Urs Hengartner

David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1

Phone: 519-888-4567 x36163
urs.hengartner@uwaterloo.ca
http://www.cs.uwaterloo.ca/~uhengart

Research Interests

My research interests are in information privacy and in computer and networks security. My focus is on security and privacy challenges that arise in the context of smartphones and mobile applications. My students and I develop privacy-preserving solutions for location-based services and mobile social-networking applications that do not require smartphones to continuously release information about their owner to application providers. We also study implicit authentication schemes for smartphones, where a smartphone continuously authenticates its owner based on the owner's behaviour without requiring deliberate actions by the owner. I have also worked on privacy-preserving location verification technologies, genomic privacy, and end-to-end voter-verifiable voting systems.

Education

Ph.D. in Computer Science, Carnegie Mellon University, August 2005.
Thesis: Access Control to Information in Pervasive Computing Environments
Advisor: Peter Steenkiste

M.S. in Computer Science, Carnegie Mellon University, Fall 2003.

Dipl. Informatik-Ing. ETH, ETH Zürich, August 1997.
Thesis: End-to-End Congestion Control
Supervisor: Thomas Gross

Publications

Journals

Kelly Grindrod, Hassan Khan, Urs Hengartner, Stephanie Ong, Alexander G. Logan, Daniel Vogel, Robert Gebotys, and Jilan Yang, "Evaluating authentication options for mobile health applications in younger and older adults". *PLoS One 2018*, (Jan 4, 2018).

Aleksander Essex and Urs Hengartner, "Hover: Trustworthy Elections with Hash-only Verification". *IEEE Security & Privacy*, 10 (5), September–October 2012, pp. 18–24.

Richard Thompson Ainsworth and Urs Hengartner, "Quebec's Module d'Enregistrement des Vents (MEV): Fighting the Zapper, Phantomware and Tax Fraud with Technology". *Canadian Tax Journal*, 57(4), December 2009, pp. 715–761.

Urs Hengartner and Peter Steenkiste, "Avoiding Privacy Violations Caused by Context-Sensitive Services". *Pervasive and Mobile Computing*, PerCom 2006 special issue, 2(4), November 2006, pp. 427–452.

Urs Hengartner and Peter Steenkiste, "Exploiting Information Relationships for Access Control in Pervasive Computing". *Pervasive and Mobile Computing*, 2(3), September 2006, pp. 344–367.

Urs Hengartner and Peter Steenkiste, "Access Control to People Location Information". *ACM Transactions on Information and System Security (TISSEC)*, 8(4), November 2005, pp. 424–456.

Refereed Conferences/Workshops

Hassan Khan, Urs Hengartner, and Daniel Vogel. Augmented Reality-based and Audiovisual Mimicry Attacks on Keystroke Authentication on Smartphones. Proc. of *16th ACM International Conference on Mobile Systems, Applications and Services (MobiSys 2018)*, Munich, Germany, June 2018, pp. 41-53.

Hassan Khan, Urs Hengartner, and Daniel Vogel. Evaluating Attack and Defense Strategies for Smartphone PIN Shoulder Surfing. Proc. of *ACM CHI Conference on Human Factors in Computing Systems (CHI 2018)*, Montreal, QC, Canada, April 2018.

Erinn Atwater, Cecylia Bocovic, Ian Goldberg, and Urs Hengartner. Netsim: Network simulation and hacking for high schoolers. Proc. of *2017 USENIX Workshop on Advances in Security Education (ASE '17)*, Vancouver, BC, Canada, August 2017.

Berker Agir, Kevin Huguenin, Urs Hengartner, and Jean-Pierre Hubaux. "On the Privacy Implications of Location Semantics". Proc. of *16th Privacy Enhancing Technologies Symposium (PETS 2016)*, Darmstadt, Germany, July 2016.

Erinn Atwater and Urs Hengartner. "Shatter: Using Threshold Cryptography to Protect Single Users with Multiple Devices". Proc. of *9th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec 2016)*, Darmstadt, Germany, July 2016, pp. 91–102.

Hassan Khan, Urs Hengartner, and Dan Vogel. "Targeted Mimicry Attacks on Touch Input Based Implicit Authentication Schemes". Proc. of *14th International Conference on Mobile Systems, Applications and Services (MobiSys 2016)*, Singapore, June 2016, pp. 387–398.

Lalit Agarwal, Hassan Khan, and Urs Hengartner. "Ask Me Again But Don't Annoy Me: Evaluating Re-authentication Strategies for Smartphones". Proc. of *12th Symposium on Usable Privacy and Security (SOUPS 2016)*, Denver, CO, June 2016, pp. 221–236.

Hassan Khan, Kelly Grindrod, Urs Hengartner, and Dan Vogel. "Poster: Evaluating Smartphone Authentication Schemes with Older Adults". Proc. of *12th Symposium on Usable Privacy and Security (SOUPS 2016)*, Denver, CO, June 2016.

Yihang Song and Urs Hengartner, "PrivacyGuard: A VPN-based Platform to Detect Information Leakage on Android Devices". Proc. of *5th Annual CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM 2015)*, Denver, CO, October 2015, pp. 15–26.

Hassan Khan, Urs Hengartner, and Dan Vogel, "Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying". Proc. of *11th Symposium On Usable Privacy and Security (SOUPS 2015)*, Ottawa, ON, July 2015, pp. 225–239.

Erinn Atwater, Cecyila Bocovich, Urs Hengartner, Ed Lank, and Ian Goldberg, "Leading Johnny to Water: Designing for Usability and Trust". Proc. of *11th Symposium On Usable Privacy and Security (SOUPS 2015)*,

Ottawa, ON, July 2015. pp. 69–88.

Hassan Khan, Aaron Atwater and Urs Hengartner, "A Comparative Evaluation of Implicit Authentication Schemes". Proc. of *17th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2014)*, Gothenburg, Sweden, September 2014, pp. 255–275.

Hassan Khan, Aaron Atwater and Urs Hengartner, "Itus: An Implicit Authentication Framework for Android", Proc. of *20th Annual International Conference on Mobile Computing and Networking (MobiCom 2014)*, Maui, HI, September 2014, pp. 507–518.

Bisheng Liu and Urs Hengartner, "pTwitterRec: A Privacy-Preserving Personalized Tweet Recommendation Framework", Proc of *9th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2014)*, Kyoto, Japan, June 2014, pp. 365–376.

Yihang Song, Madhur Kukreti, Rahul Rawat and Urs Hengartner, "Two Novel Defenses against Motion-Based Keystroke Inference Attacks", *IEEE Mobile Security Technologies workshop (MoST 2014)*, San Jose, CA, May 2014.

Hassan Khan and Urs Hengartner, "Towards Application-Centric Implicit Authentication on Smartphones", Proc. of *15th Workshop on Mobile Computing Systems and Applications (ACM HotMobile 2014)*, Santa Barbara, CA, February 2014.

Erman Ayday, Jean Louis Raisaro, Urs Hengartner, Adam Molyneaux, and Jean-Pierre Hubaux, "Privacy-Preserving Processing of Raw Genomic Data", *Proc. of 8th International Workshop on Data Privacy Management (DPM 2013)*, Egham, United Kingdom, September 2013, pp. 133–147.

Bisheng Liu and Urs Hengartner, "Privacy-preserving Social Recommendations in Geosocial Networks". *Proc. of 11th Annual Conference on Privacy, Security and Trust (PST2013)*, Tarragona, Catalonia, July 2013, pp. 69–76.

Sarah Pidcock and Urs Hengartner, "Zerosquare: A Privacy-Friendly Location Hub for Geosocial Applications". *IEEE Mobile Security Technologies workshop (MoST 2013)*, San Francisco, CA, May 2013.

Aleksander Essex, Jeremy Clark, and Urs Hengartner, "Cobra: Toward Concurrent Ballot Authorization for Internet Voting". *2012 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '12)*, Bellevue, WA, August 2012.

Aleksander Essex and Urs Hengartner, "Oblivious Printing of Secret Messages in a Multi-party Setting." *Proc. of 16th Conference on Financial Cryptography and Data Security (FC 2012)*, Bonaire, February/March 2012, pp. 359–373.

Sarah Pidcock, Rob Smits, Urs Hengartner, and Ian Goldberg, "NotiSense: An Urban Sensing Notification System To Improve Bystander Privacy". *2nd International Workshop on Sensing Applications on Mobile Phones (PhoneSense 2011)*, Seattle, WA, November 2011.

Rob Smits, Sarah Pidcock, Divam Jain, Ian Goldberg, and Urs Hengartner, "BridgeSPA: Improving Tor Bridges with Single Packet Authorization". *Proc. of 10th Workshop on Privacy in the Electronic Society (WPES 2011)*, Chicago, IL, October 2011, pp. 93–101.

Aleksander Essex, Christian Henrich, and Urs Hengartner, "Single Layer Optical-scan Voting with Fully Distributed Trust". *Proc. of 3rd International Conference on E-voting and Identity (VoteID 2011)*, Tallinn, Estonia,

September 2011, pp. 122–139.

Prima Chairunnanda, Nam Pham, and Urs Hengartner, "Privacy: Gone with the Typing! Identifying Web Users by Their Typing Pattern". *4th Hot Topics in Privacy Enhancing Technologies (HotPETs 2011)*, Waterloo, ON, July 2011.

Qi Xie and Urs Hengartner, "Privacy-Preserving Matchmaking for Mobile Social Networking Secure Against Malicious Users". *Proc. of 9th Annual Conference on Privacy, Security and Trust (PST2011)*, Montreal, QC, July 2011, pp. 252–259.

Jeremy Clark and Urs Hengartner, "Selections: An Internet Voting System with Over-the-Shoulder Coercion-Resistance". *Proc. of 15th Conference on Financial Cryptography and Data Security (FC 2011)*, Saint Lucia, February/March 2011, pp. 47–61.

Wanying Luo and Urs Hengartner, "VeriPlace: A Privacy-Aware Location Proof Architecture". *Proc. of 18th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (ACM SIGSPATIAL GIS 2010)*, San Jose, CA, November 2010, pp. 23–32.

Aleksander Essex, Jeremy Clark, Urs Hengartner, and Carlisle Adams, "Eperio: Mitigating Technical Complexity in Cryptographic Election Verification". *2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '10)*, Washington, DC, August 2010.

Jeremy Clark and Urs Hengartner, "On the Use of Financial Data as a Random Beacon". *2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '10)*, Washington, DC, August 2010.

Femi Olumofin, Piotr K. Tysowski, Ian Goldberg, and Urs Hengartner, "Achieving Efficient Query Privacy for Location Based Services". *Proc. of 10th Privacy Enhancing Technologies Symposium (PETS 2010)*, Berlin, Germany, July 2010, pp. 93–110.

Wanying Luo and Urs Hengartner, "Proving Your Location Without Giving up Your Privacy". *Proc. of 11th Workshop on Mobile Computing Systems and Applications (HotMobile 2010)*, Annapolis, MD, February 2010, pp. 7–12.

Jeremy Clark, Urs Hengartner, and Kate Larson, "Not-So Hidden Information: Optimal Contracts for Undue Influence in E2E Voting". *Proc. of 2nd International Conference on E-voting and Identity (Vote-ID 2009)*, Luxembourg, September 2009, pp. 1–17.

Wanying Luo, Qi Xie, and Urs Hengartner, "FaceCloak: An Architecture for User Privacy on Social Networking Sites". *Proc. of 2009 IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT-09)*, Vancouver, BC, August 2009, pp. 26–33.

Aleks Essex, Jeremy Clark, Urs Hengartner, and Carlisle Adams, "How to Print a Secret". *Proc. of 4th USENIX Workshop on Hot Topics in Security (HotSec 2009)*, Montreal, QC, August 2009.

Ge Zhong and Urs Hengartner, "A Distributed k-Anonymity Protocol for Location Privacy". *Proc. of 7th IEEE International Conference on Pervasive Computing and Communication (PerCom 2009)*, Galveston, TX, March 2009, pp. 253–262.

Ge Zhong and Urs Hengartner, "Toward a Distributed k-Anonymity Protocol for Location Privacy". *Proc. of*

7th Workshop on Privacy in the Electronic Society (WPES 2008), Alexandria, VA, October 2008, pp. 33–37.

Urs Hengartner, "Location Privacy based on Trusted Computing and Secure Logging". *Proc. of 4th International Conference on Security and Privacy in Communication Networks (SecureComm 2008)*, Istanbul, Turkey, September 2008.

Sumair Ur Rahman, Urs Hengartner, Usman Ismail, and S. Keshav, "Practical Security for Rural Internet Kiosks". *Proc. of 2nd ACM SIGCOMM Workshop on Networked Systems for Developing Regions (NSDR 2008)*, Seattle, WA, August 2008, pp. 13–18.

Jeremy Clark and Urs Hengartner, "Panic Passwords: Authenticating under Duress". *Proc. of 3rd USENIX Workshop on Hot Topics in Security (HotSec 2008)*, San Jose, CA, July 2008.

Aniket Kate, Greg Zaverucha, and Urs Hengartner, "Anonymity and Security in Delay Tolerant Networks", *Proc. of 3rd International Conference on Security and Privacy in Communication Networks (SecureComm 2007)*, Nice, France, September 2007.

Sumair Ur Rahman and Urs Hengartner, "Secure Crash Reporting in Vehicular Ad hoc Networks". *Proc. of 3rd International Conference on Security and Privacy in Communication Networks (SecureComm 2007)*, Nice, France, September 2007.

Allan Caine and Urs Hengartner, "The AI Hardness of CAPTCHAs does not imply Robust Network Security". *Proc. of Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM 2007)*, Moncton, NB, July/August 2007, pp. 367–382.

Ge Zhong, Ian Goldberg, and Urs Hengartner, "Louis, Lester and Pierre: Three Protocols for Location Privacy". *Proc. of 7th Privacy Enhancing Technologies Symposium (PETS 2007)*, Ottawa, ON, June 2007, pp. 62–76.

Urs Hengartner, "Hiding Location Information from Location-Based Services". *Proc. of International Workshop on Privacy-Aware Location-based Mobile Services (PALMS)*, Mannheim, Germany, May 2007, pp. 268–272.

Urs Hengartner and Ge Zhong, "Distributed, Uncertainty-Aware Access Control for Pervasive Computing". *Proc. of 4th IEEE International Workshop on Pervasive Computing and Communication Security (PerSec 2007)*, White Plains, NY, March 2007, pp. 241–246.

Urs Hengartner and Peter Steenkiste, "Securing Information Gateways with Derivation-Constrained Access Control". *Proc. of 3rd International Conference on Security in Pervasive Computing (SPC 2006)*, York, England, April 2006, pp. 181–195.

Urs Hengartner and Peter Steenkiste, "Avoiding Privacy Violations Caused by Context-Sensitive Services". *Proc. of 4th IEEE International Conference on Pervasive Computing and Communications (PerCom 2006)*, Pisa, Italy, March 2006, pp. 222–231.

Urs Hengartner and Peter Steenkiste, "Exploiting Hierarchical Identity-Based Encryption for Access Control to Pervasive Computing Information". *Proc. of 1st IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm 2005)*, Athens, Greece, September 2005, pp. 384–393.

Urs Hengartner and Peter Steenkiste, "Exploiting Information Relationships for Access Control". *Proc. of 3rd*

IEEE International Conference on Pervasive Computing and Communications (PerCom 2005), Kauai Island, HI, March 2005, pp. 269–278.

Urs Hengartner and Peter Steenkiste, "Implementing Access Control to People Location Information". *Proc. of 9th Symposium on Access Control Models and Technologies (SACMAT 2004)*, Yorktown Heights, NY, June 2004, pp. 11–20.

Nancy Miller, Glenn Judd, Urs Hengartner, Fabien Gandon, Peter Steenkiste, I-Heng Meng, Ming-Whei Feng, and Norman Sadeh, "Context-aware Computing Using a Shared Contextual Information Service". *Proc. of Pervasive 2004 Hot Spots*, Vienna, Austria, April 2004.

Urs Hengartner and Peter Steenkiste, "Access Control to Information in Pervasive Computing Environments". *Proc. of 9th Workshop on Hot Topics in Operating Systems (HotOS IX)*, Lihue, HI, May 2003, pp. 157–162.

Urs Hengartner and Peter Steenkiste, "Protecting Access to People Location Information". *Proc. of 1st International Conference on Security in Pervasive Computing (SPC 2003)*, Boppard, Germany, March 2003, pp. 25–38.

Urs Hengartner, Sue Moon, Richard Mortier, and Christophe Diot, "Detection and Analysis of Routing Loops in Packet Traces" (Short Paper). *Proc. of 2nd Internet Measurement Workshop (IMW 2002)*, Marseille, France, November 2002, pp. 107–112.

Urs Hengartner and Peter Steenkiste, "Protecting People Location Information" (Extended Abstract). *Proc. of Workshop on Security in Ubiquitous Computing*, Göteborg, Sweden, September 2002.

Andy Myers, John Chuang, Urs Hengartner, Yinglian Xie, Weiqiang Zhuang, and Hui Zhang, "A Secure, Publisher-Centric Web Caching Infrastructure". *Proc. of IEEE Infocom 2001*, Anchorage, AK, April 2001, pp. 1235–1243.

Urs Hengartner, Jürg Bolliger, and Thomas Gross, "TCP Vegas Revisited". *Proc. of IEEE Infocom 2000*, Tel Aviv, Israel, March 2000, pp. 1546–1555.

Michael Hemy, Urs Hengartner, Peter Steenkiste, and Thomas Gross, "MPEG System Streams in Best-Effort Networks". *Proc. of PacketVideo '99*, New York, NY, April 1999.

Jürg Bolliger, Thomas Gross, and Urs Hengartner, "Bandwidth Modelling for Network-Aware Applications". *Proc. of IEEE Infocom '99*, New York, NY, March 1999, pp. 1300–1309.

Selected Technical Reports

Urs Hengartner, "Access Control to Information in Pervasive Computing Environments". *Ph.D. Thesis, available as Technical Report CMU-CS-05-160, Computer Science Department, Carnegie Mellon University*, August 2005.

Jürg Bolliger, Urs Hengartner, and Thomas Gross, "The Effectiveness of End-to-End Congestion Control Mechanisms". *Technical Report #313*. Department of Computer Science, ETH Zürich, February 1999.

Invited Talks and Panels

"On Implicit Authentication", *Concordia Institute for Information Systems Engineering (CIISE), Concordia University*, Montreal, QC, March 2016.

"On Implicit Authentication", *Cheriton School of Computer Science Colloquium Series, University of Waterloo*, Waterloo ON, November 2015.

"Evaluating and Deploying Implicit Authentication", *School of Computer Science, Carleton University*, Ottawa ON, June 2015.

"Privacy-preserving Social Recommendations in Geosocial Networks", *9th Annual Pitney Bowes Privacy and Security Conference*, Stamford CT, June 2013.

"Location Privacy", *E-Voting Seminar, Bern University of Applied Sciences*, Biel, Switzerland, November 2012.

"Privacy and Security for Location-based Applications", *TCS Seminar, KTH Royal Institute of Technology*, Stockholm, Sweden, November 2012.

"Privacy and Security for Location-based Applications", *Summer Research Institute, Ecole Polytechnique Fédérale de Lausanne (EPFL)*, Lausanne, Switzerland, June 2012.

"VeriPlace: A Privacy-Aware Location Proof Architecture", *7th Annual Pitney Bowes Conference on Information Security and Communication*, Stamford CT, June 2011.

"FaceCloak: An Architecture for User Privacy on Social Networking Sites ". *Innovation Insights - Information Communication Technologies for Business*, Accelerator Centre, Waterloo ON, June 2010.

"Location Privacy and Emerging Technologies", *The Office of the Privacy Commissioner of Canada: Geospatial Information, Mobile Marketing and Location Privacy Workshop*, Ottawa ON, November 2009.

"Privacy-Enhancing Technologies for Location-Based Services", *CASCON 2009: Workshop on Cybersecurity: Security and Privacy in the 21st Century*, Markham ON, November 2009.

"Privacy-Enhancing Technologies for Location-Based Services", *5th Annual Pitney Bowes Conference on Information Security and Communication*, Stamford CT, July 2009.

"Privacy-Enhancing Technologies for Mobile Applications", *Ecole Polytechnique Fédérale de Lausanne (EPFL)*, Lausanne, Switzerland, May 2009.

"Privacy-Enhancing Technologies for Mobile Applications", *Google*, Waterloo ON, April 2009.

"Sharing Data in a Privacy-Friendly Way", *The Canadian Association of Research Ethics Boards (CAREB) Ontario Conference 2008*, Waterloo, November 2008.

"Location Privacy", *6th International Conference on Mobile Business (ICMB'07), Privacy & Security Panel*, Toronto ON, July 2007.

"Anonymity and Security in Delay Tolerant Networks", *Lake Ontario Systems and Engineering Research (LOSER) Workshop*, Niagara Falls ON, May 2007.

"Access Control to Information in Pervasive Computing Environments", *METIS Security Seminar Series, University of Ontario Institute of Technology*, Oshawa ON, November 2006.

"Access Control to Information in Pervasive Computing Environments", *Cryptography Seminar, Centre for Applied Cryptography, University of Waterloo*, Waterloo ON, November 2005.

"Access Control to Information in Pervasive Computing Environments", *School of Computer Science, University of Waterloo*, Waterloo ON, April 2005.

"Access Control to Information in Pervasive Computing", *Workshop on Content and Application Customization for Pervasive Computing, 14th Annual IBM Centers for Advanced Studies Conference (CASCON 2004)*, Markham ON, October 2004.

"Exploiting Information Relationships for Access Control", *Systems Design and Implementation (SDI) / Laboratory for Computer Systems (LCS) Seminar*, Carnegie Mellon University, Pittsburgh PA, April 2004.

Experience

Research and Technical

September 2018 - August 2019, Visiting Professor (Sabbatical), Concordia University, Montreal, QC, Canada.

July 2010 - Present, Associate Professor, University of Waterloo, Waterloo ON.

January 2012 - December 2012, Visiting Professor (Sabbatical), Ecole Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland.

September 2005 - June 2010, Assistant Professor, University of Waterloo, Waterloo ON.

August 1999 - August 2005, Graduate Student, Carnegie Mellon University, Pittsburgh PA.
For my thesis research, I examined access control to sensitive information available in future ubiquitous computing environments. Namely, I proposed exploiting relationships between information as a first-class citizen in access control. In addition, I studied ways to avoid information leaks occurring in distributed access-control architectures.

Working for the Aura research project, I explored security issues that arise if people can learn about each other's location. Moreover, I designed, implemented, and evaluated a secure people location system.

Working for the Gemini research project, I participated in the design, implementation, and evaluation of a next-generation Web cache that is able to generate documents on the fly in a secure way.

Summer 2001, Research Intern, Sprint Advanced Technology Laboratories, Burlingame CA.
Working with the IP Group, I analyzed traces of network packets from Sprint's Internet backbone links for routing loops and traffic anomalies, such as denial of service attacks. For facilitating this analysis, I designed and implemented several algorithms.

September 1998 - July 1999, Research Assistant, ETH Zürich, Switzerland.
Working for the Network-Aware Applications research project, I decomposed the newly proposed Internet congestion algorithm TCP Vegas into its parts and analyzed the effect of the individual parts on throughput and retransmission of network packets.

January 1998 - June 1998, Visiting Scholar, Carnegie Mellon University, Pittsburgh PA.
Working with Michael Hemy, I designed and implemented a protocol that selectively drops MPEG video frames according to the experienced degree of network congestion.

October 1997 - December 1997, Part-time Research Assistant, ETH Zürich, Switzerland.
Working for the Network-Aware Applications research project, I implemented several Internet congestion control algorithms in user space and examined their influence on throughput and retransmission of network packets in a large-scale Internet experiment.

November 1996 - March 1997, Research Intern, IT Camp, the Information Technology Laboratory of the UBS Bank, Basel, Switzerland.
I evaluated several audio/video communication tools. In addition, I designed and implemented a video-conferencing plugin for Netscape Navigator.

Teaching

Winter 2018: ***CS 458/658 - Computer Security and Privacy*****, University of Waterloo.**

Fall 2017: ***CS 458/658 - Computer Security and Privacy*****, University of Waterloo.**

Fall 2016: ***CS 858 - Mobile Privacy and Security*****, University of Waterloo.**

Fall 2016: ***CS 458/658 - Computer Security and Privacy*****, University of Waterloo.**

Winter 2016: ***CS 458/658 - Computer Security and Privacy*****, University of Waterloo.**

Winter 2015: ***CS 458/658 - Computer Security and Privacy*****, University of Waterloo.**

Spring 2014: ***CS 458/658 - Computer Security and Privacy*****, University of Waterloo.**

Fall 2013: ***CS 858 - Mobile Privacy and Security*****, University of Waterloo.**

Winter 2013: ***CS 458/658 - Computer Security and Privacy*****, University of Waterloo.**

Fall 2011: ***CS 458/658 - Computer Security and Privacy*****, University of Waterloo.**

Winter 2011: ***CS 458/658 - Computer Security and Privacy*****, University of Waterloo.**

Fall 2010: ***CS 858 - Hot Topics in Computer and Communication Systems Security*****, University of Waterloo.**

Fall 2010: ***CS 458/658 - Computer Security and Privacy*****, University of Waterloo.**

Winter 2010: ***CS 456/656 - Computer Networks*****, University of Waterloo.**

Fall 2009: ***CS 454/654 - Distributed Systems*****, University of Waterloo.**

Fall 2009: ***CS 458/658 - Computer Security and Privacy*****, University of Waterloo.**

Winter 2009: ***CS 858 - Hot Topics in Computer and Communication Systems Security*****, University of Waterloo.**

Winter 2009: ***CS 458/658 - Computer Security and Privacy*****, University of Waterloo.**

Fall 2008: ***CS 454/654 - Distributed Systems*****, University of Waterloo.**

Winter 2008: ***CS 489/698 - Computer Security and Privacy*****, University of Waterloo.**

Winter 2008: ***CS 854 - Hot Topics in Computer and Communication Systems Security*****, University of Waterloo.**

Fall 2007: ***CS 497 - Frontiers in Computer Science*****, University of Waterloo.**
Two lectures about current security and privacy challenges.

Winter 2007: ***CS 497 - Frontiers in Computer Science*****, University of Waterloo.**
Two lectures about current security and privacy challenges.

Winter 2007: ***CS 454/654 - Distributed Systems*****, University of Waterloo.**

Fall 2006: ***CS 854 - Hot Topics in Computer and Communication Systems Security*****, University of Waterloo.**

Winter 2006: ***CS 456/656 - Computer Networks*****, University of Waterloo.**

Students and Postdocs Supervised

Jiayi Chen (PhD), Fall 2017–present

Pierfrancesco Cervellini (MMath), Fall 2017–present

Nikita Volodin (MMath, co-supervised with Mei Nagappan), Fall 2016–present

Erinn Atwater (PhD), Fall 2013–present

Bushra Aloraini (PhD Advisory Committee [Mei Nagappan]), Fall 2018–present

Hussain Mousaid (PhD Advisory Committee [Ian McKillop]), Fall 2018–present

Peiyuan Liu (MMath), "Quantifying Location Privacy In Location-based Services", Fall 2016–Spring 2018

Hassan Khan (Postdoc), Fall 2016–Spring 2018

Cecylia Bocovich (PhD Advisory and Thesis Committee [Ian Goldberg]), Spring 2016–Spring 2018

Lianying Zhao at Concordia University, Montreal QC, Canada (PhD Thesis Committee [Mohammad Mannan]), Spring 2018

Katherine Carras, Ramandeep Farmaha, Krishn Ramesh, Anastasia Santasheva (Capstone project supervisor), Fall 2017–Winter 2018

Wei Wang (PhD Advisory Committee [Michael Godfrey]), Winter 2018–present

Chongchong Liu (PhD Comprehensive Exam Committee [Anwar Hasan]), Fall 2017.

Justin Tracey (MMath Thesis Reader [Ian Goldberg]), Spring 2017

Rongjun Yan (Undergraduate Research Assistant), Spring 2017

Lucas Palmer (Undergraduate Research Assistant), Winter 2017

Lalit Agarwal (MMath), "Evaluating Re-authentication Strategies for Smartphones", Spring 2015–Spring 2016

Hassan Khan (PhD), "Evaluating the Efficacy of Implicit Authentication Under Realistic Operating Scenarios", Fall 2012–Spring 2016

Justin Hu (Undergraduate Research Assistant), Spring 2016

Sarah Harvey (PhD/MMath, co-supervised with Charlie Clarke), Fall 2011–Spring 2016

Berker Agir at EPFL, Lausanne, Switzerland (PhD Thesis Committee [Karl Aberer]), May 2016

Monis Khan (Undergraduate Research Assistant), Fall 2015

Tao Wang (PhD Advisory Committee and Thesis Committee [Ian Goldberg]), Spring 2014–Fall 2015

Rayman Preet Singh (PhD Advisory Committee and Thesis Committee [S. Keshav]), Spring 2014–Fall 2015

AbdelRahman Mohamed Abdou at Carleton University, Ottawa ON, Canada (PhD Thesis Committee [Ashraf Matrawy & Paul Van Oorschot]), Spring 2015

Kevin Henry (PhD Advisory Committee and Thesis Committee [Doug Stinson]), Fall 2011–Spring 2015

Yihang Song (MMath), "PrivacyGuard: A VPN-Based Approach to Detect Privacy Leakages on Android Devices", Fall 2013–Spring 2015

Nik Unger (MMath Thesis Reader [Ian Goldberg]), Spring 2015

Danish Mehmood (MMath), "Muddler: Using Oblivious RAM For A Privacy Preserving Location-Based Service", Fall 2012–Fall 2014

Casey Devet (MMath Thesis Reader [Ian Goldberg]), Winter 2013

Gangqiang Yang (PhD Comprehensive Exam Committee [Mark Aagaard & Guang Gong]), Winter 2014.

A. Kadhim Hayawi (PhD Comprehensive Exam Committee [Mahesh Tripunitara]), Winter 2014.

Bisheng Liu (Postdoc), Winter 2012–Fall 2014

Ali Hussain (Undergraduate Research Assistant), Spring 2013

Andrew Tinits (Undergraduate Research Assistant), Spring 2013

Mashael AlSabah (PhD Advisory Committee and Thesis Committee [Ian Goldberg]), Spring 2011–Winter 2013

Peter Tysowski (PhD Comprehensive Exam Comittee and Thesis Committee [Anwar Hasan]), Winter 2011–Winter 2013

Sarah Pidcock (MMath), " A Privacy-Friendly Architecture for Mobile Social Networking Applications", Fall 2010–Winter 2013

Hooman Mohajeri Moghaddam (MMath Thesis Reader [Ian Goldberg]), Winter 2013

Mehrdad Nojoumian (PhD Advisory and Thesis Committee [Doug Stinson]), Fall 2010–Spring 2012.

Vincent Bindschaedler at EPFL, Lausanne, Switzerland (Master's Thesis Reader [Jean-Pierre Hubaux]), Spring 2012.

Aleksander Essex (PhD), "Cryptographic End-to-end Verification for Real-world Elections", Spring 2010–Spring 2012

Rob Smits (MMath Thesis Reader [Ian Goldberg]), Fall 2011

Femi Olumofin (PhD Advisory and Thesis Committee [Ian Goldberg]), Spring 2010–Spring 2011

Eduardo S. Barrenechea (PhD Advisory Committee [Don Cowan]), Spring 2011 - present

Jeremy Clark (PhD), "Democracy Enhancing Technologies: Toward deployable and incoercible E2E elections", Fall 2007–Spring 2011

Ryan Henry (MMath Thesis Reader [Ian Goldberg]), Fall 2010

Janna-Lynn Weber (MMath Thesis Reader [Ed Lank & Daniel Berry]), Spring 2010

Qi Xie (MMath), "Privacy-Preserving Interest Matching for Mobile Social Networking", Fall 2008–Spring 2010

Aniket Kate (PhD Advisory and Thesis Committee [Ian Goldberg]), Fall 2008 - Spring 2010

Can Tang (MMath Thesis Reader [Ian Goldberg]), Spring 2010

Georgia Kastidou (PhD Advisory and Thesis Committee [Kate Larson & Robin Cohen]), Fall 2007 - Spring 2010

Wanying Luo (MMath), "Designing a Privacy-Aware Location Proof Architecture", Fall 2008–Winter 2010

Amir Khatib Zadeh (PhD Thesis Committee [Catherine Gebotys]), Winter 2010

Karim Ali (MMath Thesis Reader [Raouf Boutaba]), Fall 2009

Usman Ismail (MMath Thesis Reader [S. Keshav]), Spring 2009

Jiang Wu (PhD Advisory Committee and Thesis Committee [Douglas Stinson]), Fall 2007 - Spring 2009

Earl Oliver (PhD Comprehensive Exam Committee [S. Keshav]), Winter 2009

Tung Tran (MMath Thesis Reader [Raouf Boutaba]), Winter 2009

Gregory M. Zaverucha (PhD Advisory Committee [Doug Stinson]), Winter 2009

Anuchart Tassanaviboon (PhD Comprehensive Exam Comittee [Guang Gong]), Winter 2009

Ben Ko (Undergraduate Research Assistant), Fall 2008

Aaditeshwar Seth (PhD Advisory and Thesis Committee [S. Keshav]), Fall 2006 - Fall 2008

Joel Reardon (MMath Thesis Reader [Ian Goldberg]), Spring 2008

Ahmed Ataullah (MMath Thesis Reader [Frank Tompa & Ashraf Aboulnaga]), Spring 2008

Agustin Dominguez Oviedo (PhD Thesis Committee [Anwar Hassan]), Spring 2008

Sumair Ur Rahman (MMath, co-supervised with S. Keshav), ”Security for Rural Public Computing”, Fall 2006–Spring 2008

Ge Zhong (MMath), “Distributed Approaches for Location Privacy”, Fall 2006–Spring 2008

Xiaoxiao Li (Undergraduate Research Assistant), Winter 2008

Jiayuan Sui (MMath Thesis Reader [Douglas Stinson]), Winter 2008

Xiaoting Sun (MMath Thesis Reader [Ian Goldberg]), Fall 2007

David Bartley (Undergraduate Research Assistant), Spring 2007

Amir H. Chinaei (PhD Advisory Committee [Frank Tompa]), Spring 2006 - Spring 2007

Philip Cavaco (Undergraduate Research Assistant), Fall 2006

Tung Tran (Undergraduate Research Assistant), Spring 2006

Omar Zia Khan (MMath Thesis Reader [Jay Black]), Fall 2005

Ge Zhong (Undergraduate Research Assistant), Fall 2005

Academic Service

Program Committee Member

17th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys 2019)

17th IEEE International Conference on Pervasive Computing and Communications (PerCom 2019)

Financial Cryptography and Data Security 2019 (FC'19)

IEEE International Conference on Computer Communications (IEEE INFOCOM 2019)

16th Annual Conference on Privacy, Security and Trust (PST 2018)

23rd ACM Symposium on Access Control Models and Technologies (SACMAT 2018)

16th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys 2018)

16th IEEE International Conference on Pervasive Computing and Communications (PerCom 2018)

IEEE International Conference on Computer Communications (IEEE INFOCOM 2018)

15th Annual Conference on Privacy, Security and Trust (PST 2017)

22nd ACM Symposium on Access Control Models and Technologies (SACMAT 2017)

15th IEEE International Conference on Pervasive Computing and Communications (PerCom 2017)

IEEE International Conference on Computer Communications (IEEE INFOCOM 2017)

6th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM 2016)

21st ACM Symposium on Access Control Models and Technologies (SACMAT 2016)

14th IEEE International Conference on Pervasive Computing and Communications (PerCom 2016)

IEEE International Conference on Computer Communications (IEEE INFOCOM 2016)

Workshop on Privacy in the Electronic Society (WPES 2015)

13th International Conference on Privacy, Security and Trust (PST 2015)

24th World Wide Web Conference (WWW 2015), Pervasive Web and Mobility Track

13th IEEE International Conference on Pervasive Computing and Communications (PerCom 2015)

Financial Cryptography and Data Security 2015 (FC'15)

Workshop on Privacy in the Electronic Society (WPES 2014)

10th International Conference on Security and Privacy in Communication Networks (SecureComm 2014)

7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2014)

12th International Conference on Mobile Systems, Applications, and Services (MobiSys 2014) (External review committee)

6th IEEE International Workshop on SEcurity and SOCial Networking (SESOC 2014)

Financial Cryptography and Data Security 2014 (FC'14)

3rd ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM 2013)

5th ASE/IEEE International Conference on Privacy, Security, Risk, and Trust (PASSAT 2013)

8th International Conference on Security and Privacy in Communication Networks (SecureComm 2013)

2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2013)

6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '13)

11th IEEE International Conference on Pervasive Computing and Communications (PerCom 2013)

11th Workshop on Privacy in the Electronic Society (WPES 2012)

8th International Conference on Security and Privacy in Communication Networks (SecureComm 2012)

4th ASE International Conference on Privacy, Security, Risk, and Trust (PASSAT 2012)

21st USENIX Security Symposium

10th International Conference on Mobile Systems, Applications, and Services (MobiSys 2012)

5th ACM Conference on Wireless Network Security (WiSec '12)

10th IEEE International Conference on Pervasive Computing and Communications (PerCom 2012)

3rd IEEE International Conference on Privcy, Security, Risk, and Trust (PASSAT 2011)

4th ACM Conference on Wireless Network Security (WiSec '11)

9th IEEE International Conference on Pervasive Computing and Communications (PerCom 2011)

6th ACM International Conference on emerging Networking EXperiments and Technologies (ACM CoNEXT 2010)

2nd IEEE International Conference on Privcy, Security, Risk, and Trust (PASSAT2010)

8th IEEE International Conference on Pervasive Computing and Communications (PerCom 2010)

5th ACM International Conference on emerging Networking EXperiments and Technologies (ACM CoNEXT 2009)

2009 IEEE International Conference on PrivAcy, Security, riSk, And Trust (PASSAT-09)

11th International Conference on Ubiquitous Computing (Ubicomp 2009)

3rd International Workshop on Privacy-Aware Location-based Mobile Services (PALMS'09)

International Workshop on Privacy in Location-Based Applications (PiLBA '08)

2nd International Workshop on Privacy-Aware Location-based Mobile Services (PALMS'08)

6th International Conference on Mobile Systems, Applications, and Services (MobiSys 2008)

Workshop on the Security and Privacy of Emerging Ubiquitous Communication Systems (SPEUCS 2007)

International Workshop on Privacy-Aware Location-based Mobile Services (PALMS 2007)

4th International Conference on Privacy, Security and Trust (PST 2006)

Organizing Activities

Privacy Track Chair for 12th Annual Conference on Privacy, Security and Trust (PST 2014)

Vice Technical Program Chair for 12th IEEE International Conference on Pervasive Computing and Communications (PerCom 2014)

Co-workshop chair for 11th IEEE International Conference on Pervasive Computing and Communications (PerCom 2013)

Editorial Activities

Member of the Editorial Board of Pervasive and Mobile Computing, 2013–2016

University Service

Associate Director of Graduate Studies, 2015–2017

Member of Graduate Studies Committee: 2015–2017

Member of School Advisory Committee on Appointments (SACA): 2014–2015, 2017–2018

Member of Tenure and Promotion Committee: 2013–2015

Member of Graduate Recruiting Committee: 2009–2011, 2013, 2015–2016

Member of CSCF Advisory Committee: 2008–2009

Member of School Space Committee: 2006–2008

Member of School Commons Committee: 2005–2008, 2011

Honours and Awards

David R. Cheriton Faculty Fellowship in Computer Science, University of Waterloo

ACM Senior Member

Google Faculty Research Award

Willi Studer-Prize for Best Final Diploma Exam in Computer Science at ETH Zürich

Personal Information

Swiss and Canadian Citizen