Keyu Man

Riverside,CA kman001@ucr.edu Google Scholar dblp github.com/mkyybx

Education

University of California, Riverside 09/2018 – Present (Exp. Grad. 2023)
Ph.D. in Computer Science • Research Track: Network/System Security • Advisor: Zhiyun Qian

Beijing University of Posts and Telecommunications 09/2014 – 06/2018
B.S. in Computer Science and Technology • Rank: 18 out of 311

Selected Projects

Automated Side-channel Discovery – Ongoing research 02/2022 – Present

- Aim to analyze control-flow and data-flow of **kernel**s and protocol implementations for detecting potential side-channel vulnerabilities.
- Customized binary dynamic **symbolic execution** based on S2E, KLEE(LLVM) and QEMU using **C++**.

DNS Cache Poisoning Attacks – CCS '20, USENIX Security '20, CCS '21 01/2019 – 11/2021

- **[P1] SADDNS(Side Channel Attacks) [GitHub 1] [GitHub 2]**
  - Devised two novel side channels in **Linux Kernel** (CVE-2020-25705, CVE-2021-20322) enabling an off-path attacker to poison the cache of any DNS resolver. Implemented attacks in **Golang** using **gopacket(libpcap)**.
  - Compromised public resolvers (e.g., Quad9) in <10 minutes and found 35% open resolvers vulnerable.
  - Built a website with online vulnerability check service using **Javascript**, **Golang(CGI)** and a customized authoritative name server.
  - Created a distributed network using 3500 **AWS EC2** instances to crack the crypto secret of Linux hosts (under authorization).
- **[P3] IP Fragment Attack**
  - Discovered the architectural flaw of DNS and the unique position of DNS forwarder, which allows an off-path attacker to inject malicious DNS resource records to any legitimate DNS response.
  - Implemented the attack in **Golang** to poison the DNS cache of home routers.

[P2] Transnational Network Performance Measurement [GitHub] – SIGMETRICS '20 02/2019 – 05/2019

- Designed a large-scale network performance measurement aiming to uncover the reason of mysterious slowdown on some transnational traffic.
- Modified the open-source project mtr(**C**) for sending customized TCP packets and deployed it to vantage points (including **AWS EC2** instances) across the world, to discover the impact of different packet types on network performance.
- Analyzed the measurement results and proposed causes for the diurnal slowdown pattern using **Java**.

Intern Experience

Meta Platforms, Inc. – Software Engineer Intern 06/2022 – 09/2022
Menlo Park, CA

- Introduced hybrid key exchange (an IETF draft on TLS 1.3) and post quantum key exchange algorithms to Meta's open-source implementation of TLS Fizz(**C++**), which is deployed on every Meta's public service like Instagram.
- Made Fizz future-proof aiming the security threat from the quantum computers.
- Incorporated several **C**-based open-source PQ algorithms into Fizz and evaluated the performance of encryption and decryption.

NetEase – Android Developer Intern 11/2017 – 07/2018
Beijing, China

- Optimized FFmpeg (native **C** library) to reduce the cumulative latency of **live stream** due to jitter by trimming playback buffer to improve the interactive experience between the audience and broadcaster.
- Implemented QR code scan feature by adapting the open-source project ZXing.

Research Experience

UCR CSE Dept. – Graduate Student Researcher 09/2018 – Present
Riverside, CA

- Performed **static analysis** on **Linux kernel** and discovered novel side channels on **UDP** and **ICMP** stack along with their root causes.
- Implemented the side-channel attacks and measured victim population (among 2M hosts) in **Golang**.

- Reverse engineered **DSRC** stack implementation using **IDA** and found time drifting attacks that can compromise the safety of **connected vehicle**s.
- Built customized **symbolic execution** engine based on **S2E**.
- Contributed code to open-source community (*e.g.,* Linux kernel, shadowsocks, S2E).

Publications

DNS Cache Poisoning Attack: Resurrections with Side Channels [Website] [P1]
Keyu Man, Xinan Zhou, Zhiyun Qian
In Proceedings of ACM Conference on Computer and Communications Security (CCS'21), November 15-19, 2021, Virtual Event, Republic of Korea. [Acceptance rate 22% (196/879)]

Themis: Ambiguity-Aware Network Intrusion Detection based on Symbolic Model Comparison [PDF]
Zhongjie Wang, Shitong Zhu, **Keyu Man**, Pengxiong Zhu, Yu Hao, Zhiyun Qian, Srikanth V. Krishnamurthy, Tom La Porta, Michael J. De Lucia
In Proceedings of ACM Conference on Computer and Communications Security (CCS'21), November 15-19, 2021, Virtual Event, Republic of Korea. [Acceptance rate 22% (196/879)]

Eluding ML-based Adblockers With Actionable Adversarial Examples [PDF]
Shitong Zhu, Zhongjie Wang, Xun Chen, Shasha Li, **Keyu Man**, Umar Iqbal, Zhiyun Qian, Kevin S. Chan, Srikanth V. Krishnamurthy, Zubair Shafiq, Yu Hao, Guoren Li, Zheng Zhang, Xiaochen Zou
In Proceedings of Annual Computer Security Applications Conference (ACSAC'21), December 6-10, 2021, Virtual Event. [Acceptance rate 24% (80/326)]

DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels [Website] [P1]
Keyu Man, Zhiyun Qian, Zhongjie Wang, Xiaofeng Zheng, Youjun Huang, Haixin Duan
In Proceedings of ACM Conference on Computer and Communications Security (CCS'20), November 9-13, 2020, Virtual Event, USA. [Acceptance rate 17% (121/715)]
[Distinguished Paper Award (1/715)][Google's VRP Reward][GeekPwn Award]

Characterizing Transnational Internet Performance and the Great Bottleneck of China [PDF] [P2]
Pengxiong Zhu, **Keyu Man**, Zhongjie Wang, Zhiyun Qian, Roya Ensafi, J. Alex Halderman, Haixin Duan
In Proceedings of ACM SIGMETRICS 2020, June 8-12, 2020, Boston, MA, USA. [Acceptance rate 20% (55/280)]

Poison Over Troubled Forwarders: A Cache Poisoning Attack Targeting DNS Forwarding Devices [PDF] [P3]
Xiaofeng Zheng, Chaoyi Lu, Jian Peng, Qiushi Yang, Dongjie Zhou, Baojun Liu, **Keyu Man**, Shuang Hao, Haixin Duan, Zhiyun Qian
In Proceedings of USENIX Security 2020, August 12-14, 2020, Boston MA, USA. [Acceptance rate 16% (157/977)]

Honors & Awards

Dissertation Year Program Award	2022
Laxmi N. Bhuyan Endowed Fellowship in Computer Science	2021
Distinguished Paper Award of ACM CCS 2020	2020
Google's Vulnerability Reward Program (VRP) Reward	2020
GeekPwn Worldwide Security Geek Contest Award	2020
Dean's Distinguished Fellowship Award	2018 – 2019

Technical Skills

Programming languages: Golang, C/C++, Java, SQL, Assembly, Bash, Python, CUDA , HTML
Tools & frameworks: Git, LaTeX, Linux, Kernel, gopacket, AWS, Wireshark, S2E, KLEE, LLVM, Apache CGI, libpcap, raw socket
Protocols: DNS, TCP/IP, QUIC

Professional Activities

Program Committee, EAI SecureComm 2023
Artifact Evaluation Committee, USENIX Security 2022