MASTOOREH (NEGIN) SALAJEGHEH

140 Governors Drive, Amherst, MA 01003 *negin@cs.umass.edu*
(916) 365-1183 *http://cs.umass.edu/~negin*

Research Interest

- My research interests are broadly in trustworthy computing and low-power embedded systems. I have worked on system security, RFID-scaled devices, probabilistic storage, near field communications, and security of medical infrastructures.

Education

- **UMass Amherst, Ph.D.**—Computer Science *2007–2012(Expected)*
  Thesis: Techniques to reduce the energy consumption of low-power devices at the limits of digital abstractions
- **Carnegie Mellon University, ini, M.Sc.**—Information Networking *2005–2006*
  Thesis: Securing hierarchical sensor networks
- **Sharif University of Technology, B.Sc.**—Computer Engineering *2000–2004*

Experience

- **Research Assistant** **UMass Amherst**
  Advisor: Dr. Kevin Fu September'07-Present
  - Enabling secure protocols without clocks on embedded devices
  - Probabilistic and energy-efficient storage for low-power devices
  - Security and privacy of medical infrastructures
- **Research Intern** **Microsoft Research Redmond**
  Mentor: Dr. Jie Liu June'11-September'11
  - P2P communication through Near Field Communication (NFC)
- **Research Assistant** **Athens Information Technology**
  Advisors: Dr. Dimitriou & Dr. Kalis January'06–June'07
  - Security and routing in wireless sensor networks
  - Multiple and/or directional antenna based MAC schemes for sensor motes
- **Teaching Assistant** **UMass, Athens Info. Tech., Sharif Univ.**
  - Courses: Electronic Identification Lab, Introduction to Computer and Network Security, Operating Systems, Web Technologies, Java Programming Language
- **System Developer** **Intralot Company**
  Athens, Greece September'06–June'07
  - Development of a security platform for a distributed mobile game system
- **Research Assistant** **Telecommunication Research Center**
  Tehran, Iran May'03–September'03
  - Research and studies about the web services at the Network Security Center

Publications

- **[USENIX Security'12]** TARDIS: Time and Remanence Decay in SRAM to Implement Secure Protocols on Embedded Devices without Clocks. Amir Rahmati, Mastooreh Salajegheh, Daniel Holcomb, Jacob Sorber, Wayne Burleson, Kevin Fu. In Proceedings of the 21st USENIX Security Symposium. Bellevue, WA, August 2012. To appear.
- **[ACM Transactions (TECS)]** Half-Wits: Software Techniques for Low-Voltage Probabilistic Storage on Microcontrollers with NOR Flash Memory, M. Salajegheh, Y. Wang, K. Fu, A. Jiang, E. Learned-Miller. ACM Transactions on Embedded Computing Systems, Special Issue on Probabilistic Embedded Computing 2012.
- **[Book Chapter]** Maximalist Cryptography and Computation on the WISP UHF RFID Tag, Book chapter in Wirelessly Powered Sensor Networks and Computational RFID. H. Chae, M. Salajegheh, D. Yeager, J. Smith, and K. Fu. Springer 2012.
- **[HotPower'11]** Ekho: Bridging the Gap Between Simulation and Reality in Tiny Energy-Harvesting Sensors. H. Zhang, M. Salajegheh, K. Fu, and J. Sorber. In Workshop on Power Aware Computing and Systems.
- **[USENIX FAST'11]** Exploiting Half-Wits: Smarter storage for low-power devices. M. Salajegheh, Y. Wang, K. Fu, A. Jiang, E. Learned-Miller. USENIX Conference on File and Storage Technologies, February 2011. (acceptance rate = 20/74 = 27%).
- **[USENIX Security'09]** CCCP: Secure remote storage for computational RFIDs. M. Salajegheh, S. Clark, B. Ransford, K. Fu, and Ari Juels. USENIX Security Symposium, August 2009. (acceptance rate = 26/176= 15%).
- **[SPIMACS'09]** HICCUPS: Health Information Collaborative Collection Using Privacy And Security. A. Molina, M. Salajegheh, Kevin Fu. ACM Security and Privacy in Medical and Home-Care Systems workshop, November 2009.
- **[DMD'09]** Home telemedicine: Encryption is not enough. (Poster). M. Salajegheh, A. Molina, and K. Fu. Design of Medical Devices Conference, April 2009.
- **[HotPower'08]** Getting things done on computational RFIDs with energy-aware checkpointing and voltage-aware scheduling. B. Ransford, S. Clark, M. Salajegheh, and K. Fu. USENIX Workshop on Power Aware Computing and Systems, December 2008.
- **[I3P'08]** Protecting Global Medical Telemetry Infrastructure. B. Defend, m. Salajegheh, K. Fu, S. Inoue , I3P white paper, March 2008.
- **[PIMRC'07]** HyMAC: Hybrid TDMA/FDMA Medium Access Control Protocol for Wireless Sensor Networks. M. Salajegheh, H. Soroush, A. Kalis. IEEE International Symposium on Personal, Indoor and Mobile Radio Communication, September 2007.
- **[Book Chapter]** Secure Frameworks, book chapter in Wireless Sensor Network Security. I. Krontiris, H. Soroush, M. Salajegheh, T. Dimitriou, Edited by Prof. Javier Lopez and Jianying Zhou, to be published by IOS Press, 2007.
- **[ICC'07]** Providing Transparent Security Services to Sensor Networks. H. Soroush, M. Salajegheh, T. Dimitriou, IEEE International Conference on Communications, June 2007.
- **[ISCTA'07]** LEE: Lightweight Energy-efficient Encryption Algorithm. N. Komninos, H. Soroush, M. Salajegheh, International Symposium on Communication Theory and Application, July 2007.

- **[REALWSN'06]** .Sense: A Secure Framework for Sensor Network Data Acquisition, Monitoring and Command (Poster). M. Salajegheh, H. Soroush, A. Thomos, T. Dimitriou, I. Krontiris, The ACM Workshop on Real-World Wireless Sensor Networks, June 2006.

Talks

- **Exploiting Half-Wits: Smarter Storage for Low-Power Devices.**
  - The 3rd Annual Non-Volatile Memories Workshop, San Diego, 2012
  - Grace Hopper Conference, New Investigators Session, 2011
  - Microsoft Research Redmond, Summer 2011
  - USENIX FAST, San Jose, 2011.
  - Department Talk in UMass Amherst Computer Science, 2011
- **CCCP: Secure Remote Storage for Computational RFIDs.**
  - Microsoft Research Redmond, Summer 2009
  - Intel Labs Seattle, Summer 2009
  - Research Experiences for Undergraduates (REU) lunch, Summer 2009
  - Systems lunch, Fall 2009

Patents

- "Methods and Systems for Zero-Power Time Keeping" by Kevin Fu, Jacob Sorber, Mastooreh Salajegheh. December 2011 (Pending).
- "Methods and Systems for Low-Power Storage for Flash Memory" by Kevin Fu, Erik Learned-Miller, Mastooreh Salajegheh. December 2010.

Achievements and Activities

- One of the 75 graduate students invited to The 2012 Google Grad CS Forum.
- One of the top four finishers of UMass Innovation Challenge Award, $1750, 2011.
- Recipient of UMass Commercial Ventures and Intellectual Property Technology Development Award, $25K for SMASH Memory, 2011.
- Recipient of Grace Hopper Celebration of Women in Computing travel grants, 2011& 2009.
- Served in the program committee of Symmetric Key Encryption workshop 2011 (SKEW'11).
- Recipient of Outstanding Synthesis Project Award, UMass Amherst, 2010.
- Recipient of USENIX FAST'11 and USENIX Security'10 travel grants.
- Served as co-chair & mentor in UMass CS Women group, Fall'08–Spring'09.
- Served in UMass diversity committee, Fall'09.
- Served as a mentor of two students in the Research Experiences for Undergraduates program, 2008.
- Served as the reviewer of several papers in conferences of IEEE Security & Privacy, Financial cryptography, and journal of IEEE security in sensor networks.

- Recipient of a 16-months full-tuition scholarship, Information Networking Institute, CMU, 2005.
- Ranked in top 0.1% among 350,000 students participating in the Nationwide Examination for Admission to the Iranian Public Universities, 2000.

Technical Skills

- Embedded Systems: IAR Embedded Benchmark, TI MSP430s Microcontrollers, X-Scale ARM Processor, Atmel AVR Microcontrollers, TinyOS
- Programming languages: C, C++, Java, MATLAB, MySQL, Python, Prolog
- Web Programming: PHP, HTML, JavaScript, ASP.NET, Applets
- Editors: LaTeX, Microsoft Office, OmniGroup Softwares, Keynote
- Operating Systems: Microsoft Windows, Mac OS, and Linux

References

- **Kevin Fu, Associate Professor**
  Department of Computer Science
  University of Massachusetts Amherst
  (616)594–0385, kevinfu@cs.umass.edu
- **Wayne Burleson, Associate Professor**
  Department of Electrical and Computer Engineering
  University of Massachusetts Amherst
  (413)545–2382, burleson@ecs.umass.edu
- **Erik Learned-Miller, Associate Professor**
  Department of Computer Science
  University of Massachusetts Amherst
  (413)545–2993, elm@cs.umass.edu
- **Andrew Jiang, Associate Professor**
  Department of Computer Science and Engineering
  Texas A&M University
  (979)845–7983, ajiang@cse.tamu.edu