1 Hacker Way
Menlo Park, CA 94025
☎ *+1 (650) 888-2679*
✉ *aaron.yzdou@gmail.com*
🖱 *aarondou.github.io*

Yanzhi (Aaron) Dou

Research Interests

Fuzz testing, anomaly detection, wireless network security, privacy-enhancing technologies, machine learning, and applied cryptography.

Education

08/2013-11/2017 **Virginia Tech**, Blacksburg, VA, USA.
Ph.D. of Computer Engineering
Advisor: Yaling Yang
GPA: **3.94**/4
Dissertation: Toward Privacy-Preserving and Secure Dynamic Spectrum Access

08/2009-06/2013 **Tsinghua University**, Beijing, China.
B.E. of Electrical Engineering
Advisor: Wei Chen & Bo Bai
Dissertation: A Mechanism for Low-Complexity Joint Resources Sharing Based on Game Theory in Cognitive Radio Networks

08/2009-06/2011 **Tsinghua University**, Beijing, China.
Academic Talent Program (Physics and Mathematics) in School of Sciences

Industry Experience

02/2018-present **Research Scientist**, Facebook HQ, Menlo Park, CA.
- Building a distributed fuzzing platform to test and harden the key components of the massive FB codebase.
- Built anomaly detection systems for alerting about unusual data movement and performing root cause analysis on detected anomalies

05/2017-08/2017 **Software Engineer Intern**, Facebook HQ, Menlo Park, CA.
Developed a powerful tool set for debugging and configuring the routing nodes in datacenters.

Research Projects

03/2019-present **Distributed fuzzing platform**.
at Facebook product security team
Key words: fuzz testing; distributed system

My high-impact work includes adding an abstraction layer to ease the flow of onboarding new fuzzers, enhancing the platform fuzzing efficiency by smart scheduling, enabling corpus sharing for cross-pollination, and developing accurate crash deduplication methods. Aside from these, I'm also leading the effort to work with security engineers closely to improve the bug triage experience. Now I'm working on a new topic to quantitatively evaluate fuzzing quality.

03/2018-03/2019 **Anomaly detection and root cause analysis.**
at Facebook realtime data infra team
Key words: anomaly detection; root cause analysis; submarket analysis; distributed system

I built a root cause analysis service for explaining outliers on top-line metrics. The service needed to meet high QPS requirements while a single request can demand huge computational resource. I overcame the challenges through careful design from both the algorithm level and the system level. The service was able to handle requests from other analytics cases, including explaining A/B test results and non-anomalous, long term trends.

09/2014-11/2017 **Preserving Users' Privacy in Dynamic Spectrum Access systems.**
joint work with Prof. Yaling Yang & Prof. Kui Ren
Key words: dynamic spectrum access (DSA); privacy; secure multiparty computation

I worked on building privacy-preserving dynamic spectrum access systems to protect users' privacy from being leaked and misused. Dynamic spectrum access was a new spectrum access technology to replace the traditional static access method for improving spectrum utilization by sharing the licensed spectrums. The technology had been successfully deployed in TV whitespaces in the US and was under promotion to expand to the 3.5GHz spectrum bands. However, it faced one vital issue: different from the TV whitespaces, the incumbent users in 3.5 GHz bands were mostly U.S. government radars (e.g., Navy aircraft carriers) and they were very sensitive about their privacy. My research was the first to identify the stringent issue and I published a series of work to design different privacy-preserving systems to address it.

08/2013-08/2014 **Malware Detection for Cognitive Radio.**
joint work with Prof. Yaling Yang & Prof. Danfeng Yao
Key words: cognitive radio (CR); anomaly detection; machine learning

Flexible software-oriented design of cognitive radio enabled adversaries to launch large scale attacks because infected cognitive radio systems could hop across different spectrum bands to interfere with the incumbents. It was challenging to do effective malware detection on cognitive radio systems because the vast amount of data flowing between hosts and radio hardware was very critical to examine but yet hard to capture. We hacked the system to collect useful data and adopted machine learning techniques to detect anomalies. We built a small cognitive radio network with GNU radio to evaluate our system.

08/2014-08/2018 **Towards Stealthy Manipulation of Road Navigation Systems.**
joint work with Dr. Kexiong Zeng, Prof. Yaling Yang, Prof. Gang Wang
Key words: GPS spoofing; navigation; route planning; user study

While GPS spoofing was a known threat, it was not yet clear if spoofing attacks could truly manipulate road navigation systems. In this project, we explored the feasibility of a stealthy manipulation attack against road navigation systems. The goal was to trigger the fake turn-by-turn navigation to guide the victim to a wrong destination without being noticed.

Selected Media Coverage

7//12/2018 **This GPS Spoofing Hack Can Really Mess With Your Google Maps Trips.**
Forbes

8//18/2018 **How to Defend Against GPS Spoofing Attacks.**
The Wall Street Journal

7//19/2018 **Researchers Mount Successful GPS Spoofing Attack Against Road Navigation Systems.**
ACM TechNews

Publications

Full papers

INFOCOM'19 He Li, Yaling Yang, **Yanzhi Dou**, Jung-Min (Jerry) Park, Kui Ren. "PeDSS: Privacy Enhanced and Database-Driven Dynamic spectrum Sharing.", *INFOCOM* 2019

USENIX Security'18 Kexiong Curtis Zeng, Shinan Liu, Yuanchao Shu, Dong Wang, Haoyu Li, **Yanzhi Dou**, Gang Wang, Yaling Yang. "All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems", *27th USENIX Security Symposium 2018*

DySPAN'18 He Li, **Yanzhi Dou**, Chang Lu, Doug Zabransky, Yaling Yang, Jung-Min (Jerry) Park. "Preserving the Incumbent Users' Location Privacy in the 3.5 GHz Band.", *IEEE International Symposium on Dynamic Spectrum Access Networks* 2018.

CrownCom'18 He Li, Yaling Yang, **Yanzhi Dou**, Chang Lu, Doug Zabransky. "Comparison of incumbent user privacy preserving technologies in database driven dynamic spectrum access systems.", *13th EAI International Conference on Cognitive Radio Oriented Wireless Networks* 2018.

ICDCS'17 **Yanzhi Dou**, He Li, Kexiong (Curtis) Zeng, Jinshan Liu, Yaling Yang, Bo Gao and Shaoqian Li. "Preserving Incumbent Users' Privacy in Server-Driven Dynamic Spectrum Access Systems.", *IEEE ICDCS* 2017.

JSAC'17 **Yanzhi Dou**, Kexiong (Curtis) Zeng, He Li, Yaling Yang, Bo Gao, Kui Ren, and Shaoqian Li. "P2-SAS: Privacy-Preserving Centralized Dynamic Spectrum Access System.", *IEEE Journal on Selected Areas in Communications*, 2017.

MobiHoc'16 **Yanzhi Dou**, Kexiong (Curtis) Zeng, He Li, Yaling Yang, Bo Gao, Chaowen Guan, Kui Ren, and Shaoqian Li. "P2-SAS: Preserving Users' Privacy in Centralized Dynamic Spectrum Access Systems.", *ACM MobiHoc* 2016. (Acceptance ratio = 35/187 = 18.70%)

INFOCOM'16 Bo Gao, Sudeep Bhattarai, Jung-Min (Jerry) Park, Yaling Yang, Min Liu, Kexiong (Curtis) Zeng, **Yanzhi Dou**. "Incentivizing Spectrum Sensing in Database-Driven Dynamic Spectrum Sharing.", *IEEE INFOCOM* 2016. (Acceptance ratio = 300/1644 = 18.25%)

INFOCOM'15 **Yanzhi Dou**, Kexiong (Curtis) Zeng, Yaling Yang and Danfeng Yao. "MadeCR: Correlation-based Malware Detection for Cognitive Radio", *IEEE INFOCOM 2015* (Acceptance ratio = 316/1640 = 19%).

JEIT'15 **Yanzhi Dou**, Bo Bai, Manxi Wang, Wei Chen, Zhigang Cao. "A Mechanism for Low-Complexity Joint Resources Sharing Based on Game Theory in Cognitive Radio Networks", *Journal of Electronics and Information Technology*, 2015.

Posters

HotMobile'17 Kexiong (Curtis) Zeng, Yuanchao Shu, Shinan Liu, **Yanzhi Dou**, and Yaling Yang. "A Practical GPS Location Spoofing Attack in Road Navigation Scenario.", *ACM HotMobile* 2017.

MobiCom'16 **Yanzhi Dou**, Kexiong (Curtis) Zeng, Yaling Yang, and Kui Ren. "Poster: Preserving Incumbent Users' Privacy in Exclusion-Zone-Based Spectrum Access Systems", *ACM MobiCom* 2016.

ICDCS'16 **Yanzhi Dou**, He Li, Kexiong (Curtis) Zeng, Jinshan Liu, Yaling Yang, Bo Gao and Shaoqian Li. "Poster: Preserving Incumbent Users' Privacy in Server-Driven Dynamic Spectrum Access Systems", *IEEE ICDCS* 2016.

MobiCom'15 **Yanzhi Dou**, Kexiong (Curtis) Zeng, Yaling Yang. "Poster: Privacy-Preserving Server-driven Dynamic Spectrum Access System.", *ACM MobiCom*, 2015.

MobiSys'15 Kexiong (Curtis) Zeng, **Yanzhi Dou**, Yaling Yang, Ranveer Chandra. "Poster: Location Verification and Recovery for Mobile In-Vehicle Applications", *ACM MobiSys*, 2015.

Presentations

"Privacy-Preserving Centralized Dynamic Spectrum Access System".

- at ACM MobiCom, New York, 10/4/2016.
- at ACM MobiHoc, Paderborn, Germany, 7/8/2016.
- at IEEE ICDCS, Nara, Japan, 6/29/2016.
- at IEEE INFOCOM Innovation Challenge Panel, San Francisco, CA, 4/14/2016.
- at CESCA Day, VT Squires Student Center, Blacksburg, VA, 04/24/2016.

"MadeCR: Correlation-based Malware Detection for Cognitive Radio".

- at IEEE INFOCOM, Hong Kong, 4/28/2015.
- at CESCA Day, Claytor Lake, VA, 04/19/2014.

Mentorships

Masters Chang Lu, Kapil Kale, Doug Zabransky, Devashree Kulkarni

Community Service

Reviewer IEEE INFOCOM 2017, 2016, 2015, IEEE WCNC 2018

Reviewer IEEE Transactions on Mobile Computing, IEEE Systems Journal

Honors and Awards

2017	CESCA Outstanding student award from VT ECE department
2016	Selected participant of ACM Student Research Competition(SRC)
2016	ACM MobiCom SRC Travel Grant
2016	ACM MobiHoc Student Travel Grant
2016	IEEE ICDCS Student Travel Grant
2015	ACM MobiCom SRC Travel Grant
2015	IEEE INFOCOM Student Travel Grant

Graduate Coursework

Spring 2016	Advanced Foundations of Networking	Y. Thomas Hou
Spring 2016	Cryptopgraphic Engineering	Patrick Schaumont
Spring 2016	Graph Theory	Ezra Brown
Fall 2015	Bayesian Statistics	Scotland Leman
Fall 2015	Statistics in Research	Anne Driscoll
Fall 2014	Network and Computer Security	Jung-Min (Jerry) Park
Fall 2014	Network Architecture and Protocols	Y. Thomas Hou
Spring 2014	Advanced Topics on System & Network Security	Danfeng (Daphne) Yao
Spring 2014	Optimization	Barbara Fraticelli
Fall 2013	Software Radios	Jeffrey H. Reed

Fall 2012 Speech Signal Processing Xi Xiao

Ph.D. Advisory Members

Prof. Yaling Yang.
Professor
Electrical & Computer Engineering
Virginia Tech
yyang8@vt.edu

Prof. Kui Ren, *IEEE Fellow*.
Professor
Computer Science & Engineering
SUNY, Buffalo
kuiren@buffalo.edu

Prof. Patrick Schaumont.
Professor
Electrical & Computer Engineering
Virginia Tech
schaum@vt.edu

Prof. Y. Thomas Hou, *IEEE Fellow*.
Bradley Distinguished Professor
Electrical & Computer Engineering
Virginia Tech
thou@vt.edu

Prof. Wenjing Lou, *IEEE Fellow*.
Professor
Computer Science
Virginia Tech
wjlou@vt.edu

B.E. Advisory Members

Prof. Wei Chen.
Professor
Electronic Engineering
Tsinghua University
wchen@tsinghua.edu.cn

Dr. Bo Bai.
Senior Researcher
Future Network Theory Lab
Huawei Technologies Co., Ltd.
ee.bobbai@gmail.com