Suman Jana

CONTACT INFORMATION

412 Mudd
Department of Computer Science
Columbia University
New York, NY 10027 USA

Voice: (212) 853-0933
Fax: (212)-666-0140
E-mail: suman@cs.columbia.edu
WWW: www.sumanj.info

RESEARCH INTERESTS

My primary research interest is in the area of computer security and privacy. More specifically, I am interested in building automated tools for detecting and fixing security and privacy vulnerabilities in large systems. I often use techniques from diverse domains like machine learning, software engineering, and operating systems, for my research.

RESEARCH & WORK EXP.

Columbia University, New York City, NY USA
Assistant Professor **Jan 2016 - Current**

Stanford University, Stanford, CA USA
Postdoctoral Researcher **Sep 2014 - Sep 2015**

Google, Mountain View, CA USA
Research Intern **Jun 2013 - Aug 2013**

Microsoft Research, Redmond, WA USA
Research Intern **Jun 2012 - Aug 2012**

Bell Laboratories, Murray Hill, NJ USA
Research Intern **Jun 2009 - Aug 2009**

Ixia Comm., **Nevis Networks**, and **Bluestar Infotech**, India
Software Engineer **Jul 2003 - Aug 2007**

EDUCATION

The University of Texas at Austin, Austin, TX USA
Department of Computer Science
Ph.D., Aug 2009 - Aug 2014

- Dissertation Topic: *Security and Privacy in Perceptual Computing*
- Advisor: Vitaly Shmatikov

University of Utah, Salt Lake City, UT USA
Department of Computer Science
M.S., Aug 2007 - Aug 2009

- Dissertation Topic: *On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews*
- Advisor: Sneha Kasera

Jadavpur University, Calcutta, India
Department of Computer Science and Engineering
B.E., Aug 1999 - May 2003

Conference Publications

1. Dongdong Shi, Kexin Pei, Dave Epstein, Junfeng Yang, Baishakhi Ray, and **Suman Jana**. *NEUZZ: Efficient Fuzzing with Neural Program Smoothing.* In Proceedings of the 40th IEEE Symposium on Security and Privacy (**Oakland**), San Jose, CA, 2019
2. Mathias Lecuyer, Vaggelis Atlidakis, Roxana Geambasu, Daniel Hsu, and Suman Jana. *Certified Robustness to Adversarial Examples with Differential Privacy.* In Proceedings of the 40th IEEE Symposium on Security and Privacy (**Oakland**), San Jose, CA, 2019
3. Shiqi Wang, Kexin Pei, Justin Whitehouse, Junfeng Yang, and **Suman Jana**. *Efficient Formal Safety Analysis of Neural Networks.* In the Thirty-second Annual Conference on Neural Information Processing Systems (NIPS), Montreal, Canada, 2018.
4. Shankara Pailoor, Andrew Aday, and **Suman Jana**. *MoonShine: Optimizing OS Fuzzer Seed Selection with Trace Distillation.* In the 27th USENIX Security Symposium (USENIX Security), Baltimore, MD, 2018. **3rd place in NYU CSAW Security Competition.**
5. Shiqi Wang, Kexin Pei, Justin Whitehouse, Junfeng Yang, and **Suman Jana**. *Formal Security Analysis of Neural Networks using Symbolic Intervals.* In the 27th USENIX Security Symposium (USENIX Security), Baltimore, MD, 2018.
6. Yuchi Tian, Kexin Pei, **Suman Jana**, and Baishakhi Ray. *DeepTest: Automated Testing of Deep-Neural-Network-driven Autonomous Cars.* In the 40th International Conference On Software Engineering (ICSE), Gothenburg, Sweden, 2018.
7. Kexin Pei, Yinzhi Cao, Junfeng Yang, and **Suman Jana**. *DeepXplore: Automated Whitebox Testing of Deep Learning Systems.* In the Twenty-Sixth Symposium on Operating Systems Principles (SOSP), Shanghai, China, 2017. **Best Paper Award. CACM Research Highlight.**
8. Theofilos Petsios, Jason Zhao, Angelos D. Keromytis, and **Suman Jana**. *SlowFuzz: Automated Domain-Independent Detection of Algorithmic Complexity Vulnerabilities.* In the 24th ACM Conference on Computer and Communications Security (CCS), Dallas, TX, 2017.
9. Theofilos Petsios, Adrian Tang, Salvatore Stolfo, Angelos D. Keromytis, and **Suman Jana**. *NEZHA: Efficient Domain-independent Differential Testing.* In Proceedings of the 38th IEEE Symposium on Security and Privacy (**Oakland**), San Jose, CA, 2017.
10. Suphannee Sivakorn, George Argyros, Kexin Pei, Angelos D. Keromytis, **Suman Jana**. *HVLearn: Automated Black-box Analysis of Hostname Verification in SSL/TLS Implementations.* In Proceedings of the 38th IEEE Symposium on Security and Privacy (**Oakland**), San Jose, CA, 2017.
11. George Argyros, Ioannis Stais, **Suman Jana**, Angelos D. Keromytis, and Aggelos Kiayias. *SFADiff: Automated Evasion Attacks and Fingerprinting Using Blackbox Differential Automata Learning.* In Proceedings of the 23rd ACM Conference on Computer and Communications Security (**CCS**), Vienna, Austria, 2016
12. Yuan J. Kang, Baishakhi Ray, and **Suman Jana**. *APEx: Automated Inference of Error Specifications for C APIs.* In 31st IEEE/ACM International Conference on Automated Software Engineering (**ASE**), Singapore, 2016.
13. **Suman Jana**, Yuan J. Kang, Samuel Roth, and Baishakhi Ray. *Automatically Detecting Error Handling Bugs using Error Specifications.*In Proceedings of the 25th USENIX Security Symposium (**USENIX Security**), Austin, TX, 2016.
14. Richard McPherson, **Suman Jana**, and Vitaly Shmatikov. *No Escape From Reality: Security and Privacy of Augmented Reality Browsers.* In Proceedings of the 24th International World Wide Web Conference (**WWW**), Florence, Italy, 2015.
15. Martin Georgiev, **Suman Jana**, and Vitaly Shmatikov. *Rethinking Security of Web-Based System Applications.* In Proceedings of the 24th International World Wide Web Conference (**WWW**), Florence, Italy, 2015.
16. David Silver, **Suman Jana**, Eric Chen, Collin Jackson, and Dan Boneh. *Password Managers: Attacks and Defenses.* In Proceedings of the 23rd USENIX Security Symposium (**USENIX Security**), San Diego, CA, 2014.

17. Chad Brubaker, **Suman Jana**, Baishakhi Ray, Sarfraz Khurshid, and Vitaly Shmatikov. *Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations.* In Proceedings of the 35th IEEE Symposium on Security and Privacy (**Oakland**), San Jose, CA, 2014. **Best Practical Paper Award.**
18. Martin Georgiev, **Suman Jana**, and Vitaly Shmatikov. *Breaking and Fixing Origin-Based Access Control in Hybrid Web/Mobile Application Frameworks.* In Proceedings of the 21st Annual Network & Distributed System Security Symposium (**NDSS**), San Diego, CA, 2014.
19. **Suman Jana**, David Molnar, Alexander Moshchuk, Alan Dunn, Benjamin Livshits, Helen J. Wang, and Eyal Ofek. *Enabling Fine-Grained Permissions for Augmented Reality Applications With Recognizers.* In Proceedings of the 22nd USENIX Security Symposium (**USENIX Security**), Washington DC, 2013.
20. **Suman Jana**, Arvind Narayanan, and Vitaly Shmatikov. *A Scanner Darkly: Protecting User Privacy from Perceptual Applications.* In Proceedings of the 34th IEEE Symposium on Security and Privacy (**Oakland**), San Francisco, CA, 2013. **PET Award Winner.**
21. **Suman Jana** and Vitaly Shmatikov. *Memento: Learning Secrets from Process Footprints.* In Proceedings of the 33rd IEEE Symposium on Security and Privacy (**Oakland**), Berkeley, CA, 2012. **Best Student Paper Award.**
22. **Suman Jana** and Vitaly Shmatikov. *Abusing File Processing in Malware Detectors for Fun and Profit.* In Proceedings of the 33rd IEEE Symposium on Security and Privacy (**Oakland**), Berkeley, CA, 2012.
23. Martin Georgiev, Subodh Iyengar, **Suman Jana**, Rishita Anubhai, Dan Boneh, and Vitaly Shmatikov. *The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software.* In Proceedings of the 19th ACM Conference on Computer and Communications Security (**CCS**), Raleigh, NC, 2012. **AT&T Best Applied Security Paper Award.**
24. Alan M. Dunn, Michael Z. Lee, **Suman Jana**, Sangman Kim, Mark Silberstein, Yuanzhong Xu, Vitaly Shmatikov, and Emmett Witchel. *Eternal Sunshine of the Spotless Machine: Protecting Privacy with Ephemeral Channels.* In Proceedings of the 10th USENIX Symposium on Operating System Design and Implementation (**OSDI**), Hollywood, CA, 2012. **PET Award Runner-Up.**
25. Yigal Bejerano, **Suman Jana**, Pramod V Koppol. *Efficient construction of directed Redundant Steiner trees.* The 37th IEEE Conference on Local Computer Networks (**LCN**), Clearwater, FL, 2012.
26. **Suman Jana**, Donald E. Porter, and Vitaly Shmatikov. *TxBox: Building Secure, Efficient Sandboxes with System Transactions.* In Proceedings of the 32nd IEEE Symposium on Security and Privacy (**Oakland**), Berkeley, CA, 2011.
27. **Suman Jana**, Sriram N. Premnath, Mike Clark, Sneha K. Kasera, Neal Patwari, and Srikanth V. Krishnamurthy. *On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments.* In Proceedings of the 15th ACM Annual International Conference on Mobile Computing and Networking (**MobiCom**), Beijing, China, 2009.
28. **Suman Jana** and Sneha K. Kasera. *On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews.* In Proceedings of the 14th ACM Annual International Conference on Mobile Computing and Networking (**MobiCom**), San Francisco, CA, 2008.

Selected Workshop Publications

29. Henry Corrigan-Gibbs and **Suman Jana**. *Recommendations for Randomness in the Operating System or, How to Keep Evil Children out of Your Pool and Other Random Facts.* In Proceedings of the 15th Workshop on Hot Topics in Operating Systems (**HotOS**), Kartause Ittingen, Switzerland, May, 2015.
30. Loris D'Antoni, Alan Dunn, **Suman Jana**, Tadayoshi Kohno, Benjamin Livshits, David Molnar, Alexander Moshchuk, Eyal Ofek, Franziska Roesner, Scott Saponas, Margus Veanes, and Helen J.

Wang. *Operating System Support for Augmented Reality Applications.* In Proceedings of the 14th Workshop on Hot Topics in Operating Systems (**HotOS**), Santa Ana Pueblo, NM, May, 2013.

31. **Suman Jana** and Vitaly Shmatikov. *EVE: Verifying Correct Execution of Cloud-Hosted Web Applications.* In Proceedings of the 3rd USENIX Workshop on Hot Topics in Cloud Computing (**HotCloud**), Portland, OR, June, 2011.

Journal Publications

32. Sriram N Premnath, **Suman Jana**, Jessica Croft, Prarthana L. Gowda, Mike Clark, Sneha K. Kasera, and Neal Patwari. *Secret key extraction from wireless signal strength in real environments.* In IEEE Transactions on Mobile Computing 12 (5): 917-930.
33. Neal Patwari, Jessica Croft, **Suman Jana**, and Sneha K. Kasera. *High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements.* In IEEE Transactions on Mobile Computing 9 (1):17-30.
34. **Suman Jana** and Sneha K. Kasera. *On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews.* In IEEE Transactions on Mobile Computing 9 (3):449 - 462.

Patents

35. Loris D'antoni, Alan M Dunn, **Suman Jana**, Tadayoshi Kohno, Benjamin Livshits, David A Molnar, Alexander N Moshchuk, Eyal Ofek, Franziska Roesner, Timothy Scott Saponas, Margus Veanes, and Helen Wang. *Managing Access by Applications to Perceptual Information.* US Patent Application 14/020,708.
36. Neal Patwari, Jessica Croft, **Suman Jana**, and Sneha K. Kasera. *Method and System for Secret Key Exchange Using Wireless Link Characteristics and Random Device Movement.* US Patent 20,110,280,397.
37. **Suman Jana** and Sneha K. Kasera. *Method and system for detecting unauthorized wireless access points using clock skews.* WO Patent WO/2010/030,950.

Research Grants

- Co-Principal Investigator for NSF, "EAGER: Finding Semantic Security Bugs with Pseudo-Oracle Testing,"$200,000, 2018-2020.
- Principal Investigator for J. P. Morgan Faculty Fellowship, $150,000, 2019-2020.
- Principal Investigator for ARO Young Investigator Program (YIP), "Building Efficient Fuzzers using Automata Learning,"$360,000, 2018-2020.
- Principal Investigator for NSF, "Towards Trustworthy Deep Neural Network Based AI: A Systems Approach," $1,200,000, 2018-2021. Lead PI: Siddharth Garg (NYU), Co-PI: Brendan Dolan-Gavitt (NYU), Anna Choromanska (NYU).
- Principal Investigator for Google Faculty Fellowship, $62,618, 2017.
- Principal Investigator for ONR, "BUDDY: TCB Hardening for Cyber Physical Systems," $2,571,137, 2017-2019. Co-PI: Simha Sethumadhavan and Sal Stolfo.
- Principal Investigator for NSF TWC, "Automated Detection and Repair of Error Handling Bugs in SSL/TLS Implementations," $500,000 2016-2019. Co-PI: Baishakhi Ray (University of Virginia).

Teaching

- Formal Logic, Security, And Machine Learning (COMS 6998), Spring 2019.
- Security I (COMS W4187), Fall 2018.
- Security Architecture & Engineering (COMS W4187), Fall 2017.
- Secure Software Development: Theory and Practice (COMS W4995), Spring 2017.
- Advanced Topics in Network Security (COMS E6183), Spring 2016.

Advising and Mentoring

PhD advisor

- Kexin Pei, Columbia University(Co-advised with Junfeng Yang).
- Shiqi Wang, Columbia University.
- Dongdong She, Columbia University.
- Dennis Rohlke, Columbia University (Co-advised with Roxana Geambasu).
- Gabriel Ryan, Columbia University (Co-advised with Sal Stolfo).

PhD thesis committee member

- George Argyros, Columbia University.
- Ghada Almashaqbeh, Columbia University.
- Preetam Dutta, Columbia University.
- Guliz Tuncay, University of Illinois at Urbana-Champaign.
- Fang-Hsiang (Mike) Su, Columbia University.
- Gang Hu, Columbia University.
- Suphannee Sivakorn, Columbia University.
- Adrian Tang, Columbia University.
- Georgios Kontaxis, Columbia University.
- Theofilos Petsios, Columbia University.
- Yuan Jochen Kang, Columbia University.
- Kanad Sinha, Columbia University.

PhD qualifying examination committee member

- Vaggelis Atlidakis, Columbia University
- Miguel Aroyo, Columbia University
- David Williams-King, Columbia University
- Suphannee Sivakorn, Columbia University
- Ihimu Uzoma Ukpo, Columbia University

Other graduate mentorship

- Eugene Ang, Columbia University.
- Shankara Pailoor, Columbia University.
- Martin Georgiev, University of Texas at Austin.
- Richard McPherson, University of Texas at Austin.
- Chad Brubaker, University of Texas at Austin.
- Benjamin Braun, Stanford University.
- David Silver, Stanford University.

Undergraduate Students

- Rahul Kataria, Columbia University.
- Crystal Ren, Columbia University.
- Dave Epstein, Columbia University.
- Abhishek Shah, Columbia University.

- Ruoxin Jiang, Columbia University (CRA Outstanding Undergraduate Honorable Mention 2017).
- Daniel Schwartz, Columbia University.
- Jason Zhao, Columbia University.
- Justin Whitehouse, Columbia University. (CRA Outstanding Undergraduate Honorable Mention 2019 & NSF Graduate Research Fellowship 2019).
- Joshua M. Zweig, Columbia University.
- John Hui, Columbia University.

Research Impact

Our work on systemic testing and verification of popular machine learning models like neural networks

Our automata-learning-based differential testing framework (`https://github.com/lightbulb-framework/lightbulb-framework`) [3] for Web Application Firewalls (WAFs) have been starred more than 343 times in GitHub.

Our research has uncovered more than **250** high-impact security and privacy vulnerabilities across a wide range of products.

NoFrak [10] has been incorporated in Apache Cordova (https://issues.apache.org/jira/browse/CB-5988).

Techniques from frankencerts [9] have been integrated into Mozilla, Samsung, and Google's testing infrastructure.

My research has been cited more than **2790** times according to Google Scholar.

Media Coverage

Most Dangerous Code in the World. [15]
Ars Technica, Threatpost, Hacker News, Slashdot, Schneier, Reddit, LWN.net, The H, SC Magazine, Softpedia, Heise, it republik.

Frankencerts. [9]
Reddit, Golem, Heise.

Password Managers: Attacks and Defenses. [8]
Schneier, Reddit, Mac Performance Guide, Learning Tree

A Scanner Darkly. [12]
Freedom to Tinker, VPN Creative.

Memento. [13]
CACM, Mocana.

Honors and Awards

Research Awards

- CACM Research Highlight, 2019.
- ARO Young Investigator Award, 2018.
- J. P. Morgan Faculty Fellowship, 2019.
- NYU-Poly CSAW Applied Research Competition, 2012(1st), 2017(2nd), 2018(2nd and 3rd).
- Google Faculty Fellowship, 2017.
- SOSP Best Paper Award, 2017.
- PET Award for Outstanding Research in Privacy Enhancing Technologies [12], 2014.

- IEEE Security & Privacy Symposium Best Practical Paper Award [9], 2014.
- Runner-up for the PET Award for Outstanding Research in Privacy Enhancing Technologies [16], 2013.
- IEEE Security & Privacy Symposium Best Student Paper Award [13], 2012.

Graduate Research Fellowships

- Google U.S./Canada Fellowship in Security, 2012-2014.
- Microelectronics and Computer Development (MCD) Fellowship from the University of Texas at Austin, 2009-2012.

Professional Services

Program Committee

- The 23rd International Symposium on Formal Methods (**FM**), 2019.
- ICML Workshop on the Security and Privacy of Machine Learning, 2019.
- Workshop on Formal methods for ML-enabled autonomous systems (FoMLAS), 2019.
- the third workshop on Machine Learning Technique for Software Quality Evaluation (MaLTeSQuE), 2019.
- 27th USENIX Security Symposium (**USENIX Sec**), 2018.
- ACM Asia Conference on Computer and Communications Security (**AsiaCCS**), 2018.
- Second International Workshop on The Bright and Dark Sides of Computer Vision: Challenges and Opportunities for Privacy and Security (**CV-COPS**), 2018.
- 26th USENIX Security Symposium (**USENIX Sec**), 2017.
- ACM Conference on Computer and Communications Security (**CCS**), 2017.
- 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (**WiSec**), 2017.
- ACM Asia Conference on Computer and Communications Security (**AsiaCCS**), 2017.
- First International Workshop on The Bright and Dark Sides of Computer Vision: Challenges and Opportunities for Privacy and Security (**CV-COPS**), 2017.
- 24th International World Wide Web Conference (**WWW**) Security and Privacy Track, 2016.
- 4th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (**SPSM**), 2015.
- 24th International World Wide Web Conference (**WWW**) Security and Privacy Track, 2015.
- 4th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (**SPSM**), 2014.
- Workshop on Privacy in the Electronic Society (**WPES**), 2014.

Invited Talks

Scalable Training of Verifiably Robust Neural Networks. Keynote at Verified Neural NetworksWorkshop (VNN). Stanford University, March 2019.

Security Testing and Verification of Machine Learning Systems. Center for Resilient Infrastructures, Systems, and Processes (CRISP) Conference Purdue University, March 2019.

Security Testing and Verification of Machine Learning Systems. Systems Seminar, Princeton University, Nov 2018.

Systematic Testing and Verification of Deep Learning Systems. Keynote at Dependable and Secure Machine Learning (DSML) Workshop, Luxembourg, Jun 2018.

Automated Systematic Testing of Deep Learning Systems. Special Session in Design Automation Conference (DAC), San Francisco, Jun 2018.

Security and Safety challenges in Deep Learning for Autonomous Driving. AutoSens Conference, Detroit, May 2018.

How to Build Safe and Secure Machine Learning Systems?. Google, New York, April, 2018.

How to Build Safe and Secure Machine Learning Systems?. IBM Research, Yorktown Heights, Dec 2017.

Security & privacy in a hyper-connected world. Data Science Day, Data Science Institute (DSI), Columbia University, April 2017.

Securing software systems: beyond whack-a-mole. Data Science Institute's (DSI) Colloquium Series, Columbia University, March, 2017.

SSL/TLS Certificate Validation: Problems and Solutions. University of California, Davis, CA, July 2014.

SSL/TLS Certificate Validation: Problems and Solutions. SRI International, Menlo Park, CA, June 2014.

Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations. Google, Mountain View, CA, May 2014.

Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations. Microsoft Research Silicon Valley, Mountain View, CA, May 2014.

Password Managers: Risks, Pitfalls, and Improvements. Stanford Security Workshop. Stanford, CA, April 2014.

Password Managers: Risks, Pitfalls, and Improvements. Berkeley-Stanford Security Meetup. Stanford, CA, April 2014.

Enabling Fine-Grained Permissions for Augmented Reality Applications With Recognizers. Stanford Security Lunch, Stanford, CA, January 2014.

Others

Invited to the ARO Workshop on Adversarial Learning 2017, an invitation-only workshop organized by ARO to bring together researchers working on security aspects of machine learning systems.

Invited to the Workshop on Data Science for Secure and Privacy-aware (DSSP) Large Data Management and Mining 2016, an invitation-only workshop organized by NSF to bring together security and privacy researchers.

Invited to the Google Security and Privacy Research Summit 2017, an invitation-only workshop arranged by Google for bringing together security and privacy researchers.