# Vaibhav Rastogi

**Assistant Scientist**
Computer Sciences, University of Wisconsin-Madison

Office: Computer Sciences 7387 1210 W. Dayton St., Madison, WI 53705
Email: vrastogi@u.northwestern.edu
Web: http://pages.cs.wisc.edu/~vrastogi
Google Scholar: https://scholar.google.com/citations?user=ODCUXBgAAAAJ
DBLP: http://dblp.uni-trier.de/pers/hd/r/Rastogi:Vaibhav

## Research Interests

Security and Privacy, Computer Systems, Mobile Systems, Web

## Appointments

- Senior Software Engineer, Google
  - June 2019 - *Present*
- Assistant Scientist, Computer Sciences, University of Wisconsin-Madison
  - October 2018 - June 2019
- Research Associate, Computer Sciences, University of Wisconsin-Madison
  - August 2015 - August 2018
- Software Engineer, part-time, Tala Security
  - November 2016 - August 2018
- Research Associate, Computer Science and Engineering, Pennsylvania State University
  - August 2015 - July 2016
- Research Assistant, Electrical Engineering and Computer Science, Northwestern University
  - September 2009 - June 2015

## Education

- PhD. in Electrical Engineering and Computer Science, Northwestern University
  - September 2009 - June 2015
  - Advisor: Prof. Yan Chen
  - Dissertation: Towards a Trustworthy Android Ecosystem
  - GPA: 3.973/4.0
- B.Tech. and M.Tech. in Computer Science and Engineering, Indian Institute of Technology Delhi
  - July 2004 - May 2009
  - Advisor: Vinay Ribeiro
  - GPA: B.Tech. - 8.905/10.0; M.Tech. - 9.5/10.0

## Publications

***Peer-reviewed Conferences, Journals, and Workshops***

- J. Chen, X. Wu, V. Rastogi, Y. Liang, and S. Jha, "Towards Understanding Limitations of Pixel Discretization Against Adversarial Attacks," in Proceedings of the 4th IEEE European Symposium on Security and Privacy (EuroS&P), 2019. To appear.
- J. Zhao, A. Albarghouthi, V. Rastogi, S. Jha, and D. Octeau, "Neural-Augmented Static Analysis of Android Communication," in Proceedings of the Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the

Foundations of Software Engineering (ESEC/FSE), 2018.

- R. Shao, V. Rastogi, Y. Chen, X. Pan, G. Guo, S. Zou, and R. Riley, “Understanding In-app Ads and Detecting Hidden Attacks through the Mobile App-Web Interface,” IEEE Transactions on Mobile Computing, vol. 17, no. 11, 2018.
- V. Rastogi, C. Niddodi, S. Mohan, and S. Jha, “New Directions for Container Debloating,” in Proceedings of the 2017 Workshop on Forming an Ecosystem Around Transformation (FEAST), 2017.
- D. Davidson, V. Rastogi, M. Christodorescu, and S. Jha, “Enhancing Android Security through App Splitting,” in Proceedings of the 13th International Conference on Security and Privacy in Communication Networks (SecureComm), 2017.
- V. Rastogi, D. Davidson, L. De Carli, S. Jha, and P. McDaniel, “Cimplifier: Automatically Debloating Containers,” in Proceedings of the 11th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE), 2017.
- S. Alam, Z. Qu, R. Riley, Y. Chen, and V. Rastogi, “DroidNative: Automating and optimizing detection of Android native code malware variants,” Computers & Security, vol. 65, pp. 230–246, 2017.
- Z. Qu, G. Guo, Z. Shao, V. Rastogi, Y. Chen, H. Chen, and W. Hong, “AppShield: Enabling Multi-entity Access Control Cross Platforms for Mobile App Management,” in Proceedings of the 12th International Conference on Security and Privacy in Communication Networks (SecureComm), 2016.
- V. Rastogi, R. Shao, Y. Chen, X. Pan, S. Zou, and R. Riley, “Are These Ads Safe: Detecting Hidden Attacks through the Mobile App-Web Interfaces,” in Proceedings of the Network and Distributed System Security Symposium (NDSS), 2016.
- V. Rastogi, Z. Qu, J. McClurg, Y. Cao, and Y. Chen, “Uranine: Real-time Privacy Leakage Monitoring without System Modification for Android,” in Proceedings of the 11th International Conference on Security and Privacy in Communication Networks (SecureComm), 2015.
- V. Rastogi and A. Agrawal, “All your Google and Facebook logins are belong to us: A case for single sign-off,” in Proceedings of the Eighth International Conference on Contemporary Computing (IC3), 2015, pp. 416–421.
- B. He, V. Rastogi, Y. Cao, Y. Chen, V. N. Venkatakrishnan, R. Yang, and Z. Zhang, “Vetting SSL Usage in Applications with SSLint,” in Proceedings of the 36th IEEE Symposium on Security and Privacy (Oakland), 2015.
- Z. Qu, V. Rastogi, X. Zhang, Y. Chen, T. Zhu, and Z. Chen, “AutoCog: Measuring the Description-to-permission Fidelity in Android Applications,” in Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS), 2014.
- Y. Cao, C. Yang, V. Rastogi, Y. Chen, and G. Gu, “Abusing Browser Address Bar for Fun and Profit - An Empirical Investigation of Add-on Cross Site Scripting Attacks,” in Proceedings of the 10th International Conference on Security and Privacy in Communication Networks (SecureComm), 2014.
- V. Rastogi, Y. Chen, and X. Jiang, “Catch Me If You Can: Evaluating Android Anti-Malware Against Transformation Attacks,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 1, pp. 99–108, 2014.

- V. Rastogi, Y. Chen, and X. Jiang, “DroidChameleon: Evaluating Android Anti-malware Against Transformation Attacks,” in Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security (ASIACCS), 2013, pp. 329–334.
- V. Rastogi, Y. Chen, and W. Enck, “AppsPlayground: Automatic Security Analysis of Smartphone Applications,” in Proceedings of the Third ACM Conference on Data and Application Security and Privacy (CODASPY), 2013, pp. 209–220.
- Y. Cao, V. Rastogi, Z. Li, Y. Chen, and A. Moshchuk, “Redefining Web Browser Principals with a Configurable Origin Policy,” in Dependable Systems and Networks (DSN), 2013 43rd Annual IEEE/IFIP International Conference on, 2013, pp. 1–12.
- Y. Cao, Z. Li, V. Rastogi, Y. Chen, and X. Wen, “Virtual browser: A Virtualized Browser to Sandbox Third-party JavaScripts with Enhanced Security,” in Proceedings of the 7th ACM SIGSAC symposium on Information, computer and communications security (ASIACCS), 2012, pp. 8–9.
- Z. Li, Y. Tang, Y. Cao, V. Rastogi, Y. Chen, B. Liu, and C. Sbisa, “WebShield: Enabling Various Web Defense Techniques without Client Side Modifications,” in Proceedings of the Network and Distributed System Security Symposium (NDSS), 2011.
- V. Rastogi, V. J. Ribeiro, and A. D. Nayar, “Measurements in OLPC Mesh Networks,” in Proceedings of the 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt), 2009, pp. 1–6.

***Non-peer-reviewed and Posters***

- V. Rastogi, “Towards a Trustworthy Android Ecosystem,” PhD thesis, Northwestern University, 2015.
- V. Rastogi, Y. Chen, and X. Jiang, “Evaluating Android Anti-malware Against Transformation Attacks,” Department of Electrical Engineering and Computer Science, Northwestern University, NU-EECS-13-01, 2013.
- Y. Cao, Z. Li, V. Rastogi, and Y. Chen, “Virtual Browser: A Web-level Sandbox to Secure Third-party JavaScript without Sacrificing Functionality,” in Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS), 2010, pp. 654–656. Poster abstract.

## Artifacts

All artifacts here are freely available research purposes.

- *AppsPlayground*: A tool for automatically interacting with and driving Android applications. Please see our CODASPY 2013 paper for details. The version available here was rewritten from scratch for our NDSS 2016 paper. It incorporates largely the same techniques described in the former paper and is able to work with new versions of Android.
- *DroidChameleon*: A tool that incorporates a bunch of transformations on Android applications. The tool was used in our DroidChameleon papers (ASIACCS 2013 and TIFS 2014) to prepare malware variants that evade commercial anti-malware tools. DroidChameleon has also been used by a number of academic and industry researchers to test the effectiveness of their own malware detection schemes.

- *Ad library list*: A list of Android ad libraries discovered as part of the work for our NDSS 2016 paper.

## Patents

- Yan Chen, Zhengyang Qu, and Vaibhav Rastogi, "System and Method for Determining Description-to-permission Fidelity in Mobile Applications", filed on May 13, 2015, awarded on February 12, 2019. U.S. Patent No. 10,204,225. U.S. Patent Application No. 14/711,157.
- Sanjay Sawhney, Swapnil Bhalode, Drew Davidson, Somesh Jha, and Vaibhav Rastogi, "Method for Detecting Malicious Scripts Through Modeling of Script Structure", filed on April 16, 2018. U.S. Patent Application No. 15/953,953.
- Yan Chen, Zhengyang Qu, and Vaibhav Rastogi, "System and Method for Proxy-based Data Access Mechanism in Enterprise Mobility Management", filed on September 14, 2016. U.S. Patent Application No. 15/264,944.
- Yan Chen, Vaibhav Rastogi, Zhengyang Qu, and Jedidiah McClurg, "System and Method for Privacy Leakage Detection and Prevention Without Operating System Modification.", filed on February 5, 2015. U.S. Patent Application No. 14/615,254.

## Press

- Wired UK. Google can't do much about fake Fortnite downloads for Android.
  https://www.wired.co.uk/article/fortnite-on-android-download-apk-malware-scam
- Wall Street Journal. Samsung to Install Antivirus Software in Android Phones.
  http://online.wsj.com/news/articles/SB10001424127887324202304579053412932547056
- ACM Tech News. Android Antiviral Products Easily Evaded, Northwestern Study Says.
  http://technews.acm.org/archives.cfm?fo=2013-06-jun/jun-03-2013.html#657930
- Zee News. Top 10 Android anti-virus useless before 'certain' attacks: Study.
  http://zeenews.india.com/news/science/top-10-android-anti-virus-useless-before-certain-attacks-study_852109.html
- Science Daily. Android antiviral products easily evaded.
  http://www.sciencedaily.com/releases/2013/05/130530132539.htm
- McCormick Northwestern News. Android Antiviral Products Easily Evaded, Northwestern Study Says.
  http://www.mccormick.northwestern.edu/news/articles/2013/05/android-antiviral-products-easily-evaded-northwestern-study-says-yan-chen.html
- VirusFreePhone. Mobile AV Apps Fail To Detect Disguised Malware.
  http://virusfreephone.com/2013/05/mobile-av-apps-fail-to-detect-disguised-malware-23/
- Tech News Daily. Android Anti-Virus Software Easily Fooled.
  http://www.technewsdaily.com/17982-android-antivirus-serious-weakness.html
- EFY Times. Android Virus Scanners Can Be Tricked: Report.
  http://www.efytimes.com/e1/fullnews.asp?edid=105498
- Help Net Security. Top Android AV software fooled by common evasion techniques.
  http://www.net-security.org/secworld.php?id=14862
- ISS Source. Android Virus Scanners Easy to Trick. http://www.isssource.com/android-virus-scanners-easy-to-trick/
- NBC News. Android Anti-Virus Software Easily Fooled.
  http://www.nbcnews.com/id/51809212#.UoPCfcO342w

- heise Security. Android-Virenscanner sind leicht auszutricksen. http://www.heise.de/security/meldung/Android-Virenscanner-sind-leicht-auszutricksen-1855331.html
- The H. Android virus scanners are easily fooled. http://www.h-online.com/security/news/item/Android-virus-scanners-are-easily-fooled-1856133.html
- Slashdot. Popular Android Anti-Virus Software Fooled By Trivial Techniques. http://it.slashdot.org/story/13/05/07/0226229/popular-android-anti-virus-software-fooled-by-trivial-techniques
- Security Week. Anti-Virus Software for Android Fooled by Common Techniques, Researchers Say. http://www.securityweek.com/anti-virus-software-android-fooled-common-techniques-researchers-say
- Information Week. Mobile AV Apps Fail To Detect Disguised Malware. http://www.informationweek.in/security/13-05-05/mobile_av_apps_fail_to_detect_disguised_malware.aspx
- Dark Reading. Mobile AV Apps Fail To Detect Disguised Malware. http://www.darkreading.com/end-user/mobile-av-apps-fail-to-detect-disguised/240153843

**Talks**

- "New Directions for Container Debloating", the 2017 Workshop on Forming an Ecosystem Around Transformation (FEAST), 2017, Dallas, TX.
- "Vetting SSL Usage in Applications with SSLint", invited talk at SRI International, April 2016, Menlo Park, CA.
- "Are These Ads Safe: Detecting Hidden Attacks Through Mobile App-web Interfaces", the 2016 Network and Distributed Systems Security System (NDSS), February 2016, San Diego, CA.
- "Uranine: Real-time Privacy Leakage Monitoring without System Modification for Android", the 11th International Conference on Security and Privacy in Communication Networks (SecureComm), October 2015, Dallas, TX.
- "Towards Trustworthy Operating System Ecosystems", invited talk at Georgia Institute of Technology, April 2015, Atlanta, GA.
- "AppsPlayground: Automatic Security Analysis of Smartphone Applications", the Third ACM Conference on Data and Application Security and Privacy (CODASPY), February 2013, San Antonio, TX.

**Honors and Rewards**

- Confeerence Travel Grant, IEEE Symposium on Security and Privacy (Oakland), 2015.
- Confeerence Travel Grant, ACM Conference on Computer and Communications Security (CCS), 2014.
- Royal E. Cabell Terminal Year Fellowship, 2014-2015, Northwestern University.
- Murphy Fellowship, Winter 2010, Northwestern university.
- Recognized for top GPA in the department for 5 semesters, Indian Institute of Technlogy Delhi.

**Teaching**

Teaching assistant at Northwestern University for:

- EECS 101, An Introduction to Computer Science for Everyone, Fall 2012. Instructor: Jason Hartline.
- EECS 230, Programming for Engineers. Spring 2012. Peter Scheuermann.
- EECS 395/495, Web Information Retrieval and Extraction, Spring 2011. Instructor:

Doug Downey.

- EECS 230, Programming for Engineers. Winter 2011. Goce Trajcevski.
- EECS 348, Introduction to Artificial Intelligence, Spring 2010. Instructor: Doug Downey.

Teaching assistant at Indian Institute of Technology Delhi for:

- CSL 101, Introduction to Computers and Programming, Fall 2008. Instructor: Sandeep Sen.
- CSL 102, Introduction to Computer Science, Spring 2009. Instructor: Saroj Kaushik.

**Professional Service**

Associate Editor:

- IEEE Access 2018 - *Present*

Technical Program Committee Member:

- IEEE CNS 2019 2018 2017
- RAID 2018
- IEEE DSS 2018
- IEEE ICCCN 2019 2018
- EAI SecureComm 2019 2017
- IEEE SmartData 2017

Conference Reviewer:

- NeurIPS 2019
- ICML 2019

Journal Reviewer:

- ACM Computing Surveys
- ACM Transactions on Information and System Security
- Elsevier Computers & Security
- Elsevier Expert Systems With Applications
- Elsevier Information Systems
- Elsevier Journal of Information Security and Applications
- Hindawi Mobile Information Systems
- InderScience International Journal of Business Intelligence and Data Mining
- IEEE Access
- IEEE/ACM Transactions on Networking
- IEEE Transactions on Dependable and Secure Computing
- IEEE Transactions on Information Forensics and Security
- IEEE Transactions on Mobile Computing
- IEEE Transactions on Vehicular Technology
- IET Information Security
- MDPI Applied Sciences
- MDPI Symmetry
- Springer Human-centric Computing and Information Sciences

External Reviewer:

- IEEE ICDM 2017 2016
- ACM CIKM 2017
- ACM/IEEE ICSE 2017

- IEEE BigData 2016
- IEEE WiMob 2016
- DIMVA 2016
- IEEE SMC 2015
- IEEE IPDPS 2015
- ISOC NDSS 2015 2014 2012 2011 2010
- ACM CCS 2015 2014
- IEEE INFOCOM 2014 2013 2012 2011 2010
- IEEE S&P (Oakland) 2013
- ICST SecureComm 2011
- IEEE DSN 2010