QIAO KANG

(+1) 346-317-2056, qiaokang1213@gmail.com, wechat: buaakq
https://qiaokang.org

EDUCATION

Rice University, USA Aug 2018 - Dec 2020
MS in Computer Science (early termination of PhD)

Beihang University, China Sep 2014 - Jun 2017
MS in Software Engineering

Beihang University, China Sep 2010 - Jun 2014
BS in Software Engineering

WORK EXPERIENCE

OS kernel (ESXi) developer, VMware, Palo Alto April 2021 - Present

Pensando SmartNIC development.

OS kernel (ESXi) developer, VMware, Beijing April 2017 - Jun 2018

Developed an ESXi NIC driver for the Virtio virtualization framework from scratch, enabling ESXi to run on top of the KVM hypervisor's Virtio virtual NIC. Maintained the Solarflare 10G/40G NIC drivers.

SKILLS

Familiar with C, C++ and Python

Familiar with OS kernel development (network device drivers)

Familiar with P4-based network data plane programming

RESEARCH EXPERIENCE

At Rice University, my research work centers around emerging network hardware, such as P4-programmable switches and SmartNICs. My first two projects (Poise and NetWarden) seek to leverage P4 switches to build more secure networks. My third project (P4wn) contributes a novel profiling tool for stateful P4 programs. My fourth project (Clara) aims at providing performance prediction for SmartNIC offloading.

Poise: Programmable In-Network Security for BYOD Policies (project lead) Aug 2018 - Sep 2019

We present a new security paradigm called programmable in-network security (Poise) for enforcing access control policies in enterprise networks. Administrators write security policies using an easy-to-use, high-level language, and our Poise compiler can generate P4 programs, which will be installed in programmable switches, to enforce these policies. Poise outperforms traditional solutions which are based on OpenFlow networks, and is resilient to control plane saturation attacks. (**USENIX Security'20**)

NetWarden: Mitigating Network Covert Channels without Performance Loss May 2019 - Nov 2019

Network covert channels are an advanced class of attacks to modern networks. Traditional solutions rely on general-purpose CPUs to detect and mitigate them, but they can incur high performance overhead. We propose NetWarden, which leverages P4 switches to mitigate network covert channels at switch data planes. Our experiments show that NetWarden can achieve similar detection accuracy and mitigation effectiveness compared with existing solutions, but without hurting end-to-end TCP performance. (**USENIX Security'20**)

P4wn: Probabilistic Profiling of Stateful Data Planes (project lead) May 2019 - Dec 2020

There is a flurry of projects that develop networked systems in P4-programmable switches, but existing program profiling tools are unable to catch up. We develop P4wn, a program profiler that can analyze stateful program behaviors of recent P4 systems, as well as the behavior probabilities, in a scalable manner. We show P4wn is

useful to discovering adversarial inputs to these P4 systems by distinguishing and stressing the program "edge cases". (**CSET'19, ASPLOS'21**)

Clara: Performance Clarity for SmartNIC Offloading April 2021 - Oct 2021

Offloading packet processing programs from CPUs to SmartNICs can bring significant performance benefits, but the developer has no easy way to understand the offloaded performance beforehand. We develop Clara, an automated tool to analyze a legacy NF in its unported form, identify acceleration opportunities, and predict its offloaded performance. Our experiments using Click NFs and a Netronome SmartNIC demonstrate that Clara can provide useful offloading hints and reasonable prediction accuracy. (**HotNets'20, SOSP'21**)

RESEARCH PUBLICATIONS

Automating SmartNIC Offloading Insights for Network Functions
Yiming Qiu, Jiarong Xing, Kuo-Feng Hsu, **Qiao Kang**, Ming Liu, Srinivas Narayana, and Ang Chen
The 28th ACM Symposium on Operating Systems Principles October 25-28, 2021 (**SOSP'21**), Virtual, Oct 2021

Probabilistic Profiling of Stateful Data Planes for Adversarial Testing
Qiao Kang*, Jiarong Xing*, Yiming Qiu, and Ang Chen
26th International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS'21**), Virtual, April 2021

Clara: Performance Clarity for SmartNIC Offloading
Yiming Qiu*, **Qiao Kang***, Ming Liu, and Ang Chen
19th ACM Workshop on Hot Topics in Networks (**HotNets'20**), Virtual, Nov 2020

Mitigating Network Covert Channels while Preserving Performance
Jiarong Xing, **Qiao Kang**, and Ang Chen
29th USENIX Security Symposium (**Security'20**), Virtual, Aug 2020

Programmable In-Network Security for Context-aware BYOD Policies
Qiao Kang*, Lei Xue*, Adam Morrison*, Yuxin Tang, Ang Chen, and Xiapu Luo
29th USENIX Security Symposium (**Security'20**), Virtual, Aug 2020

Automated Attack Discovery in Data Plane Systems
Qiao Kang, Jiarong Xing and Ang Chen
12th USENIX Workshop on Cyber Security Experimentation and Test (**CSET'19**), Santa Clara, CA, USA, Aug 2019

(* indicates equal contributions)

TALKS

Qiao Kang, "Programmable In-Network Security for Context-aware BYOD Policies"
USENIX Security'20 (online), Aug 2020

Qiao Kang, "Programmable In-Network Security for Context-aware BYOD Policies"
Computer Systems Lab, University of Washington (online), Jul 2020

Qiao Kang, "Programmable In-Network Security for Context-aware BYOD Policies"
P4 Expert Roundtable Series (online), Apr 2020

Qiao Kang, "Automated Attack Discovery in Data Plane Systems"
CSET'19, Santa Clara, CA, USA, Aug 2019