Fan Zhang

Basic Information

Name: Fan Zhang
Dept. of Computer Science
Cornell University
Ithaca, NY 14850

http://fanzhang.me
fanz@cs.cornell.edu
+1-607-262-0738

Education

Ph.D. Candidate in Computer Science — August 2014–
Advisor: Prof. Ari Juels
Dept. of Computer Science
Cornell University

B.S. in Electronic Engineering — Aug, 2010 – Jul, 2014
Dept. of Electronic Engineering
Tsinghua University, Beijing, China
GPA: 91.1 (out of 100)

Research Interests

I'm interested in systems security and applied cryptography. In particular, my recent projects explore a security model offered by a combination of blockchains and trusted hardware (e.g. Intel SGX).

Working Experience

Researcher intern — Jul, 2017 – Aug, 2017
SPR (Security & Privacy Research), Intel Labs — Hillsboro, OR

- Worked on SGX-based confidential off-chain smart contracts.

System developer intern — Jun, 2013 – May, 2014
Intel Opensource Technology Center (01.org) — Beijing, China

- Contributed to the secure NFC payment component in Tizen OS
- Revamped the CVE scanner for Tizen OS

Professional Activity

- PC Member: The 5th Workshop on Bitcoin and Blockchain Research (BITCOIN'18). In association with Financial Crypto 2018.

Publications

[1] F. Zhang, P. Daian, I. Bentov, and A. Juels, *Paralysis proofs: Safe access-structure updates for cryptocurrencies and more*, Cryptology ePrint Archive, Report 2018/096, 2018.

[2] I. Bentov, Y. Ji, F. Zhang, Y. Li, X. Zhao, L. Breidenbach, P. Daian, and A. Juels, *Tesseract: Real-time cryptocurrency exchange using trusted hardware*, Cryptology ePrint Archive, Report 2017/1153, 2017.

[3] E. Cecchetti, F. Zhang, Y. Ji, A. Kosba, A. Juels, and E. Shi, "Solidus: Confidential distributed ledger transactions via pvorm," in *ACM CCS 2017*, 2017.

[4] F. Zhang, I. Eyal, R. Escriva, A. Juels, and R. van Renesse, "Rem: Resource-efficient mining for blockchains," in *USENIX Security 17*, 2017.

[5] F. Tramer, F. Zhang, H. Lin, J.-P. Hubaux, A. Juels, and E. Shi, "Sealed-glass proofs: Using transparent enclaves to prove and sell knowledge," in *EuroS&P'17*, 2017.

[6] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *ACM CCS'16*, ser. CCS '16, Vienna, Austria: ACM, 2016, pp. 270–282, ISBN: 978-1-4503-4139-4. DOI: 10.1145/2976749.2978326.

[7] F. Tramer, F. Zhang, A. Juels, M. Reiter, and T. Ristenpart, "Stealing machine learning models via prediction APIs," in *USENIX Security'16*, Austin, TX: USENIX Association, 2016.

[8] L. Yang, Y. Cui, F. Zhang, J. P. Pollak, S. Belongie, and D. Estrin, "Plateclick: Bootstrapping food preferences through an adaptive visual interface," in *Proceedings of the 24th ACM International on Conference on Information and Knowledge Management*, ACM, 2015, pp. 183–192.

Invited Talks

Paralysis Proof

- 5th Bitcoin Workshop, Financial Crypto'18, Curacao. March 2nd, 2018

REM

- USENIX Security'17, Vancouver BC, Canada. August, 2017

Town Crier

- Silicon Valley Ethereum Meetup, Santa Clara, CA. August, 2017
- IC3 Retreat, San Francisco, CA. March, 2017
- CCS'16, Vienna, Austria. October, 2016
- IC3 Retreat, New York City. May, 2016

Software Artifacts

[1] Town Crier: an Authenticated Data Feed For Smart Contracts
`http://github.com/bl4ck5un/Town-Crier`

[2] mbedtls-SGX: a SGX-friendly TLS stack (ported from mbedtls)
`https://github.com/bl4ck5un/mbedtls-SGX`

Teaching Experience

Part-time Teaching Assistant 2015, Fall
CS 5435: Security and Privacy in the Wild

Teaching Assistant 2015, Spring
CS5300: The Architecture of Large-scale Information Systems

Teaching Assistant 2014, Fall
CS4410: Operating Systems

Honors and Awards

IBM PhD Fellowship Award 2018

Academic Excellence Scholarship 2013
from Tsinghua University

National Scholarship 2012
from the Ministry of Education of China

Freshman Scholarship 2010
from Tsinghua University