Jason Franklin

Email: jfrankli@cs.cmu.edu
Web: http://www.cs.cmu.edu/~jfrankli
Phone: 262 960 0275

EDUCATION

Carnegie Mellon University (2005 - 2012)
M.S., Ph.D. in Computer Science
Thesis: “Abstractions for Model Checking System Security”

University of Wisconsin at Madison (2000 - 2004)
B.S. Computer Science, B.S. Mathematics, Business Certificate
Graduated with Highest Distinction (GPA 3.92)

RESEARCH INTERESTS

System and network security, mobile security, model checking, big-data systems, cluster and distributed computing.

PROFESSIONAL EXPERIENCE

Symantec Research Labs, Mountain View, CA Oct. 2011 - Current
Principal Research Engineer

- Responsible for advanced technology design and prototyping
- Developing next-generation security technology with focus on technological and commercial potential

Carnegie Mellon University Aug. 2005 - May 2012
Research assistant in Computer Science Department under advisement of Professor Anupam Datta

- Conducting research on principled design and analysis of secure systems
- Design and implementation of energy-efficient big-data systems (w. Professor David Andersen)

Microsoft Research, Redmond, Washington June - Sept. 2010
Research Intern

- Applied automated verification techniques to prove safety and liveness properties of web browser

International Computer Science Institute (ICSI) June - Sept. 2006
ICIR networking intern

- Analyzed transformation of Internet-based criminal activity from reputation economy to cash economy
- Performed first systematic exploration into measuring and analyzing an underground e-crime market

Sandia National Laboratory, Livermore, California May 2004 - Feb. 2006
Computer security research intern

- Designed and implemented distributed 802.11b sensor network monitoring system
- Developed first distributed stepping stone detection tool
- Lead development and evaluation of wireless device driver fingerprinting technique

University of Wisconsin at Madison Jan. - Dec. 2004
Undergraduate research assistant in Computer Science Department under direction of Professor Mary Vernon

- Developed and evaluated effectiveness of probe-response attacks against Internet sensor networks

University of Wisconsin at Madison May - Sept. 2003
Undergraduate research assistant in Computer Science Department under direction of Professor Eric Bach

- Researched asynchronous extensions to block cipher modes of operation and authored survey paper

IBM, Rochester, Minnesota June - Dec. 2002
Computer science intern

- Developed supply chain and database index management software

Ferguson Enterprises, Milwaukee, Wisconsin June 2001 - August 2001
Summer Intern

- Implemented handheld product management system and data processing infrastructure
- Trained personnel to operate part management system and manage data tier

TSInternet Web Services, Milwaukee, Wisconsin June 2000 - August 2001

CEO and Founder

- Founded and managed web site design and web services consulting business
- Performed SEO for customer websites and grew traffic to 150,000+ hits per year
- Responsible for advertising campaigns and lead generation

REFEREED PUBLICATIONS

1. Jason Franklin, Sagar Chaki, Anupam Datta, Jonathan M. McCune, and Amit Vasudevan. Parametric Verification of Address Space Separation. In *First Conference on Principles of Security and Trust (POST)*, 2012.
2. Deepak Garg, Jason Franklin, Dilsun Kaynar, and Anupam Datta. Compositional System Security with Interface-Confined Adversaries. In *Proceedings of Mathematical Foundations of Programming Semantics (MFPS) Conference*, 2010.
3. Jason Franklin, Sagar Chaki, Anupam Datta, and Arvind Seshadri. Scalable parametric verification of secure systems: How to verify reference monitors without worrying about data structure size. In *Proceedings of IEEE Symposium on Security and Privacy (Oakland '10)*, 2010.
4. David Andersen, Jason Franklin, Michael Kaminsky, Amar Phanishayee, Lawrence Tan, and Vijay Vasudevan. FAWN: A fast array of wimpy nodes. In *Proceedings of ACM Symposium on Operating System Principles (SOSP'09)*, Oct. 2009.
5. Vijay Vasudevan, Jason Franklin, David Andersen, Amar Phanishayee, Lawrence Tan, Michael Kaminsky, and Iulian Moraru. Fawndamentally power-efficient clusters. In *Proceedings of 12th Workshop on Hot Topics in Operating Systems (HotOS XII)*, May 2009.
6. Anupam Datta, Jason Franklin, Deepak Garg, and Dilsun Kaynar. A logic of secure systems and its application to trusted computing. In *Proceedings of IEEE Symposium on Security and Privacy (Oakland '09)*, May 2009.
7. Deepak Garg, Jason Franklin, Dilsun Kaynar, and Anupam Datta. A logic for reasoning about networked secure systems. In *Joint Workshop on Foundations of Computer Security, Automated Reasoning for Security Protocol Analysis, and Issues in the Theory of Security (FCS-ARSPA-WITS)*, June 2008.
8. Jason Franklin, Mark Luk, Jonathan M. McCune, Arvind Seshadri, Adrian Perrig, and Leendert van Doorn. Remote detection of virtual machine monitors with fuzzy benchmarking. *ACM SIGOPS OS Review (Special Issue on Computer Forensics)*, April 2008.
9. Jason Franklin, Vern Paxson, Adrian Perrig, and Stefan Savage. An inquiry into the nature and causes of the wealth of internet miscreants. In *Proceedings of 14th ACM Conference on Computer and Communications Security (CCS'07)*, November 2007.
10. Tal Garfinkel, Keith Adams, Andrew Warfield, and Jason Franklin. Compatibility is not transparency: VMM detection myths and realities. In *Proceedings of 11th Workshop on Hot Topics in Operating Systems (HotOS XI)*, May 2007.
11. James Newsome, David Brumley, Jason Franklin, and Dawn Song. Replayer: Automatic protocol replay by binary analysis. In *Proceedings of 13th ACM Conference on Computer and Communications Security (CCS '06)*, November 2006.
12. Jason Franklin, Damon McCoy, Parisa Tabriz, Vicentiu Neagoe, Jamie Van Randwyk, and Douglas Sicker. Passive data link layer 802.11 wireless device driver fingerprinting. In *Proceedings of 15th USENIX Security Symposium*, August 2006.
13. John Bethencourt, Jason Franklin, and Mary Vernon. Mapping internet sensors with probe response attacks. In *Proceedings of 14th USENIX Security Symposium*, August 2005.

OTHER ARTICLES

14. David Andersen, Jason Franklin, Michael Kaminsky, Amar Phanishayee, Lawrence Tan, and Vijay Vasudevan. FAWN: A fast array of wimpy nodes. *To Appear in Communications of the Association for Computing Machinery (CACM)*, 2011.
15. Anupam Datta, Jason Franklin, Deepak Garg, Limin Jia, and Dilsun Kaynar. On Adversary Models and Compositional Security. In *IEEE Security & Privacy, Volume 9, Issue 3*, May 2011.
16. Deepak Garg, Jason Franklin, Dilsun Kaynar, and Anupam Datta. Compositional system security with interface-confined adversaries. In *Proceedings of Mathematical Foundations of Programming Semantics (MFPS) Conference*, 2010.

17. Vijay Vasudevan, David Andersen, Michael Kaminsky, Lawrence Tan, Jason Franklin, and Iulian Moraru. Energy-efficient cluster computing with FAWN: Workloads and implications. In *Proceedings of 1st International Conference on Energy-Efficient Computing and Networking (e-Energy 2010)*, April 2010.

18. Jason Franklin, Mark Luk, Arvind Seshadri, and Adrian Perrig. PRISM: Enabling personal verification of code integrity, untampered execution, and trusted I/O or human-verifiable code execution. Technical Report CMU-CyLab-07-010, CMU Cylab Technical Report, Feb. 2007.

SELECTED HONORS AND AWARDS

- Best Paper Nomination, First Conference on Principles of Security and Trust (POST) 2012
- Best Paper, 22nd ACM Symposium on Operating System Principles (SOSP'09)
- Best Paper, 14th USENIX Security Symposium (Security '05)
- National Science Foundation Graduate Research Fellowship
- Department of Homeland Security (DHS) Graduate Fellowship
- Department of Homeland Security (DHS) Undergraduate Scholarship
- Member, Phi Kappa Phi, Phi Eta Sigma, National Society of Collegiate Scholars academic honor societies
- UW-Madison Dean's Honor List for 7 Semesters

RESEARCH EXPERIENCE

FAWN: A Fast Array of Wimpy Nodes We are developing a new cluster architecture for low-power data-intensive computing. FAWN couples low-power embedded CPUs to small amounts of local flash storage, and balances computation and I/O capabilities to enable efficient, massively parallel access to data. The key contributions of this project are the principles of the FAWN architecture and the design and implementation of FAWN-KV—a consistent, replicated, highly available, and high-performance key-value storage system built on a FAWN prototype. Our design centers around purely log-structured datastores that provide the basis for high performance on flash storage, as well as for replication and consistency obtained using chain replication on a consistent hashing ring. Our evaluation demonstrates that FAWN clusters can handle roughly 350 key-value queries per Joule of energy—two orders of magnitude more than a disk-based system.

ToSS: Theory of Secure Systems The primary goal of the ToSS project is to develop a formal framework for modeling and analysis of secure systems at two levels of abstraction–system architecture (specification) and system implementation. A specific issue that we plan to address in developing and using this framework is to provide rigorous definitions of security and adversary models, a relatively unexplored area in systems security. In addition, we hope to identify design principles for secure systems, as well as a core set of basic building blocks from which complex systems can be constructed via secure composition.

ET: Emerging Threats This project is based on the premise that there exists an important class of security threats which defy conventional means of defense. Countering these *emerging threats* requires fundamentally new approaches which may utilize heuristic or otherwise unconventional techniques. To better understand these threats we study a variety of largely unexplored topics including: device-driver fingerprinting, human-verifiable code execution, probe-response attacks, software-only tamper-evident functions, underground e-crime markets, and virtual machine monitor and virtual machine-based rootkit (VBMR) detection.