Jonathan Kirsch

2225 Sharon Road
Apartment 124
Menlo Park, CA 94025

http://www.cs.jhu.edu/~jak
jonkirsch@jhu.edu
(516) 312-1270

PROFESSIONAL INTERESTS

- Systems: distributed systems, critical infrastructure, cloud computing
- Algorithms: distributed algorithms, intrusion tolerance, fault-tolerant replication
- Cyber security

EDUCATION

Ph.D. Computer Science May 2010
The Johns Hopkins University, Baltimore, MD
Advisor: Prof. Yair Amir
Dissertation Title: Intrusion-Tolerant Replication Under Attack

M.S.E. Computer Science May 2007
The Johns Hopkins University, Baltimore, MD
GPA 3.83

B.S. Computer Science May 2004
Yale University, New Haven, CT
GPA 3.80

SKILLS

- **Expertise:** Large-scale, high-performance distributed systems, including replication systems and group communication systems.
- **Languages:** C, C++, Java, Python, Perl
- **Operating Systems:** Linux, Microsoft Windows, OS X

PROFESSIONAL EXPERIENCE

Research Scientist March 2010 - Present
Siemens Technology-To-Business Center, Berkeley, CA

- **Big Data Technology Evaluation** September 2012 - Present
  Scouted for innovative external technologies in the areas of Big Data and Business Analytics, with the goal of building mutually beneficial partnerships between Siemens business units and the technology inventors. As technical lead for several Big Data pilot projects, engaged directly with both Siemens business units and startup companies and performed deep due diligence of the technologies deemed most relevant.

- **Survivable SCADA** March 2010 – Present
  Technical lead for project focusing on building highly available, highly secure next-generation Supervisory Control and Data Acquisition (SCADA) systems for electricity distribution. Designed and implemented high-performance, multi-threaded, intrusion-tolerant replication engine resilient to malicious attacks. Ported code to Linux, Windows, OS X, and iOS. Integrated replication engine with a large and widely-deployed Siemens SCADA product, resulting in a prototype of the first survivable SCADA system. Demonstrated for utility customers the system's ability to continue operating correctly and with good performance under attack. Aided business case analysis and marketing.

Research Intern Summer 2006, Summer 2008
Telcordia Technologies, Piscataway, NJ

- **Intrusion-Tolerant Group Management for Mobile Ad-Hoc Networks** (Summer 2008)
  Designed, implemented, and proved the correctness of a partitionable and intrusion-tolerant group key agreement service for the ZODIAC project as part of the DARPA Intrinsically Assurable Mobile Ad-Hoc Networks (IAMANET) program. Collaborated daily with professional researchers on both design and implementation. Presented project results to the Applied Research department and at the Applied Research 2008 Strategic Program Review. Code and approach to intrusion tolerance were integrated into the full ZODIAC system. Work resulted in a patent (issued May 2012).

- **Mitigating Performance Attacks in Intrusion-Tolerant Replication Systems** (Summer 2006)
  Developed algorithms and protocol design guidelines for achieving high-performance wide-area database replication even when the system is under attack by intelligent adversaries. Presented project results to the Applied Research department.

ACADEMIC RESEARCH EXPERIENCE

Research Assistant 2004 - 2010
The Johns Hopkins University, Baltimore, MD
Distributed Systems and Networking Lab (http://www.dsn.jhu.edu)

- **Prime: Intrusion-Tolerant Replication Under Attack**
  Designed and developed Prime, the first intrusion-tolerant replication protocol that guarantees a meaningful level of performance even when a subset of the replicas is compromised. Defined a new performance-oriented correctness criterion, Bounded-Delay, to augment traditional safety and liveness properties. Demonstrated the vulnerability of existing protocols to performance degradation by intelligent adversaries and identified design patterns for building new protocols that mitigate this vulnerability.

- **Scalable Intrusion-Tolerant Replication for Wide-Area Networks**
  Designed, implemented, and proved the correctness of Steward, the first hierarchical, wide-area intrusion-tolerant replication protocol. System successfully survived a DARPA Red-Team attack as part of the Self-Regenerative Systems (SRS) project. Developed a customizable architecture for wide-area replication, allowing one to choose the desired level of fault tolerance based on perceived risk and performance requirements.

- **Fault-tolerant Replication**
  Designed and implemented Paxos for System Builders, a complete specification of the Paxos algorithm such that system builders can understand it. Developed innovative variations on the Congruity replication engine, a high-performance tool for peer data store replication, to increase protocol robustness in partitionable environments.

Visiting Researcher October 2008 - November 2008
University of Lisboa, Portugal
Navigators Distributed Systems Research Team

- Conducted research on intrusion-tolerant replication systems with Prof. Paulo Veríssimo and his team. Analyzed the robustness of randomized replication protocols to performance degradation by malicious attackers. Designed a hybrid architecture for wide-area intrusion-tolerant replication that resists performance attacks while achieving good normal-case performance.

Research Assistant Summer 2002
Yale University, New Haven, CT
Supervisor: Prof. Michael J. Fischer

- Designed and developed GUI for an implementation of a "Discreet" Vickrey Auction for Linux.

TEACHING EXPERIENCE

Instructor Fall 2008
The Johns Hopkins University, Baltimore, MD

- **Advanced Distributed Systems and Networks**
  Co-taught an advanced, research-oriented course consisting of three students. Helped lead bi-weekly discussions and provided feedback on projects. Projects included extending Bluetooth devices to run over the Internet and implementing a 3G/Wifi handoff for smartphones.

Teaching Assistant 2005, 2006, 2008, 2009
The Johns Hopkins University, Baltimore, MD

- **Distributed Systems** (Fall 2006, Spring 2008, Fall 2009)
  Aided undergraduate and graduate students on protocol design and implementation. Graded project submissions. Course sizes ranged from approximately 25 to 45 students.

- **Intermediate Programming** (Fall 2005, Spring 2006)
  An introduction to programming in C and C++. Helped design course assignments. Worked one-on-one with students to teach concepts. Course consisted of approximately 30 students.

PUBLICATIONS

Software

S-3 Paxos for System Builders (Paxos-SB). Yair Amir and Jonathan Kirsch. (www.dsn.jhu.edu). A high-performance fault-tolerant replication engine based on a complete specification of the Paxos algorithm. Related papers: I-1, TR-3.

S-2 The Prime intrusion-tolerant replication system. Y. Amir, B. Coan, J. Kirsch, J. Lane. (www.dsn.jhu.edu). First released June 2010. An intrusion-tolerant replication engine. The first Byzantine fault-tolerant replication system to provide performance guarantees while under attack. Related papers: J-2, C-8, C-7, C-5.

S-1 The STEWARD scalable intrusion-tolerant replication system. Y. Amir, C. Danilov, D. Dolev, J. Kirsch, J. Lane, C. Nita-Rotaru, J. Olsen, D. Zage. (www.dsn.jhu.edu). First released February 2010. An experimental intrusion-tolerant replication engine. The first to provide efficient Byzantine fault-tolerant replication over large-scale wide-area networks. Related papers: J-1, C-4, C-2.

Journals

J-2 Prime: Byzantine Replication Under Attack. Y. Amir, B. Coan, J. Kirsch, and J. Lane. The *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 8(4), pages 564-577, July 2011.

J-1 STEWARD: Scaling Byzantine Fault-Tolerant Replication to Wide-Area Networks. Y. Amir, C. Danilov, D. Dolev, J. Kirsch, J. Lane, C. Nita-Rotaru, J. Olsen, D. Zage. The *IEEE Transactions on Dependable and Secure Computing (TDSC)*. 7(1), pages 80-93, January 2010.

Refereed Conferences and Workshops

C-10 Intrinsically Resilient Energy Control Systems. F. Sheldon, J. Huang, J. Dang, D. Fetzer, S. Goose, J. Kirsch, D. Manz, T. Morris, D. Wei. In *Proceedings of the Cyber Security and Information Intelligence Research Workshop (CSIIRW12)*.

C-9 Using Semantic Web Technologies to Develop Intrinsically Resilient Energy Control Systems. F. Sheldon, J. Huang, J. Dang, D. Fetzer, S. Goose, J. Kirsch, D. Manz, T. Morris, D. Wei. In *Proceedings of the 7th International Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS 2012)*.

C-8 Toward Intrusion-Tolerant SCADA for Industrial Automation. J. Kirsch, S. Goose. In *Proceedings of the 2012 AUTOMATION Congress,* Baden-Baden, Germany, June 2012.

C-7 Toward Intrusion-Tolerant SCADA. J. Kirsch, S. Goose, Y. Amir, P. Skare. In *Proceedings of the Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW11),* Oak Ridge, TN, October 2011.

C-6 Intrusion-Tolerant Group Management for Mobile Ad-Hoc Networks. J. Kirsch, B. Coan. In *Proceedings of the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009)*.

C-5 Byzantine Replication Under Attack. Y. Amir, B. Coan, J. Kirsch, J. Lane. In *Proceedings of the 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2008)*, Anchorage, Alaska, June 2008, pp. 197-206.

C-4 Customizable Fault Tolerance for Wide-Area Replication. Y. Amir, B. Coan, J. Kirsch, J. Lane. In *Proceedings of the IEEE International Symposium on Reliable Distributed Systems (SRDS 2007)*, Beijing, China, October 2007, pp. 66-80.

C-3 Secret Handshakes with Dynamic and Fuzzy Matching. G. Ateniese, M. Blanton, J. Kirsch. In *Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS 2007)*, San Diego, California, February 2007.

C-2 Scaling Byzantine Fault-Tolerant Replication to Wide Area Networks. Y. Amir, C. Danilov, D. Dolev, J. Kirsch, J. Lane, C. Nita-Rotaru, J. Olsen, D. Zage. In *Proceedings of the IEEE International Conference on Dependable Systems and Networks (DSN 2006)*, Philadelphia, Pennsylvania, June 2006, pp. 105-114. **Award Paper**.

C-1 Load-Balancing and Locality in Range-Queriable Data Structures. J. Aspnes, J. Kirsch, A. Krishnamurthy. In *Proceedings of the ACM Symposium on Principles of Distributed Computing (PODC 2004)*, Newfoundland, Canada, July 2004, pp. 115-124.

Invited Papers

I-1 Paxos for System Builders: An Overview. J. Kirsch, Y. Amir. In *Proceedings of the 2008 Workshop on Large-Scale Distributed Systems and Middleware (LADIS 2008)*, Yorktown, New York, September 2008, pp. 1-6.

Additional Technical Reports

TR-4 An Attack-Resilient Architecture for Large-Scale Intrusion-Tolerant Replication. Y. Amir, B. Coan, J. Kirsch, J. Lane. Tech. Rep. CNDS-2009-5, October 2009.

TR-3 Paxos for System Builders. J. Kirsch, Y. Amir. Tech. Rep. CNDS-2008-2, March 2008.

TR-2 Towards Key-Privacy in a Fuzzy Identity-Based Encryption Scheme. J. Kirsch. May 2005.

TR-1 An Implementation and Analysis of the Skip Graph Data Structure. J. Kirsch. May 2004.

PATENTS

Awarded Patents

AP-1 Intrusion-Tolerant Group Management for Mobile Ad-Hoc Networks. Brian Coan, Jonathan Kirsch. US 8189789, May 29, 2012.

Pending Patents

PP-5 Method for Dynamically Updating Replica Software in a State Machine Replication System. Stuart Goose and Jonathan Kirsch. US patent pending ID: 2012P20178US, 2012.

PP-4 SKYDA: Secure Cloud-Based SCADA-as-a-Service. Stuart Goose, Jonathan Kirsch, and Dong Wei. US patent pending ID: 2012P08847US, 2012.

PP-3 Byzantine Fault-Tolerant SCADA System. Stuart Goose and Jonathan Kirsch. US patent pending ID: 2011P18902US01, 2011.

PP-2 Fault-Tolerant Replication Architecture. Stuart Goose and Jonathan Kirsch. US patent pending ID: 2011P06390US01, 2011.

PP-1 Replicated State Machine Utilizing View Change Protocol Resilient to Performance Attacks. Stuart Goose and Jonathan Kirsch. US patent pending ID: 2011P060389US01, 2011.

AWARDS

- **Student Scholarship** 2009
  Trusted Infrastructure Workshop (TIW 2009)
  Advanced Summer School on Architectures for Trustworthy Computing

- **Award paper** for Scaling Byzantine Fault-Tolerant Replication to Wide-Area Networks. 2006
  Y. Amir, C. Danilov, D. Dolev, J. Kirsch, J. Lane, C. Nita-Rotaru, J. Olsen, D. Zage.
  In the IEEE International Conference on Dependable Systems and Networks, 2006.

- **Tau Beta Pi Engineering Honor Society** 2004

- **Letter of Commendation** 2003
  Professor Michael J. Fischer, Yale University. For work in Database Systems course.

EXTERNAL PROFESSIONAL SERVICE

- Program Committee member for the Cyber Security and Information Intelligence Research Workshop (CSIIRW 2011, CSIIRW 2012).
- Program Committee member for the 12th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2010).
- Reviewer for IEEE Transactions on Computers (TC), IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE Communications Letters, ACM Transactions on Computer Systems (TOCS), Frontiers of Computer Science (FCS), Security and Communication Networks (SCN).

PRESENTATIONS

- Toward Survivable SCADA for Industrial Automation. 2012 AUTOMATION Congress, Baden-Baden, Germany, June 2012.
- Toward Survivable SCADA. 11th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW11), Oak Ridge, TN, October 2011.
- Toward Partitionable and Intrusion-Tolerant Group Services. Applied Research 2008 Strategic Program Review, Telcordia Technologies, Piscataway, New Jersey, July 2008. Invited talk.
- Byzantine Replication Under Attack. 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2008), Anchorage, Alaska, June 2008.
- Customizable Fault Tolerance for Wide-Area Replication. IEEE International Symposium on Reliable Distributed Systems (SRDS 2007), Beijing, China, October 2007.