Brendan D. Saltaformaggio

Georgia Institute of Technology
School of Electrical and Computer Engineering
Atlanta, GA 30332
(404) 894-8362
brendan@ece.gatech.edu
https://saltaformaggio.ece.gatech.edu

Research Interests

Computer systems security and cyber forensics with focuses on memory forensics, binary analysis and instrumentation, vetting of untrusted software, and cloud computing security.

Current Position

Assistant Professor — July 2017 to Present
Georgia Institute of Technology — Atlanta, GA
School of Electrical and Computer Engineering
School of Computer Science (By Courtesy)

Education

Ph.D. in Computer Science — December 2016
Purdue University — West Lafayette, IN
Dissertation: *Convicted by Memory: Automatically Recovering Spatial-Temporal Evidence from Memory Images*
Advisors: Dr. Dongyan Xu and Dr. Xiangyu Zhang

Master of Science in Computer Science — December 2014
Purdue University — West Lafayette, IN

Bachelor of Science with Honors in Computer Science — May 2012
University of New Orleans — New Orleans, LA
Thesis: *Forensic Carving of Wireless Network Information from the Android Linux Kernel*
Advisor: Dr. Golden G. Richard III
Minor: Mathematics

Honors & Awards

Inaugural Recipient of the Emil Stefanov Memorial Fellowship — 2016
Presented by the Stefanov family in recognition of outstanding contributions in cyber security research

Symantec Research Labs Graduate Fellowship — 2016
$20,000 over 1 year to fund "innovative research that has real-world value" [Link]

Best Paper Award
ACM Conference on Computer and Communications Security (CCS) — 2015

Best Student Paper Award
USENIX Security Symposium (USENIX Security) — 2014

Former Positions

Postdoctoral Researcher — January 2017 to July 2017
Purdue University — West Lafayette, IN
Advisor: Dr. Dongyan Xu

Graduate Research Assistant — August 2012 to December 2016
Purdue University — West Lafayette, IN
Advisors: Dr. Dongyan Xu and Dr. Xiangyu Zhang

Research Intern — May 2016 to August 2016
Symantec Research Labs — Mountain View, CA
Advisors: Mr. Darren Shou (Senior Director of Global Research) and Dr. Susanta Nanda

Research Intern — May 2012 to August 2012
MIT Lincoln Laboratories — Lexington, MA
Advisors: Dr. Robert Cunningham and Mr. Joseph Cooley

Research Assistant — August 2011 to May 2012
Greater New Orleans Center for Information Assurance — New Orleans, LA
at the University of New Orleans (GNOCIA)
Advisor: Dr. Golden G. Richard III

Research Assistant — February 2010 to May 2011
University of New Orleans — New Orleans, LA
Advisor: Dr. Daniel Bilar

Publications

Peer-Reviewed Articles

Y. Kwon, **B. Saltaformaggio**, I. Kim, K. Lee, X. Zhang, D. Xu. A2C: Self Destructing Exploit Executions via Input Perturbation. In *Network and Distributed System Security Symposium (NDSS'17)*, 2017. Acceptance rate: 16%.

K. Pei, Z. Gu, **B. Saltaformaggio**, S. Ma, F. Wang, Z. Zhang, L. Si, X. Zhang, D. Xu. HERCULE: Attack Story Reconstruction via Community Discovery on Correlated Log Graph. In *Annual Computer Security Applications Conference (ACSAC'16)*, 2016. Acceptance rate: 22.8%.

H. Lu, **B. Saltaformaggio**, C. Xu, U. Bellur, D. Xu. BASS: Improving I/O Performance for Cloud Block Storage via Byte-Addressable Storage Stack. In *ACM Symposium on Cloud Computing (SOCC'16)*, 2016. Acceptance rate: 25%.

B. Saltaformaggio, R. Bhatia, X. Zhang, D. Xu, G. Richard III. Screen after Previous Screens: Spatial-Temporal Recreation of Android App Displays from Memory Images. In *USENIX Security Symposium (USENIX Security'16)*, 2016. Acceptance rate: 15.6%.
Invited for TechTalk presentation by Google's Anti-Abuse Research Team.

B. Saltaformaggio, H. Choi, K. Johnson, Y. Kwon, Q. Zhang, X. Zhang, D. Xu, J. Qian. Eavesdropping on Fine-Grained User Activities Within Smartphone Apps Over Encrypted Network Traffic. In *USENIX Workshop on Offensive Technologies (WOOT'16, in conjunction with Security'16)*, 2016. Acceptance rate: 47.7%.

H. Lu, A. Srivastava, **B. Saltaformaggio**, D. Xu. StorM: Enabling Tenant-Defined Cloud Storage Middle-Box Services. In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'16)*, 2016. Acceptance rate: 22.3%.

Y. Kwon, D. Kim, W. Sumner, K. Kim, **B. Saltaformaggio**, X. Zhang, D. Xu. LDX: Causality Inference by Lightweight Dual Execution. In *ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'16)*, 2016. Acceptance rate: 22%.

B. Saltaformaggio, R. Bhatia, Z. Gu, X. Zhang, D. Xu. GUITAR: Piecing Together Android App GUIs from Memory Images. In *ACM Conference on Computer and Communications Security (CCS'15)*, 2015. Acceptance rate: 19.8%.
Best Paper Award.

B. Saltaformaggio, R. Bhatia, Z. Gu, X. Zhang, D. Xu. VCR: App-Agnostic Recovery of Photographic Evidence from Android Device Memory Images. In *ACM Conference on Computer and Communications Security (CCS'15)*, 2015. Acceptance rate: 19.8%.

Z. Deng, **B. Saltaformaggio**, X. Zhang, D. Xu. iRiS: Vetting Private API Abuse in iOS Applications. In *ACM Conference on Computer and Communications Security (CCS'15)*, 2015. Acceptance rate: 19.8%.
Led to the removal of hundreds of privacy-violating apps from Apple's App Store.

C. Xu, **B. Saltaformaggio**, S. Gamage, R. Kompella, D. Xu. vRead: Efficient Data Access for Hadoop in Virtualized Clouds. In *ACM/IFIP/USENIX Middleware Conference (Middleware'15)*, 2015. Acceptance rate: 19.5%.

H. Lu, **B. Saltaformaggio**, R. Kompella, D. Xu. vFair: Latency-Aware Fair Storage Scheduling via Per-IO Cost-Based Differentiation. In *ACM Symposium on Cloud Computing (SOCC'15)*, 2015. Acceptance rate: 21.6%.

B. Saltaformaggio, Z. Gu, X. Zhang, D. Xu. DSCRETE: Automatic Rendering of Forensic Information from Memory Images via Application Logic Reuse. In *USENIX Security Symposium (USENIX Security'14)*, 2014. Acceptance rate: 19.1%.
Best Student Paper Award.

Z. Gu, **B. Saltaformaggio**, X. Zhang, D. Xu. Face-Change: Application-Driven Dynamic Kernel View Switching in a Virtual Machine. In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'14)*, 2014. Acceptance rate: 30%.

B. Saltaformaggio, D. Xu, X. Zhang. BusMonitor: A Hypervisor-Based Solution for Memory Bus Covert Channels. In *European Workshop on Systems Security (EuroSec'13, in conjunction with EuroSys'13)*, 2013. Acceptance rate: 29.6%.

D. Bilar, **B. Saltaformaggio**. Using a Novel Behavioral Stimuli-Response Framework to Defend against Adversarial Cyberspace Participants. In *CCDCOE International Conference on Cyber Conflict (ICCC3)*, 2011. Acceptance rate: 40%.

Theses

B. Saltaformaggio. Convicted by Memory: Automatically Recovering Spatial-Temporal Evidence from Memory Images. In *Purdue University Theses and Dissertations*, 2016.

B. Saltaformaggio. Forensic Carving of Wireless Network Information from the Android Linux Kernel. In *University of New Orleans Theses and Dissertations*, 2012.

Teaching

ECE 8803-B: Software Vulnerabilities and Security — Fall 2017
Georgia Institute of Technology — Atlanta, GA
3 credits

Students Advised

Qi Zhang (BS, Purdue University, 2016) contributed to several smartphone forensics and execution investigation projects which culminated in two publications. After graduating, she joined Facebook's New York City Office.

Praseem Banzal (MS, Purdue University, 2014) conducted his MS thesis work, a cloud-hosted distributed provenance tracking system, under my guidance. After graduating, he became a member of Google's infrastructure team.

Invited Talks

Convicted by Memory: Recovering Spatial-Temporal Digital Evidence from Memory Images.
- Georgia Tech School of ECE Advisory Board Meeting, Cupertino, CA — 2017
- University of Wisconsin-Madison, Madison, WI — 2017
- Georgia Institute of Technology, Atlanta, GA — 2017

Convicted by Memory: Recent Advances in Android Memory Forensics.
- Google Anti-Abuse Research Group, Mountain View, CA — 2016

Holistic (Temporal, Behavioral, and Spatial) APT Defense.
- Cisco Research Partners Meeting, San Diego, CA — 2016
- Raytheon, Cambridge, MA — 2015

Automatically Recovering Human-Understandable Evidence from Memory Images.
- 17^{th} Annual CERIAS Security Symposium, West Lafayette, IN — 2016
- IBM T.J. Watson Research Center, Yorktown Heights, NY — 2015
- Colorado School of Mines, Golden, CO — 2015

Applications of Dynamic Binary Slicing for Security and Forensics.
- Greater New Orleans Center for Information Assurance, New Orleans, LA — 2014

DSCRETE: Automatic Rendering of Forensic Information from Memory Images via Application Logic Reuse.
- CERIAS Security Seminar Series, West Lafayette, IN — 2014
- DARPA BET Program PI Meeting, Arlington, VA — 2014

Guest-Transparent Provenance Tracing for Cross-Host Cyber Attacks against Cloud Infrastructures.
- Intelligent Automation, Inc., Rockville, MD — 2014

Service

Program Committee Member

World Wide Web Conference, Security & Privacy Track (WWW) 2017

Shadow Program Committee Member

ACM Asia Conference on Computer and Communications Security (ASIACCS) 2017

IEEE Symposium on Security and Privacy (S&P) 2016

Journal Reviewer

IEEE Transactions on Dependable and Secure Computing (TDSCSI) Special Issue Paradigm Shifts in Cryptographic Engineering 2017

ACM Transactions on Privacy and Security (TOPS) 2016

IEEE Transactions on Dependable and Secure Computing (TDSC) 2015

External Reviewer (Total = 24)

International Conference on Software Engineering (ICSE) 2017

Network and Distributed System Security Symposium (NDSS) 2014 to 2017

ACM Conference on Computer and Communications Security (CCS) 2013 to 2016

Annual Computer Security Applications Conference (ACSAC) 2013 to 2016

Digital Forensics Research Workshop (DFRWS) 2013 to 2016

International Symposium on Research in Attacks, Intrusions, and Defenses (RAID) 2015 to 2016

ACM International Symposium on the Foundations of Software Engineering (FSE) 2016

IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2016

ACM Asia Conference on Computer and Communications Security (ASIACCS) 2016

IEEE Symposium on Security and Privacy (S&P) 2015

International Conference on Security and Privacy in Communication Networks (SecureComm) 2015

Outreach Efforts

Invited Full Day Moderator 2015

GenCyber: Intensive Cyber Security Outreach Workshop For High School Teachers

Select Media Coverage

Full list available on my website

New Technique Could Help Law Enforcement Collect Smartphone Data.
IEEE Electronics360.

RetroScope opens doors to the past in smart phone investigations.
ScienceDaily, NSF, CACM - ACM TechNews.

Forensics tool nabs data from Signal, Telegram, WhatsApp.
The Register.

RetroScope, a tool developed by Purdue University that shows the previous screens viewed on an Android device.
Stanford Cyber Initiative.

Encryption or not, your smartphone data will now be easily recovered with this forensic tool.
Techworm.

Purdue research team details new smart phone forensic data strategy.
Homeland Preparedness News.

Apple blacklists hundreds of apps that stole personal user data.
Digital Journal.

YiSpecter: First iOS Malware That Attacks Non-jailbroken Apple iOS Devices by Abusing Private APIs.
Palo Alto Networks.