Prateek Saxena

Associate Professor
Computer Science Department, School of Computing
National University of Singapore
COM3-02-03, 11 Research Link, Singapore 119391

Phone: +65-66011898
Citation Profile: [Google Scholar]
Web: www.comp.nus.edu.sg/~prateeks/
E-mail: prateeks@comp.nus.edu.sg

Employment

- Associate Professor, **National University of Singapore**
  Computer Science Department, 2019 –
- Assistant Professor, **National University of Singapore**
  Computer Science Department, 2012 – 2019

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.

Awards & Fellowships

- Google Security and Privacy Researcher Award, 2018.
- MIT TR35 Top 10 Innovators Under 35, Asia, 2017.
- NUS Young Researcher Award, 2017.
- David J. Sakrison Memorial Award for *doctoral research work* at EECS, UC Berkeley, 2012.
- Best Paper Awards at ACM ASIACCS 2021, 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 national awards for senior year project – LIZARD: GDB-Replay Debugger, 2004

Professional Service

- Award selection committee for Caspar Bowden Awards for Outstanding Research in Privacy Enhancing Technologies (PET Award), 2024
- Area Chair for "ML Security" for the Program Committee of ACM CCS 2020 and 2021.
- Program Committee for Usenix Security (2013-2015, 2017, 2019).
- Program Committee of IEEE Symposium on Security & Privacy (2014-2016, 2018, 2020).

Primary PhD Thesis Advisor

- (2024) Aashish Kolluri (*Research Postdoc*, Microsoft Research, UK)
- (2024) Teodora Baluta (*Assistant Professor*, Georgia Tech, USA)
- (2021) Shiqi Shen (*Researcher*, Huawei Research, China)
- (2018) Shweta Shinde (*Assistant Professor*, ETH Zurich, Switzerland)
- (2018) Shruti Tople (*Principal Researcher*, Microsoft Research, UK)
- (2017) Loi Luu (*Founder and CEO* - Kyber Networks and Caliber, Singapore)

Research Grants

- A New and Versatile Hardware-Software Interface for Software Security.
  Funded by MOE - Singapore (Sole PI 2025-)
- Security via Programming Language Lifting.
  Funded by Cisco University Research Program Fund, USA (Sole PI 2023-2024)
- CRYSTAL: Cryptocurrency, Security, Tools, and Algorithms—University Center at NUS.
  Funded by multiple industrial research grants. (Director & Lead PI 2018-now)
- TSUNAMi: Trustworthy Systems from UN-trusted component AMalgamations.
  Funded by NRF-Singapore (Co-PI, 2017-2021)
- A Hybrid Approach to Automatic Programming.
  Funded by MOE - Singapore (Sole PI, 2020-2024)
- Algorithmic Advances For Program Fuzzing.
  Funded by MOE - Singapore (Sole PI, 2021-2024)
- Deep Learning for Binary Reverse Engineering.
  Funded by DSO National Labs, Singapore (Sole PI, 2017-2021)
- WEBINSPECT: A Security Architecture for Web Applications with Auditability Guarantees.
  Funded by NUS ODPRT (Sole PI, 2012-2015)
- Privicols: Practical Protocols for Private Computation.

Funded by MOE - Singapore (Sole PI, 2014-2017)

- A Fast and Secure Web Platform.
  Funded by Intel University Grant (Sole PI, 2015 and 2016)
- New Trusted Computing Primitives.
  Funded by Symantec Research Grant (Sole PI, 2013)

RESEARCH PUBLICATIONS (H-INDEX: 47) (CITATIONS:17K+)

1. De Zhang Lee, Aashish Kolluri, Prateek Saxena, Ee-Chien Chang.
   A Practical and Secure Byzantine Robust Aggregator.
   To Appear at the *ACM Conference on Computer and Communications Security (**CCS**), 2025*
2. Jason Zhijingcheng Yu*, Fangqi Han*, Kaustab Choudhury, Trevor E. Carlson, Prateek Saxena.
   Securing Mixed Rust with Hardware Capabilities.
   To Appear at the *ACM Conference on Computer and Communications Security (**CCS**), 2025*
3. Jason Zhijingcheng Yu, Mingkai Li, Trevor E. Carlson, Michael Swift, Prateek Saxena.
   Caplification: Bridging Capability-Aware and Capability-Oblivious Software.
   In Proceedings of *ACM Symposium on Access Control Models and Technologies (**SACMAT**), 2025*
4. Bo Wang*, Tianyu Li*, Ruishi Li, Umang Mathur, and Prateek Saxena.
   Program Skeletons for Automated Program Translation.
   In Proceedings of *ACM Programming Language Design and Implementation (**PLDI**), 2025*
5. Ruishi Li, Bo Wang, Tianyu Li, Prateek Saxena, and Ashish Kundu.
   Translating C To Rust: Lessons from a User Study.
   In Proceedings of the *Network and Distributed System Security Symposium (**NDSS**), 2025*
6. Sarthak Choudhary, Aashish Kolluri, and Prateek Saxena.
   Attacking Byzantine Robust Aggregation in High Dimensions.
   In Proceedings of the *IEEE Symposium on Security and Privacy (**IEEE S&P**), 2024*.
7. Bo Wang, Ruishi Li, Mingkai Li, and Prateek Saxena.
   TransMap: Pinpointing Mistakes in Neural Code Translation.
   In Proceedings of the *ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (**FSE**), 2023*.
8. Teodora Baluta, Ivica Nikolic, Racchit Jain, Divesh Aggarwal, and Prateek Saxena.
   Unforgeability in Stochastic Gradient Descent.
   In Proceedings of the *ACM Conference on Computer and Communications Security (**CCS**), 2023*.
9. Bo Wang, Aashish Kolluri, Ivica Nikolic, Teodora Baluta, and Prateek Saxena.
   User-customizable Transpilation for Scripting Languages.
   In Proceedings of the *ACM SIGPLAN Conference on Object-Oriented Programming Systems, Languages, and Applications (**OOPSLA**), Oct 2023.*
10. Jason Zhijingcheng Yu, Conrad Watt, Aditya Badole, Trevor Carlson, and Prateek Saxena.
    CAPSTONE: A Capability-based Foundation for Trustless Secure Memory Access.
    In Proceedings of the 32^{nd} *Usenix Security Symposium (**Usenix Security**), Aug 2023*.
11. Jinhua Cui, Shweta Shinde, Satyaki Sen, Prateek Saxena, and Pinghai Yuan.
    Dynamic Binary Translation for SGX Enclaves.
    In Proceedings of the *ACM Transactions on Privacy and Security (**TOPS 2022**)*.
12. Aashish Kolluri, Teodora Baluta, Bryan Hooi, and Prateek Saxena.
    LPGNet: Link Private Graph Networks for Node Classification.
    In Proceedings of the *ACM Conference on Computer and Communications Security (**CCS**), 2022*.
13. Teodora Baluta, Shiqi Shen, S. Hitarth, Shruti Tople, and Prateek Saxena.
    Membership Inference Attacks and Generalization: A Causal Perspective.
    In Proceedings of the *ACM Conference on Computer and Communications Security (**CCS**), 2022*.
14. Kaihang Ji, Jun Zeng, Yuancheng Jiang, Zhenkai Liang, Zheng Leong Chua, Prateek Saxena, and Abhik Roychoudhury.
    FlowMatrix: GPU-Assisted Information-Flow Analysis through Matrix-Based Representation.
    In Proceedings of the *Usenix Security Symposium (**Usenix Security**), 2022.*

15. Jason Zhijingcheng Yu, Shweta Shinde, Trevor Carlson, and Prateek Saxena.
ELASTICLAVE: An Efficient Memory Model for Enclaves.
In Proceedings of the *Usenix Security Symposium (**Usenix Security**), 2022*.

16. Ruomu Hou, Haifeng Yu, and Prateek Saxena.
Using Throughput-Centric Byzantine Broadcast to Tolerate Malicious Majority in Blockchains.
In Proceedings of the *IEEE Symposium on Security and Privacy (**IEEE S&P**), 2022*.

17. Jinhua Cui, Jason Zhijingcheng Yu, Shweta Shinde, Prateek Saxena, and Zhiping Cai.
SmashEx: Smashing SGX Enclaves Using Exceptions.
In Proceedings of the *ACM Conference on Computer and Communications Security (**CCS**), 2021*.

18. Aashish Kolluri, Teodora Baluta, and Prateek Saxena.
Private Hierarchical Clustering in Federated Networks.
In Proceedings of the *ACM Conference on Computer and Communications Security (**CCS**), 2021*.

19. Teodora Baluta, Zheng Leong Chua, Kuldeep S. Meel, and Prateek Saxena.
Scalable Quantitative Verification For Deep Neural Networks.
In Proceedings of the *International Conference on Software Engineering (**ICSE**), 2021*.

20. Bo Wang, Teodora Baluta, Aashish Kolluri, and Prateek Saxena. SynGuar: Guaranteeing Generalization in Programming by Example. In Proceedings of the *ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (**ESEC/FSE**), 2021*.

21. Ivica Nikolic, Radu Mantu, Shiqi Shen, and Prateek Saxena.
Refined Grey-Box Fuzzing with SIVO.
In Proceedings of *Detection of Intrusions and Malware & Vulnerability Assessment (**DIMVA**), 2021*.

22. Shiqi Shen, Aashish Kolluri, Zhen Dong, Prateek Saxena, and Abhik Roychoudhury.
Localizing Vulnerabilities Statistically From One Exploit.
In Proceedings of the *ACM Asia Conference on Computer and Communications Security (**AsiaCCS**), 2021*.

23. Yaoqi Jia, Shruti Tople, Tarik Moataz, Deli Gong, Prateek Saxena, and Zhenkai Liang.
Robust P2P Primitives Using SGX Enclaves.
In Proceedings of the *International Symposium on Research in Attacks, Intrusions and Defenses (**RAID**), 2020*.

24. Shweta Shinde, Shengyi Wang, Pinghai Yuan, Aquinas Hobor, Abhik Roychoudhury, Prateek Saxena.
BesFS: A POSIX Filesystem for Enclaves with a Mechanized Safety Proof.
In Proceedings of the *Usenix Security Symposium (**Usenix Security**), 2020*.

25. Haifeng Yu, Ivica Nikolic, Ruomu Hou, Prateek Saxena.
OHIE: Blockchain Scaling Made Simple.
In Proceedings of the *IEEE Symposium on Security and Privacy (**Oakland**), 2020*.

26. Quantitative Verification of Neural Networks and Its Security Applications.
Teodora Baluta, Shiqi Shen, Shweta Shinde, Kuldeep S. Meel, Prateek Saxena.
In Proceedings of the *ACM Conference on Computer and Communications Security (**CCS**), 2019*.

27. Aashish Kolluri, Ivica Nikolic, Ilya Sergey, Aquinas Hobor, Prateek Saxena.
Exploiting the laws of order in smart contracts.
In Proceedings of the *ACM SIGSOFT International Symposium on Software Testing and Analysis (**ISSTA**), 2019*.

28. Deli Gong, Muoi Tran, Shweta Shinde, Hao Jin, Vyas Sekar, Prateek Saxena, Min Suk Kang.
Practical Verifiable In-network Filtering for DDoS defense.
In Proceedings of the *IEEE International Conference on Distributed Computing Systems (**ICDCS**), 2019*.

29. Shiqi Shen, Shweta Shinde, Soundarya Ramesh, Abhik Roychoudhury, Prateek Saxena.
Neuro-Symbolic Execution: Augmenting Symbolic Execution with Neural Constraints.
In Proceedings of the *Network and Distributed System Security Symposium (**NDSS**), 2019*.

30. One Engine To Serve'em All: Inferring Taint Rules Without Architectural Semantics.

Zheng Leong Chua, Yanhao Wang, Teodora Baluta, Prateek Saxena, Zhenkai Liang, Purui Su.
In Proceedings of the *Network and Distributed System Security Symposium (**NDSS**), 2019*.

31. Shruti Tople, Soyeon Park, Min Suk Kang, and Prateek Saxena.
VeriCount: Verifiable Resource Accounting Using Hardware and Software Isolation.
In Proceedings of the *International Conference on Applied Cryptography and Network Security (**ACNS**), 2018*.

32. Muoi Tran, Loi Luu, Min Suk Kang, Iddo Bentov, Prateek Saxena.
Obscuro: A bitcoin mixer using trusted execution environments.
In Proceedings of the *Annual Computer Security Applications Conference (**ACSAC**), 2018*.

33. Ivica Nikolic, Aashish Kolluri, Ilya Sergey, Prateek Saxena, Aquinas Hobor.
Finding the greedy, prodigal, and suicidal contracts at scale.
In Proceedings of the *Annual Computer Security Applications Conference (**ACSAC**)*, 2018.

34. Ruomu Hou, Irvan Jahja, Loi Luu, Prateek Saxena, and Haifeng Yu.
Randomized View Reconciliation in Permissionless Distributed Systems.
In Proceedings of the *IEEE International Conference on Computer Communications (**INFOCOM**), 2018*.

35. Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena.
A Traceability Analysis of Monero's Blockchain.
In Proceedings of the *European Symposium on Research in Computer Security (**ESORICS**), 2017*.

36. Sourav Das, Aashish Kolluri, Prateek Saxena, Haifeng Yu.
On the Security of Blockchain Consensus Protocols.
In Proceedings of the *International Conference on Information Systems Security (**ICISS**), 2018. (*Invited paper)*

37. Loi Luu, Yaron Velner, Jason Teutsch and Prateek Saxena.
SmartPool: Practical Decentralized Pooled Mining.
In Proceedings of the *Usenix Security Symposium (**Usenix Security**), Aug 2017*.
*** See project at the SmartPool web page**

38. Zheng Leong Chua, Shiqi Shen, Prateek Saxena, Zhenkai Liang.
Neural Nets Can Learn Function Type Signatures From Binaries.
In Proceedings of the *Usenix Security Symposium (**Usenix Security**), Aug 2017*.

39. Shruti Tople and Prateek Saxena.
On the Trade-Offs in Oblivious Execution Techniques.
In Proceedings of the *Detection of Intrusions and Malware & Vulnerability Assessment (**DIMVA**), July 2017*.

40. Shweta Shinde, Dat Tien Le, Shruti Tople, and Prateek Saxena.
Panoply: Low-TCB Linux Applications With SGX Enclaves.
In Proceedings of the *Network and Distributed System Security Symposium (**NDSS**), 2017*.

41. Shiqi Shen, Shruti Tople, and Prateek Saxena.
AUROR: Defending Against Poisoning Attacks in Collaborative Deep Learning Systems.
In Proceedings of the *Annual Computer Security Applications Conference (**ACSAC**), 2016*.

42. Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, Aquinas Hobor.
Making Smart Contracts Smarter.
In Proceedings of the *ACM Conference on Computer and Communications Security (**CCS**), 2016*.
*** See discussion on Reddit, and open-source release.**

43. Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, Prateek Saxena.
A Secure Sharding Protocol For Open Blockchains.
In Proceedings of the *ACM Conference on Computer and Communications Security (**CCS**), 2016*.
*** Deployed at the Zilliqa public blockchain**

44. Yaoqi Jia, Zheng Leong Chua, Hong Hu, Shuo Chen, Prateek Saxena, Zhenkai Liang.
The Web/Local Boundary Is Fuzzy — A Security Study of Chrome's Process-based Sandboxing.

In Proceedings of the *ACM Conference on Computer and Communications Security (**CCS**), 2016*.

45. Yaoqi Jia, Guangdong Bai, Prateek Saxena, and Zhenkai Liang.
Anonymity in Peer-assisted CDNs: Inference Attacks and Mitigation.
In Proceedings of the *Privacy Enhancing Technologies (**PETS**), 2016*.

46. Yaoqi Jia, Tarik Moataz, Shruti Tople, and Prateek Saxena.
OblivP2P: An Oblivious Peer-to-Peer Content Sharing System.
In Proceedings of the *Usenix Security Symposium (**Usenix Security**), 2016*.

47. Hong Hu, Shweta Shinde, Sendroiu Adrian, Zheng Leong Chua, Prateek Saxena, Zhenkai Liang.
Data-Oriented Programming: On the Expressiveness of Non-Control Data Attacks.
In Proceedings of the *IEEE Symposium on Security and Privacy (**IEEE S&P**), 2016*.

48. Shweta Shinde, Zheng Leong Chua, Viswesh Narayanan, and Prateek Saxena.
Preventing Page Faults from Telling your Secrets.
In Proceedings of *ACM Asia Conference on Computer & Communications Security (**AsiaCCS**), 2016*.

49. Jason Teutsch, Sanjay Jain and Prateek Saxena.
When Cryptocurrencies Mine Their Own Business.
In Proceedings of the *Financial Cryptography and Data Security (**FC**), 2016*.

50. 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 Proceedings of the *Workshop on Bitcoin Research (**BITCOIN**), 2016*.

51. Loi Luu, Jason Teutsch, Raghav Kulkarni, and Prateek Saxena.
Demystifying Incentives in the Consensus Computer.
In Proceedings of the *ACM Conference on Computer and Communications Security (**CCS**) 2015*.

52. Pratik Soni, Enrico Budianto, and Prateek Saxena.
The SICILIAN Defense: Signature-based Whitelisting of Web JavaScript.
In Proceedings of the *ACM Conference on Computer and Communications Security (**CCS**) 2015*.

53. Hong Hu, Zheng Leong Chua, Zhenkai Liang, and Prateek Saxena.
Identifying Arbitrary Memory Access Vulnerabilities in Privilege-Separated Software.
In Proceedings of the *European Symposium on Research in Computer Security (**ESORICS**), 2015*.

54. Behnaz Hassanshahi, Yaoqi Jia, Roland Yap, Prateek Saxena, and Zhenkai Liang.
Web-to-Application Injection Attacks on Android: Characterization and Detection.
In Proceedings of the *European Symposium on Research in Computer Security (**ESORICS**), 2015*.

55. 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 Proceedings of *Journal of Computers and Security (**JCS**), 2015*.

56. Hong Hu, Zheng Leong Chua, Sendroiu Adrian, Prateek Saxena, and Zhenkai Liang.
Automatic Generation of Data-Oriented Exploits.
In Proceedings of the *Usenix Security Symposium (**Usenix Security**), 2015*.

57. Anh Dinh, Prateek Saxena, Chang Ee-chien, Chungwang Zhang, and Beng Chin Ooi.
M2R: Enabling Stronger Privacy in MapReduce Computation.
In Proceedings of the 24^{rd} *Usenix Security Symposium (**Usenix Security**), 2015*.

58. Inian Parameshwaran, Enrico Budianto, Shweta Shinde, Hung Dang, Atul Sadhu, Prateek Saxena.
Auto-Patching DOM-based XSS At Scale.
In Proceedings of the *Foundations of Software Engineering (**FSE**), 2014*.

59. Loi Luu, Ratul Saha, Inian Parameshwaran, Prateek Saxena, Aquinas Hobor.
On Power Splitting Games in Distributed Computation: The Case of Bitcoin Pooled Mining.
In Proceedings of the *IEEE Computer Security Foundations Symposium (**CSF**), 2015*.

60. Mattia Fazzini, Prateek Saxena, and Alessandro Orso.
AUTOCSP: Automatically Retrofitting CSP to Web Applications.

In Proceedings of the *International Conference on Software Engineering (**ICSE**), 2015*.

61. Stevens Le Blond, Adina Uritesc, Cedric Gilbert, Zheng Leong Chua, Prateek Saxena, Engin Kirda.
A Look at Targeted Attacks Through the Lense of an NGO.
In Proceedings of the *Usenix Security Symposium (**Usenix Security**), 2014*.

62. 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 Proceedings of the *Symposium on Research in Attacks, Intrusions and Defenses (**RAID**), 2014*.

63. Loi Luu, Shweta Shinde, Prateek Saxena, and Brian Demsky.
A Model Counter for Constraints Over Unbounde Strings.
In Proceedings of the *International Symposium on Programming Language Design and Implementation (**PLDI**), 2014*.

64. Yaoqi Jia, Xinshu Dong, Zhenkai Liang and Prateek Saxena.
I Know Where You've Been: Geo-Inference Attacks via the Browser Cache.
In Proceedings of the *Web 2.0 Security and Privacy 2014 (**W2SP**), 2014*
Journal version: In IEEE *Internet Computing*, Jan 2015.

65. Xiaolei Li, Hong Hu, Guangdong Bai, Yaoqi Jia, Zhenkai Liang, and Prateek Saxena.
DroidVault: A Trusted Data Vault for Android Devices.
In Proceedings of *Intl. Conference on Engineering of Complex Computer Systems (**ICECCS**), 2014*.

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

67. Xinshu Dong, Zhaofeng Chen, Hossein Siadati, Shruti Tople, Prateek Saxena, and Zhenkai Liang.
Protecting Sensitive Web Content from Client-side Vulnerabilities with CRYPTONS.
In Proceedings of the *ACM Conference on Computer and Communications Security (**CCS**), 2013*.

68. Akshay Narayan and Prateek Saxena.
The Curse of 140 Characters: Evaluating The Efficacy of SMS Spam Detection on Android.
In Proceedings of the ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (**SPSM**), 2013.

69. Xinshu Dong, Hong Hu, Prateek Saxena, and Zhenkai Liang.
A Quantitative Evaluation of Privilege Separation in Web Browser Designs.
In Proceedings of the *European Symposium on Research in Computer Security (**ESORICS**), 2013*.

70. Devdatta Akhawe, Frank Li, Warren He, Prateek Saxena, Dawn Song.
Data-confined HTML5 Applications.
In Proceedings of the *European Symposium on Research in Computer Security (**ESORICS**), 2013*.

71. 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 Proceedings of the *Network and Distributed System Security Symposium (**NDSS**), 2013*.

72. Devdatta Akhawe, Prateek Saxena, and Dawn Song.
Privilege Separation in HTML5 Applications.
In Proceedings of the *Usenix Security Symposium (**Usenix Security**), 2012*.
*** See Dropbox's deployment of the proposed privilege separation in 2015**
*** This research influenced the design of Google Store Apps.**

73. Mike Samuel, Prateek Saxena, Dawn Song.
Context-Sensitive Auto-Sanitization in Web Templating Languages Using Type Qualifiers.
In Proceedings of the *ACM Conference on Computer and Communications Security (**CCS**), 2011*.
*** Deployed in the Google Closure compiler, which protects Google+ and other apps**

74. Pieter Hooimeijer, Ben Livhsits, David Molnar, Prateek Saxena, Margus Veanes.
Fast and Precise Sanitizer Analysis with BEK.
In Proceedings of the *20th Usenix Security Symposium (**Usenix Security**), Aug 2011*.

*** Available online at Microsoft Research Rise4Fun Portal**

75. Prateek Saxena, David Molnar, Benjamin Livshits.
SCRIPTGARD: Automatic Context-Sensitive Sanitization for Large-Scale Legacy Web Applications.
In Proceedings of the *ACM Conference on Computer and Communications Security (**CCS**), 2011.*

76. 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 the *European Symposium on Research in Computer Security (**ESORICS**), 2011.*

77. Prateek Saxena, Devdatta Akhawe, Steve Hanna, Stephen McCamant, Feng Mao, Dawn Song.
A Symbolic Execution Framework for JavaScript.
In Proceedings of the *IEEE Symposium on Security and Privacy (**IEEE S&P**), 2010.*
*** Awarded the AT&T Award for Best Applied Security Research Paper 2010**

78. Prateek Saxena, Steve Hanna, Pongsin Poosankam, Dawn Song.
FLAX: Systematic Discovery of Client-side Validation Vulnerabilities in Rich Web Applications.
In Proceedings of the *Annual Network and Distributed System Security Symposium (**NDSS**), 2010.*

79. Adam Barth, Adrienne Porter Felt, Prateek Saxena, and Aaron Boodman.
Protecting Browsers from Extension Vulnerabilities.
In Proceedings of the *Annual Network and Distributed System Security Symposium (**NDSS**), 2010.*
*** Deployed as the Google Chrome Extensions Platform**

80. 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.*

81. 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**), 2009.* (Supercedes TR No. UCB/EECS-2009-34, EECS Department UC, Berkeley).

82. Yacin Nadji, Prateek Saxena, Dawn Song.
Document Structure Integrity: A Robust Basis for Cross-site Scripting Defense.
In Proceedings of the *Annual Network and Distributed System Security Symposium (**NDSS**), 2009.*

83. Lorenzo Cavallaro, Prateek Saxena, R. Sekar.
On the Limits of Information Flow Techniques for Malware Analysis and Containment.
In Proceedings of *Detection of Intrusions and Malware & Vulnerability Assessment (**DIMVA**), 2008.*

84. 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**), 2008.*

85. 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. (* Invited paper)
In Proceedings of the *International Conference on Information Systems Security (**ICISS**), 2008*