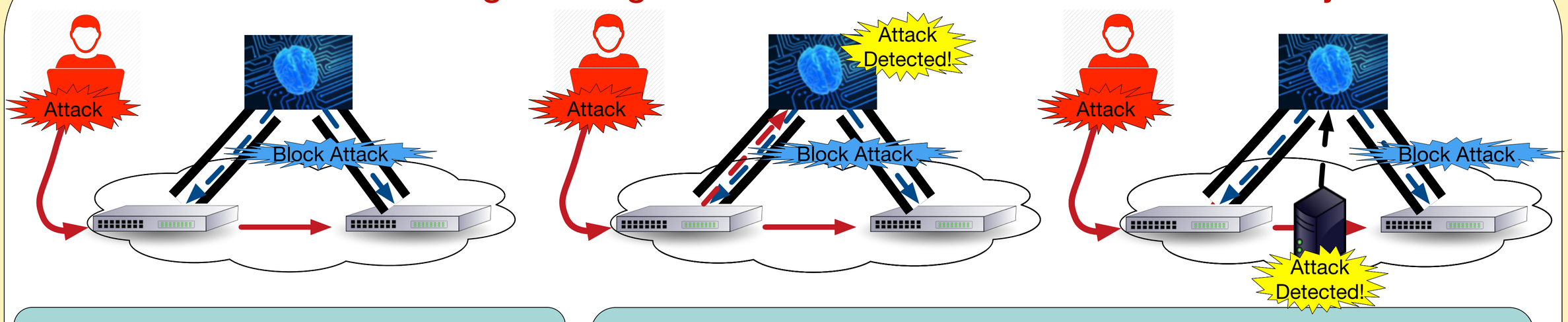
Switch-level Network Security With The OpenFlow Extension Framework (OFX)

PIs: Eric Keller, Adam J. Aviv, and Jonathan M. Smith

The Challenge: Using Software-defined Networks for Security

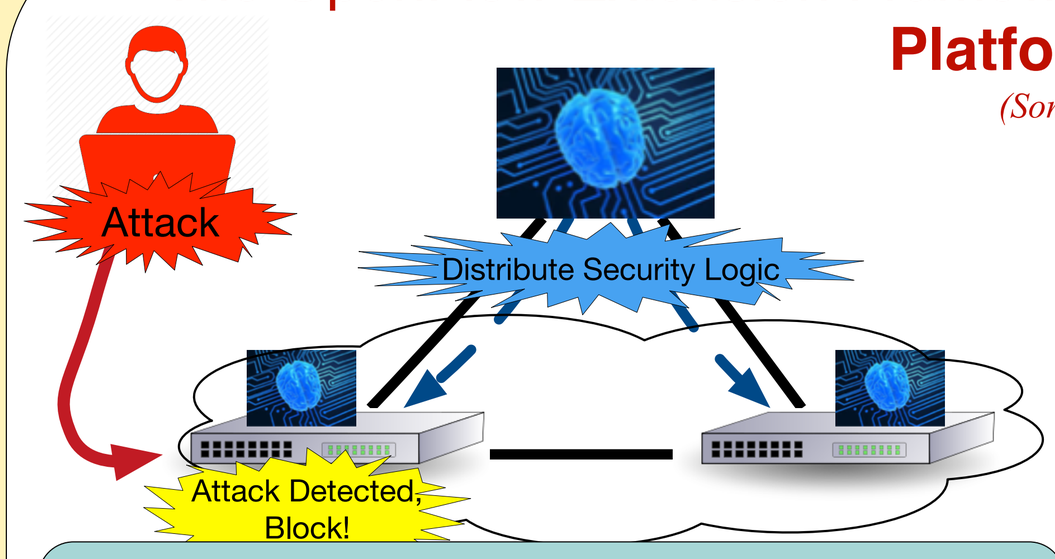


SDNs are a compelling platform for security applications because they enable **programmatic control** over network traffic.

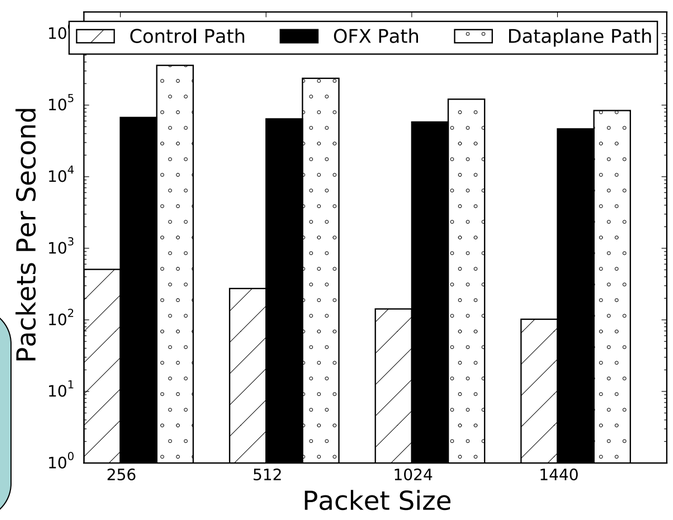
However, the forwarding engines of SDN switches only support simple packet processing, so a network security application must implement much of its **monitoring** and **advanced security related actions** on either the SDN controller (limiting ***performance***) or middleboxes (limiting ***scalability***).

The OpenFlow Extension Framework (OFX): A **High Performance, Scalable Platform for SDN Security**

(Sonchack, J. et al. NDSS '16)



OFX is a framework that allows SDN controllers to push **security logic** down to **switch CPUs**, so it can be **distributed** across the network and process packets with **minimal overhead.**

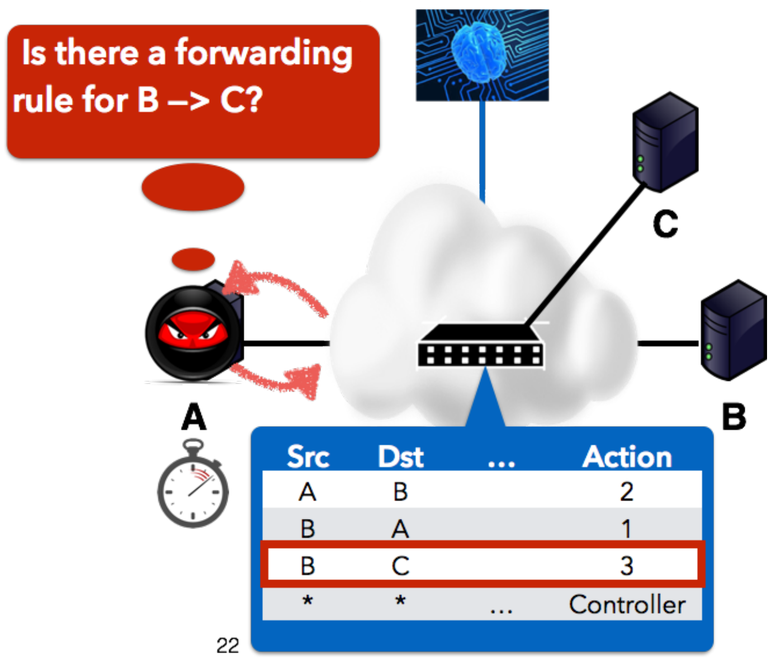


Processing packets at the switch-level OFX agent instead of the controller reduced overhead by **15-500x.**

Statistic	Control Path	OFX Path	Data Path
Min Latency	3.604 ms	0.251 ms	0.169 ms
Avg Latency	4.039 ms	0.31 ms	0.232 ms
Max latency	8.08 ms	0.405 ms	0.292 ms
Max TCP Throughput	1.2 Mbps	584 Mbps	847 Mbps
UDP Drop % @ 5MBPS	72 %	0 %	0%
UDP Drop % @ 50MBPS	-	0.13 %	0%
UDP Drop % @ 500MBPS	-	3.6%	0%

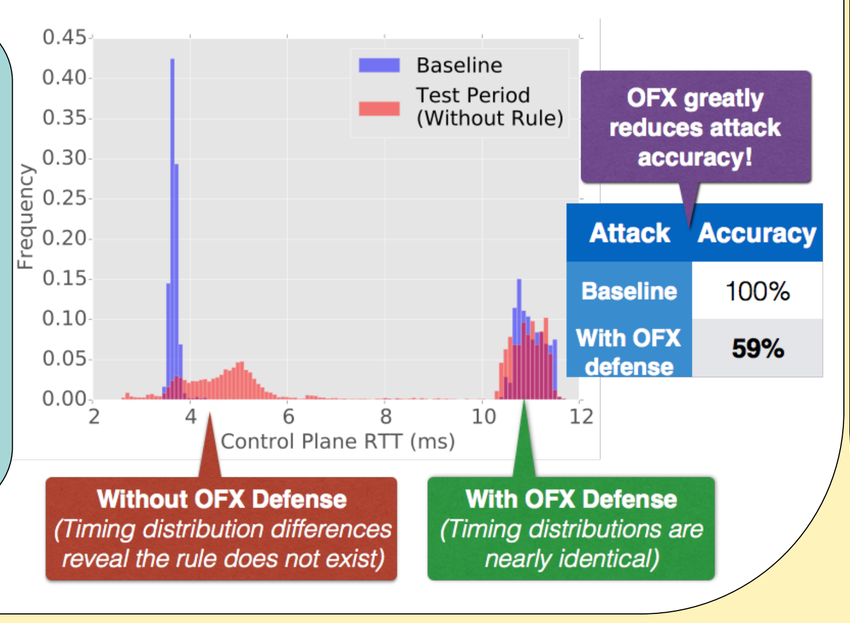
OFX Application: Normalizing SDN Timing

(Sonchack, J. et al. ACSAC'16)



We discovered a non-intrusive timing attack that allows adversaries to learn sensitive details about an SDN by **timing the controller to infer the contents of switch flow tables.**

We wrote an **OFX module that mitigates the attack** by normalizing the controller's response time and **tested it on real OpenFlow hardware.**

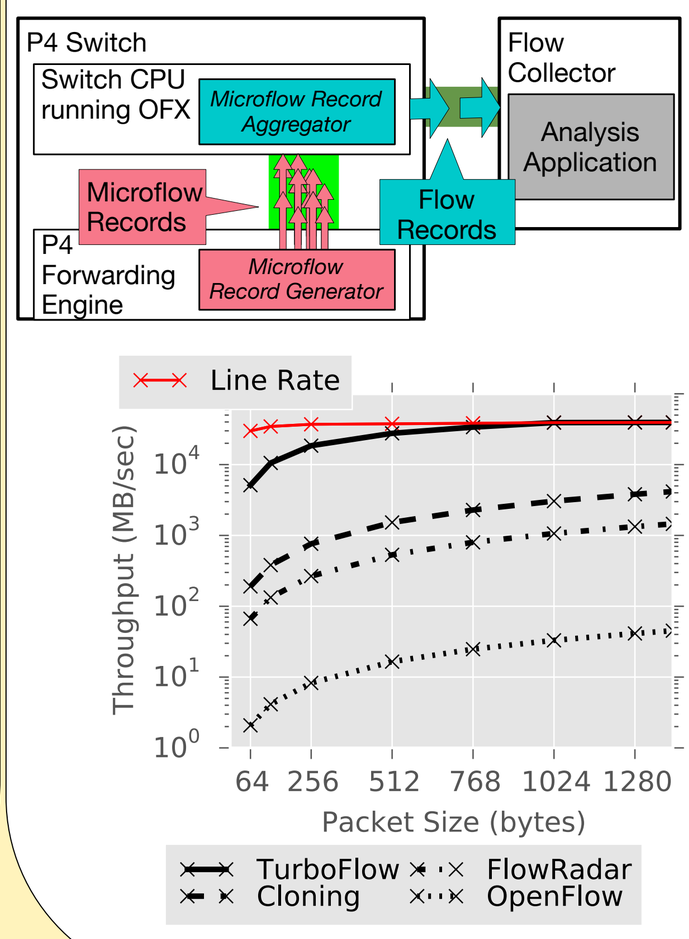


Attack	Accuracy
Baseline	100%
With OFX defense	**59%**

OFX Application: High Speed Monitoring

(In Submission)

Many security applications rely on **flow records** *(e.g., records of TCP connections or UDP streams)*. Current SDN switches can only generate flow records **by installing a monitoring rule for each flow** *(wasting limited memory)* or **sampling flows** *(reducing accuracy)*.



We are extending OFX to work with **next generation forwarding engines (i.e. P4)**, and have developed a hybrid flow record generation algorithm that leverages both the switch CPUs and forwarding engines of commodity switches to generate flow records flow records for high speed networks.

Interested in meeting the PIs? Attach post-it note below!