black hat® ASIA 2019

MARCH 26-29, 2019

MARINA BAY SANDS / SINGAPORE

See Like a Bat

Using Echo-Analysis to Detect Man-in-the-Middle Attacks in LANs

Speaker: *Yisroel Mirsky, PhD*

Ben-Gurion University, Israel

Co-authors:

Naor Kalbo,

Dr. Asaf Shabtai,

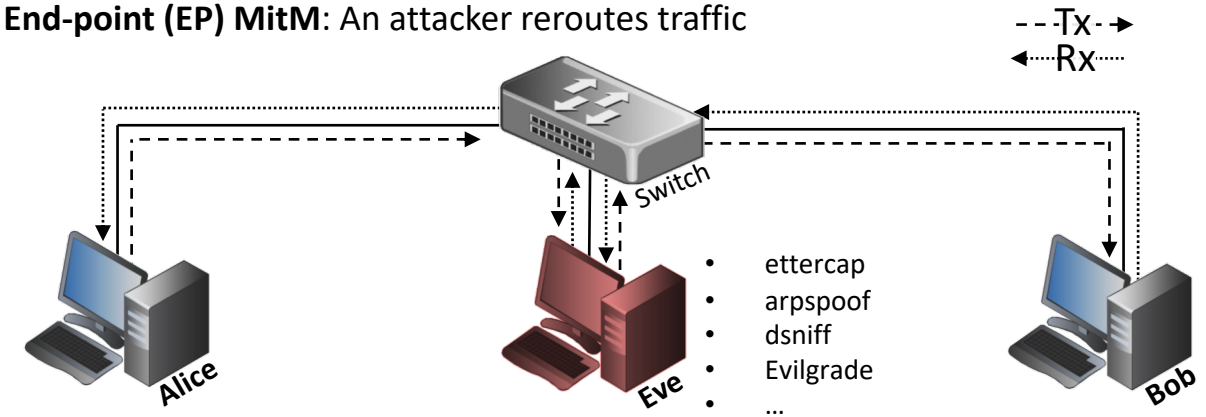
Prof. Yuval Elovici

CBG

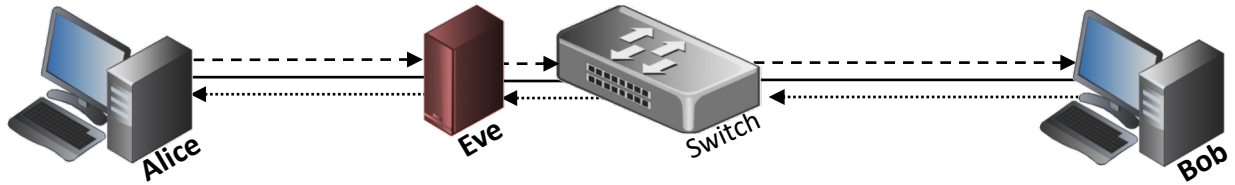
Cyber@Ben-Gurion
University of the Negev

Motivation

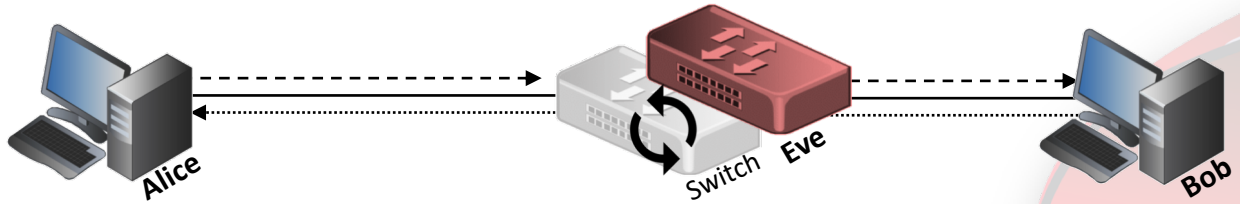
End-point (EP) MitM: An attacker reroutes traffic



In-line (IL) MitM: An attacker physically intercepts traffic



In-Point (IP) MitM: An attacker replaces an existing network switch

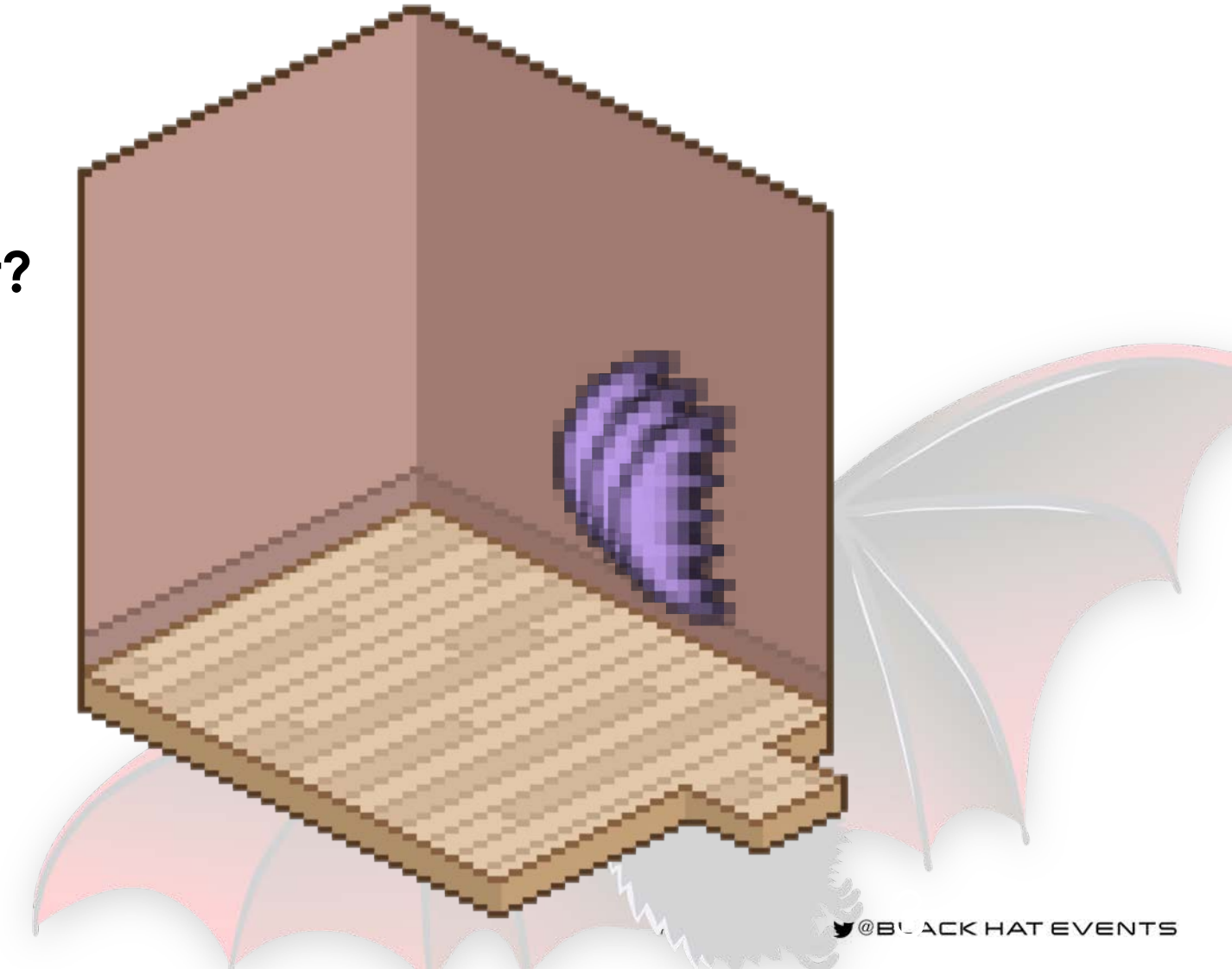


Current Detection Methods:

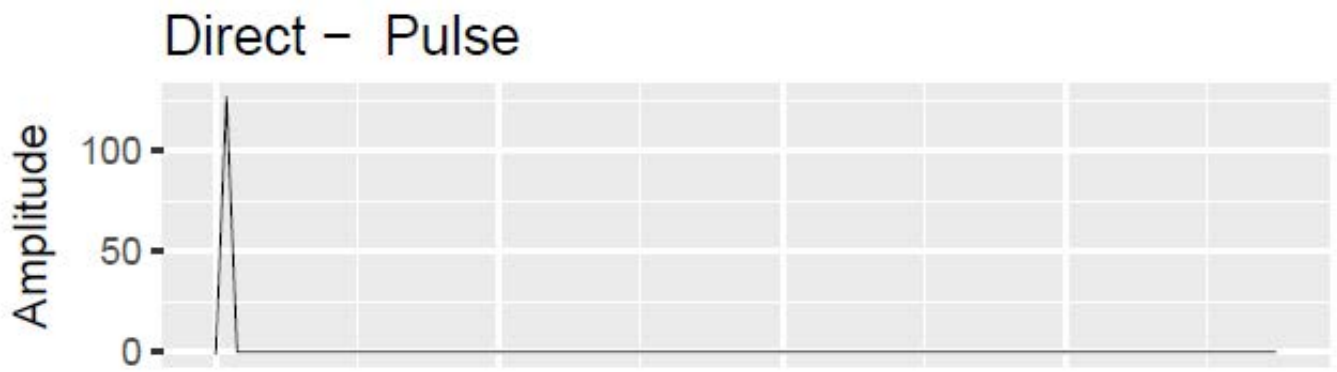
- Don't generalize to different attacks
- Not portable (e.g., expensive NIDS)
- Generate false positives
  (are passive, thus subject to noise and activity).

Instead of **passive sensing**, let's use **active sensing.**

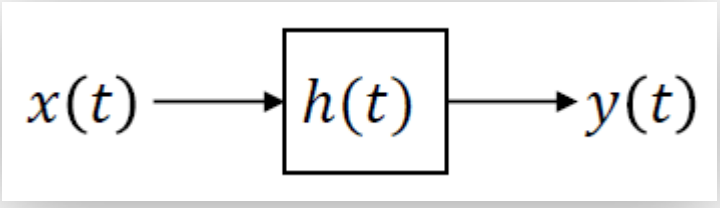
What if we could see like a bat?

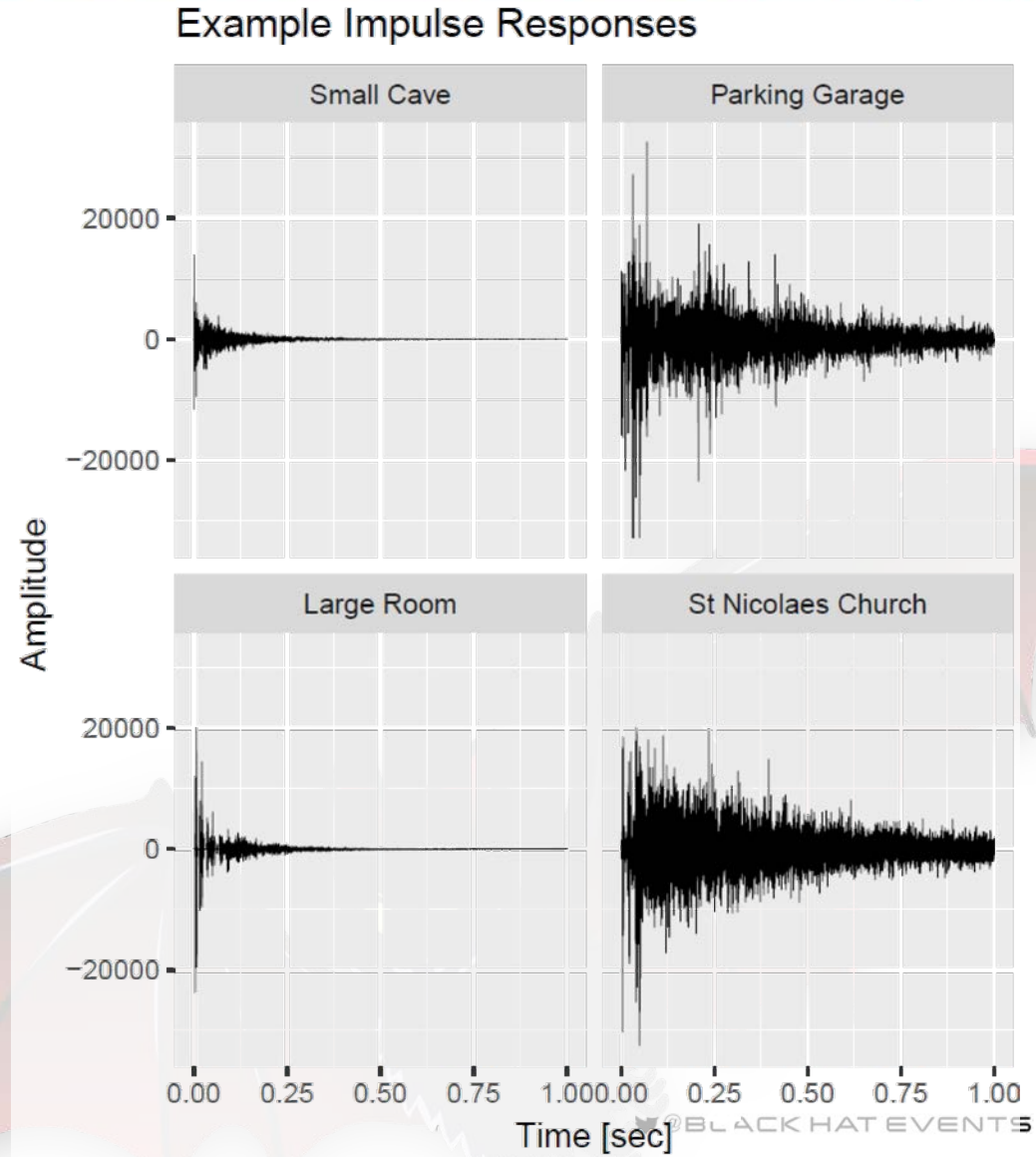


Physical World: (acoustics) Environment Modeling



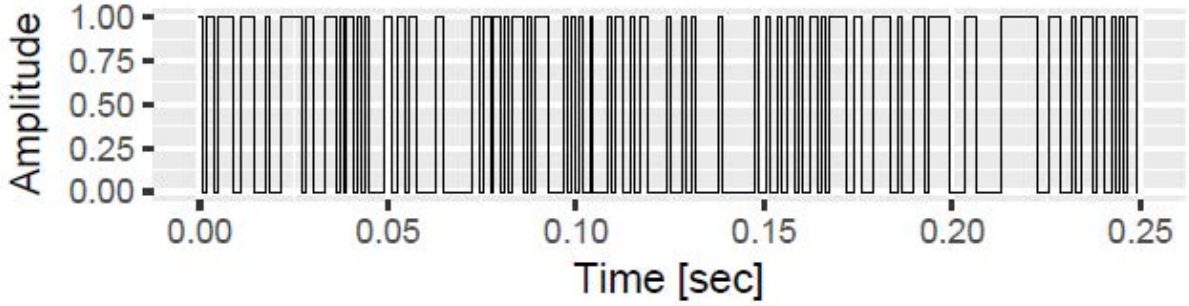
LTI – Linear Time Invariant System





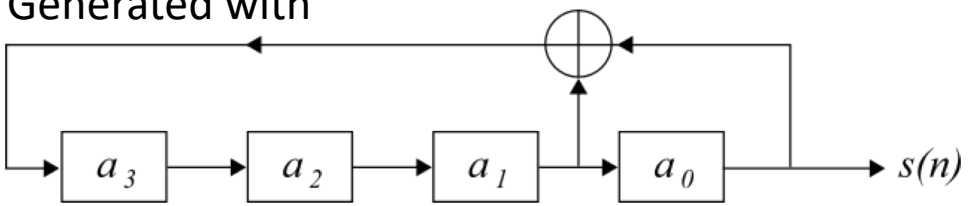
Physical World: (acoustics) Environment Modeling

Indirect – **Maximum Length Sequence (MLS)**

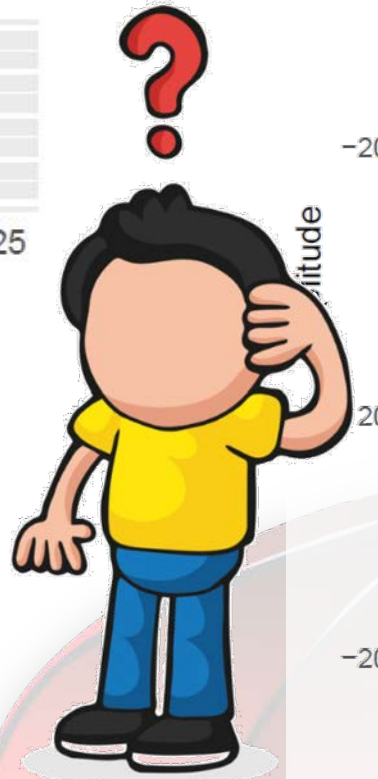


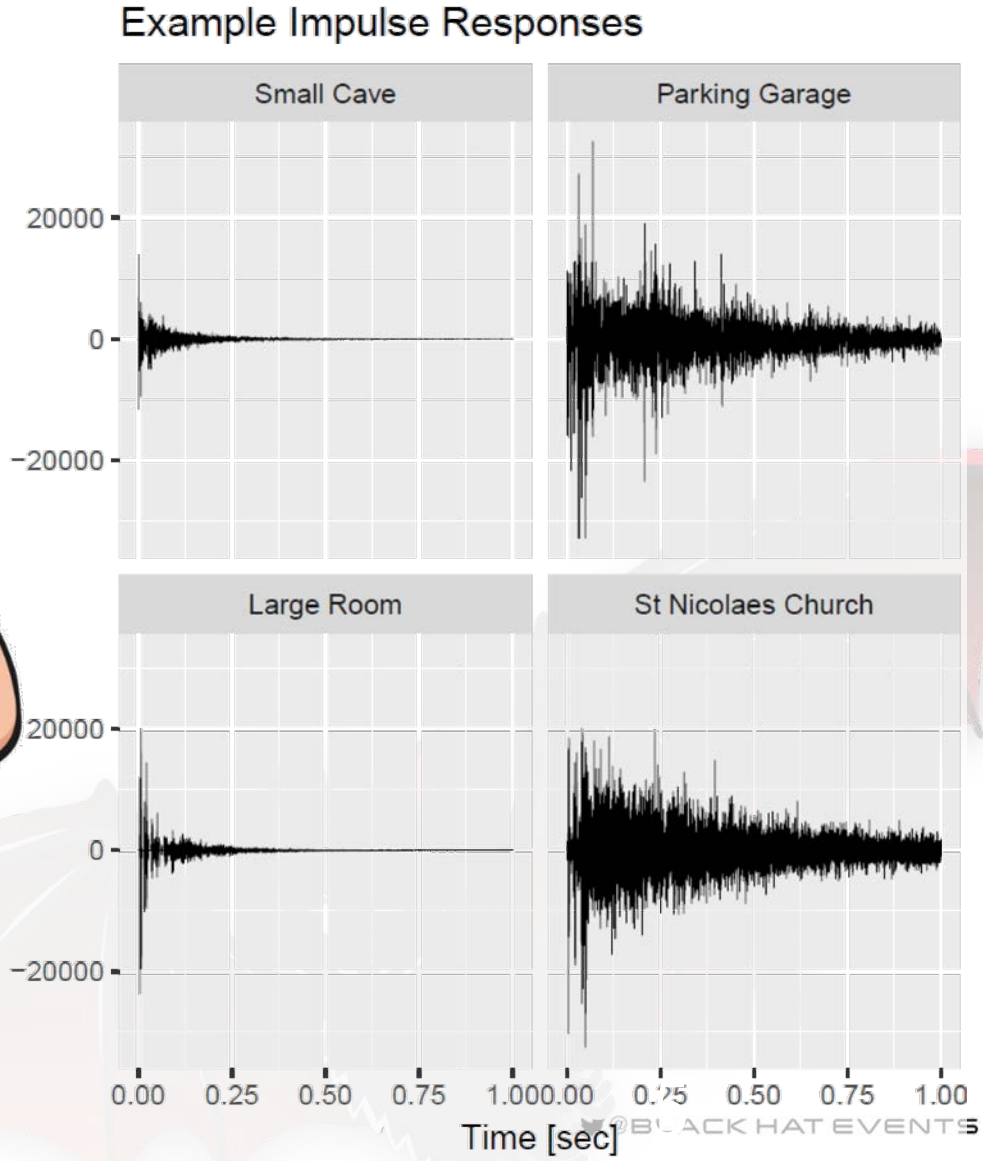
1101001011010010011011010001001…

Generated with



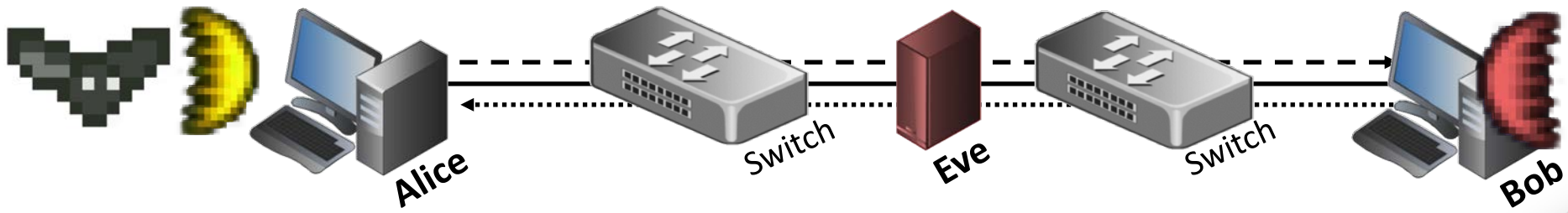
Seeded with AES-256

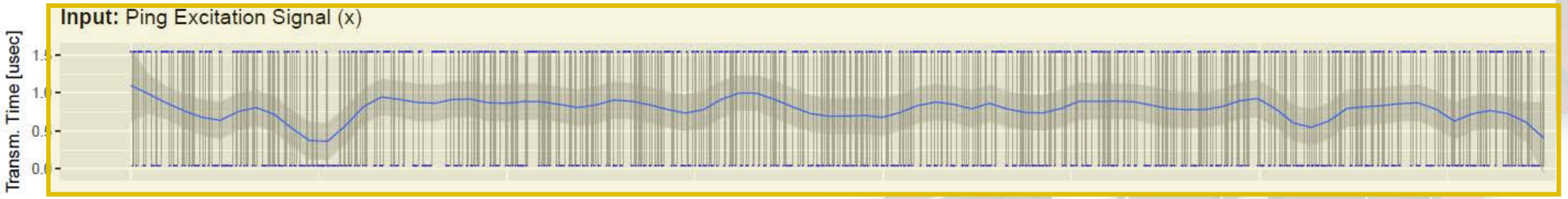


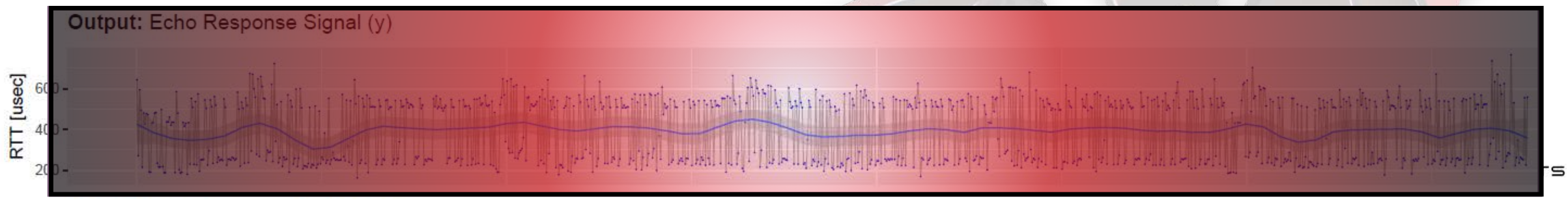


Virtual World: Environment Modeling

How can we apply this to a LAN?



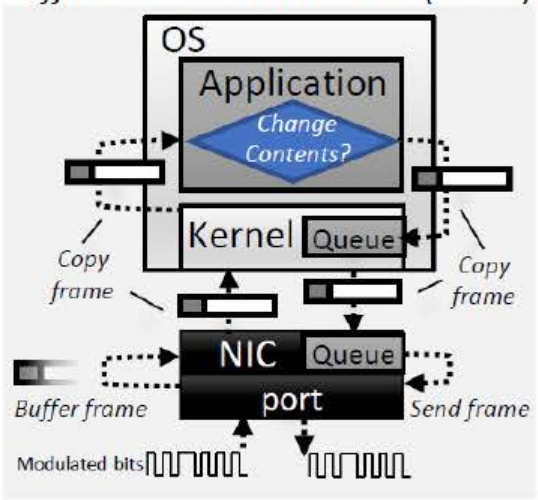




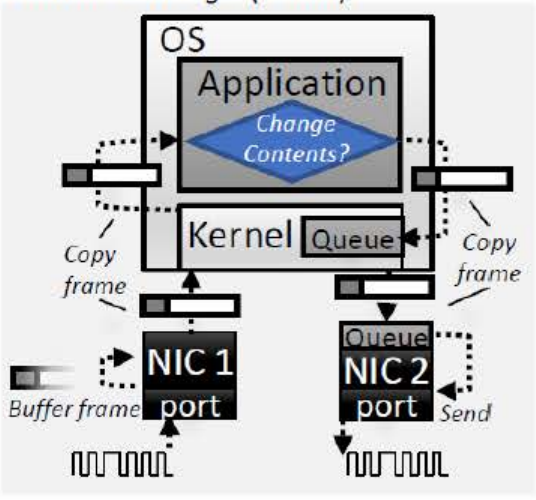
Virtual World: Environment Modeling

All MitM attacks buffer packets to read/change them.
The software/hardware affect the processing time **of a burst.**

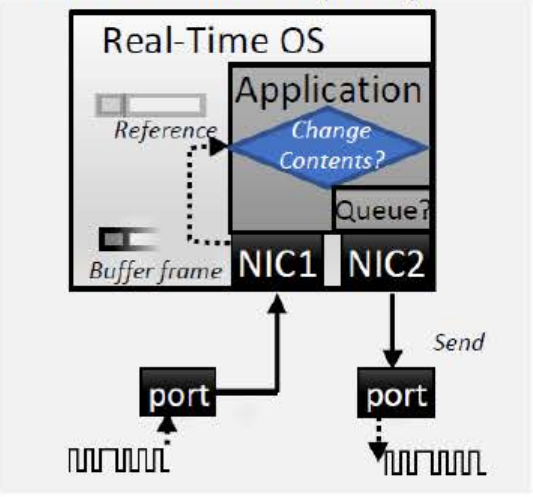
(1) End-Point MitM using a *Traffic Diversion* such as ARP (EP-TD)



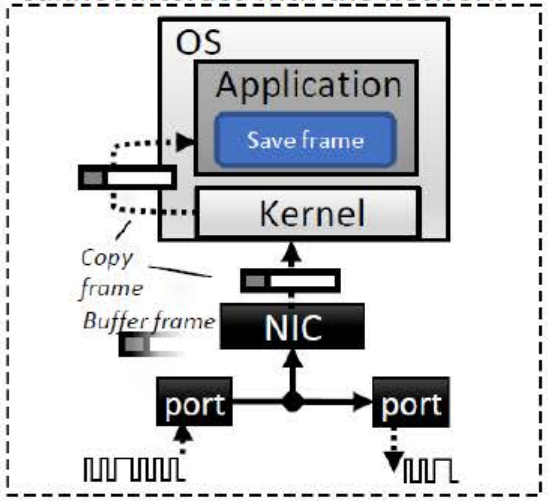
(2) In-Line MitM using a *Network Bridge* (IL-NB)

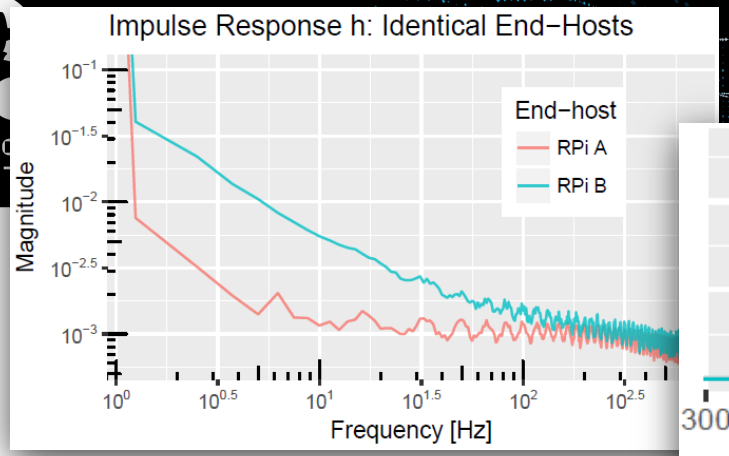


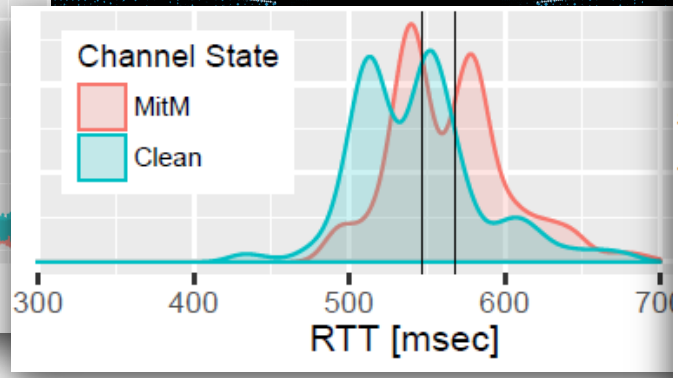
(3,4) In-Line/In-Point MitM using *Dedicated Hardware* (IL-DH)

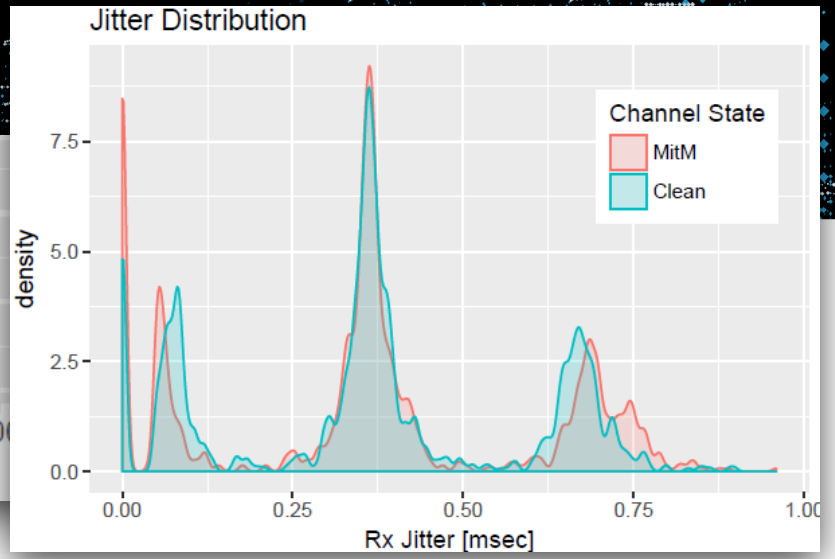


(5) In-Line Passive Wiretap (IL-PW)
Cannot interact with the network









$$E_h = \frac{1}{N}\sum_{k=1}^{N}\left|\frac{Y[k]}{X[k]}\right|^2$$

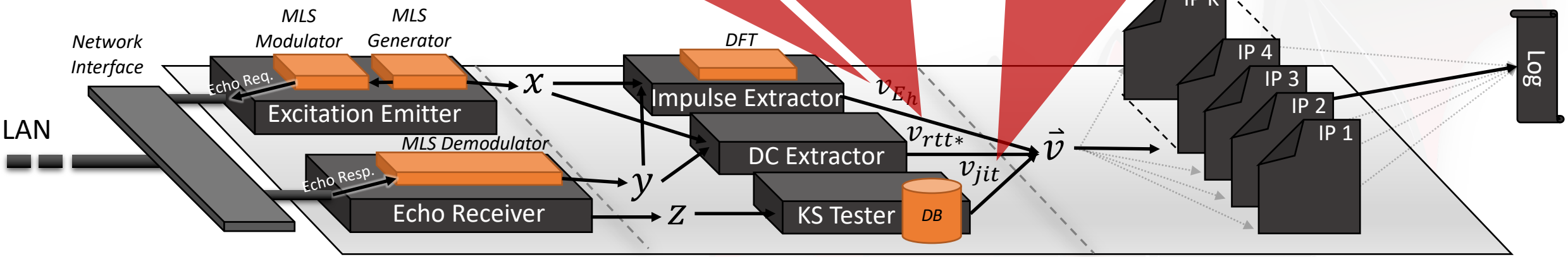
The Impulse Response's Average Energy

$$v_{jit} = \frac{2}{N}\sum y[i]\cdot x[i]$$

The Average RTT of the largest packets in the probe

$$p_{jit} = \log[max\{p_{z_0,z_1}, p_{z_0,z_2}, \cdots p_{z_0,z_m}\}]$$

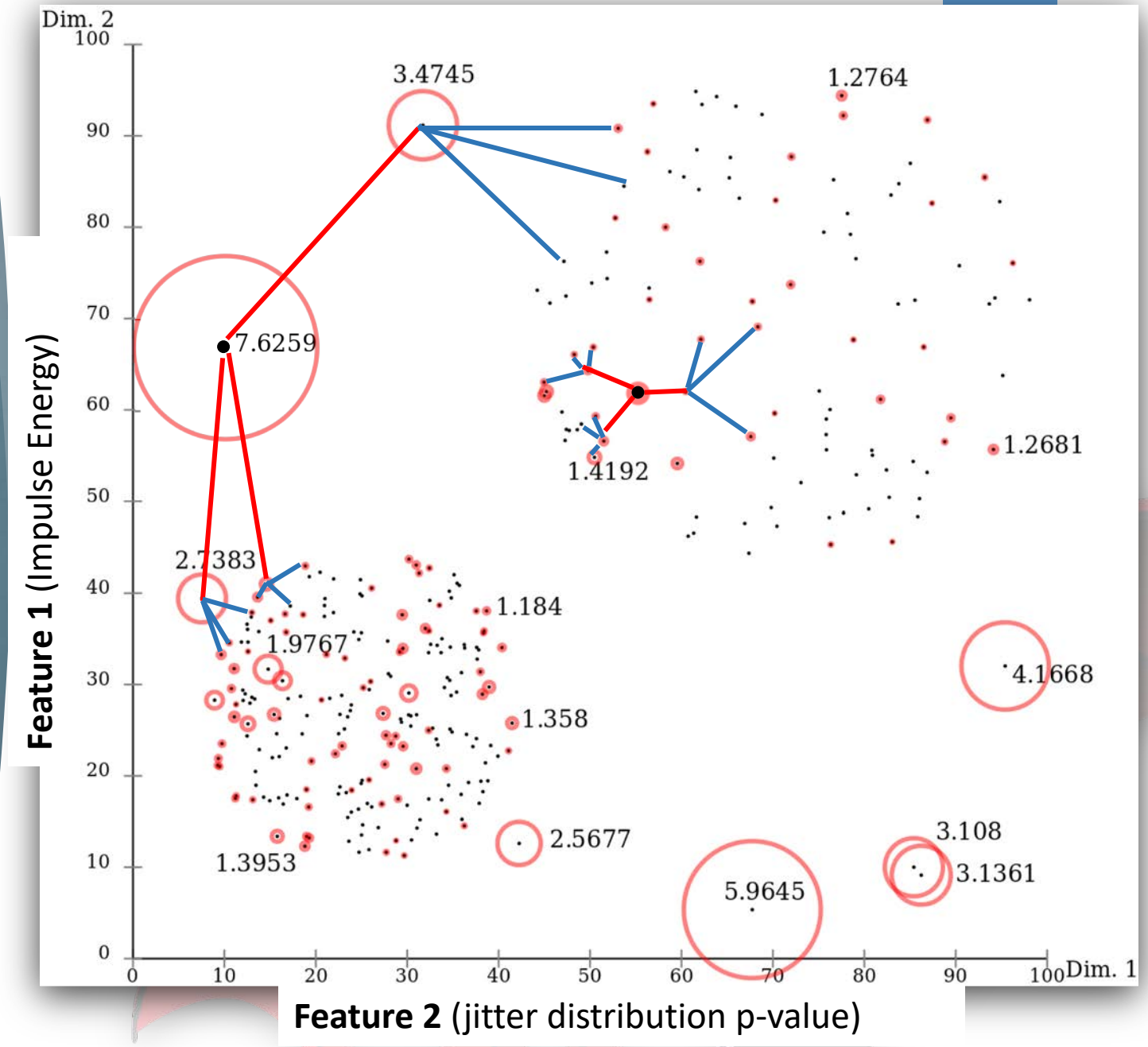
The p-value of the response's jitter



Building a Profile for a Target IP

Local Outlier Factor

The abnormality of an observation is relative to its neighbor's density (not just distance)



Vesper: Evaluation Setup

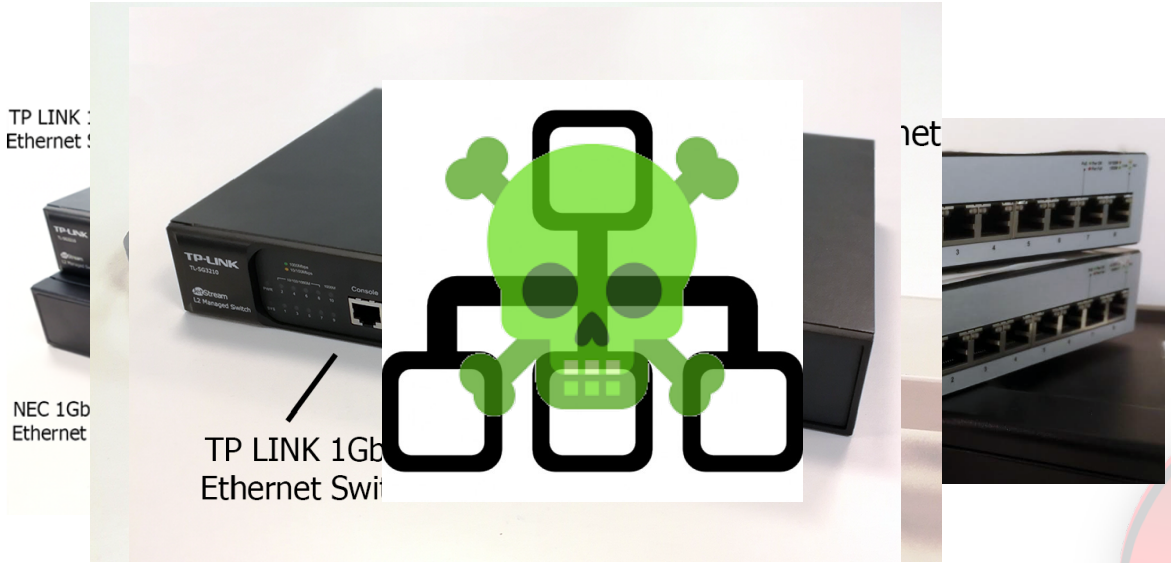
Attacks:

Traffic Diversion: ARP Poisoning

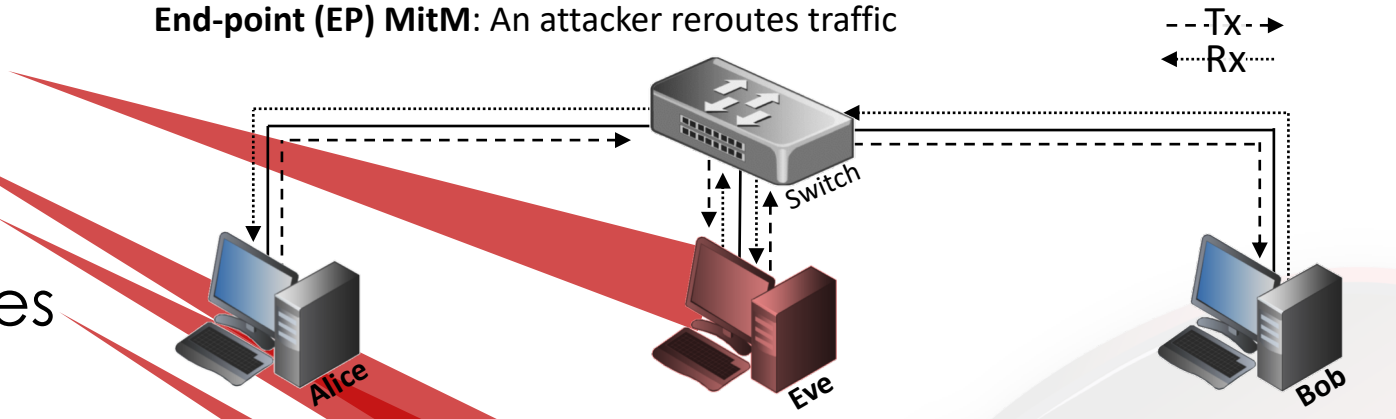
Network Bridge: Raspberry Pi

Network Bridge: Switch (1Gbps)

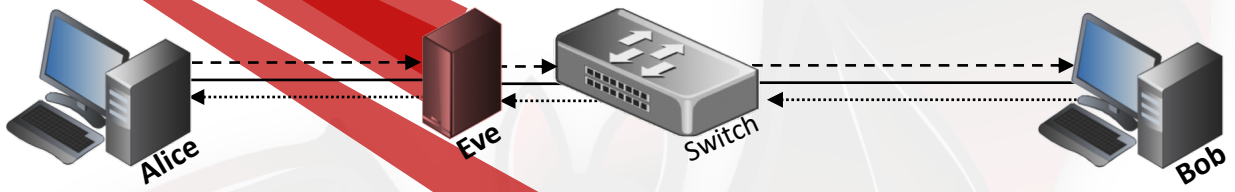
Device Swapping: 1Gps Switches



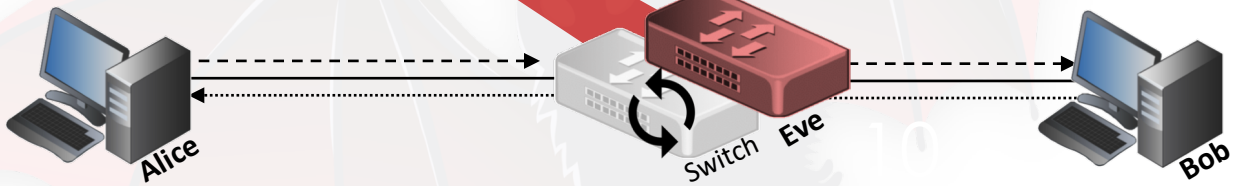
End-point (EP) MitM: An attacker reroutes traffic



In-line (IL) MitM: An attacker physically intercepts traffic



In-Point (IP) MitM: An attacker replaces an existing network switch



Vesper: Evaluati
Setup

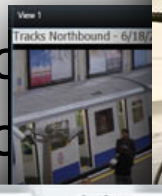
Networks:

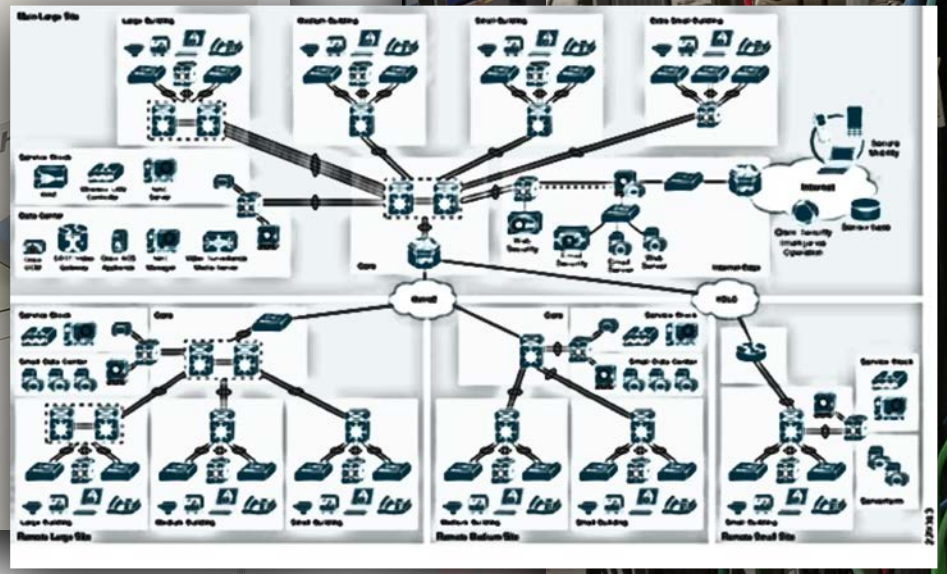
Surveillance Network: 7 switches, 13 netwo

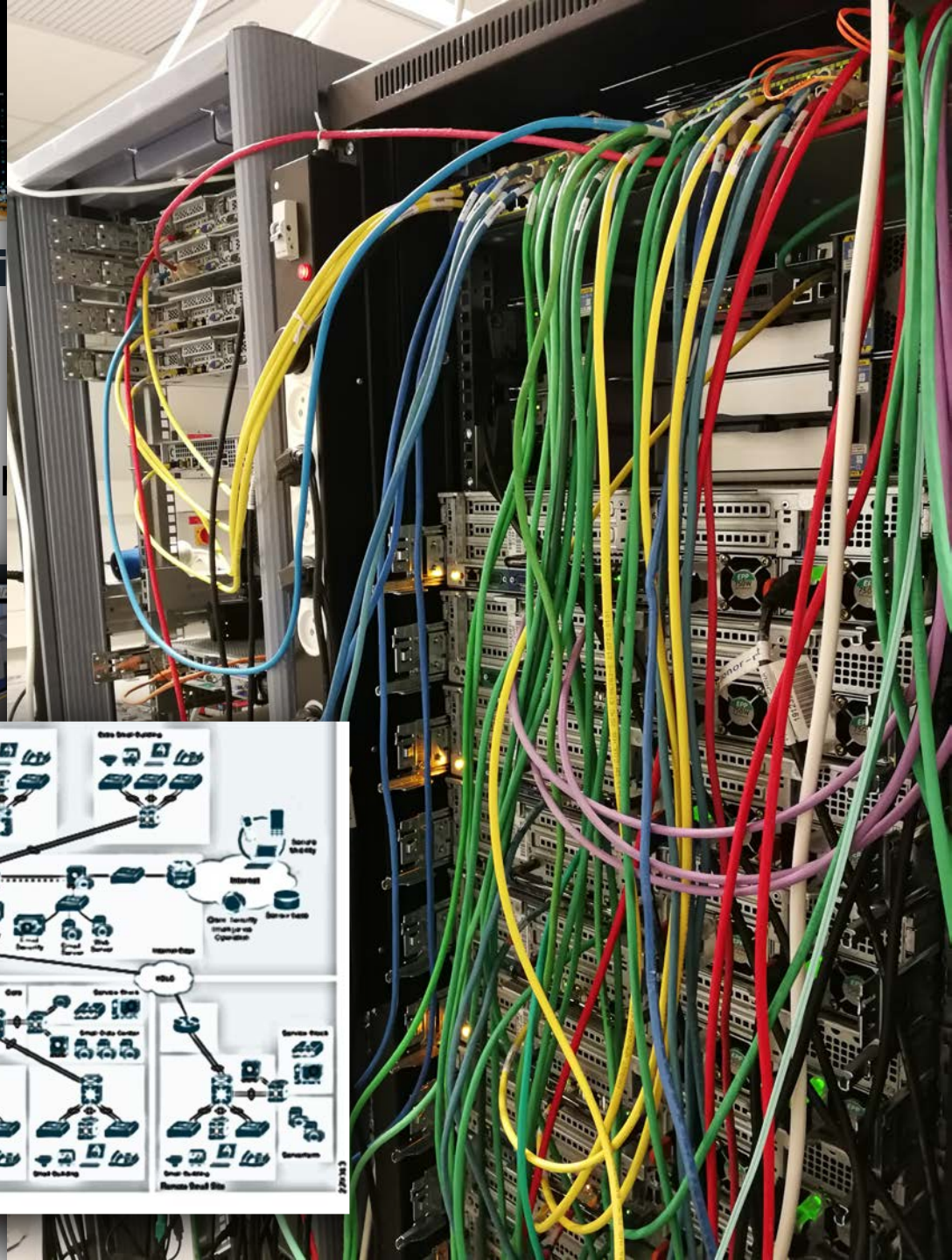
Server Network: 3 switches, 61 servers

La etwo

nd c

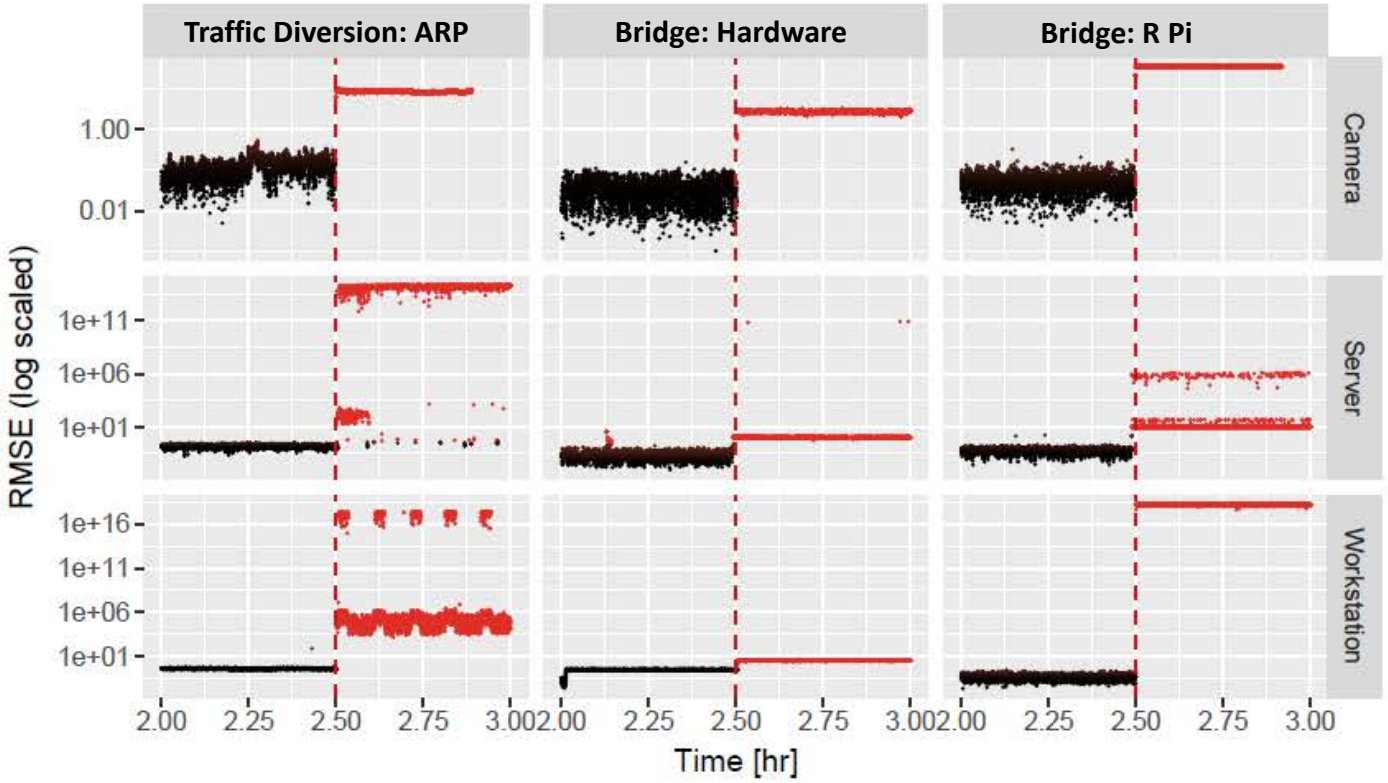


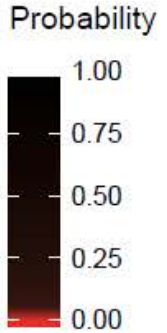


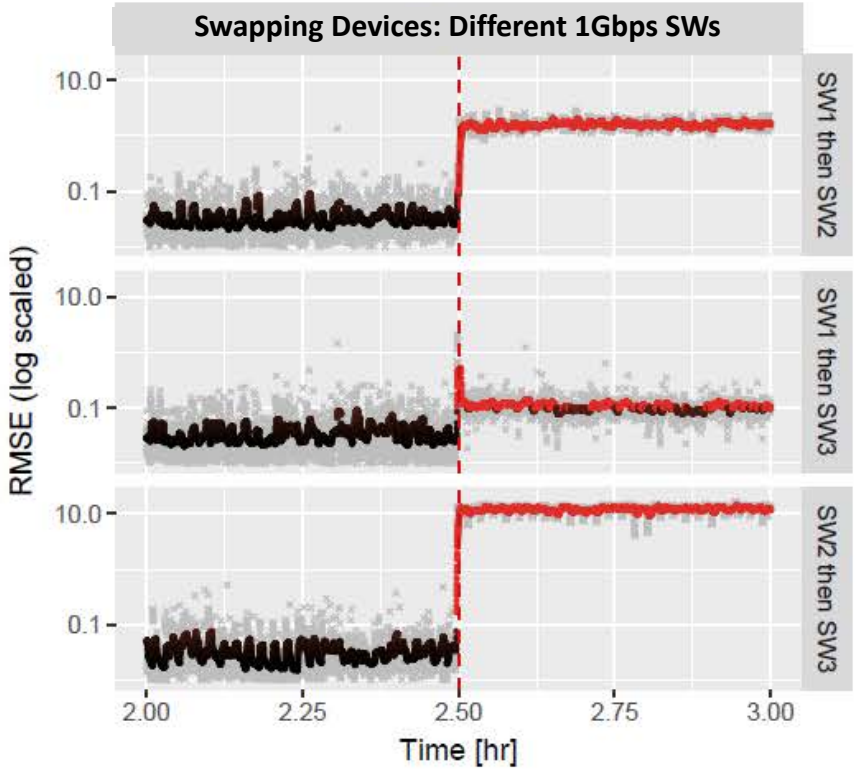


Vesper: Evaluation

One Intermediary Switch



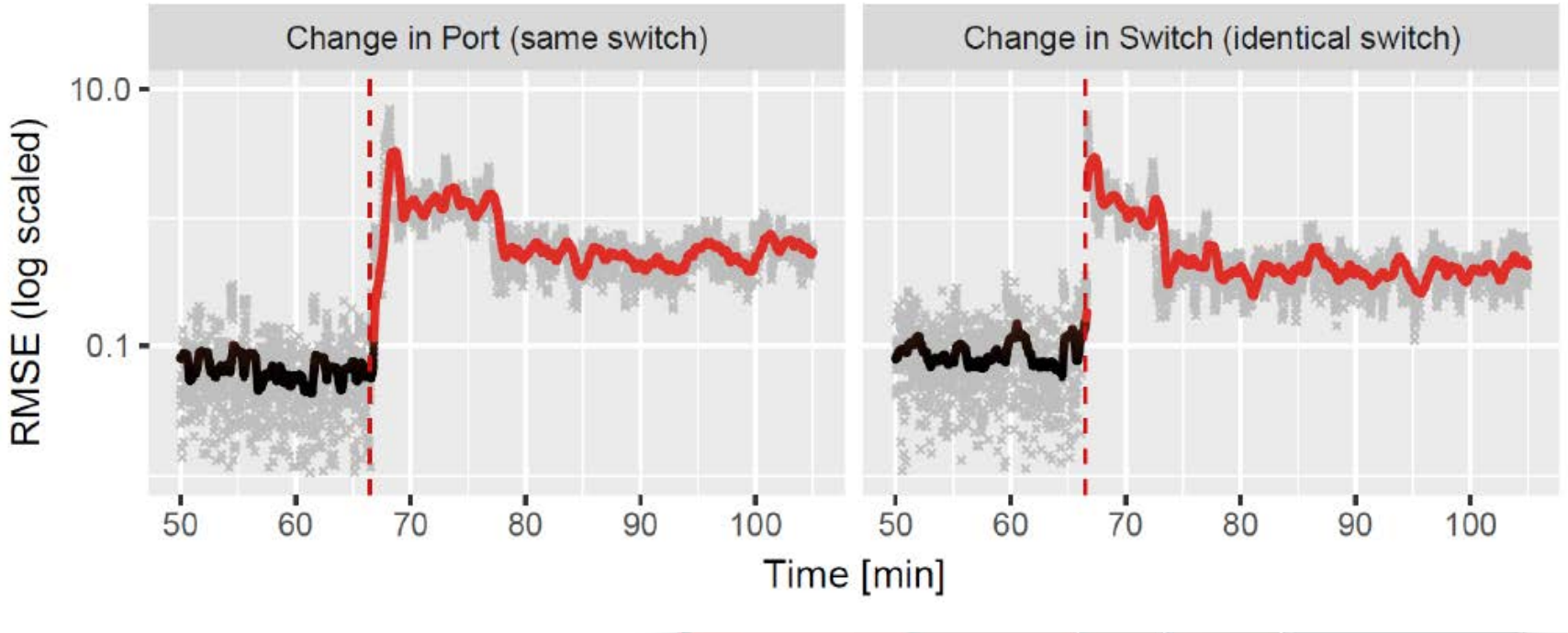




Vesper: Evaluation

One Intermediary Switch

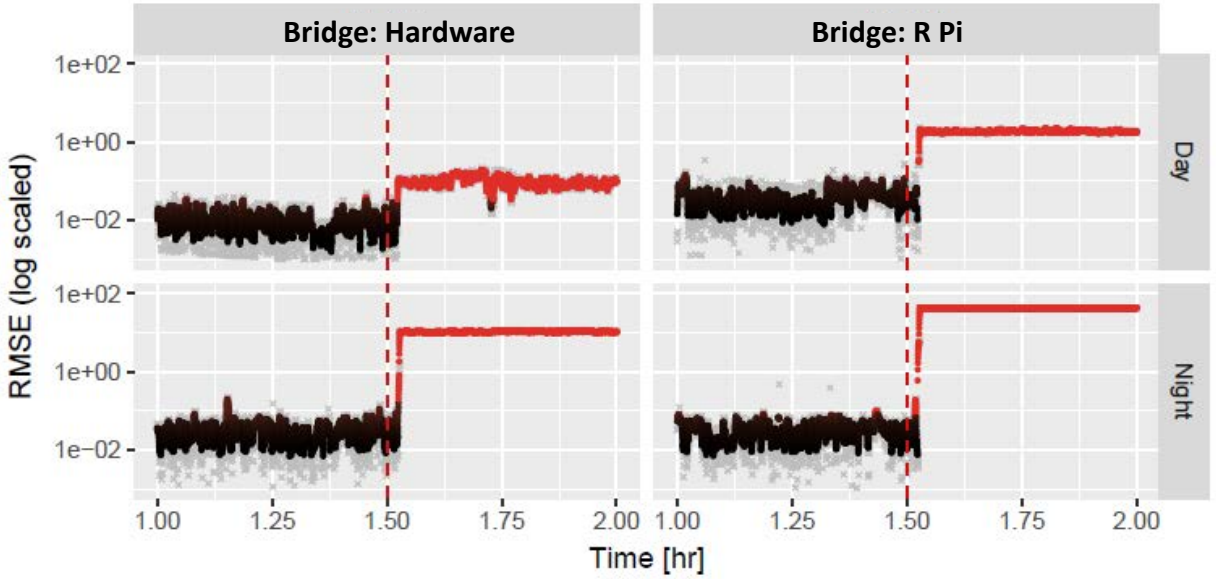
Swapping Devices: Identical 1Gbps SWs



Vesper: Evaluation

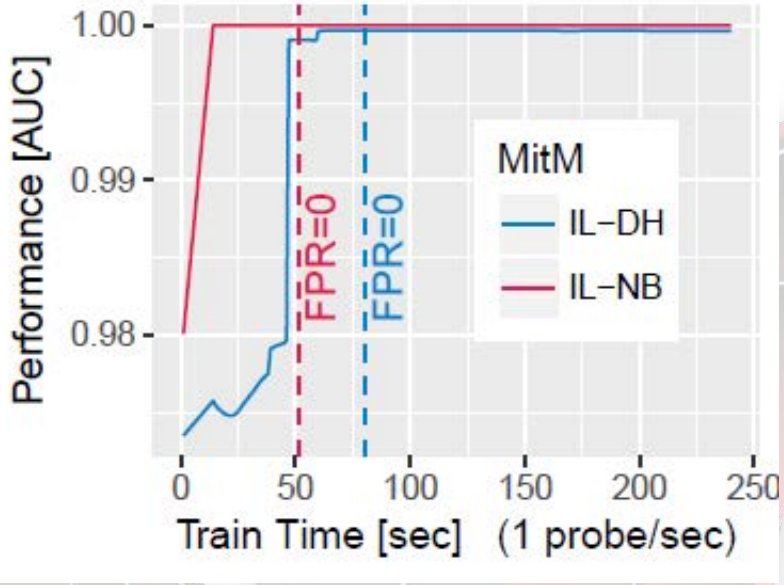
Multiple Intermediary Switches

Across 5 large switches with 350 active hosts



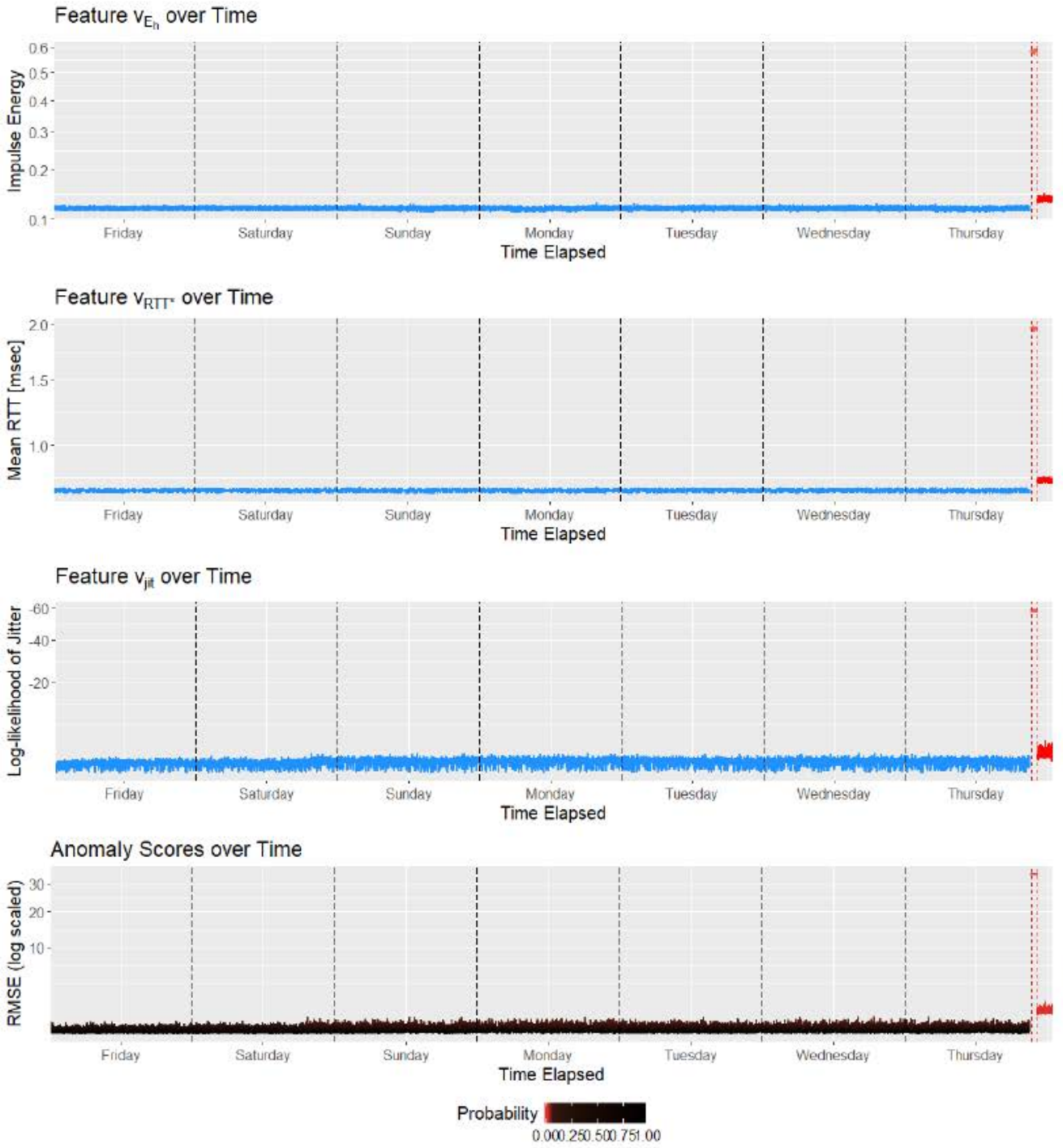
(Attacking our secretary)

Affect of Probe size and Train Time



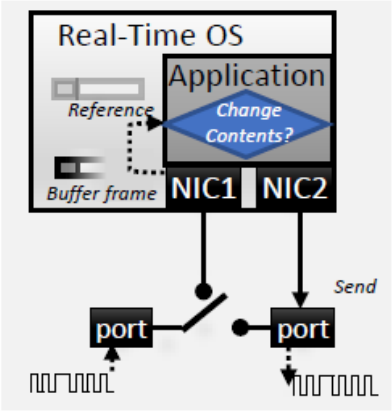
Vesper: Evaluation

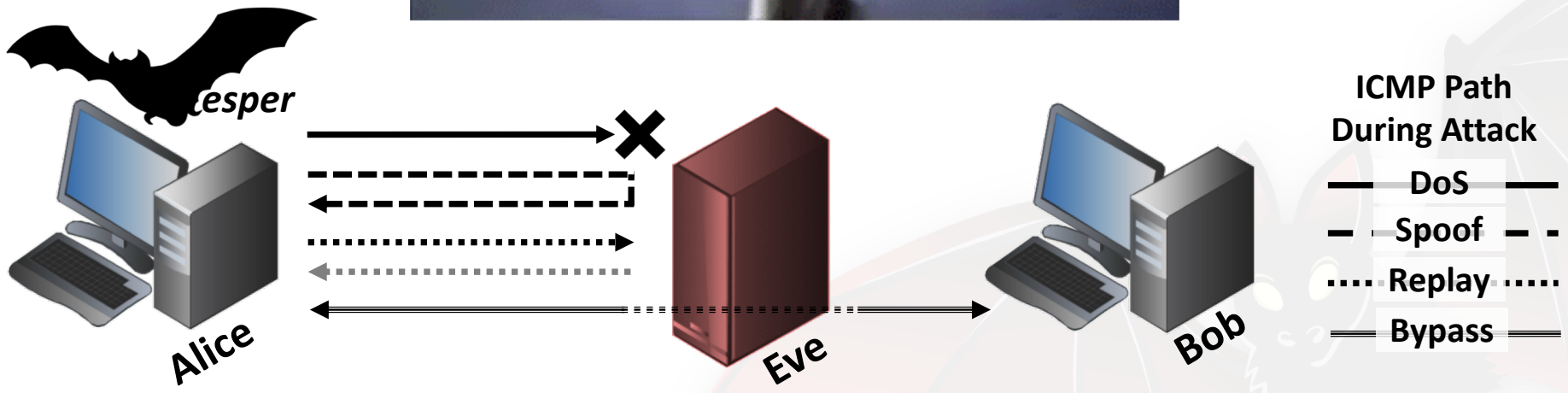
Long-term: 7 days



Attacks Against Vesper

In-Line MitM using *Dedicated Hardware* (IL-DH), and has a bypass to evade detection.





Attacks Against Vesper

		Adversarial Attack											
		DoS			*Spoof*			*Replay*			*Bypass*		
		EP	IL	IP	EP	IL	IP	EP	IL	IP	EP	IL	IP
Feature	v_{E_h}	●	●	●	○	●	●	●	●	●	-	○	○
	v_{rtt*}	●	●	●	○	○	○	○	○	○	-	○	○
	v_{jit}	●	●	●	●	●	●	○	○	○	-	○	○

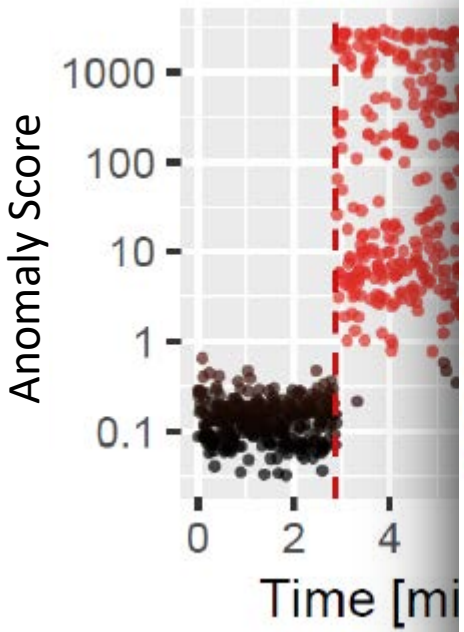
EP: End-Point MitM
IL: In-Line MitM
IP: In-Point MitM

Detection
○ *Weak*
○ *Modest*
● *Strong*

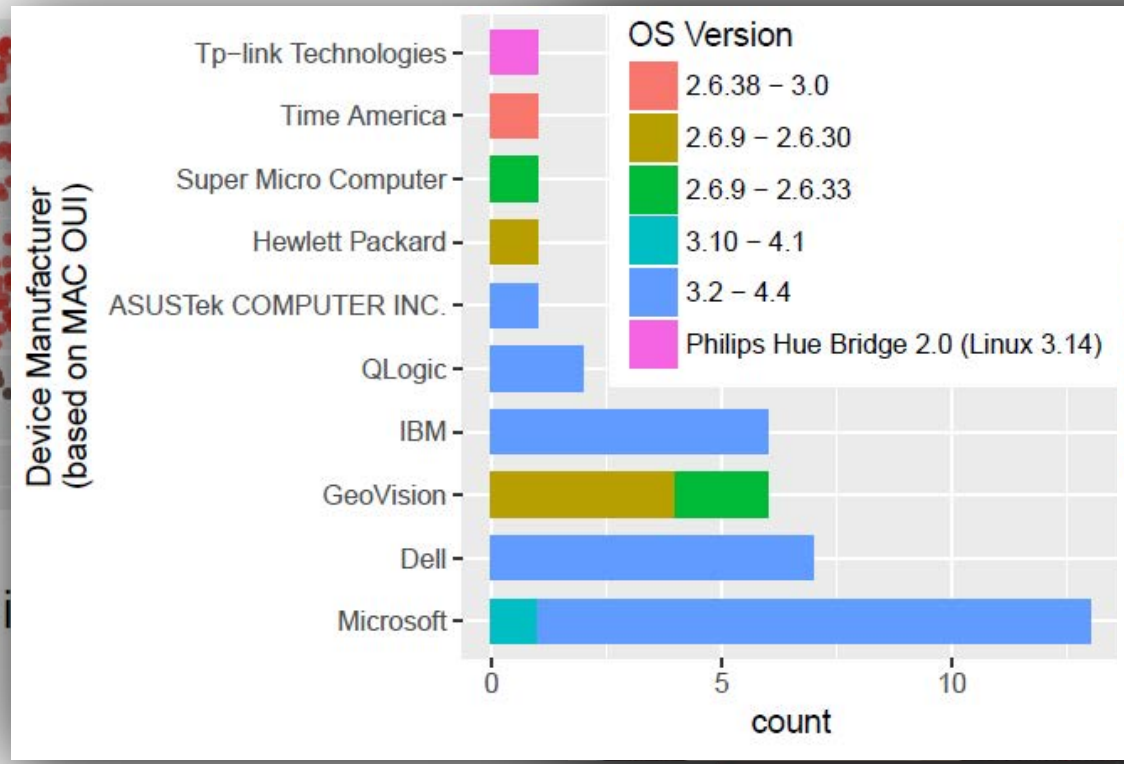
		Strengths	Weaknesses
Feature	v_{E_h}	Detecting Replay Attacks	Has 1D Collision Space
	v_{rtt*}	Detecting Additional Hops	Detecting Spoof Attacks
	v_{jit}	Detecting Spoofing Attacks	Detecting Replay Attacks

Attacks Against Vesper

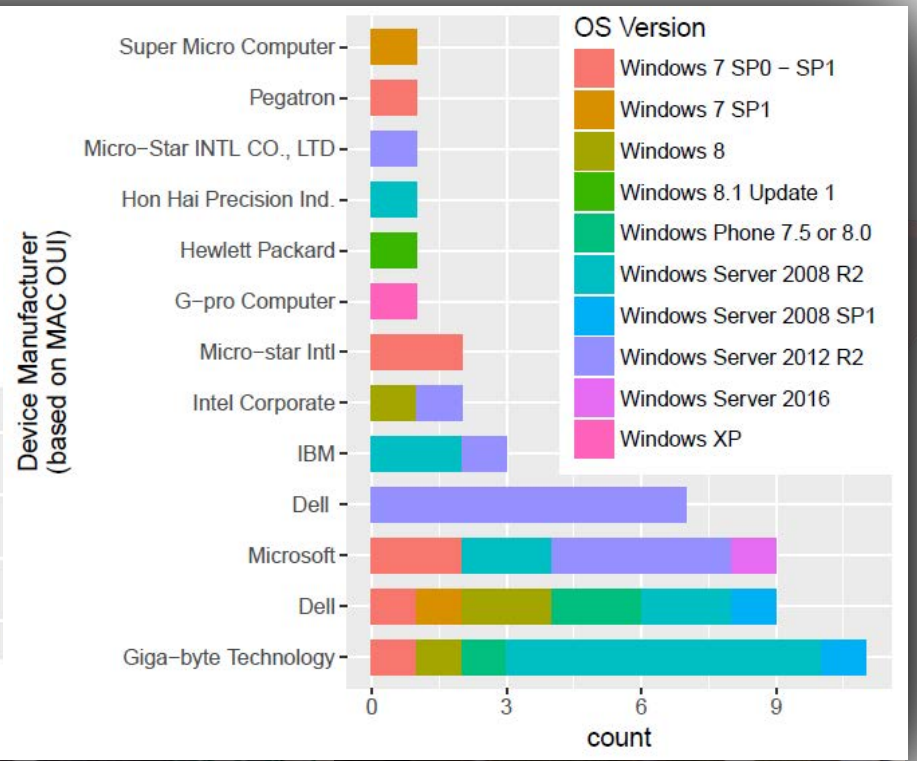
Replay



Bypass



Spoof



Download Vesper

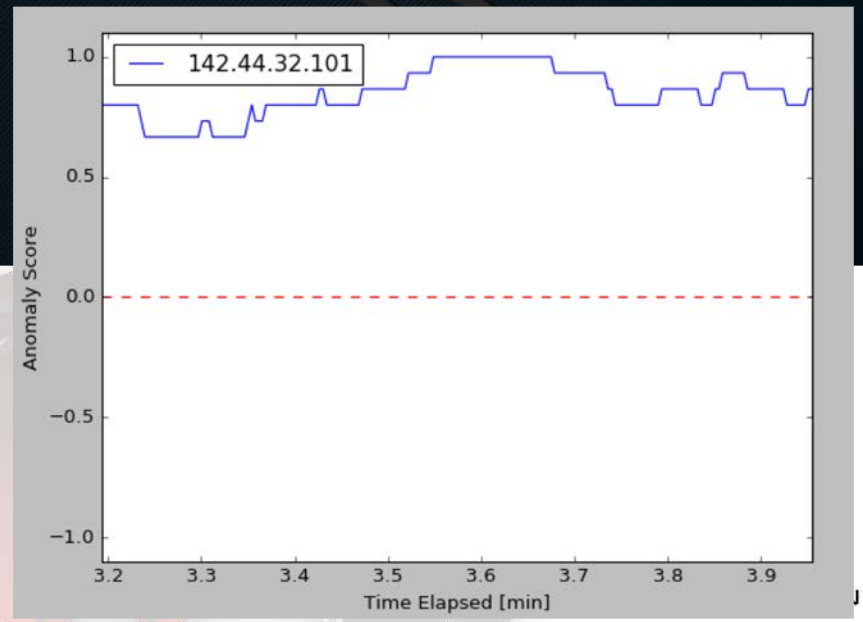
https://github.com/ymirsky/Vesper

GitHub

A lite version of Vesper (v1.0):

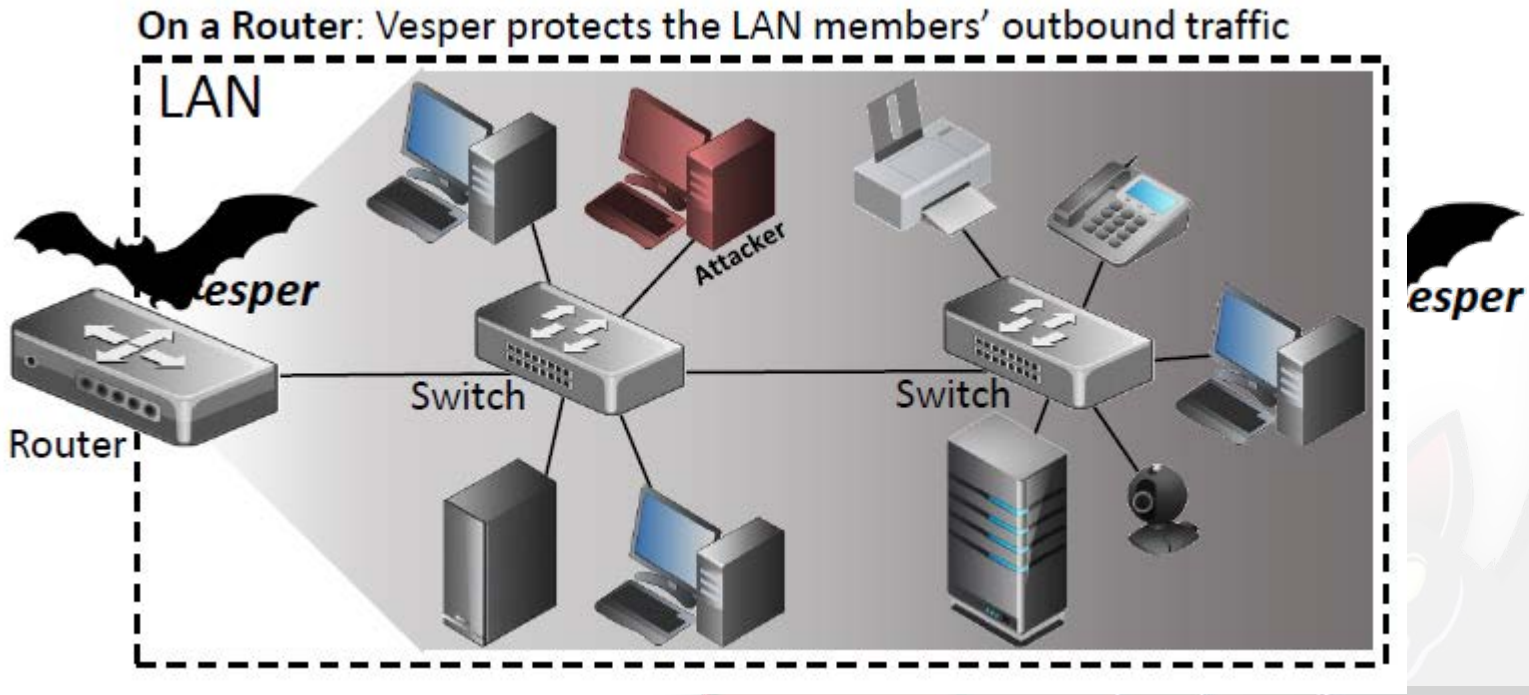
- Python with C++ cython wrapper
- Linux only (tested on Kali)
- Monitors and plots multiple IPs
- Will not alert during adversarial attacks
- Will not detect swapping with identical devices, but will detect different models.

```
Vesper Status  --  Runtime: 0:03:57.293602
+--------------+--------+-------+---------+-------------+----------------+------+
|      IP      | Status | Score | Profile | Tx Freq [kH] | Probe Duration | Note |
+--------------+--------+-------+---------+-------------+----------------+------+
| 142.44.32.101 | Normal |  0.87 | Trained |     1.56     |   158.26 ms    |      |
+--------------+--------+-------+---------+-------------+----------------+------+
Sent 1,049 probes.
```



esper

Vesper: Deployment Strategies

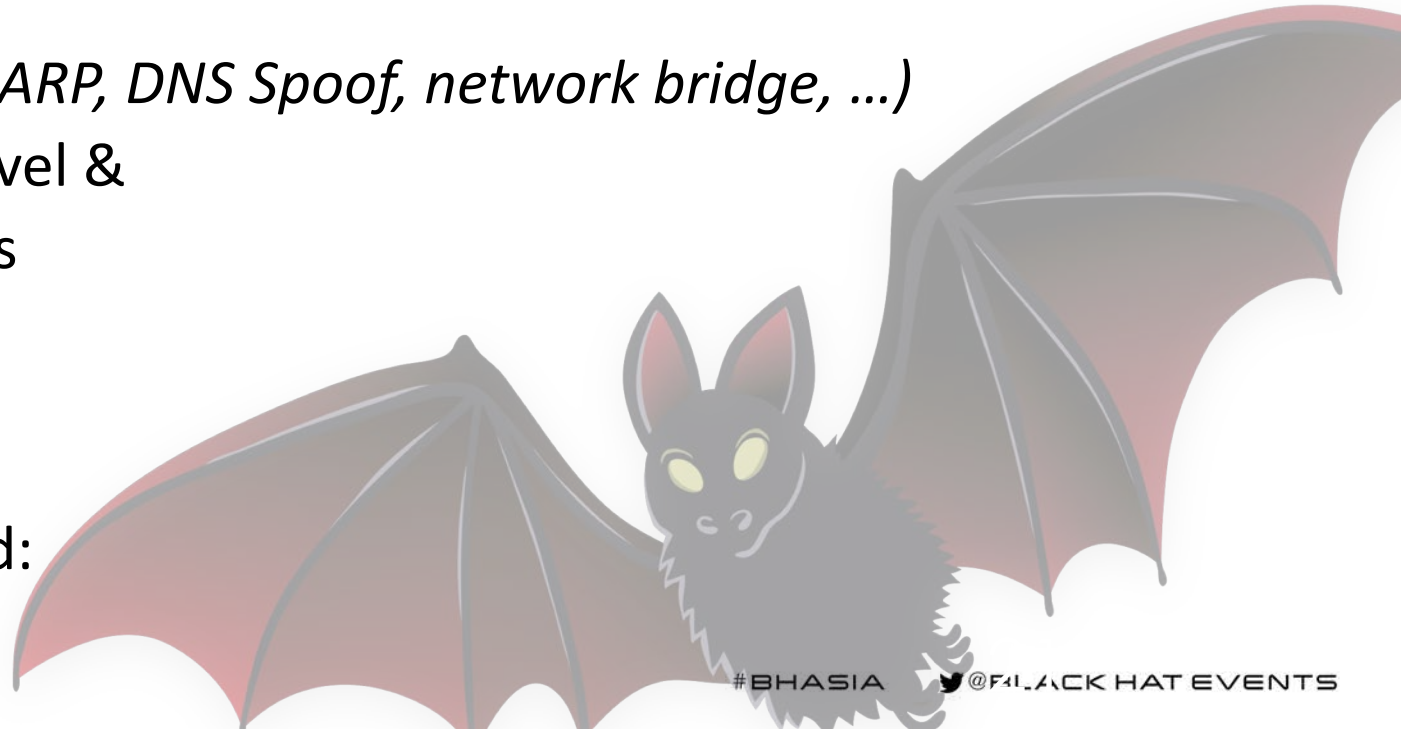


Black Hat Sound Bytes

- In a LAN, we can detect a MitM by “bouncing” virtual signals off hosts.
- The approach detects all LAN-based MitM attacks regardless of
  - Forensic evidence or
  - Attack implementation *(ARP, DNS Spoof, network bridge, …)*
- Implemented at software level & Robust to adversarial attacks

Tool and whitepaper available for download:

https://github.com/ymirsky/Vesper



black hat ASIA 2019

MARCH 26-29, 2019

MARINA BAY SANDS / SINGAPORE

See Like a Bat

Using Echo-Analysis to Detect Man-in-the-Middle Attacks in LANs

Speaker: *Yisroel Mirsky, PhD*

Ben-Gurion University, Israel

yisroel@post.bgu.ac.il

Co-authors:

Naor Kalbo,

Dr. Asaf Shabtai,

Prof. Yuval Elovici

https://github.com/ymirsky/Vesper

CBG

Cyber@Ben-Gurion University of the Negev