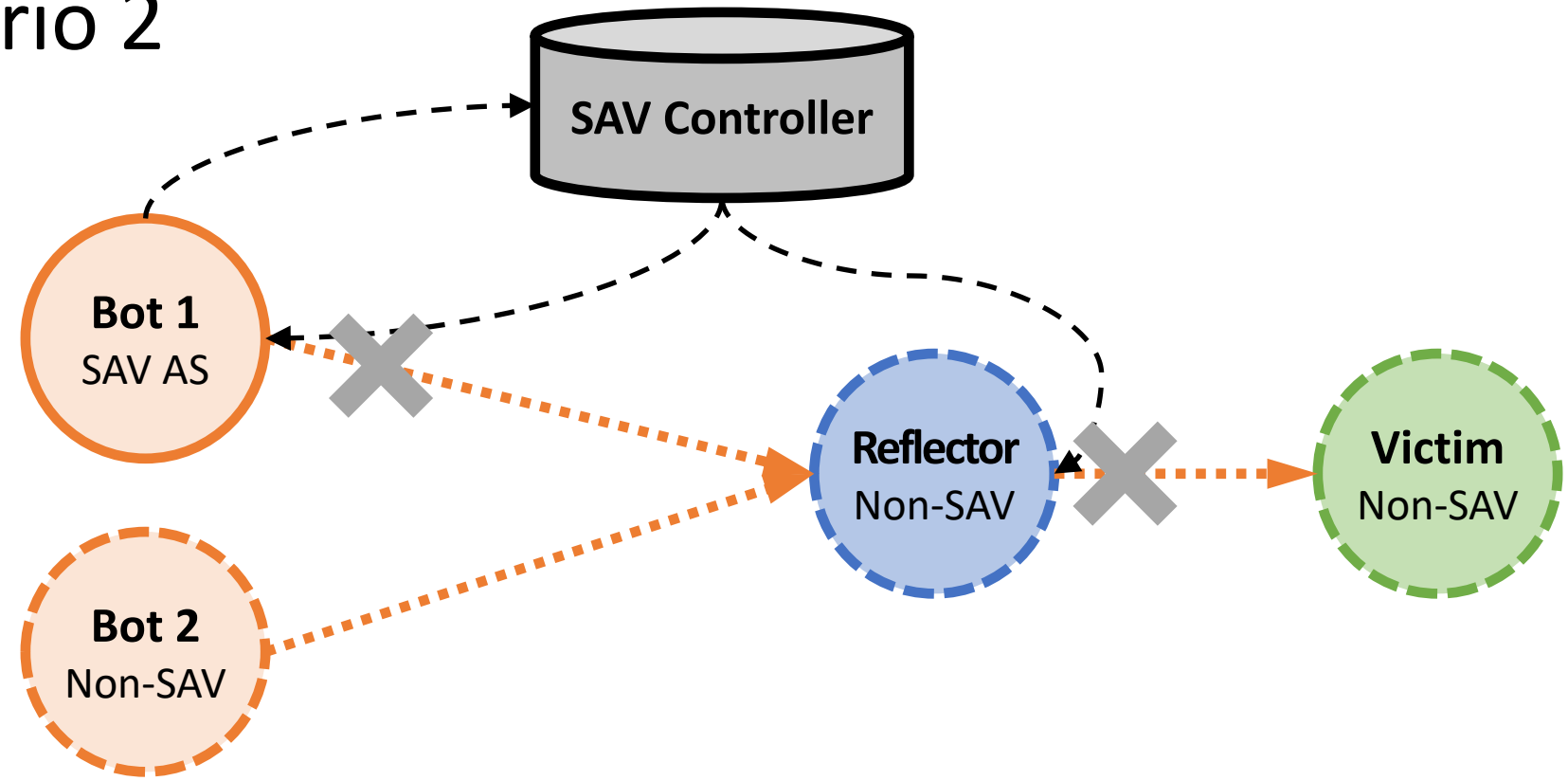
Scenario 1



Conclusion: Bot2 spoofed packets in Non-SAV AS can be filtered

SAV-D Use Case - Reflection DDoS Attack

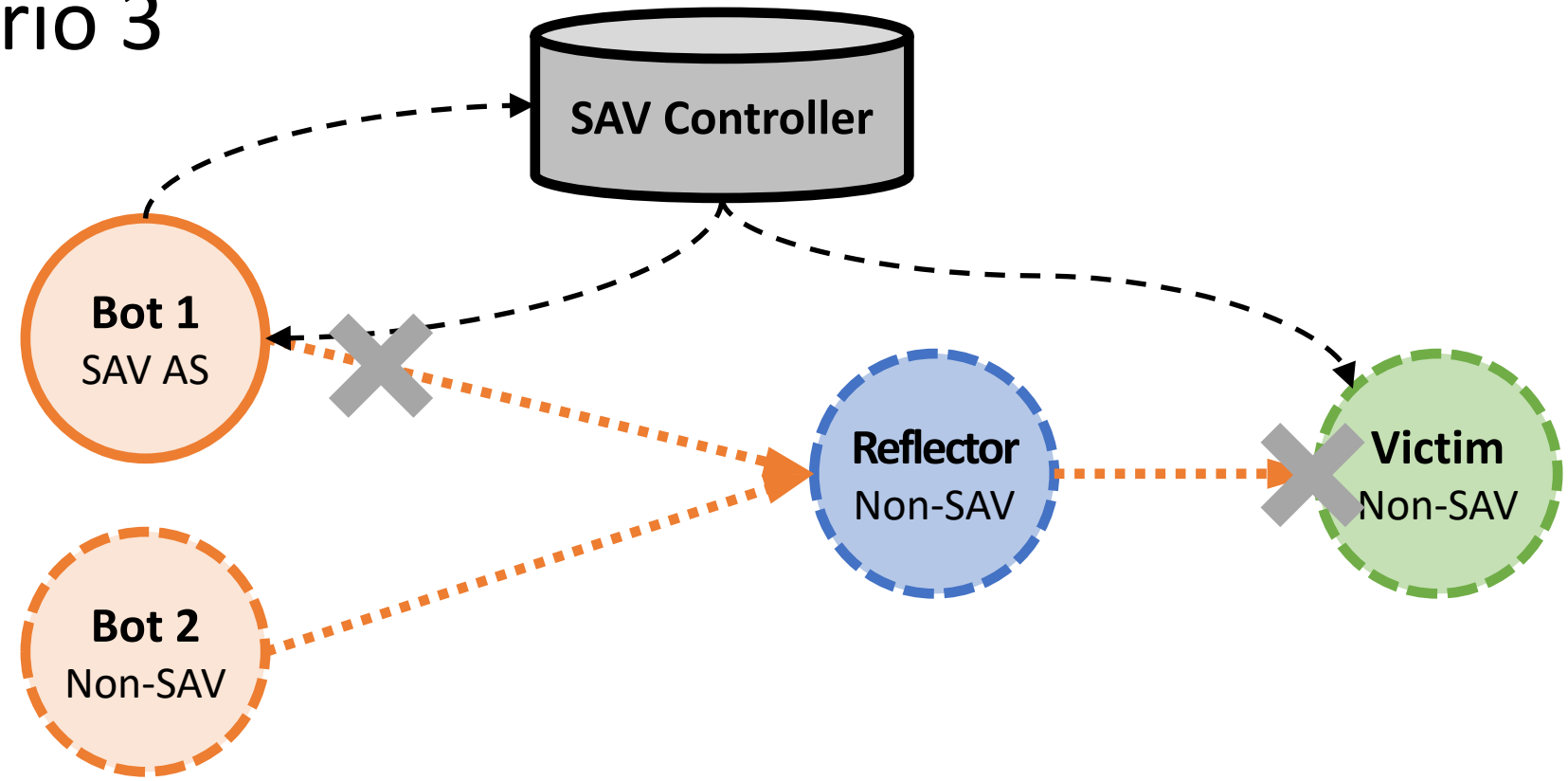
Scenario 2



Conclusion: Reflected packets can be filtered in SAV/Non-SAV ASes

SAV-D Use Case - Reflection DDoS Attack

Scenario 3



Conclusion: SAV-D can help victim to filter reflected packtes

Summary

SAV-D：SAV-based Anti-DDoS Architecture

- Each SAV device functions as a honeypot to capture more threat data
- The controller detects ongoing attacks and generate defense policies
- Both SAV and non-SAV devices can filter malicious packets
- Threat information is shared with the victims to assist their defenses

Next, we will implement SAV-D to show its effectiveness.

Thanks!

Q&A