

Jonathan Kirsch

Department of Computer Science
The Johns Hopkins University
3400 N. Charles Street
Baltimore, MD 21218

<http://www.cs.jhu.edu/~jak>
Email: jak@cs.jhu.edu
Phone: (410) 516-5562
Cell: (516) 312-1270

PROFESSIONAL INTERESTS

- Distributed systems and algorithms, computer systems
- Survivability and intrusion tolerance, computer and network security
- Fault tolerance, reliability

EDUCATION

- Ph.D. Computer Science** Expected October 2009
The Johns Hopkins University, Baltimore, MD
Advisor: Prof. Yair Amir
Thesis Topic: 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

ACADEMIC RESEARCH EXPERIENCE

- Research Assistant** 2004 - Present
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 up to less than one-third of the replicas are 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 performance.

Research Assistant

Summer 2002

Yale University, New Haven, CT

Supervisor: Prof. Michael J. Fischer

- Designed and developed a graphical user interface for an implementation of a “Discreet” Vickrey Auction for Linux.

INDUSTRY EXPERIENCE

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 are currently being integrated into the full ZODIAC system, and a provisional patent has been filed.
- **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.

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

The Johns Hopkins University, Baltimore, MD

- **Distributed Systems** (Fall 2006, Spring 2008)
Aided undergraduate and graduate students on protocol design and implementation. Graded project submissions. Course consisted of approximately 25 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

All publications are available on my webpage (<http://www.cs.jhu.edu/~jak>).

Journals

- J-1** STEWARD: Scaling Byzantine Fault-Tolerant Replication to Wide-Area Networks. Yair Amir, Claudiu Danilov, Danny Dolev, Jonathan Kirsch, John Lane, Cristina Nita-Rotaru, Josh Olsen, David Zage. To appear in IEEE Transactions on Dependable and Secure Computing (TDSC).

Conferences

- C-5** Byzantine Replication Under Attack. Yair Amir, Brian Coan, Jonathan Kirsch, John 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. Yair Amir, Brian Coan, Jonathan Kirsch, John 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. Giuseppe Ateniese, Marina Blanton, Jonathan 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. Yair Amir, Claudiu Danilov, Danny Dolev, Jonathan Kirsch, John Lane, Cristina Nita-Rotaru, Josh Olsen, David 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-Queryable Data Structures. James Aspnes, Jonathan Kirsch, Arvind Krishnamurthy. In Proceedings of the ACM Symposium on Principles of Distributed Computing (PODC 2004), Newfoundland, Canada, July 2004, pp. 115-124.

Workshops

- W-1** Intrusion-Tolerant Group Management for Mobile Ad-Hoc Networks. Jonathan Kirsch, Brian Coan. Accepted to the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009).

Invited Papers

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

In Submission

- S-2** Prime: Byzantine Replication Under Attack. Yair Amir, Brian Coan, Jonathan Kirsch, John Lane. Submitted to IEEE Transactions on Dependable and Secure Computing (TDSC).
- S-1** Customizable Byzantine Fault Tolerance for Wide-Area Replication. Yair Amir, Brian Coan, Jonathan Kirsch, John Lane. Submitted to IEEE Transactions on Parallel and Distributed Systems (TPDS).

Additional Technical Reports

- TR-4** Intrusion-Tolerant Group Management for Mobile Ad-Hoc Networks. Jonathan Kirsch, Brian Coan. Tech. Rep. CNDS-2009-2, March 2009.
- TR-3** Paxos for System Builders. Jonathan Kirsch, Yair Amir. Tech. Rep. CNDS-2008-2, March 2008.
- TR-2** Towards Key-Privacy in a Fuzzy Identity-Based Encryption Scheme. Jonathan Kirsch. May 2005.
- TR-1** An Implementation and Analysis of the Skip Graph Data Structure. Jonathan Kirsch. May 2004.

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
Yair Amir, Claudiu Danilov, Danny Dolev, Jonathan Kirsch, John Lane, Cristina Nita-Rotaru, Josh Olsen, David Zage. In the 2006 IEEE International Conference on Dependable Systems and Networks.
- **Tau Beta Pi Engineering Honor Society** 2004
- **Letter of Commendation** 2003
Professor Michael J. Fischer, Yale University. For work in Database Systems course.

PRESENTATIONS

- 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.

REFERENCES

- Dr. Yair Amir, Professor
Department of Computer Science
The Johns Hopkins University
Baltimore, MD 21218
yairamir@cs.jhu.edu
- Dr. Giuseppe Ateniese, Associate Professor
Department of Computer Science
The Johns Hopkins University
Baltimore, MD 21218
ateniese@cs.jhu.edu
- Dr. Brian Coan, Director
Distributed Computing Research Group
Telcordia Technologies
Piscataway, NJ 08854
coan@research.telcordia.com
- Dr. Cristina Nita-Rotaru, Associate Professor
Department of Computer Science
Purdue University
West Lafayette, IN 47907
crisn@cs.purdue.edu