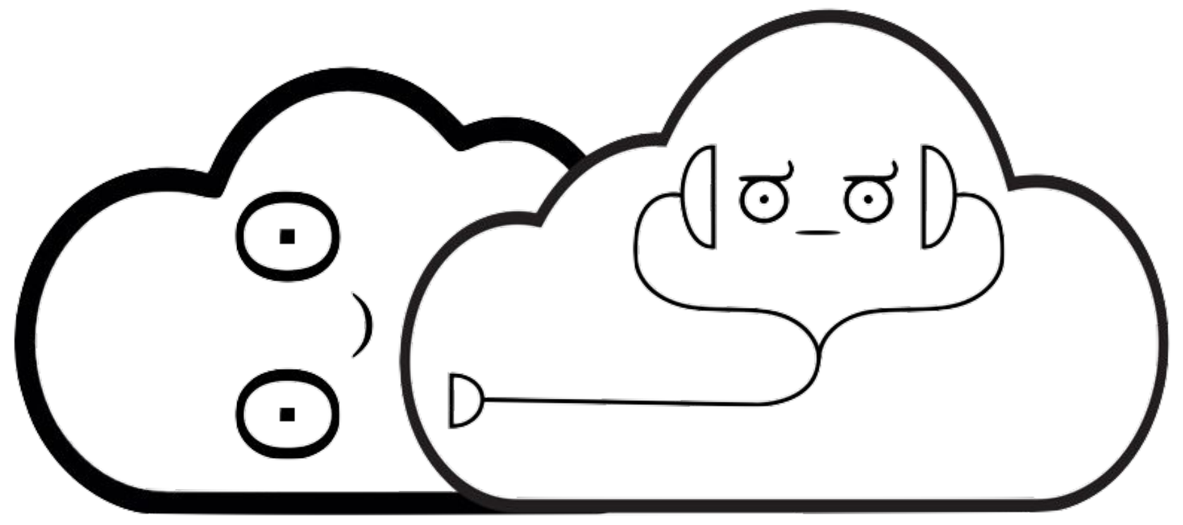


Moving in Next Door:

Network Flooding as a Side Channel in Cloud Environments

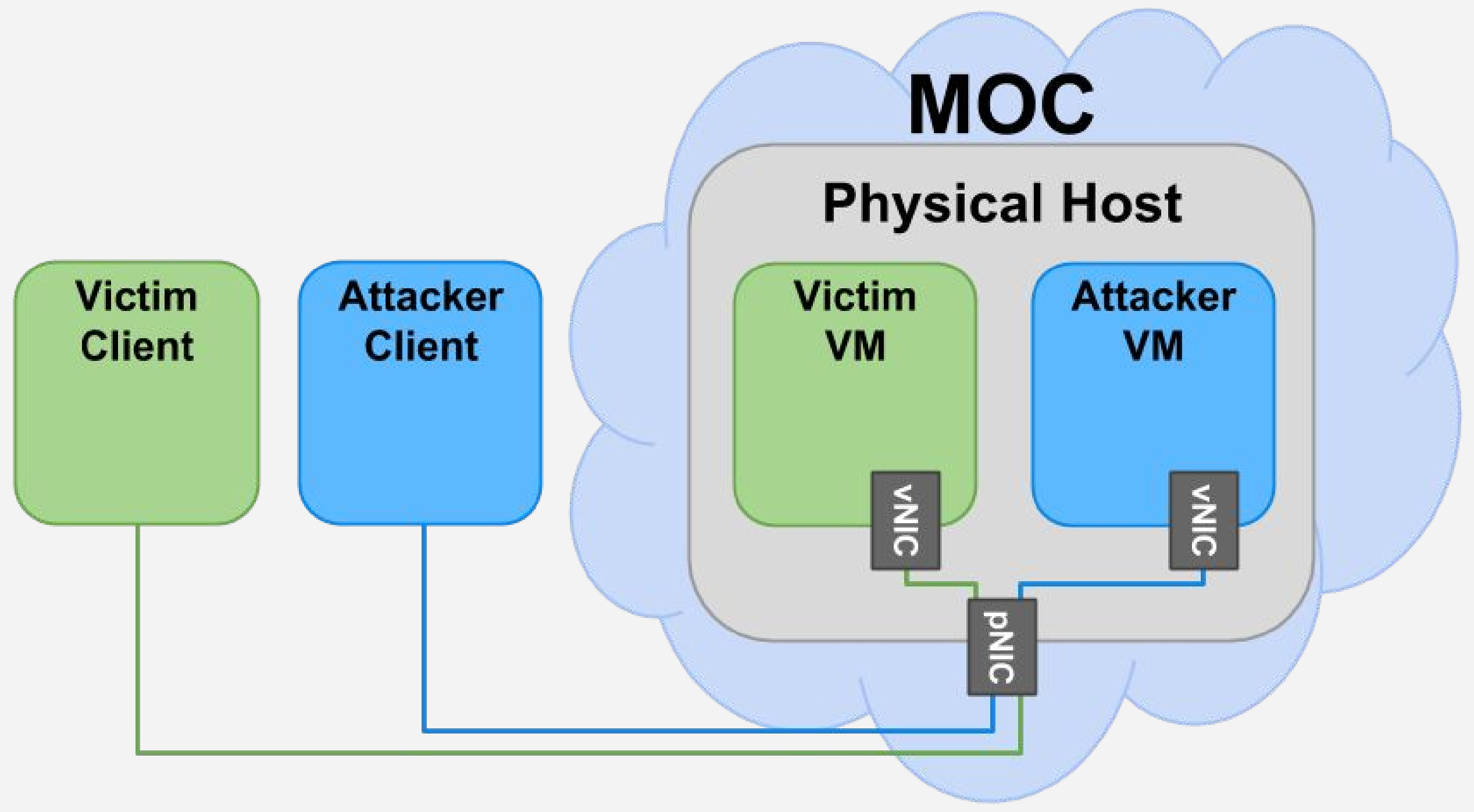
Yatharth Agarwal, Vishnu Murale, Jason Hennessey, Kyle Hogan, and Mayank Varia

Overview

Cloud providers often co-locate multiple tenant's virtual machines (VMs) onto one physical host. This requires the tenants to share hardware, opening up side channels as cross VM attack vectors. Here we focus on the shared physical Network Interface Controller (pNIC). By saturating the host's network interface, we demonstrate passive load measurement to perform traffic analysis attacks on production clouds like the Massachusetts Open Cloud (MOC).

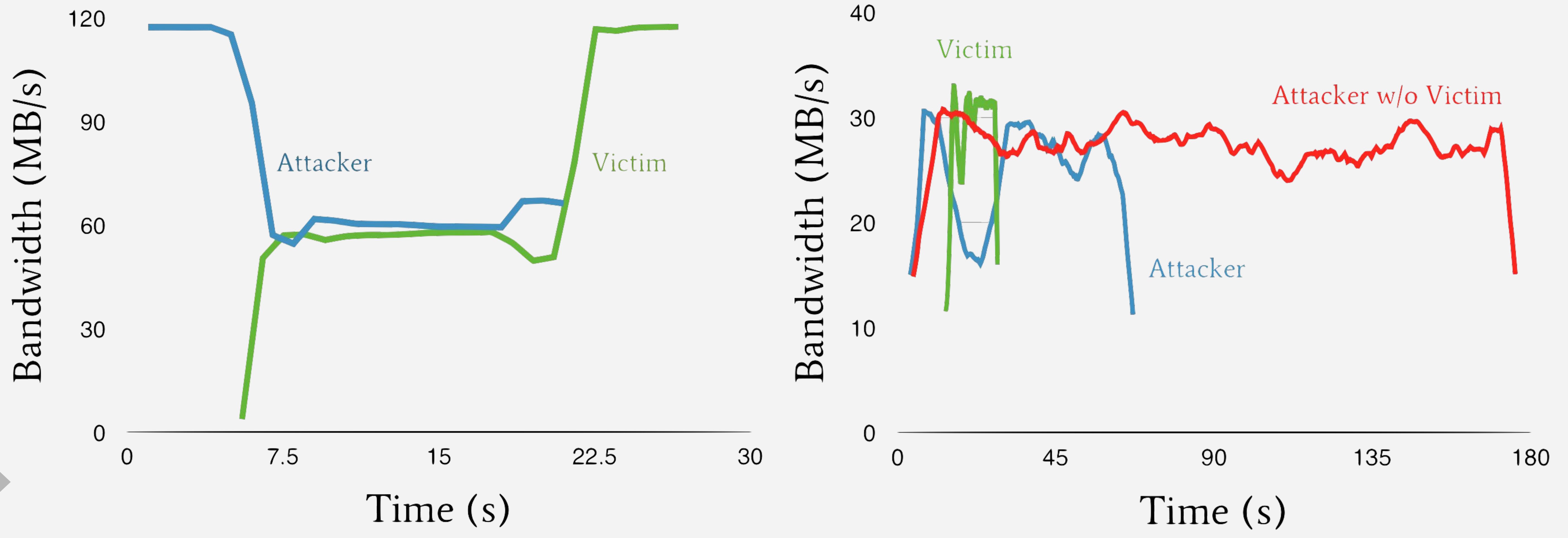
Setup

Attacker VM and Victim VM co-located on physical host



Passive Load Measurement

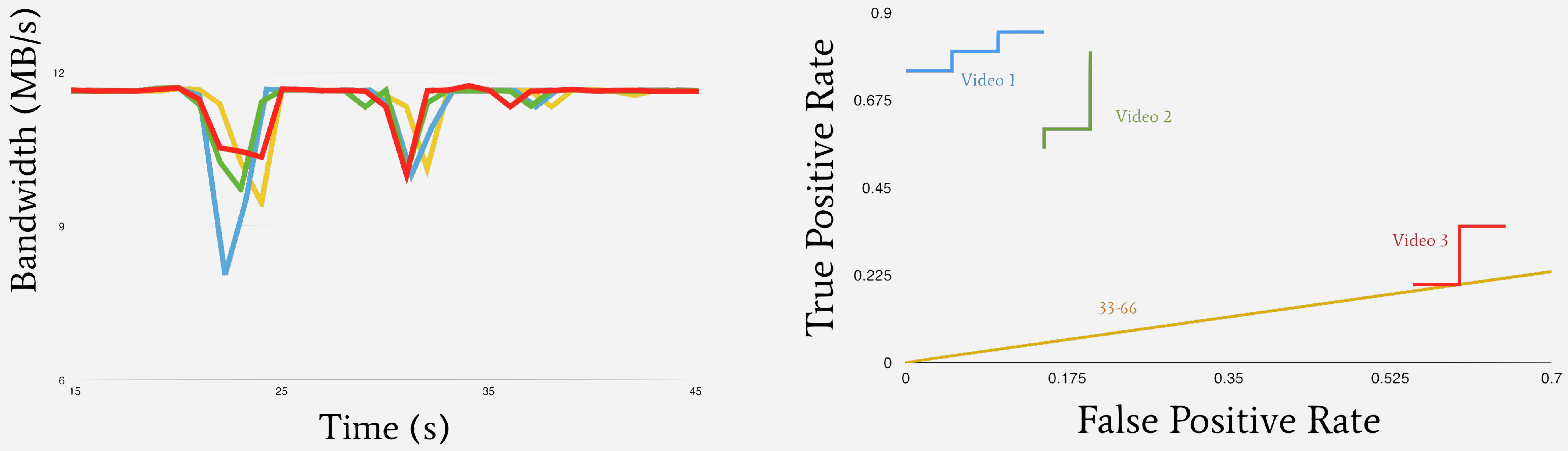
An attacker saturating the network sees a corresponding drop in their bandwidth when a Victim begis sending packets. This demonstrates that an attacker flooding the network can identify segments of time when a co-located victim is active.



Right additionally overlays (in red) Attacker throughput without Victim activity. Note that Victim-caused fluctuations are larger than environmental factors-caused ones.

Classification

A saturating attacker is able to clarify which of three YouTube videos a co-located victim was streaming. This demonstrates that an attacker is also able to identify what sort of traffic a victim is sending over the network.



Left shows Victim load while streaming same video over multiple trials. Right shows ROC curves for our algorithm. Curve for random classification is in orange.

Future Work

Classification: Improve adversary's algorithm to distinguish among a larger variety of traffic patterns;
Detection: Network saturation is easily detectable. Using frequent microbursts instead of constant saturation could mask the attacker and avoid rate limiting while still providing high enough granularity for accurate classification.