Karl Koscher

4174 3rd Ave #27
San Diego, CA 92103

(814) 422 5488
kkoscher@cs.ucsd.edu

Education

University of Washington, Ph.D. Computer Science, September 2014.
Dissertation Title: "Securing Embedded Systems: Analyses of Modern
Automotive Systems and Enabling Near-Real Time Dynamic Analysis"

University of Washington, M.S. Computer Science, March 2009.

University of Washington, B.S. Computer Engineering, June 2006.

Publications

Koscher, K., Kohno, T., Molnar, D. "SURROGATES: Enabling Near-Real-Time
Dynamic Analyses of Embedded Systems." In the Proceedings of 9th Workshop
on Offensive Technologies (WOOT '15).

Foster, I., Prudhomme, A., Koscher, K., Savage, S. "Fast and Vulnerable: A
Story of Telematics Failures." In the Proceedings of 9th Workshop on Offensive
Technologies (WOOT '15).

Ernst, M. D., Just, R., Millstein, S., Dietl, W., Pernsteiner, S., Roesner, F.,
Koscher, K., Barros, P., Bhoraskar, R., Han, S., Vines, P., Wu, E. X.
"Collaborative Verification of Information Flow for a High-Assurance App
Store." In the Proceedings of the 21st ACM Conference on Computer and
Communications Security (CCS '14).

Koscher, K. "Securing Embedded Systems: Analyses of Modern Automotive
Systems and Enabling Near-Real Time Dynamic Analysis." Doctoral
Dissertation, University of Washington, 2014.

Czeskis, A., Mah, D., Sandoval, O., Smith, I., Koscher, K., Appelbaum, J.,
Kohno, T., Schneier, B. "DeadDrop/StrongBox Security Assessment". UW
CSE Tech Report 13-08-02.

Appelbaum, J., Ray, M., Koscher, K., Finder, I. "vpwns: Virtual Pwned
Networks." In the Proceedings of the 2nd USENIX Workshop on Free and
Open Communications on the Internet (FOCI '12).

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S.,
Koscher, K., Czeskis, A., Roesner, F., Kohno, T. "Comprehensive Experimental
Analyses of Automotive Attack Surfaces." In the Proceedings of the 20th Usenix
Security Symposium (USENIX Security '11).

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S.,
McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S. "Experimental
Security Analysis of a Modern Automobile." In the Proceedings of 31st IEEE
Symposium on Security and Privacy (Oakland '10).

Matuszek, C., Fox, D., Koscher, K. "Following Directions Using Statistical
Machine Translation." In the Proceedings of the 5th ACM/IEEE International
Conference on Human-Robot Interaction (HRI '10).

Koscher, K., Juels, A., Brajkovic, V., Kohno, T. "EPC RFID Tag Security
Weaknesses and Defenses: Passport Cards, Enhanced Drivers Licenses, and
Beyond." In the Proceedings of the 16th ACM Conference on Computer and
Communications Security (CCS '09).

Publications (continued)	Denning, T., Matuszek, C., Koscher, K., Smith, J. R., Kohno, T. "A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons." In the Proceedings of the 11th International Conference on Ubiquitous Computing (UbiComp '09).
	Welbourne, E., Koscher, K., Soroush, E., Balazinska, M., Borriello, G. "Study of a Building-Wide Passive RFID Deployment." In the Proceedings of The 7th Annual International Conference on Mobile Systems, Applications and Services (MobiSys '09).
	Czeskis, A., Koscher, K., Friedman, F., Kohno, T. "The International Criminal Tribunal for Rwanda Information Heritage Project (aka Voices of the Rwanda Tribunal): Integrity Verification Architecture." UW CSE Tech Report 09-01-02.
	Koscher, K., Juels, A., Kohno, T., Brajkovic, V. "EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licneses, and Beyond." UW CSE Tech Report 08-10-02.
	Czeskis, A., Koscher, K., Smith, J. R., Kohno, T. "RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads Through Context-Aware Communications." In the Proceedings of the 15th ACM Conference on Computer and Communications Security, October 2008.
	Czeskis, A., St. Hilaire, D., Koscher, K., Gribble, S., Kohno, T., Schneier, B. "Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications." In the Proceedings of the 3rd USENIX Workshop on Hot Topics in Security, July 2008.
	Choudhury, T., et. al. "The Mobile Sensing Platform: An Embedded System for Capturing and Recognizing Human Activities." IEEE Pervasive Computing, April 2008.
	Borriello, G., Hartung, C., Hemingway, B. Koscher, K., Mayton, B. "Multi-player Soccer and Wireless Embedded Systems." In proceedings of the 39th ACM Technical Symposium on Computer Science Education, March 2008.
	Andrew, A. Anokwa, Y., Koscher, K., Lester, J., Boriello, G. "Context to Make Your More Aware." Proceedings of the 27th International Conference on Distributed Computing Systems Workshops, June 2007.
Patents	Kohno, T., Czeskis, A., Koscher, K., Smith, J. R. "Radio frequency identification secret handshakes." US Patent 8,643,475. Issued Feb 4, 2014.
Professional Experience	**Postdoctoral Scholar** (September 2014–Present) UC San Diego, San Diego, CA Supervisors: Stefan Savage and Kirill Levchenko

- Investigated the security properties of high-assurance cyber-physical systems
- Investigated techniques to automatically discover security vulnerabilities in complex embedded systems
- Mentored students working on a variety of systems and security projects

Software Engineering Intern (September 2011–December 2011)
Google, Seattle, WA
Supervisor: Charlie Reis

- Improved Chrome's security and stability by implementing cross-process JavaScript calls and messages, significantly simplifying Chrome's multi-process model

Professional Experience (continued)

Software Engineering Intern (June 2010–September 2010)
Google, Seattle, WA
Supervisor: Charlie Reis

- Built a research prototype of a system that allows web developers to safely incorporate untrusted third-party code

Research/Teaching Assistant (September 2007–September 2014)
University of Washington, Seattle, WA
Supervisors: Tadayoshi Kohno and Gaetano Borriello

- Supported embedded systems used in various ubiquitous computing projects
- Investigated the feasibility of using passive RFID tags with sensing and computing capabilities to enhance security
- Investigated the implications of using EPC Gen2 RFID tags in security applications and the feasibility of improving Gen2 security
- Developed a framework for ensuring the integrity of a corpus of video interviews over multiple lifespans
- Experimentally analyzed the security of modern car computers and networks
- Developed tools to enable dynamic analysis of complex embedded systems
- Assisted students with their assignments
- Developed new assignments
- Graded assignments

Research Engineer (June 2006–September 2007)
University of Washington, Seattle, WA
Supervisor: Gaetano Borriello

- Contributed to the design of new labs and hardware platform for an embedded systems class
- Developed Linux drivers for the new hardware platform
- Developed and maintained firmware for mobile sensors boards
- Developed and conducted experiments on RFID system performance
- Coordinated the deployment of a pervasive RFID system
- Contributed to the design and implementation of a wearable system that provides opportunistic suggestions to increase physical activity

Teaching Assistant (April 2006–June 2006)
University of Washington, Seattle, WA
Supervisor: Bruce Hemingway
Course: Software for Embedded Systems (CSE 466)

- Assisted students with their lab assignments
- Graded lab assignments
- Updated lab assignments, developing associated software as needed
- Maintained course web site

Student Lab Assistant (September 2005–June 2006)
University of Washington, Seattle, WA
Supervisor: Bruce Hemingway

- Assisted students with their lab assignments
- Diagnosed and repaired problems with lab hardware
- Developed applications to facilitate lab administration

Professional Experience (continued)	**Research Assistant** (June 2005–September 2005) University of Washington, Seattle, WA Supervisor: Zoran Popović ▪ Contributed to the development and evaluation of three-dimensional visualizations of urban development simulation data, and games based on an urban development simulator ▪ Integrated GIS data ▪ Provided assistance to others in solving difficult bugs
Honors	▪ UW Engineering Ford Motor Company Fellowship, 2011-2012 ▪ UW CSE Industrial Affiliates People's Choice Award, 2010 ▪ NSF Graduate Research Fellowship Program, Honorable Mention, 2009
Invited Talks	▪ Miller, C., Koscher, K.. "Hacking Cars." Invited talk at the 2014 r00tz Asylum conference (formerly known as DEFCON Kids). ▪ Koscher, K. "Comprehensive Security Analysis of a Modern Automobile." Lecture at the Battelle CyberAuto Challenge 2014. ▪ Koscher, K. "Comprehensive Security Analysis of a Modern Automobile." Invited talk at the 2013 Northwest Regional Women in Computing conference ▪ Koscher, K. "Comprehensive Security Analysis of a Modern Automobile." Lecture at the Battelle CyberAuto Challenge 2013. ▪ Koscher, K., Czeskis, A. "Comprehensive Security Analysis of a Modern Automobile." Lecture at the ECRYPT Summer School: Challenges in Security Engineering 2012. ▪ Checkoway, S., Koscher, K. "Comprehensive Security Analysis of a Modern Automobile." Keynote at the 6th Workshop on Embedded Systems Security (WESS '11). ▪ Clement, A., Koscher, K., Hasbrouck, E., Calabrese, C. "Border-line ID: 'Enhancing' the drivers license - for security or surveillance?" Panel at Computers, Freedom, and Privacy Conference, 2009
Other Talks	▪ Koscher, K. "Shattring Your Secrets: Coercion-Resistant Full Disk Encryption and More!" ToorCon 2014. ▪ Koscher, K., Butler, E. "The Secret Life of SIM Cards." DEFCON 2013. ▪ Kohno, K., Callas, J., Czeskis, A., Halperin, D., Koscher, K., Piatek, M. "Hacking in the Name of Science." Panel at DEFCON 2008.
Posters and Demos	▪ "A Spotlight on Security and Privacy for Future Household Robots: Attacks, Lessons, and Framework". USENIX Security Symposium 2009. ▪ Enhanced Drivers License/RFID demonstration. The 9th Privacy Enhancing Technologies Symposium, 2009. ▪ "RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications." USENIX Security Symposium 2008.
Teaching	▪ Undergrad Computer Security (Winter 2008, Winter 2011) ▪ Professional Masters Computer Security (Spring 2010) ▪ Graduate Computer Security (Autumn 2008) ▪ Society and Technology Seminar (Spring 2007) ▪ Embedded Systems (Spring 2006) ▪ Introduction to Digital Design (Autumn 2005, Winter 2006, Spring 2006)
Professional Activities & Service	**Program Committees:** ▪ The 1st Cyber-Physical System Security Workshop (CPSS '15) ▪ The 7th USENIX Workshop on Offensive Technologies (WOOT '13)

Professional Activities & Service (continued)

External Reviews:

- 23rd USENIX Security Symposium (USENIX Security '14)
- 35th IEEE Symposium on Security and Privacy (Oakland '14)
- 7th USENIX Workshop on Offensive Technologies (WOOT '13)
- 32nd IEEE Symposium on Security and Privacy (Oakland '11)
- 17th ACM Conference on Computer and Communications Security (CCS '10)
- 16th ACM Conference on Computer and Communications Security (CCS '09)
- 15th ACM Conference on Computer and Communications Security (CCS '08)
- The 29th IEEE Symposium on Security and Privacy (Oakland '08)

Outreach:

- Public Talk: "Computer Security and the Modern Car." Science on Tap, Seattle, WA, September 2012.
- High School Visits: Tahoma High School, Covington, WA, May 2012, Roosevelt High School, Seattle, WA, October 2010.
- UW Computer Science Summer Camp Presentations: 2012, 2013, 2014
- UW Computer Science and Engineering Open House: 2012, 2013
- UW College of Engineering Open House/Discovery Days: 2005, 2006, 2007

Other:

- UW CSE Prospective Student Committee: 2008–2014
- UW CSE New Graduate Student Mentor: 2008, 2009, 2012, 2013

Press Coverage

- "DARPA Dan." 60 Minutes, CBS. February 8, 2015.
- "Im Visier der Hacker - Wie gefährlich wird das Netz?" NDR. July 14, 2014.
- "What Happens At Def Con Stays With Us All." TechCrunch. August 4, 2013.
- "Smart card: What your ORCA never forgets." Crosscut. February 13, 2013.
- "This clever hack allows you to add MIDI files of your choice to the Moog Google doodle." TheNextWeb. May 25, 2012.
- "Taking Credit: Identity Theft in the Electronic Age." 16:9 The Bigger Picture, Global News. January 23, 2011.
- "Taking Over a Car." Technology Review. September 2010.
- "Cars' Computer Systems Called at Risk to Hackers." The New York Times. May 14, 2010.
- "Hacking Automotive Systems." Slashdot. May 14, 2010.
- "Car Hackers Can Kill Brakes, Engine, and More." PC World. May 13, 2010.
- "What happens when good robots go 'bad'?" MSNBC. November 5, 2009.
- "How Dangerous Could a Hacked Robot Possibly Be?" The New York Times/IDG. October 8, 2009.
- "The Dangers of Rogue Household Robots." Popular Science. October 8, 2009.
- "UW researchers: Border crossing cards are flawed." KING TV. August 15, 2009.
- "A Tool to Verify Digital Records, Even as Technology Shifts." The New York Times. January 26, 2009.
- "Borderline Security." Technology Review. October 31, 2008.
- "Researchers Find Problems With RFID Passport Cards." Slashdot. October 24, 2008.
- "Border-Crossing Cards Can Be Copied." The Wall Street Journal. October 23, 2008.
- "Researchers find problems with RFID passport cards." The New York Times/IDG. October 23, 2008.
- "UW researchers uncover gap in border security." KOMO TV. October 23, 2008.

Selected Courses

- Computer Graphics
- Compiler Construction
- Operating Systems
- Artificial Intelligence
- Software for Embedded Systems
- Networks
- Data Mining
- Statistical Methods
- Computer Vision
- Technology and Society
- Data Compression
- Theory of Computation
- Robotics
- Security
- Algorithms
- HCI