Shweta Shinde

Assistant Professor
ETH Zurich

CONTACT INFORMATION

CAB F 71.2
Universitatstrasse 6,
8092 Zurich

Web: https://shwetashinde.org
E-mail: shweta.shivajishinde@inf.ethz.ch
Citation Profile: [Google Scholar]

RESEARCH INTERESTS

System Security, Programming Languages, Formal Verification

EDUCATION

National University of Singapore, Singapore
Ph.D., Computer Science, 08/2013 - 12/2018

College of Engineering Pune (COEP), University of Pune, India
B.Tech., Information Technology, 08/2008 - 05/2012

PEER-REVIEWED PUBLICATIONS

1. BESFS: A POSIX Filesystem for Enclaves with A Mechanized Safety Proof.
Shweta Shinde*, Shengyi Wang*, Pinghai Yuan, Aquinas Hobor, Abhik Roychoudhury, and Prateek Saxena.
Proceedings of the *29th USENIX Security Symposium (***USENIX***), August 2020.*
2. KEYSTONE: An Open Framework for Architecting TEEs.
Dayeol Lee, David Kohlbrenner, **Shweta Shinde**, Krste Asanovic, and Dawn Song.
Proceedings of the *15th European Conference on Computer Systems (***EuroSys***), April 2020.*
3. Quantitative Verification of Neural Networks And its Security Applications.
Teodora Baluta, Shiqi Shen, **Shweta Shinde**, Kuldeep S. Meel, and Prateek Saxena.
Proceedings of the *26th ACM Conference on Computer and Communications Security (***CCS***), November 2019.*
4. Practical Verifiable In-network Filtering for DDoS defense.
Deli Gong, Muoi Tran, **Shweta Shinde**, Hao Jin, Vyas Sekar, Prateek Saxena, and Min Suk Kang.
Proceedings of the *39th IEEE International Conference on Distributed Computing Systems (***ICDCS***), July 2019.*
5. Neuro-Symbolic Execution: Augmenting Symbolic Execution with Neural Constraints.
Shiqi Shen, **Shweta Shinde**, Changze Cui, Soundarya Ramesh, Prateek Saxena, and Abhik Roychoudhury.
Proceedings of the *26th Annual Network and Distributed System Security Symposium (***NDSS***), February 2019.*
6. Panoply: Low-TCB Linux Applications with SGX Enclaves.
Shweta Shinde, Dat Le Tien, Shruti Tople, and Prateek Saxena.
Proceedings of the *24th Annual Network and Distributed System Security Symposium (***NDSS***), March 2017.*
7. Preventing Page Faults from Telling your Secrets.
Shweta Shinde, Zheng Leong Chua, Viswesh Narayanan, and Prateek Saxena.
Proceedings of the *11th ACM Asia Conference on Computer and Communications Security (***ASIACCS***), June 2016.*
8. Data-Oriented Programming: On the Expressiveness of Non-Control Data Attacks.
Hong Hu, **Shweta Shinde**, Sendroiu Adrian, Zheng Leong Chua, Prateek Saxena, and Zhenkai Liang.
Proceedings of the *36th IEEE Symposium on Security and Privacy (***S&P***), May 2016.*

9. Auto-patching DOM-Based XSS At Scale.
Inian Parameshwaran, Enrico Budianto, **Shweta Shinde**, Hung Dang, Atul Sadhu, and Prateek Saxena.
Proceedings of the *10th ACM SIGSOFT Symposium on the Foundations of Software Engineering (***FSE***), August 2015.*

10. A Model Counter for Constraints Over Unbounded Strings.
Loi Luu, **Shweta Shinde**, Prateek Saxena and Brian Demsky.
Proceedings of the *35th Annual ACM SIGPLAN Conference on Programming Language Design and Implementation (**PLDI**), June 2014.*

11. AutoCrypt: Enabling Homomorphic Computation on Servers To Protect Sensitive Web Content.
Shruti Tople, **Shweta Shinde**, Zhaofeng Chen, and Prateek Saxena.
Proceedings of the *20th ACM Conference on Computer and Communications Security* **(CCS)**, *October 2013.*

Technical Reports

12. Elasticlave: An Efficient Memory Model for Enclaves
Zhijingcheng Yu, **Shweta Shinde**, Trevor E. Carlson, Prateek Saxena.
arXiv 2020.

13. Binary Compatibility For SGX Enclaves
Shweta Shinde, Jinhua Cui, Satyaki Sen, Pinghai Yuan, Prateek Saxena
arXiv 2020.

14. Privado: Practical and Secure DNN Inference with Enclaves.
Karan Grover, Shruti Tople, **Shweta Shinde**, Ranjita Bhagwan, and Ramachandran Ramjee.
arXiv 2019.

15. PodArch: Protecting Legacy Applications with a Purely Hardware TCB.
Shweta Shinde, Shruti Tople, Deepak Kathayat, and Prateek Saxena.
Tech Report. February 2015.

MISC

16. DexterJS: Robust Testing Platform for DOM-based XSS Vulnerabilities.
Inian Parameshwaran, Enrico Budianto, **Shweta Shinde**, Hung Dang, Atul Sadhu, and Prateek Saxena.
Proceedings of the *10th ACM SIGSOFT Symposium on the Foundations of Software Engineering (***FSE***), August 2015.*

17. Poster: PodArch: Protecting Legacy Applications with a Purely Hardware TCB.
Shweta Shinde, Shruti Tople, Deepak Kathayat, and Prateek Saxena.
*35th IEEE Symposium on Security and Privacy (**S&P**), May 2015.*

Grants

- **Keystone: An Open Framework for Architecting TEEs ($100,000)**
Funded by Berkeley Center for Long-Term Cybersecurity
With David Kohlbrenner and Dawn Song

Professional Activities

Reviewer
- PriSC 2021
- ICISS 2019, 2020
- IEEE TIFS
- IEEE Security & Privacy Magazine

Sub-reviewer
- USENIX Security Symposium 2013

- USENIX Security Symposium 2014
- IEEE Symposium on Security & Privacy 2014
- IEEE Symposium on Security & Privacy 2015
- IEEE Symposium on Security & Privacy 2016

Program Chair/Co-Chair
- ASIACCS-SBC 2021

Organizer
- Open-Source Enclaves Workshop (OSEW 2019), Berkeley

Teaching Experience

- Lecturer, 252-2603-00L Seminar on Systems Security, Spring 2021
- Lecturer, 263-0009-00L Information Security Lab, Autum 2020
- Teaching Assistant, CS5331 Web Security, Spring 2014
- Guest Lecture, CS5331 Web Security, Spring 2015, Injection Flaws: Mime Attacks
- Guest Lecture, CS3235 System Security, Spring 2018, Preserving Computation Integrity in Cloud with Trusted Computing
- Guest Lecture, CS4257 Algorithmic Foundations of Privacy, Spring 2018, Cloud Security & Privacy with Trusted Computing

Honors and Awards

Dean's Graduate Research Excellence Award, 2017-18
President Graduate Fellowship, National University of Singapore, 2013-17
Professional Activities Grant, ACM SIGPLAN, 2014
Postgraduate Travel Grant, National University of Singapore, 2014-17

Professional Experience

Assistant Professor, ETH Zurich	10/2020 - Present
Postdoctoral Scholar, University of California Berkeley	01/2019 - 04/2020
Research Assistant, National University of Singapore	09/2017 - 12/2018
Graduate Intern Technical, Intel Labs, Hillsboro	06/2017 - 08/2017
Research Intern, National University of Singapore	08/2012 - 08/2013
Research Intern, India Storage Lab, IBM Corporation	01/2012 - 05/2012
Undergraduate Intern, Cummins India Limited	06/2011 - 08/2011

Talks

- A Model Counter for Constraints Over Unbounded Strings
  ACM International Symposium on Programming Language Design and Implementation (PLDI), Edinburgh UK, 2014
- Protecting Legacy Applications with a Purely Hardware TCB
  Google PhD Student Summit on Web Application Security, Munich Germany, 2016
- Preventing Page Faults from Telling your Secrets
  ACM Asia Conference on Computer and Communications Security (ASIACCS), Xi'an China, 2016
- Wallets and the parable of lost coin
  Advanced Hands-on Workshop on Blockchain: Technology, Applications, Challenges, Hyderabad India, 2017
- Proof of elapsed time with Intel Sawtooth Lake
  Advanced Hands-on Workshop on Blockchain: Technology, Applications, Challenges, Hyderabad India, 2017
- Panoply: Low-TCB Linux Applications With SGX Enclaves
  Network & Distributed System Security Symposium (NDSS), San Diego USA, 2017
- Panoply: Low-TCB Linux Applications with SGX Enclaves
  Intel Labs, Hillsboro USA, 2017

- Privado: Practical and Secure DNN Inference with Enclaves
  Intel Corporation, Folsom USA, 2019
- Towards End-to-end TEE Verification with Keystone
  Open-Source Enclaves Workshop, Berkeley USA, 2019
- Keystone: An Open Framework for Architecting TEEs
  SRI International, Stanford USA, 2019
- BesFS: A POSIX Filesystem for Enclaves with A Mechanized Safety Proof.
  USENIX Security Symposium (USENIX), 2020
- Dancing in the Land of Academic Job Search.
  Computing Research Week, National University of Singapore, 2020
- Better Foundations for Secure Software: Minimize Trust and Verify It
  Duke University, February 2020
  University of California San Diego, March 2020
  Columbia University, March 2020
  Georgia Institute of Technology, March 2020
  University of Michigan Ann Arbor, March 2020
  ETH Zurich, March 2020
  University of Waterloo, March 2020
  Harvard University, March 2020
  Princeton University, March 2020
  University of Maryland, College Park, April 2020
  Penn State University, April 2020
  Rice University, April 2020
  Carnegie Mellon University, April 2020
  University of Texas Austin, April 2020
  Anjuna Security, July 2020
  Futurewei Technologies, September 2020
  Zurich Information Security and Privacy Center, November 2020