Prateek Saxena

Dean's Chair Assistant Professor,
COM2-03-40, 13 Computing Drive
Computer Science Department, School of Computing
National University of Singapore

Phone: +65-6601-1898
E-mail: prateeks@comp.nus.edu.sg
Citation Profile: [Google Scholar]
Web: www.comp.nus.edu.sg/~prateeks/

RESEARCH INTERESTS

Computer Security

EDUCATION

- Ph.D., **University of California, Berkeley, CA, USA**
  Computer Science, 2007 – 2012
- M.S., **Stony Brook University, NY, USA**
  Computer Science, 2005 – 2007
- B.E., **University of Pune, India**,
  Computer Engineering, 2000 – 2004.

PUBLICATIONS

1. Shweta Shinde, Dat Tien Le, Shruti Tople, and Prateek Saxena. Panoply: Low-TCB Linux Applications With SGX Enclaves. To appeat at 24^{th} *Network and Distributed System Security Symposium (**NDSS**), Feb 2017.*
2. Shiqi Shen, Shruti Tople, and Prateek Saxena AUROR: Defending Against Poisoning Attacks in Collaborative Deep Learning Systems. In the Proceedings of the 32^{nd} *Annual Computer Security Applications Conference (**ACSAC**), Dec 2016.*
3. Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, Aquinas Hobor. Making Smart Contracts Smarter. In the Proceedings of the 23^{rd} *ACM Conference on Computer and Communications Security (**CCS**), Oct 2016.*
   *** See discussion on Reddit, and deployment in the Ethereum codebase.**
4. Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, Prateek Saxena. A Secure Sharding Protocol For Open Blockchains. In the Proceedings of the 23^{rd} *ACM Conference on Computer and Communications Security (**CCS**), Oct 2016.*
   *** Commercialized and Deployed at an (undisclosed) financial institution in Aug 2016**
5. Yaoqi Jia, Zheng Leong Chua, Hong Hu, Shuo Chen, Prateek Saxena, Zhenkai Liang. The Web/Local Boundary Is Fuzzy — A Security Study of Chromes Process-based Sandboxing. In the Proceedings of the 23^{rd} *ACM Conference on Computer and Communications Security (**CCS**), Oct 2016.*
6. Yaoqi Jia, Guangdong Bai, Prateek Saxena, and Zhenkai Liang. Anonymity in Peer-assisted CDNs: Inference Attacks and Mitigation. In the Proceedings of the *Privacy Enhancing Technologies (**PETS**), Aug 2016.*
7. Yaoqi Jia, Tarik Moataz, Shruti Tople, and Prateek Saxena. OblivP2P: An Oblivious Peer-to-Peer Content Sharing System. In the Proceedings of the 25^{th} *Usenix Security Symposium (**Usenix Security**), Aug 2016.*
8. Hong Hu, Shweta Shinde, Sendroiu Adrian, Zheng Leong Chua, Prateek Saxena, and Zhenkai Liang. Data-Oriented Programming: On the Expressiveness of Non-Control Data Attacks. In the Proceedings of the 37^{th} *IEEE Symposium on Security and Privacy (**Oakland**), May 2016.*
9. Shweta Shinde, Zheng Leong Chua, Viswesh Narayanan, and Prateek Saxena. Preventing Page Faults from Telling your Secrets. In the Proceedings of the 11^{th} *ACM Asia Conference on Computer and Communications Security (**AsiaCCS**), May 2016.*
10. Jason Teutsch, Sanjay Jain and Prateek Saxena. When Cryptocurrencies Mine Their Own Business. In the Proceedings of the 20^{th} *Financial Cryptography and Data Security (**FC**), Feb 2016.*
11. Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba,

Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gun Sirer, Dawn Song, and Roger Wattenhofer. On Scaling Decentralized Blockchains (A Position Paper). In the Proceedings of the 3^{rd} *Workshop on Bitcoin Research (**BITCOIN**), 2016*.

12. Loi Luu, Jason Teutsch, Raghav Kulkarni, and Prateek Saxena. Demystifying Incentives in the Consensus Computer. In the Proceedings of the 22^{nd} *ACM Conference on Computer and Communications Security (**CCS**) 2015*.
13. Pratik Soni, Enrico Budianto, and Prateek Saxena. The SICILIAN Defense: Signature-based Whitelisting of Web JavaScript. In the Proceedings of the 22^{nd} *ACM Conference on Computer and Communications Security (**CCS**) 2015*.
14. Hong Hu, Zheng Leong Chua, Zhenkai Liang, and Prateek Saxena. Identifying Arbitrary Memory Access Vulnerabilities in Privilege-Separated Software. In the Proceedings of the 20^{th} *European Symposium on Research in Computer Security (**ESORICS**), Sep 2015*.
15. Behnaz Hassanshahi, Yaoqi Jia, Roland Yap, Prateek Saxena, and Zhenkai Liang. Web-to-Application Injection Attacks on Android: Characterization and Detection. In the Proceedings of the 20^{th} *European Symposium on Research in Computer Security (**ESORICS**), Sep 2015*.
16. Yaoqi Jia, Yue Chen, Xinshu Dong, Prateek Saxena, Jian Mao, and Zhenkai Liang. Man-in-the-Browser-Cache: Persisting HTTPS Attacks via Browser Cache Poisoning In the Proceedings of *Journal of Computers and Security (**JCS**), 2015*.
17. Hong Hu, Zheng Leong Chua, Sendroiu Adrian, Prateek Saxena, and Zhenkai Liang. Automatic Generation of Data-Oriented Exploits. In the Proceedings of the 24^{rd} *Usenix Security Symposium (**Usenix Security**), Aug 2015*.
18. Anh Dinh, Prateek Saxena, Chang Ee-chien, Chungwang Zhang, and Beng Chin Ooi. M2R: Enabling Stronger Privacy in MapReduce Computation. In the Proceedings of the 24^{rd} *Usenix Security Symposium (**Usenix Security**), Aug 2015*.
19. Inian Parameshwaran, Enrico Budianto, Shweta Shinde, Hung Dang, Atul Sadhu, and Prateek Saxena. Auto-Patching DOM-based XSS At Scale. In the Proceedings of the *Foundations of Software Engineering (**FSE**), 2014*.
20. Loi Luu, Ratul Saha, Inian Parameshwaran, *Prateek Saxena*, Aquinas Hobor. On Power Splitting Games in Distributed Computation: The Case of Bitcoin Pooled Mining. To Appear at the 28^{th} *IEEE Computer Security Foundations Symposium (**CSF**), July 2015*.
21. Mattia Fazzini, *Prateek Saxena*, and Alessandro Orso. AUTOCSP: Automatically Retrofitting CSP to Web Applications. In the Proceedings of the 37^{th} *International Conference on Software Engineering (**ICSE**), May 2015*.
22. Stevens Le Blond, Adina Uritesc, Cedric Gilbert, Zheng Leong Chua, *Prateek Saxena*, and Engin Kirda. A Look at Targeted Attacks Through the Lense of an NGO. In the Proceedings of the 23^{rd} *Usenix Security Symposium (**Usenix Security**), Aug 2014*.
23. Enrico Budianto, Yaoqi Jia, Xinshu Dong, *Prateek Saxena*, and Zhenkai Liang. You Can't Be Me: Enabling Trusted Paths & User Sub-Origins in Web Browsers. In the Proceedings of the 17^{th} *Symposium on Research in Attacks, Intrusions and Defenses (**RAID**), Sep 2014*.
24. Loi Luu, Shweta Shinde, *Prateek Saxena* and Brian Demsky. A Model Counter for Constraints Over Unbounde Strings. In the Proceedings of the 35^{th} *International Symposium on Programming Language Design and Implementation (**PLDI**), June 2014*.
25. Yaoqi Jia, Xinshu Dong, Zhenkai Liang and *Prateek Saxena*. I Know Where You've Been: Geo-Inference Attacks via the Browser Cache In the Proceedings of the *Web 2.0 Security and Privacy 2014 (**W2SP**), May 2014)*
    Journal version: In IEEE *Internet Computing*, Jan 2015.
26. Xiaolei Li, Hong Hu, Guangdong Bai, Yaoqi Jia, Zhenkai Liang, and *Prateek Saxena*. DroidVault: A Trusted Data Vault for Android Devices. In the Proceedings of the 19^{th}

*Intl. Conference on Engineering of Complex Computer Systems (**ICECCS**), May 2014.*

27. Shruti Tople, Shweta Shinde, Zhaofeng Chen, and *Prateek Saxena*. AUTOCRYPT: Enabling Homomorphic Computation on Servers To Protect Sensitive Web Content. In the Proceedings of the 20^{th} *ACM Conference on Computer and Communications Security (**CCS**), Oct 2013.*
28. Xinshu Dong, Zhaofeng Chen, Hossein Siadati, Shruti Tople, *Prateek Saxena*, and Zhenkai Liang. Protecting Sensitive Web Content from Client-side Vulnerabilities with CRYPTONS. In the Proceedings of the 20^{th} *ACM Conference on Computer and Communications Security (**CCS**), Oct 2013.*
29. Akshay Narayan and *Prateek Saxena*. The Curse of 140 Characters: Evaluating The Efficacy of SMS Spam Detection on Android. In the Proceedings of the 3^{rd} ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (**SPSM**), Oct 2013.
30. Xinshu Dong, Hong Hu, *Prateek Saxena*, and Zhenkai Liang. A Quantitative Evaluation of Privilege Separation in Web Browser Designs. In the Proceedings of the 18^{th} *European Symposium on Research in Computer Security (**ESORICS**), Sep 2013.*
31. Devdatta Akhawe, Frank Li, Warren He, *Prateek Saxena*, Dawn Song. Data-confined HTML5 Applications. In the Proceedings of the 18^{th} *European Symposium on Research in Computer Security (**ESORICS**), Sep 2013.*
32. Guangdong Bai, Jike Lei, Guozhu Meng, Sai Sathyanarayan Venkatraman, *Prateek Saxena*, Jun Sun, Yang Liu, and Jin Song Dong. AUTHSCAN: Automatic Extraction of Web Authentication Protocols from Implementations. In the Proceedings of the 20^{th} *Network and Distributed System Security Symposium (**NDSS**), Feb 2013.*
33. Devdatta Akhawe, *Prateek Saxena*, and Dawn Song. Privilege Separation in HTML5 Applications. In the Proceedings of the 21^{st} *Usenix Security Symposium (**Usenix Security**), Aug 2012.*
    *** See Dropbox's deployment of the proposed privilege separation in 2015**
    *** This research influenced the design of Google Store Apps.**
34. Mike Samuel, *Prateek Saxena*, Dawn Song. Context-Sensitive Auto-Sanitization in Web Templating Languages Using Type Qualifiers. In the Proceedings of the 18^{th} *ACM Conference on Computer and Communications Security (**CCS**), Oct 2011.*
    *** Deployed in the Google Closure compiler, which protects Google+ and other apps**
35. Pieter Hooimeijer, Ben Livhsits, David Molnar, *Prateek Saxena*, Margus Veanes. (*Authors listed alphabeltically*). Fast and Precise Sanitizer Analysis with BEK. In the Proceedings of the *20th Usenix Security Symposium (**Usenix Security**), Aug 2011.*
    *** Available online at Microsoft Research Rise4Fun Portal**
36. *Prateek Saxena*, David Molnar, Benjamin Livshits. SCRIPTGARD: Automatic Context-Sensitive Sanitization for Large-Scale Legacy Web Applications. In the Proceedings of the 18^{th} *ACM Conference on Computer and Communications Security (**CCS**), Oct 2011.*
37. Joel Weinberger, *Prateek Saxena*, Devdatta Akhawe, Matthew Finifter, Richard Shin, Dawn Song. A Systematic Analysis of XSS Sanitization in Web Application Frameworks. In Proceedings of *European Symposium on Research in Computer Security (**ESORICS**), Sep 2011.*
38. *Prateek Saxena*, Devdatta Akhawe, Steve Hanna, Stephen McCamant, Feng Mao, Dawn Song. A Symbolic Execution Framework for JavaScript. In Proceedings of the 31^{st} *IEEE Symposium on Security and Privacy (**IEEE S&P**), May 2010.*
    *** Awarded the AT&T Award for Best Applied Security Research Paper 2010**
39. *Prateek Saxena*, Steve Hanna, Pongsin Poosankam, Dawn Song. FLAX: Systematic Discovery of Client-side Validation Vulnerabilities in Rich Web Applications. In Proceedings of the *17th Annual Network and Distributed System Security Symposium (**NDSS**), Feb 2010.*
40. Adam Barth, Adrienne Porter Felt, *Prateek Saxena*, and Aaron Boodman. Protecting Browsers

from Extension Vulnerabilities. In Proceedings of the *17th Annual Network and Distributed System Security Symposium (**NDSS**), Feb 2010.*
*** Deployed as the Google Chrome Extensions Platform**

41. Steve Hanna, Richard Shin, Devdatta Akhawe, Arman Boehm, *Prateek Saxena*, Dawn Song. The Emperors New APIs: On the (In)Secure Usage of New Client Side Primitives. In Proceedings of the *4th Web 2.0 Security and Privacy Workshop (**W2SP**), Oakland, May 2010.*
42. *Prateek Saxena*, Pongsin Poosankam, Stephen McCamant, Dawn Song. Loop-Extended Symbolic Execution on Binary Programs. In Proceedings of the *18th International Symposium on Software Testing and Analysis (**ISSTA**), Jul 2009.* (Supercedes TR No. UCB/EECS-2009-34, EECS Department UC, Berkeley).
43. Yacin Nadji, *Prateek Saxena*, Dawn Song. Document Structure Integrity: A Robust Basis for Cross-site Scripting Defense. In Proceedings of the *16th Annual Network and Distributed System Security Symposium (**NDSS**), Feb 2009.*
44. Lorenzo Cavallaro, *Prateek Saxena*, R. Sekar. On the Limits of Information Flow Techniques for Malware Analysis and Containment. In Proceedings of the *Detection of Intrusions and Malware & Vulnerability Assessment (**DIMVA**), Jul 2008.*
45. *Prateek Saxena*, R. Sekar, Varun Puranik. Efficient fine-grained binary instrumentation with applications to taint-tracking. In Proceedings of the *International Symposium on Code Generation and Optimization (**CGO**), Apr 2008.*
46. Dawn Song, David Brumley, Heng Yin, Juan Caballero, Ivan Jager, Min Gyung Kang, Zhenkai Liang, James Newsome, Pongsin Poosankam, *Prateek Saxena*. BITBLAZE: A New Approach to Computer Security via Binary Analysis. In Proceedings of the *International Conference on Information Systems Security (*Invited paper) (**ICISS**), Dec 2008.*

PATENTS

- ELASTICO: A Secure Sharding-Based Architecture For Open Blockchains.
  Loi Luu, Prateek Saxena, Seth Gilbert. Filed in September 2016.
- Trusted Data Service.
  Tien Tuan Anh Dinh, Prateek Saxena, Ee-Chien CHANG, Beng Chin OOI, Chunwang ZHANG. Filed in March 2015.
- SCRIPTGARD: Automatic Context-Sensitive Sanitization.
  Filed with David Molnar, Patrice Godefroid, Benjamin Livshits, Microsoft Research. Filed in Dec 2010.
- BEK: String Operations with Transducers
  Filed with David Molnar, Benjamin Livshits, Pieter Hooimeijer, Margus Veanes, Microsoft Research. Filed in Dec 2010. Renewed in 2015.

RESEARCH PROJECTS

- WEBINSPECT: A Security Architecture for Web Applications with Auditability Guarantees, MOE-Singapore (PI)
- Privicols: Practical Protocols for Private Computation, MOE-Singapore (PI)
- A Fast and Secure Web Platform, Intel University Grant (PI) for 2015 and renewed in 2016.
- New Trusted Computing Primitives, Symantec Research Grant (PI)
- TSUNAMi: Trustworthy Systems from UN-trusted component AMalgamations, NRF-Singapore (Co-PI)

STARTUPS

- Co-founded **Anquan Capital** in Sep 2015, to provide high-security blockchain infrastructure to financial services.
- Technical Advisor to **Dexecure**, a *Y-Combinator Fellowship* company co-founded in Oct 2015, to enable fast and self-optimizing web applications.

PROFESSIONAL SERVICE

- Served on the Program Committee for Usenix Security (2013,2014,2015), IEEE Symposium on Security & Privacy (2014, 2015, 2016)

- Invited Talks: TRUST Seminar at UC Berkeley (Fall 2011), Google (Summer 2011), Mozilla (Summer 2011), Intel (2014), Symantec (2015).

Awards & Fellowships

- Received the David J. Sakrison Memorial Award for *outstanding doctoral research* from the EECS Department, UC Berkeley, 2012.
- Dean's Chair Assistant Professor Title at NUS (2012 – 2015, renewed for 2015 – 2018)
- Best Paper Awards at W2SP 2014, ICECCS 2014.
- Symantec Research Lab Graduate Fellowship & Winner of Intern Project Competition, 2011.
- AT&T Best Applied Security Research Paper Award, 2010.
- Multiple India-level awards for senior year project – LIZARD: GDB-Replay Debugger (2004)

Professional Experience

- **Assistant Professor** July 2012 - Present
  National University of Singapore.
- **Visiting Researcher** May 2015 - July 2015
  Microsoft Research, Redmond, US.
- **Graduate Student Researcher** Aug 2007 - June 2012
  University of California, Berkeley, CA, USA.
- **Research Intern** July 2011 - Aug 2011
  Symantec Research Labs, Mountain View, CA, USA.
- **Research Intern** Jun 2010 - Aug 2010
  Microsoft Research, Redmond, WA, USA.
- **Research Assistant** Aug 2005 - Jul 2007
  Stony Brook University, NY, USA.
- **Software Developer** Jul 2004 - Jul 2005
  GNU Tools group, Codito Technologies, India.