

Kevin Fu

Department of Computer Science
University of Massachusetts Amherst
kevinfu@cs.umass.edu
<http://www.cs.umass.edu/~kevinfu/>

Computer Science Building
140 Governors Drive
University of Massachusetts
Amherst, MA 01003-9264

Research Areas Computer system security: Security and privacy for low-power computational RFIDs, security and privacy for implantable medical devices, secure content distribution.

Education **Massachusetts Institute of Technology** Cambridge, MA
PhD in Electrical Engineering and Computer Science, September 2005.
Thesis: Integrity and access control in untrusted content distribution networks
Advisors: Frans Kaashoek and Ron Rivest

Massachusetts Institute of Technology Cambridge, MA
MEng in Electrical Engineering and Computer Science, GPA 4.9/5.0, June 1999.
Thesis: Group sharing and random access in cryptographic storage file systems
Advisor: Ron Rivest

Massachusetts Institute of Technology Cambridge, MA
SB in Computer Science and Engineering, GPA 4.5/5.0, June 1998.

Academic positions **Beth Israel Deaconess Medical Center** Boston, MA
Visiting scientist. *Beginning August 2009.*

Microsoft Research Redmond, WA
Visiting researcher. *July 2009.*

Department of Computer Science, UMass Amherst Amherst, MA
Assistant professor. *Fall 2005–present.*

Department of Computer Science, UMass Amherst Amherst, MA
Research scientist. *Summer 2005.*

Awards **Alfred P. Sloan Research Fellowship**
The Sloan Research Fellowships seek to stimulate fundamental research by early-career scientists and scholars of outstanding promise. These two-year fellowships are awarded yearly to 118 researchers in recognition of distinguished performance and a unique potential to make substantial contributions to their field. *2009.*

NSF CAREER Award
The Faculty Early Career Development (CAREER) Program is a Foundation-wide activity that offers the National Science Foundation's most prestigious awards in support of junior faculty who exemplify the role of teacher-scholars through outstanding research, excellent education and the integration of education and research within the context of the mission of their organizations. *2009.*

IEEE Security & Privacy (Oakland) Outstanding Paper Award

Award for the best overall paper entitled, “Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses” at the 29th Annual IEEE Symposium on Security & Privacy out of 249 submissions. 11.2% acceptance rate. *May 2008.*

**UMass Commercial Ventures & Intellectual Property
Technology Development Fund Award**

UMass CVIP awards researchers whose work evidences strong potential for commercial development. \$30K for “Zero-Power Telemetry for Implantable Medical Devices.” *March 2008.*

Intel Foundation PhD Fellowship Award

Intel Fellows recommend the candidates for this award, which provides a year of support and an opportunity to conduct research at Intel. *June 2004.*

10th USENIX Security Symposium Best Student Paper Award

“Dos and Don’ts of Client Authentication on the Web.” *August 2001.*

ACM International Student Research Contest, First Place Graduate Award

Award for a poster and presentation on the SFS Read-Only File System. *February 2001.*

AT&T Student Research Day

Third place graduate award for a poster on the SFS Read-Only File System. *October 2000.*

USENIX Scholar

The USENIX Scholars Fellowship provides a year of funding to students with exceptional research ability and promise. *January 2000.*

**Research
experience**

Johns Hopkins Information Security Institute

Baltimore, MD

Visiting scholar for secure file systems, proxy re-encryption, and RFID security & privacy. *2003–2005.*

MIT Parallel and Distributed Operating Systems Group

Cambridge, MA

Researcher in secure file systems and Web authentication at the MIT Lab for Computer Science. *1998–2005.*

Hewlett-Packard Labs

Palo Alto, CA

Internship in cryptographic key regression for secure storage. *Summer 2002.*

MIT Applied Security Reading Group

Cambridge, MA

Founded the Applied Security Reading Group at the MIT Lab for Computer Science. Conducted 50 seminars that attracted students, faculty, staff, and guests from industry. The seminar included several invited talks from leading experts in security. Attendance ranged from a few members to nearly 100. *1999–2003.*

Bellcore (Telcordia) — Security Research Group

Morristown, NJ

Internship in home automation, secure email revocation, a fast stream cipher for video, and approximate message authentication codes for watermarking images. *Summers 1996–1998 and Fall 1998.*

MIT Media Lab, Gesture and Narrative Language

Cambridge, MA

Undergraduate researcher on Renga, a system for children around the world to collaboratively write a story in real time. Fall 1995.

**Industrial
experience****Sightpath/Cisco Systems**

Waltham/Boxborough, MA

As an employee at a startup company, I advised software engineers about security. 1999–2002.

MIT Information Systems – Network Security Team

Cambridge, MA

Technical support. I responded to intrusions, tracked down computer crackers, reverse engineered encrypted exploits, encouraged the use of secure communication, and assisted law enforcement. 1994–2002.

Holland Community Hospital

Holland, MI

As a member of technical support, I participated in the roll out of a new computing environment. Computers were placed in all medical areas; medical personnel used solid-state authentication keys to access medical data. I also programmed a directory indexing system and created scripts to detect incorrect general ledger entries. 1993–1996.

**Refereed
journal
publications**

[J6] “Clinically Significant Magnetic Interference of Implanted Cardiac Devices by Portable Headphones” by Sinjin Lee, Kevin Fu, Tadayoshi Kohno, Benjamin Ransford, and William H. Maisel. To appear in *Heart Rhythm*, October 2009.

[J5] “Power-up SRAM State as an Identifying Fingerprint and Source of True Random Numbers” by Daniel Holcomb, Wayne Burleson, and Kevin Fu. In *IEEE Transactions on Computers*, 58(9):1198–1210, September 2009 (an earlier version appears in *RFIDSec* 2007).

[J4] “Electromagnetic Interference (EMI) of Implanted Cardiac Devices by MP3 Player Headphones” by Sinjin Lee, Beth Israel Deaconess Medical Ctr, Boston, MA; Benjamin Ransford, Kevin Fu, Univ of Massachusetts, Amherst, MA; Tadayoshi Kohno, Univ of Washington, Seattle, WA; William H Maisel, Beth Israel Deaconess Medical Ctr, Boston, MA. Accepted for Presentation, 2008 American Heart Association Annual Scientific Sessions and *CIRCULATION* journal.

[J3] “Security and Privacy for Implantable Medical Devices” by Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. In *IEEE Pervasive Computing, Special Issue on Implantable Electronics*, January–March, 2008.

[J2] “Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage” by Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. In *ACM Transactions on Information and System Security (TISSEC)*, 9(1), February 2006 (an earlier version appears in *NDSS* 2005).

[J1] “Fast and Secure Distributed Read-Only File System” by Kevin Fu, M. Frans Kaashoek, and David Mazières. In *ACM Transactions on Computer Systems*, 20(1):1–24, February 2002 (A version appears in *Proceedings of the 4th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, October 2000).

**Refereed
conference
publications**

[C12] “CCCP: Secure Remote Storage for Computational RFIDs” by Mastrooreh Salajegheh, Shane Clark, Benjamin Ransford, Kevin Fu, Ari Juels. In *Proceedings of the 18th USENIX Security Symposium*, August 2009 (acceptance rate=26/176=**15%**).

[C11] “Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses” by Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, William H. Maisel. In *Proceedings of the 29th IEEE Symposium on Security and Privacy*, May 2008 (**outstanding paper award**, acceptance rate=28/249= **11.2%**).

[C10] “Maximalist cryptography and computation on the WISP UHF RFID tag” by Hee-Jin Chae, Daniel J. Yeager, Joshua R. Smith, and Kevin Fu. In *Proceedings of the Conference on RFID Security*, July 2007 (acceptance rate=13/26= **50%**).

[C9] “Initial SRAM state as a fingerprint and source of true random numbers for RFID tags” by Daniel E. Holcomb, Wayne P. Burleson, and Kevin Fu. In *Proceedings of the Conference on RFID Security*, July 2007 (acceptance rate=13/26= **50%**).

[C8] “Vulnerabilities in First-Generation RFID-enabled Credit Cards” by Thomas S. Heydt-Benjamin, Daniel V. Bailey, and Kevin Fu, Ari Juels, Tom O’Hare. In the *Proceedings of Eleventh International Conference on Financial Cryptography and Data Security*, February 2007 (acceptance rate=17/84 = **20%**, an extended version appears as University of Massachusetts Amherst, Tech Report 06-055, October 2006).

[C7] “Key Regression: Enabling Efficient Key Distribution for Secure Distributed Storage” by Kevin Fu, Seny Kamara, and Tadayoshi Kohno. In *Proceedings of the 13th Annual Network and Distributed System Security Symposium (NDSS)*, February 2006 (acceptance rate=**13.6%**).

[C6] “Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage” by Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. In *Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS)*, February 2005 (Acceptance rate = 16/124 = **12.9%**, an extended version appears in ACM TISSEC).

[C5] “REX: Secure, Extensible Remote Execution” by Michael Kaminsky, Eric Peterson, Daniel B. Giffin, Kevin Fu, David Mazières, and M. Frans Kaashoek. In *Proceedings of the 2004 USENIX Annual Technical Conference (USENIX)*, June 2004 (acceptance rate = 21/164 = **13%**, An earlier version appears as MIT-LCS Tech Report #884).

[C4] “Plutus: Scalable Secure File Sharing on Untrusted Storage” by Mahesh Kallahalla, Erik Riedel, Ram Swaminathan, Qian Wang, and Kevin Fu. In *Proceedings of the 2nd USENIX Conference on File and Storage Technologies (FAST)*, March 2003 (acceptance rate = 18/67 = **27%**).

[C3] “Dos and Don’ts of Client Authentication on the Web” by Kevin Fu, Emil Sit, Kendra Smith, and Nick Feamster. In *Proceedings of the 10th USENIX Security Symposium*, August 2001 (**best student paper award**, acceptance rate = **28.9%**, an extended version appears as MIT-LCS Tech Report #818).

[C2] “Fast and secure distributed read-only file system” by Kevin Fu, M. Frans Kaashoek, David Mazières. In the *Proceedings of the 4th USENIX Symposium on Operating Systems Design and Implementation (OSDI 2000)*, October 2000 (nominated to ACM TOCS, acceptance rate = 24/111 = **21.6%**).

[C1] “Revocation of Unread Email in an Untrusted Network” by Avi Rubin, Dan Boneh, and Kevin Fu. In *Proceedings of the Australasian Conference on Information Security and Privacy*, Springer-Verlag, LNCS 1270, July 1997.

**Refereed
workshop
publications**

[W6] “Towards Autonomously-Powered CRFIDs” by Shane S. Clark, Jeremy Gummeson, Kevin Fu, Deepak Ganesan. In *Workshop on Power Aware Computing and Systems (HotPower 2009)*, October 2009.

[W5] “Getting Things Done on Computational RFIDs with Energy-Aware Checkpointing and Voltage-Aware Scheduling” by Benjamin Ransford, Shane Clark, Mastooreh Salajegheh, Kevin Fu. In *USENIX Workshop on Power Aware Computing and Systems (HotPower 2008)*, December 2008.

[W4] “Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security” by Tamara Denning, Kevin Fu, and Tadayoshi Kohno. In *USENIX Hot Topics in Security Workshop (HotSec)*, July 2008 (acceptance rate=**32%**).

[W3] “Cryptanalysis of Two Lightweight RFID Authentication Schemes” by Benessa Defend, Kevin Fu, and Ari Juels. In the *Proceedings of Fourth IEEE International Workshop on Pervasive Computing and Communication Security (PerSec) Workshop*, March 2007 (acceptance rate = **29%**).

[W2] “Secure software updates: disappointments and new challenges” by Anthony Bellissimo, John Burgess, and Kevin Fu. In *USENIX Hot Topics in Security Workshop (HotSec)*, July 2006 (acceptance rate=**19.6%**).

[W1] “Privacy for public transportation” by Thomas S. Heydt-Benjamin, Hee-Jin Chae, Benessa Defend, and Kevin Fu. In *6th Workshop on Privacy Enhancing Technologies (PET)*, Lecture Notes in Computer Science, June 2006 (acceptance rate=**26%**).

**Invited
columns**

[Col3] “Inside Risks, Reducing Risks of Implantable Medical Devices: A prescription to improve security and privacy of pervasive health care” by Kevin Fu. Inside Risks Column in *Communications of the ACM (CACM)* 52(6), June 2009.

[Col2] “Using SFS for a Secure Network File System” by Kevin Fu, Michael Kaminsky, and David Mazières. In *login: The USENIX Magazine*, December 2002.

[Col1] “Web Cookies: Not Just a Privacy Risk” by Emil Sit and Kevin Fu. Inside Risks Column in *Communications of the ACM (CACM)* 44(9), September 2001.

**Unrefereed
articles,
demos, and
posters**

[U9] “Privacy of home telemedicine: Encryption is not enough (poster)” by Mastooreh Salajegheh, Andres Molina, Kevin Fu. Presented at *Design of Medical Devices Conference*, Minneapolis, MN, April 2009.

- [U8] “Demonstration of an RFID-enabled espresso machine” by Hee-Jin Chae, Benessa Defend, and Kevin Fu. MIT RFID Academic Convocation, January 2006.
- [U7] “Dos and Don’ts of Client Authentication on the Web” by Kevin Fu, Emil Sit, Kendra Smith, and Nick Feamster. MIT-LCS Tech Report #818. May 2001 (a condensed version appears in USENIX Security 2001).
- [U6] “In Memory of David Huffman.” In *ACM Crossroads Magazine* 6(3), Spring 2000.
- [U5] “RTLinux: An Interview with Victor Yodaiken.” In *ACM Crossroads Magazine* 6(1), Fall 1999.
- [U4] “Linux” (guest editor). In *ACM Crossroads Magazine* 6(1), Fall 1999.
- [U3] “Group Sharing and Random Access in Cryptographic Storage File Systems.” MIT MEng Thesis, May 1999.
- [U2] “Approximate Message Authentication Codes” by Richard Graveman and Kevin Fu. In *Army Research Labs, Advanced Telecommunications & Information Distribution Research Program*, February 1999.
- [U1] “Networks and Distributed Systems” (guest editor). In *ACM Crossroads Magazine* 5(2), Winter 1998.

**Research
funding**

- [G22] NSF Major Research Instrumentation: “MRI: Acquisition of an RFID Testbed Using Renewable Energy for Object Identification and Habitat Monitoring.” \$450,010. Kevin Fu (PI). CoPIs & Sr. Pers.: Charles Ross, Yanlei Diao, Deepak Ganesan, Wayne Burleson, Mark Corner, Prashant Shenoy. NSF CNS Award #0923313. 8/2009–7/2012. Recommended.
- [G21] NSF Cyber Trust, JHU Subcontract: “CT-T Collaborative Research: Security for Smart Tags.” \$50K. Kevin Fu (PI), Wayne Burleson (Co-PI). NSF CNS Award #0627476. 8/2009–7/2010.
- [G20] NSF Cyber Trust travel supplement for collaboration in France and Switzerland: “CT-T Collaborative Research: Security for Smart Tags.” \$15K. Kevin Fu (PI), Wayne Burleson (Co-PI). NSF CNS Award #0935326. 6/2009–8/2010. Recommended.
- [G19] NSF Cyber Trust REU: “CT-ISG: Improving Security and Privacy in Pervasive Healthcare.” \$16K. Kevin Fu (PI). NSF CNS Award #0937762. 6/2009–8/2011.
- [G18] NSF Cyber Trust REU: “CT-T Collaborative Research: Security for Smart Tags.” \$16K. Kevin Fu (PI). NSF CNS Award #0938267. 6/2009–8/2010. Pending.
- [G17] NSF Trustworthy Computing: “CAREER: Computational RFID for Securing Zero-Power Pervasive Devices.” \$400K. Kevin Fu (single PI). NSF CNS Award #. 9/2009–8/2014. Recommended.

- [G16] NSF Cyber Trust REU: “Collaborative Research CT-ISG: New directions and applications of proxy re-cryptography.”
\$16K. Kevin Fu (PI). NSF CNS Award #0716386. 6/2009–8/2010.
- [G15] Alfred P. Sloan Research Fellowship.
\$50K. (<http://www.sloan.org/fellowships/page/19>) 9/2009-8/2011.
- [G14] NSF Cyber Trust: “CT-ISG: Improving Security and Privacy in Pervasive Health-care.” \$449,685. Kevin Fu (single PI). NSF CNS Award #0831244. 9/2008–8/2011.
- [G13] UMass President’s Science & Technology (S&T) Fund
“Integrated Payment Systems: Consortium on Security and Privacy.”
\$125K. PI: Wayne Burleson. Co-PIs: John Collura, Kevin Fu, Marguerite Zarrillo.
8/2008-7/2010.
- [G12] Institute for Information Infrastructure Protection (I3P) at Dartmouth College:
“I3P Scholar Program. Research on securing medical cyberinfrastructure.”
\$90K. Kevin Fu (single PI). Scholar: Shane Clark. 8/2008-8/2009.
- [G11] UMass Commercial Ventures & Intellectual Property (CVIP)
Technology Development Fund Award
“Zero-Power Telemetry for Implantable Medical Devices.”
\$30K. Kevin Fu (single PI). 6/2008-5/2009.
- [G10] NSF Cyber Trust REU: “Collaborative Research CT-T: Security for Smart Tags.”
\$6K. Kevin Fu (PI). NSF CNS Award #0627529. 6/2008–8/2009.
- [G9] Gift from RSA Labs (Security Division of EMC Corporation). \$40K, 3/2008.
- [G8] Institute for Information Infrastructure Protection (I3P) at Dartmouth College:
“Protecting Global Medical Telemetry Infrastructure.”
\$25K. Kevin Fu (single PI). 11/2007-12/2007.
- [G7] NSF Cyber Trust: “Collaborative Research CT-ISG: New directions and applications of proxy re-cryptography.”
\$276,142 (\$62,980 UMass, \$213,163 JHU). Susan Hohenberger (Lead PI), Giuseppe Ate-
niese (JHU co-PI), Kevin Fu (UMass PI). NSF CNS Award #0716386. 9/2007–8/2010.
- [G6] NSF Cyber Trust Supplement for Collaboration in Japan: “Collaborative Research
CT-T: Security for Smart Tags.”
\$40K Kevin Fu (PI). NSF CNS Award #0627529. 9/2007–8/2009.
- [G5] NSF Cyber Trust REU: “Collaborative Research CT-T: Security for Smart Tags.”
\$15K. Kevin Fu (PI). NSF CNS Award #0627529. 6/2007–8/2008.
- [G4] Gift from RSA Labs (Security Division of EMC Corporation). \$10K, 2006–2007.
- [G3] Intel Research Seattle. RFID equipment donation valued at \$7,600 in 2007.
- [G2] ThingMagic. RFID equipment donation valued at \$5,000 in 2007.

**Invited
talks and
panels**

[G1] NSF Cyber Trust: “Collaborative Research CT-T: Security for Smart Tags.” \$1.1 million (\$750K UMass, \$350K JHU). Kevin Fu (Lead PI), Wayne Burleson (co-PI), Adam Stubblefield (JHU PI), Ari Juels (RSA Labs senior personnel). NSF CNS Award #062752. 9/2006–8/2010.

[T33] Invited speaker. “Security and Privacy for Wireless Implantable Devices: Pacing, Defibrillators, and More,” CMOS Workshop, Banff, Canada, 2009.

[T32] Invited speaker. “Energy-aware circuits for RFID,” CMOS Workshop, Banff, Canada, 2009.

[T31] Invited speaker. “Implantable Medical Devices: Security and Privacy for Pervasive, Wireless Healthcare,” University of Massachusetts Amherst, Isenberg School of Management, The Institute for Operations Research and the Management Sciences (INFORMS) Seminar Series, December 2008.

[T30] Invited speaker. “Security Vulnerabilities in Wireless Implantable Medical Devices,” Microsoft Research Redmond, September 2008.

[T29] Invited speaker. “Implantable Medical Devices: Security and Privacy for Pervasive, Wireless Healthcare,” Johns Hopkins University Security Seminar Series, September 2008.

[T28] Invited speaker. “Security Vulnerabilities in Wireless Implantable Medical Devices,” UMass Amherst ECE Security Seminar, September 2008.

[T27] Invited speaker. “Security Vulnerabilities in Wireless Implantable Medical Devices,” Texas Instruments, September 2008.

[T26] Invited co-speaker. “New Classes of Security and Privacy Vulnerabilities for Implantable Wireless Medical Devices,” Black Hat USA Briefings 2008, Las Vegas, August 2008.

[T25] Invited speaker. “Pay on the Go: Consumers & Contactless Payment” Federal Trade Commission Town Hall Meeting, Seattle, July 2008.

[T24] Invited panelist. “Is it Legal?” panel on wireless privacy and security at the ACM/USENIX MobiSys Conference, Denver, June 2008.

[T23] Invited panelist. “RFID Security & Privacy: What’s in Your Pocket?” 8th Payments Conference: Payments Fraud, Perception versus Reality hosted by the Federal Reserve Bank of Chicago, June 2008.

[T22] Invited Speaker. “Maximalist cryptography and computation on the WISP UHF RFID tag,” Intel Research Seattle, January 2008.

[T21] Invited Speaker. “I can see you: RFID — The Next Generation Identity Theft Threat,”

17th Annual International Fraud Investigators Conference hosted by the Toronto Police Service-Fraud Squad, December 2007.

[T20] Invited Speaker. "Security & Privacy for Pervasive Computation: RFID and Implantable Medical Devices,"
EMC Corporation Innovation Conference, Franklin, MA, October 2007.

[T19] Invited Speaker. "RFID Security and Privacy: Fundamental Lessons and Principles,"
19th Workshop on Info. Sec. and Cryptography, Cheonan, Korea, September 2007;
National Security Research Institute, Daejeon, Korea, September 2007;
Korea University, Division of Computer & Comm. Eng., Seoul, Korea, September 2007.

[T18] Invited Panelist. "RFID Privacy,"
MITRE Privacy Technical Exchange, Bethesda, MD, June 2007.

[T17] Invited Speaker. "Data Security Risks: RFID Lab Research,"
Boston Federal Reserve, Emerging Payments Research Group, May 2007.

[T16] Invited Panelist. "Ubiquitous Computing in the Retail Store of the Future,"
17th Annual Computers, Freedom and Privacy Conference, May 2007.

[T15] Invited Panelist and Moderator. "Wireless ID Issues: Privacy, Efficiency and Security,"
Dartmouth College Centers Forum on Freedom and Technology, April 2007.

[T14] Invited Speaker. "Vulnerabilities in First-Generation RFID-Enabled Credit Cards,"
UC Berkeley TRUST seminar, March 2007;
Katholieke Universiteit (KU) Leuven Seminar, Belgium, March 2007.

[T13] Invited Panelist. "RFID: How can privacy and security be built into the technology,"
8th Annual TACD Meeting with EC and US government officials, Brussels, Belgium,
March 2007 (<http://www.tacd.org/events/meeting8/>).

[T12] Panel Moderator. "RFID Security & Privacy Panel,"
Financial Cryptography Conference, Tobago/Trinidad, February 2007.

[T11] Invited Speaker. "Computer System Security and Medical Devices,"
Food and Drug Administration (FDA), Office of Science and Engineering Laboratories,
Center for Devices and Radiological Health, October 2006.

[T10] Invited Speaker. "Building RFID applications with security and privacy,"
Workshop on RFID Security, Graz, Austria, July 2006.

[T9] Invited Panelist. "When public databases cause security vulnerabilities,"
American Association for the Advancement of Science (AAAS), St. Louis, MO, February,
2006.

[T8] Invited Speaker. “Secure content distribution using untrusted servers,” January–April, 2005

Boston University; Dartmouth College; DoCoMo Labs; Florida State University; Georgia Institute of Technology; Intel Research, Pittsburgh; Microsoft Research, Redmond; Microsoft Research, Silicon Valley; Palo Alto Research Center (PARC); Pennsylvania State University; University of Massachusetts Amherst; University of Wisconsin, Madison; University of Michigan; University of Virginia; University of Texas at Austin.

[T7] Invited Speaker. “Dos and Don’ts of Client Authentication on the Web”

Harvard Extension School, Cambridge, MA, April 2006;

MIT Network and Computer Security Class, Cambridge, MA, 2001, 2002, 2004, 2005;

Johns Hopkins Network Security Class, Baltimore, MD, 2003;

Hope College Computer Science Colloquium, Holland, MI, March 3, 2003;

UC San Diego CSE Speakers Series, San Diego, CA, February 10, 2003;

Stanford Security Seminar, Palo Alto, CA, March 18, 2002;

HP Labs Computer Systems Colloquium, Palo Alto, CA, March 18, 2002.

[T6] Invited Speaker. “The Failure of Client Authentication on the Web.” MIT Lincoln Laboratory, Lexington, MA, April 18, 2001.

[T5] Invited Speaker. “Computer Insecurity.” Northeastern University College of Computer Science, Boston, MA, February 26, 2001.

[T4] Instructor. “Concepts in Computer and Network Insecurity” by Roger Dingledine, Andy Ellis, and Kevin Fu. MIT Network Security Team, Cambridge, MA, January 2002.

[T3] “Why on Earth Would Software Engineers Study the Classics?” by Ian Anderson and Kevin Fu. National Junior Classical League, New Orleans, LA, July 19, 2001.

[T2] Instructor. “Concepts in Computer and Network Insecurity” by Roger Dingledine and Kevin Fu. MIT Network Security Team, Cambridge, MA, January 2000 and 2001.

[T1] Instructor. “Practical Security for UNIX” by Kevin Fu, Geoff Goodell, and Angie Kelic. MIT Network Security Team, Cambridge, MA, January 19, 2000.

**Professional
service**

7th ACM Conference on Embedded Networked Sensor Systems Berkeley, CA
SenSys 2009 Program Committee. *November 2009.*

7th ACM/USENIX MobiSys Conference Kraków, Poland
Program Committee. *June 2009.*

30th IEEE Symposium on Security & Privacy Oakland, CA
Program Committee. *May 2009.*

Institute for Information Infrastructure Protection (I3P) Hanover, NH
UMass Amherst representative. *July 2007–.*

RFID Security Conference/Workshop (RFIDSec) Europe
Steering Group Member. *September 2007–.*

K. Fu (10/14)

29th IEEE Symposium on Security & Privacy Program Committee. <i>May 2008.</i>	Oakland, CA
12th International Conference on Financial Cryptography and Data Security Program Committee. <i>January 2008.</i>	Cozumel, Mexico
16th USENIX Security Symposium Program Committee. <i>August 2007.</i>	Boston, MA
5th International Conference on Applied Cryptography and Network Security (ACNS) Program Committee. <i>June 2007.</i>	Zhuhai, China
Security, Privacy, Reliability and Ethics Track 16th World Wide Web Conference Program Committee. <i>May 2007.</i>	Banff, Canada
27th IEEE Symposium on Security & Privacy Program Committee. <i>May 2006.</i>	Oakland, CA
Security, Privacy, and Ethics Track, 15th World Wide Web Conference Program Committee. <i>May 2006.</i>	Edinburgh, Scotland
Network & Distributed System Security Symposium Program Committee. <i>February 2006.</i>	San Diego, CA
3rd IEEE International Security in Storage Workshop (SISW) Program Committee. <i>December 2005.</i>	San Francisco, CA
The Storage Security and Survivability (StorageSS) Workshop Program Committee. <i>November 2005.</i>	Fairfax, VA
Network & Distributed System Security Symposium Program Committee. <i>February 2004.</i>	San Diego, CA
12th USENIX Security Symposium Program Committee. Works-in-Progress Chair. <i>August 2003.</i>	Washington, D.C.
Security and Privacy Track, 12th International World Wide Web Conference Program Committee. <i>May 2003.</i>	Budapest, Hungary
11th USENIX Security Symposium Program Committee. Works-in-Progress Chair. <i>August 2002.</i>	San Francisco, CA

**Patent
issued**

“Method and system for relating cryptographic keys” by Kevin Fu, Mahesh Kallahalla, Ram Swaminathan. Patent #7,313,238. Hewlett-Packard Labs. Filed 2003. Issued 2007.

K. Fu (11/14)

Patent filed “Windowed backward key rotation” by Kevin Fu, Mahesh Kallahalla, Ram Swaminathan. Hewlett-Packard Labs. Filed 2003.

Degrees conferred **Masters of Science (advisor role)**
Hee-Jin Chae (2007), Benessa Defend (2008), Thomas S. Heydt-Benjamin (2007), Robert Lychev (2008).

Current students **PhD track (advisor role)**
Shane Clark, Benessa Defend, Andres Molina, Benjamin Ransford, Mastooreh Salajegheh.

Masters track (advisor role)
None.

Thesis committees outside CS department (member role)
Daniel Holcomb (ECE, masters 2007), Lang Lin (ECE, masters in-progress), Penny Ridgill (Math, PhD in-progress), Weifeng Xu (ECE, PhD 2007), Serge Zhilyaev (ECE, masters-in-progress).

Thesis committees within CS department (member role)
None.

Undergrad Research (supervisor role)
John Brattin (CS, 2009), Shane Clark (CS, 2006-07), David Eiselen (ECE, 2007), Jean Fredo Louis (REU, 2008), William Morgan (CS, 2007), Rene Santiago (ECE, 2007), Deepti Sreepathi (microbiology, 2009), John Tuttle (CS, 2008), Zak Wirima (REU, 2008), Mankin Yuen (CS, 2008).

Non-REU Independent Study (supervisor role)
Timur Alperovich (CS, 2006-07), Robert Lychev (CS, 2005-07), Justin Katsugi (EE, 2007), Russell Silva (CS, 2006), Anthony Swochak (ECE, 2007).

Teaching **Architecture & Assembly Language (cs201, 4 credits)**
Spring 2009. Instructor. An introduction to the architecture and machine-level operations of modern computers at the logic, component, and system levels.

Applied Cryptography (cs591d, 3 credits)
Spring 2008, 2007, 2006. Instructor. I designed this course to teach upper-level undergraduates both the foundations of applied cryptography and the humility of building practical systems that rely on cryptography.

RFID Electronic Identification Lab (cs291e, 1 credit)
Fall 2007. Instructor. I designed this first offering of the RFID lab to teach sophomores about hands-on problem solving in the context of RFID.

Advanced Information Assurance (cs615/691cc, 3 credits)
Fall 2007, instructor; Fall 2006, co-instructor. This course teaches beginning graduate students the material necessary to make a research contribution to the field of information assurance.

Hot Topics in Information Security (cs691i, 1 credit)

Fall 2007, instructor; Fall 2005, co-instructor. This seminar covers cutting-edge papers to identify novel research problems in security.

First-Year TAP Seminar (cs191a, 1 credit)

Fall 2006, co-organizer. This seminar introduces first-year undergraduates to major topics in Computer Science. Each week there is a new guest lecturer.

RFID Security and Privacy (1 day)

USENIX Security Tutorial by Kevin Fu, Ari Juels, and Adam Stubblefield. Vancouver, Canada, August 2006. 20 students.

RFID Security Summer School (1 lecture)

“Special topics in RFID security,” Technical University of Graz, Austria, July 2006. ~75 German/Austrian students.

MIT’s Network and Computer Security (6.857)

Head TA and guest lecturer (Fall 2001, Fall 2002).

MIT’s Computer System Engineering Lab (6.906)

Lab TA (Spring 1998, Spring 1999).

MIT’s Computer System Engineering (6.033)

TA (Spring 1998), Head TA (Spring 1999).

MIT’s Introduction to the Theory of Computation (6.840)

Grader (Fall 1998).

Departmental service

Awards Committee, 2009–2010; Distinguished Lecture Series (DLS)/Special Events Chair, 2008–2009; ECE Senior Faculty Search Committee, 2008–2009; Personnel Committee, 2007–2008; Graduate Program Committee, 2007–2009; Admissions Committee, 2006–2007, 2009–2010; Computing Committee, 2005–2007; Recruiting Committee, 2005–2006.

Other service

Ad hoc reviewer

ACM Transactions on Information and System Security (TISSEC); IEEE/ACM Transactions on Networking (TON); ACM Transactions on Sensor Networks (TOSN); ACM Transactions on Computer Systems (TOCS); NordSec; IEEE Security & Privacy Magazine; IEEE Internet Computing; International Conference on Distributed Computing Systems (ICDCS); International Workshop on Information Security Applications (WISA); USENIX Annual Technical Conference; Symposium on Operating Systems Principles (SOSP); USENIX Conference on File and Storage Technologies (FAST); International Workshop on Peer-to-Peer Systems (IPTPS); Workshop on Hot Topics in Operating Systems (HotOS); Symposium on Operating Systems Design and Implementation (OSDI).

Graduate Resident Tutor — MIT Residential Life

Burton-Conner

As a live-in “life” tutor for 30 undergraduates, I facilitated conflict resolution, off-campus retreats, medical emergencies, and culinary productions. 2000–2003.

Academic Advising — MIT Department of EECS

Cambridge, MA

As an associate academic advisor, I helped undergraduates develop their four-year academic plans. I co-advised with Alex d'Arbeloff, MIT Chairman of the Corporation. 1999–2003.

Association of Computing Machinery

New York, NY

General editor and contributor to the *ACM Crossroads Magazine*. 1998–2000

(<http://www.acm.org/crossroads/>).

French Culinary Institute

New York, NY

Received certificate of achievement in artisanal bread making while producing the bread for the student-run L'Ecole restaurant. *June 2004*.

Culinary Institute of America

Hyde Park, NY

Received certificate of achievement in basic culinary practice. *August 2003*.

**Selected
media
coverage**

“A Heart Device Is Found Vulnerable to Hacker Attacks” by Barnaby J. Feder. In *The New York Times*, Business Section, Mar 12, 2008.

“Heart-Device Hacking Risks Seen” by Keith J. Winstein. In *The Wall Street Journal*, March 12, 2008.

“Questions on Credit Card Safety” by John Schwartz. In *The New York Times*, Business Section, Page B1, October 23, 2006.

“Smart cards are quick, but are they safe?” In *NBC Today Show*, October 26, 2006.

“No-Swipe Credit Cards Could Make ID Theft Easier.” In *ABC Good Morning America*, October 24, 2006.

“Portals: More Scary Tales Involving Big Holes in Web-site Security” by Lee Gomes. In *The Wall Street Journal* CCXLII(22):B1, February 2, 2004.

“Portals: Biggest Web problem Isn't about Privacy, It's Sloppy Security” by Lee Gomes. In *The Wall Street Journal* CCXLII(17):B1, January 26, 2004.

“What's the Password? Hackers May Already Know.” In *BusinessWeek Magazine*, November 15, 1999.