Cloud-based Testbed for Simulation of Cyber Attacks

Author : Daniel Kouˇril, Tom´aˇs Rebok, Tom´aˇs Jirsı´k, Jakub ˇCegan,
Martin Draˇsar, Martin Vizv´ary, Jan Vykopal
Masaryk University, Institute of Computer Science
Botanick´a 68a, 602 00 Brno, Czech Republic
{lastname}@ics.muni.cz

NOMS 2014 - IEEE/IFIP Network Operations and Management Symposium

Outline

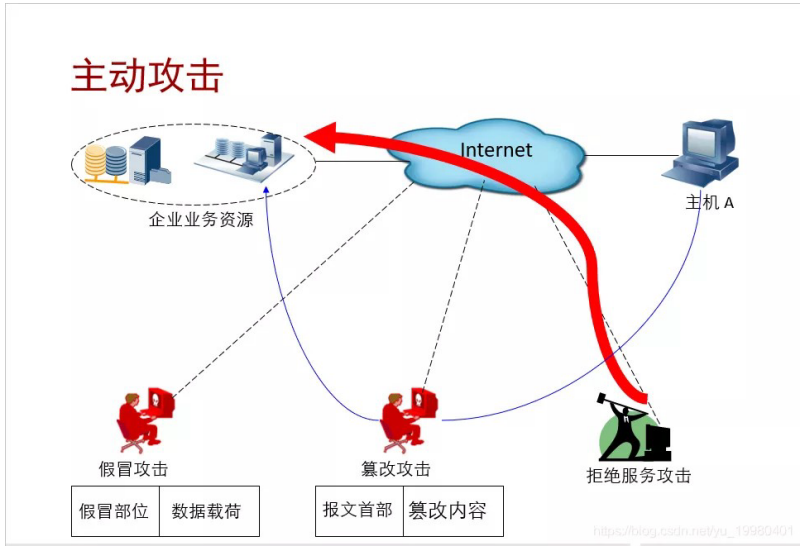
1. Problem Statement
2. Cloud-based security testbed
3. Modeling Security Scenarios
4. Experiment
5. Discussion

Problem Statement

Three questions:

- Can we build an artificial environment that can provide sufficient isolation and control all related activities?
- Can we find the right balance between flexibility and usability of the environment?
- Given such an environment exists, is it possible to describe an arbitrary attack and model it in the environment so it can be studied properly?

How to build an environment that can simulate and research attacks?

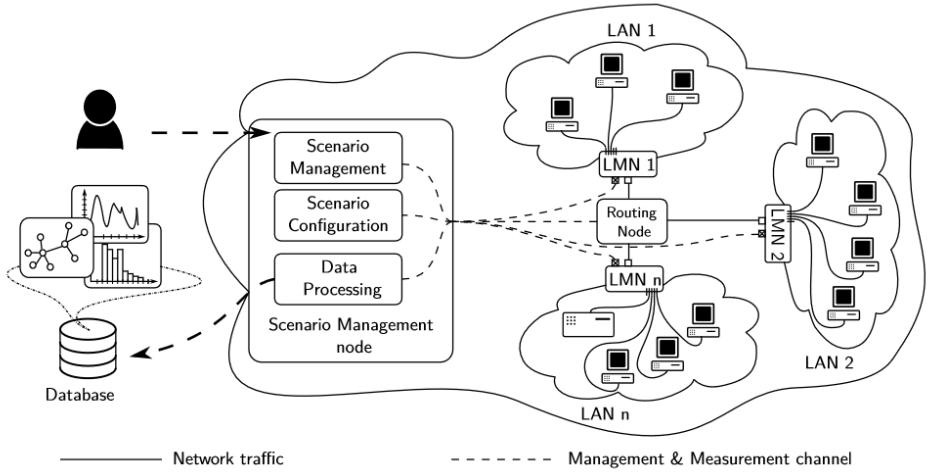


This Paper : Proposed a framework that is deployed on the testbed of a lass cloud server.

Cloud-based security testbed

Requirements for the intended testbed:

- Network-related : allow users to have complete control over the network Layer 3 arrangement.
- Hosts-related : support various hosts configurations.
- Monitoring : monitor network links between any two nodes in the defined virtual topology and collect monitoring data about network flows.
- Testbed Control: orchestrate and control all its components easily.
- Deployment : expect just widely-used middleware for testbed operations so that one is able to deploy it over an existing cloud-based infrastructure providing supported interfaces.



Cloud-based security testbed

The Proposed Framework CPG (Cybernetic Proving Ground)

1. LMN : LAN management nodes
   - Manage Local virtual nodes at L3 Layer.
   - Use VLAN at L2 Layer

2. Network Monitor infrastructure
   - Prober
   - Data processing unit
   - Database

3. Hosts Monitor infrastructure
   - Monitor CPU and memory usage

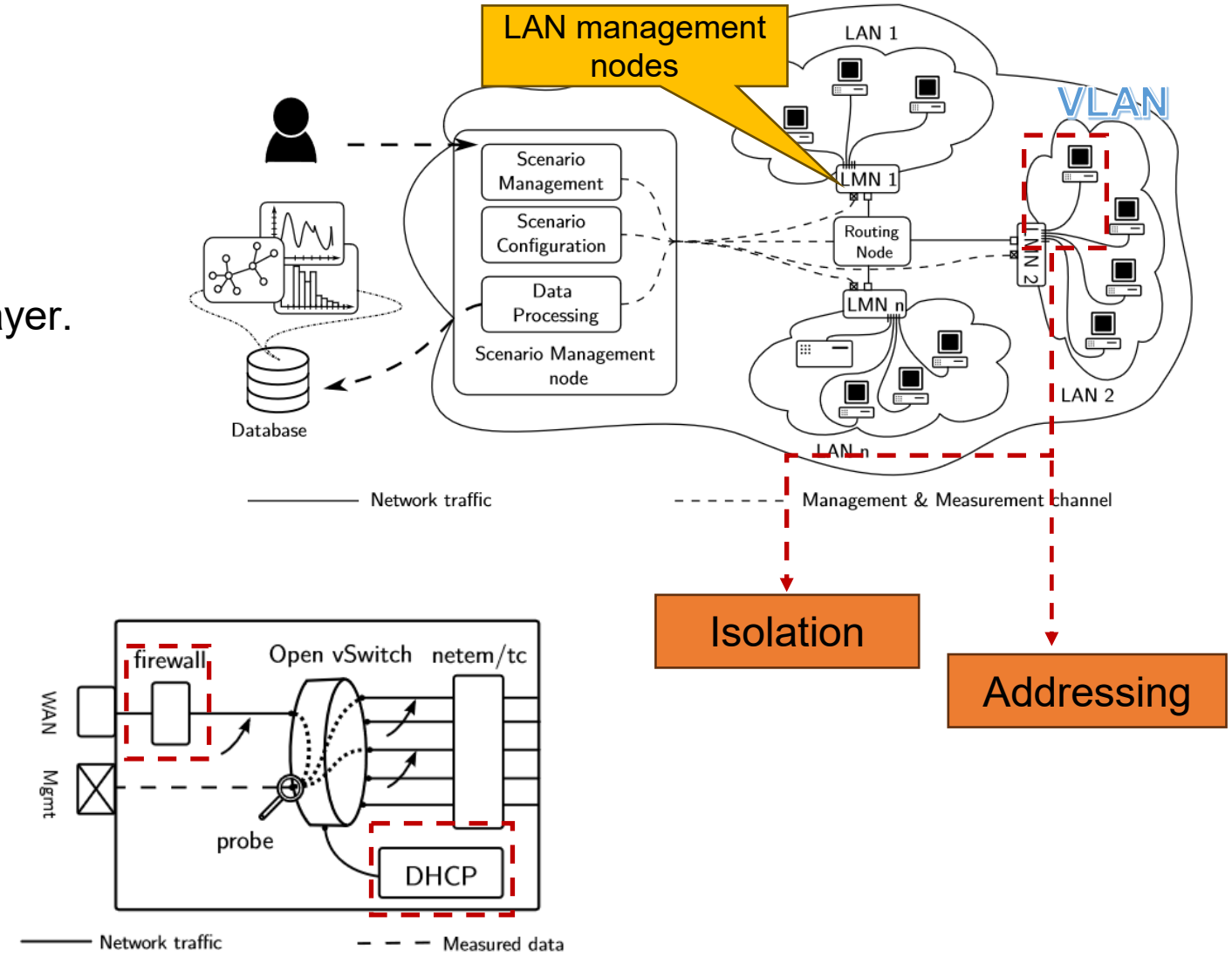


Fig. 2. Schema of LAN Management Node

Modeling Security Scenarios

Scenario:

1. In the first phrase : the initialization, network and logical topologies of the environment are established and parameters of the attack are set.

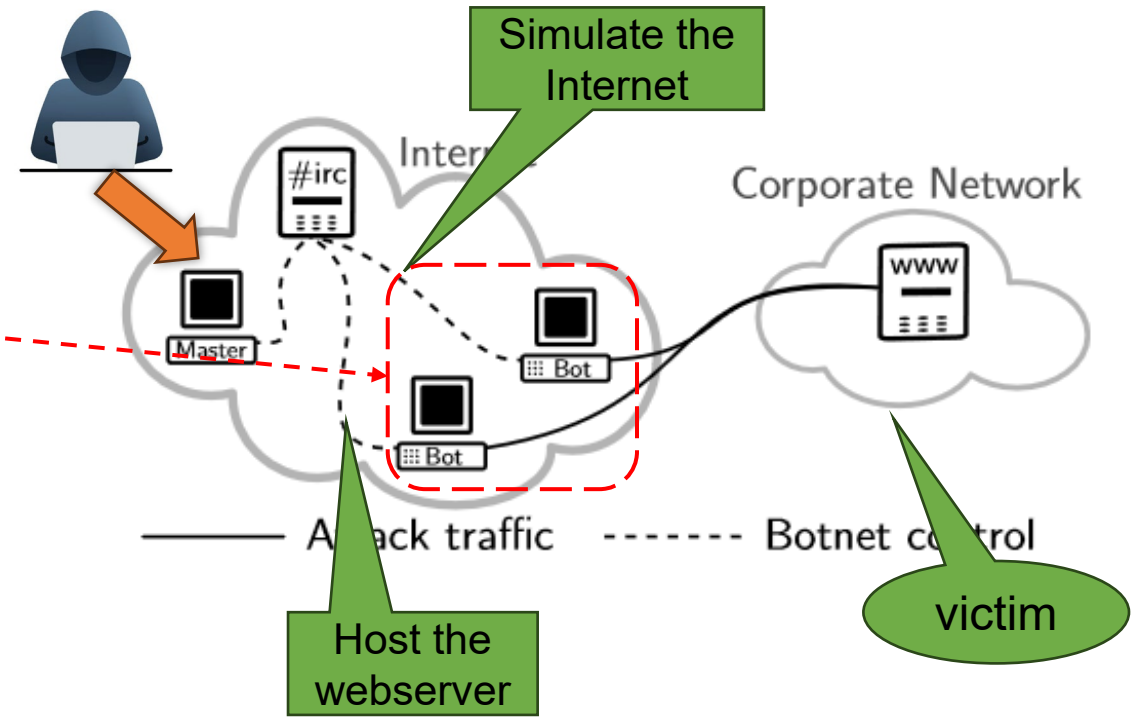
2. In the second phrase : the scenario run, the actual experiment is done. Both network and host monitoring infrastructures capture data from the scenario.

3. In the third phrase : the evaluation, serves for an analysis of the experiment. Captured data is stored for later work, scenario modifications and its re-run.

Experiment

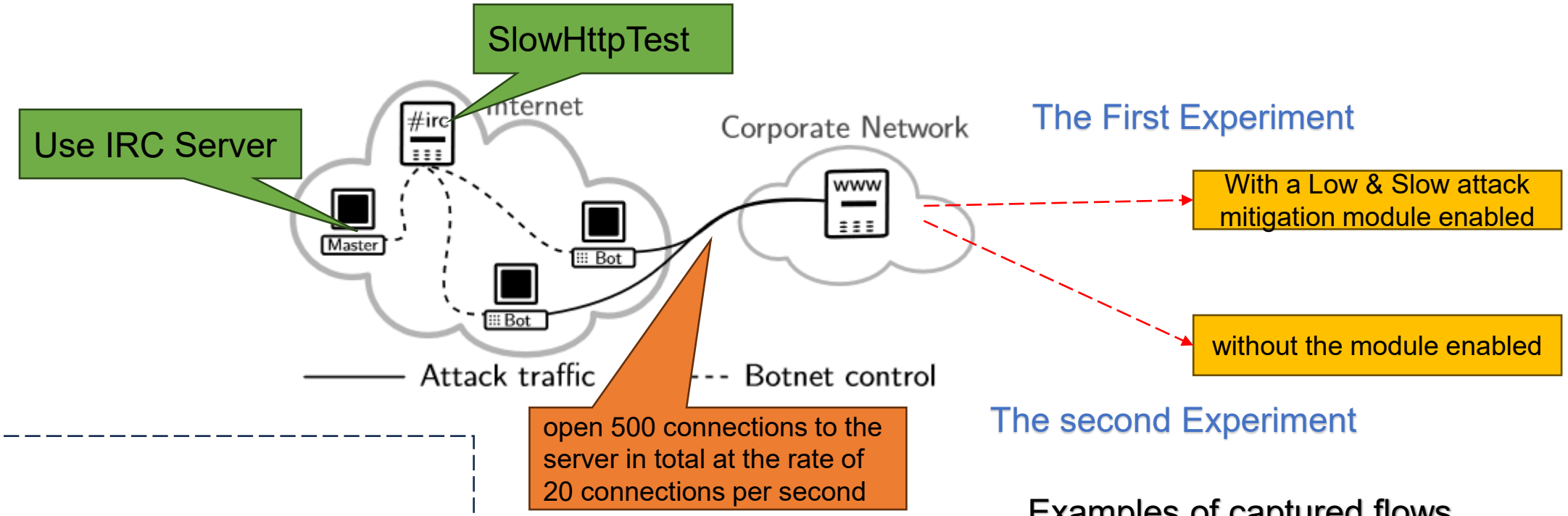
Four types of nodes

- Victim : the victim node is a Linux-based operating system with the Apache web server.
- Bot : this node is the source of attack traffic against the victim.
- Attacker : this node gives commands to the botnet through the IRC server
- IRC : The nodes were divided into two networks, one simulating the Internet with the attackers and another one hosting the victim web server (Corporate Network).



Experiment

Attack: chose to orchestrate a Low & Slow attack against a web server as DDoS attacks are ubiquitous.



Result:

- The first experiment: return HTTP 400.
- The second experiment : the server became unavailable after 14 seconds.
- Successfully monitor abnormal flow.

Examples of captured flows

#	Type	Duration	Packets	Bytes	HTTP Code
1	REQ	0.002	7	612	-
	RESP	0.001	5	4203	200
2	REQ	75.050	12	959	-
	RESP	60.050	8	930	400
3	REQ	600.950	36	3034	-
	RESP	600.950	34	2282	400

Discussion

- Can a detection module be added when creating a simulation attack environment ?
- The difference between cloud environment simulation and non cloud environment simulation