Brendan Dolan-Gavitt

CONTACT INFORMATION

800 Peachtree St NE #8217
Atlanta, GA 30308 USA

Voice: (617) 913-9060
Fax: (404) 385-4272
E-mail: brendan@cc.gatech.edu
WWW: `http://cc.gatech.edu/~brendan/`

RESEARCH INTERESTS

Systems and Network Security, Reverse Engineering, Privacy and Anonymity

EDUCATION

Georgia Institute of Technology, Atlanta, Georgia USA

Ph.D. Student, Computer Science (expected graduation date: August 2014)

- Research Area: Virtualization security
- Advisor: Wenke Lee

Wesleyan University, Middletown, Connecticut USA

B.A. Computer Science, May, 2006
B.A. Mathematics, May, 2006

HONORS AND AWARDS

NSF Graduate Research Fellowship Program, Honorable Mention, 2009

AT&T Best Applied Security Paper Award, Finalist, 2011

Wesleyan University: Honors in Computer Science, Senior Prize in Computer Science, 2006

PUBLICATIONS

Brendan Dolan-Gavitt, Tim Leek, Josh Hodosh, and Wenke Lee. Tappan Zee (North) Bridge: Mining Memory Accesses for Introspection. Proceedings of the ACM Conference on Computer and Communications Security (CCS). Berlin, Germany, November 2013.
Available: `http://www.cc.gatech.edu/~brendan/tzb_author.pdf`

Brendan Dolan-Gavitt, Tim Leek, Michael Zhivich, Jonathon Giffin, and Wenke Lee. Virtuoso: Narrowing the Semantic Gap in Virtual Machine Introspection. IEEE Symposium on Security and Privacy. Oakland, California, May 2011.
Available: `http://www.cc.gatech.edu/~brendan/virtuoso.pdf`

Brendan Dolan-Gavitt, Abhinav Srivasta, Patrick Traynor, and Jonathon Giffin. Robust Signatures for Kernel Data Structures. Proceedings of the ACM Conference on Computer and Communications Security (CCS). Chicago, Illinois, November 2009.
Available: `http://www.cc.gatech.edu/~brendan/ccs09_siggen.pdf`

Brendan Dolan-Gavitt. Forensic analysis of the Windows registry in memory. Digital Investigation, Volume 5, Supplement 1, September 2008, Pages S26-S32.
Available: `http://www.dfrws.org/2008/proceedings/p26-dolan-gavitt.pdf`

Brendan Dolan-Gavitt. The VAD tree: A process-eye view of physical memory. Digital Investigation, Volume 4, Supplement 1, September 2007, Pages 62-64.
Available: `http://www.dfrws.org/2007/proceedings/p62-dolan-gavitt.pdf`

Brendan Dolan-Gavitt. Timing Attacks in Anonymity-Providing Systems. Honors Thesis, 2006. Wesleyan University.
Available: `http://kurtz.cs.wesleyan.edu/~bdolangavitt/thesis/verbiage/tor-thesis.pdf`

Talks and Presentations

The VAD Tree: A Process-Eye View of Physical Memory. Digital Forensic Research Workshop (DFRWS). Pittsburgh, Pennsylvania. August 13, 2007.

Interactive Memory Exploration With Volatility. Open Memory Forensics Workshop (OMFW). Baltimore, Maryland. August 10, 2008.

Forensic Analysis of the Windows Registry in Memory. Digital Forensic Research Workshop (DFRWS). Baltimore, Maryland. August 11, 2008.

Registry Analysis and Memory Forensics, Together at Last. SANS Forensics and Incident Response Summit. Washington, DC. July 7, 2009.

Robust Signatures for Kernel Data Structures. GTISC Information Security Seminar. Atlanta, Georgia. October 1, 2009.

Robust Signatures for Kernel Data Structures. ACM Conference on Computer and Communications Security. Chicago, Illinois. November 12, 2009.

Robust Signatures for Kernel Data Structures. Wesleyan University Computer Science Seminar. Middletown, Connecticut. November 30, 2009.

Recent Advances in Memory analysis. SANS Incident Detection Summit. Washington, DC. December 10, 2009.

Volatility: A Framework for Volatile Memory Analysis. Malware Technical Exchange Meeting (MTEM2010). Lexington, Massachusetts. July 16, 2010.

Virtualization Security (Tutorial). NSERC ISSNet Summer School. Vancouver, British Columbia. July 19, 2010.

Virtuoso: Narrowing the Semantic Gap in Virtual Machine Introspection. STAR Center Workshop. Atlanta, GA. February 9, 2011.

Virtuoso: Narrowing the Semantic Gap in Virtual Machine Introspection. GTISC Information Security Seminar. Atlanta, GA. April 8, 2011.

Virtuoso: Narrowing the Semantic Gap in Virtual Machine Introspection. IEEE Symposium on Security and Privacy. Berkeley, CA. May 24, 2011.

Monitoring Untrusted Modern Applications with Collective Record and Replay. Microsoft Research. Redmond, WA. August 5, 2011. Available: `http://research.microsoft.com/apps/video/dl.aspx?id=152832`

Toward Ubiquitous Application Monitoring and Coverage Measurement. MIT Lincoln Laboratory. Lexington, MA. February 17, 2012.

Virtuoso: Narrowing the Semantic Gap in Virtual Machine Introspection. Northeastern University/MIT Lincoln Laboratory Cyber Security Meeting. Boston, MA. March 30, 2012.

Tappan Zee (North) Bridge: Mining Memory Accesses for Introspection. MIT Lincoln Laboratory. Lexington, MA. August 2, 2013.

Tappan Zee (North) Bridge: Mining Memory Accesses for Introspection. ACM Conference on Computer and Communications Security. Berlin, Germany, MA. August 2, 2013.

Understanding Closed-Source Systems for Security. Columbia University. New York, NY. November 22, 2013

Academic Service

- External reviewer, Network and Distributed Systems Symposium 2009
- External reviewer, IEEE Security and Privacy 2009
- External reviewer, Financial Cryptography 2010
- External reviewer, USENIX Security 2010
- External reviewer, IEEE Security and Privacy 2011
- Program Committee Member, Digital Forensics Research Workshop 2013
- External reviewer, ACM CCS 2013
- Program Committee Member, Digital Forensics Research Workshop 2014

Research Experience

Georgia Institute of Technology, Atlanta, Georgia USA

Graduate Research Assistant **August 2008 - Present**

Performed research into virtualization security and forensic memory analysis, including methods of differentiating human vs. automated behavior in virtual machines, developing robust memory signatures for kernel data structures, and protection of dynamic kernel data.

MIT Lincoln Laboratory, Lexington, Massachusetts USA

Summer researcher **May, 2012 - July 2012**

Researched novel file format visualization and reverse engineering techniques. Helped create novel dynamic analysis system (PANDA) and helped port record and replay support to same. Developed new techniques for live application introspection.

Microsoft Research, Redmond, Washington USA

Summer Research Intern **May 2011 - March 2012**

Researched novel record and replay strategies to enable continuous monitoring and test case generation across large populations of users on both mobile (Windows Phone) and desktop (Windows 7) platforms.

MIT Lincoln Laboratory, Lexington, Massachusetts USA

Summer researcher **May, 2010 - July 2010**

Researched methods of automatically generating secure, cross-platform virtual machine introspection routines. This work resulted in a paper published at the IEEE Symposium on Security and Privacy in 2011.

MIT Lincoln Laboratory, Lexington, Massachusetts USA

Summer researcher **May, 2009 - July 2009**

Extended dynamic malware analysis and information flow platform, iFerret, to analyze Windows malware. Began research on automatic generation of virtual machine introspection routines.

Professional Experience

MITRE Corporation, Bedford, Massachusetts USA

Infosec Eng./Scientist **June 2006 - July 2008**

Worked with security operations team to build, deploy, and maintain intrusion detection sensor infrastructure in McLean, VA and Bedford, MA, as well as numerous smaller sites. Served as IDS analyst, monitoring intrusion detection systems for signs of possible compromise on the MITRE network, and performed forensic investigation into security incidents. Assisted in a research project to study techniques for constructing phylogenetic trees of malicious code (see `http://www.mitre.org/news/events/exchange09/05MSR116.pdf` for more details on the project). Assisted OVAL

(Open Vulnerability Assessment Language) team in tool development, Linux software packaging, and getting other operating systems (e.g., FreeBSD) to provide OVAL content.

Wesleyan University, Middletown, Connecticut USA

Consultant, Wesleyan Security Audit **January 2005 - May 2005**

Found and exploited security vulnerabilities in university systems as part of a semester-long project to improve information security at Wesleyan. Advised Wesleyan Information Technology Services (ITS) on ways to mitigate and protect against the attacks performed.

Professional Societies

Member of the IEEE, ACM, and USENIX.

Developed Software

- **Virtuoso** – A tool for automatic generation of introspection programs.
- **PANDA** – A Platform for Architecture Neutral Dynamic Analysis. Developed in collaboration with Northeastern University and MIT Lincoln Laboratory.
- **Creddump** – Extract Windows credentials from registry hives.
- **PDBParse** – A Python-based parser for the Visual Studio debug symbol format.
- **VADTools** – A set of Python scripts for extracting information about Virtual Address Descriptors from Windows memory images.
- I am a contributor to **Volatility**, an open-source memory forensics framework.
- **PyXa** – A Python wrapper for XenAccess, and a patch that allows Volatility to analyze the memory of a running virtual machine.
- I have written a number of Volatility plugins listed at `http://www.cc.gatech.edu/~brendan/volatility/`