Reza Shokri

Curriculum Vitae

Department of Computer Science
National University of Singapore, School of Computing,
13 Computing Drive, Computing 1, #03-27,
Singapore 117417.

+65-6516-4464
reza@comp.nus.edu.sg
http://www.shokri.org

Research Interests

Security and Privacy, with the focus on Data and Machine Learning Privacy

Academic Positions

National University of Singapore

Assistant Professor at *Computer Science Department* — Aug. 2017 — Present

Cornell University

Postdoctoral Associate at *Cornell Tech* — Oct. 2014 — Jul. 2017
Host: Prof. Vitaly Shmatikov

ETH Zurich

Postdoctoral Associate at *Institute of Information Security* — Oct. 2013 — Sep. 2014
Host: Prof. Srdjan Capkun

EPFL

Research Assistant at *Laboratory for Communications and Applications* — Oct. 2007 — Sep. 2013

University of Tehran

Research Assistant at *Router Laboratory* — Sep. 2005 — Jul. 2007

Education

PhD. in Computer and Communication Sciences, EPFL, Switzerland — Mar. 2013
Thesis: Quantifying and Protecting Location Privacy
Advisor: Prof. Jean-Pierre Hubaux

MSc. in Computer Software Engineering, University of Tehran, Iran — Jul. 2007

BSc. in Computer Software Engineering, University of Isfahan, Iran — Mar. 2003

Awards and Honors

Swiss National Science Foundation post-doctoral fellowship, 87'000 USD — 2013

Runner-up for the PET Award for Outstanding Research in Privacy Enhancing Technologies — 2012

Most cited research paper published at IEEE Symposium on Security and Privacy — since 2011

Program Committee Chair

Hot Topics in Privacy Enhancing Technologies (HotPETs) 2013 — 2014

Editorial Board

Proceedings on Privacy Enhancing Technologies 2015, 2017

Award Committee Member

Award for Outstanding Research in Privacy Enhancing Technologies 2015 — 2016

Program Committee Member

ACM Conference on Computer and Communications Security (CCS) 2017

USENIX Security Symposium 2015 — 2016

Network and Distributed System Security Symposium (NDSS) 2016 — 2017

IEEE European Symposium on Security and Privacy (Euro S&P) 2017

International World Wide Web Conference – Security Track (WWW) 2016

Privacy Enhancing Technologies Symposium (PETS) 2013 — 2015, 2017

ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) 2014 — 2016

Conference on Decision and Game Theory for Security (GameSec) 2015 — 2016

International Workshop on Obfuscation: Science, Technology, and Theory 2017

ACM Workshop on Privacy in the Electronic Society (WPES) 2012, 2015

NDSS Workshop on Understanding and Enhancing Online Privacy (UEOP) 2016

ASIACCS Workshop on IoT Privacy, Trust, and Security (IoTPTS) 2015 — 2016

International Conference on Privacy, Security and Trust (PST) 2014

Selected Peer-Reviewed Publications

[SSSS17] R. Shokri, M. Stronati, C. Song, and V. Shmatikov. "Membership Inference Attacks against Machine Learning Models". *To appear in the IEEE Symposium on Security and Privacy (***S&P, Oakland***) 2017.*

[BSG17] V. Bindschaedler, R. Shokri, and C. Gunter. "Plausible Deniability for Privacy-Preserving Data Synthesis". *To appear in the Proceedings of the VLDB Endowment International Conference on Very Large Data Bases (***PVLDB***) 2017.*

[BS16] V. Bindschaedler and R. Shokri. "Synthesizing Plausible Privacy-Preserving Location Traces". *In IEEE Symposium on Security and Privacy (***S&P, Oakland***) 2016.*

[STT16] R. Shokri, G. Theodorakopoulos, and C. Troncoso. "Privacy Games along Location Traces: A Game-Theoretic Framework for Optimizing Location Privacy". *To appear in the ACM Transactions on Privacy and Security (***TOPS***) 2016.*

[OHS+16] AM. Olteanu, K. Huguenin, R. Shokri, M. Humbert, and JP. Hubaux. "Quantifying Interdependent Privacy Risks with Location Data". *In IEEE Transactions on Mobile Computing (***TMC***) 2016.*

[S15] R. Shokri. "Privacy Games: Optimal User-Centric Data Obfuscation". *In Proceedings on Privacy Enhancing Technologies (***PETS***) 2015.*

[SS15] R. Shokri and V. Shmatikov. "Privacy-Preserving Deep Learning". *In ACM Conference on Computer and Communications Security (***CCS***) 2015. Also appeared at the Annual Allerton Conference on Communication, Control, and Computing (***Allerton***) 2015.*

[BHM+15] I. Bilogrevic, K. Huguenin, S. Mihaila, R. Shokri, and JP. Hubaux. "Predicting Users' Motivations behind Location Check-Ins and Utility Implications of Privacy Protection Mechanisms". *In Network and Distributed System Security Symposium (***NDSS***) 2015.*

[GSS+15] A. Gervais, R. Shokri, A. Singla, S. Capkun, and V. Lenders. "Quantifying Web-Search Privacy". *In ACM Conference on Computer and Communications Security (***CCS***) 2014.*

[OHSH14] A. M Olteanu, K. Huguenin, R. Shokri, and JP. Hubaux. "Quantifying the Effect of Co-location Information on Location Privacy". *In Privacy Enhancing Technologies Symposium (***PETS***) 2014.*

[STP+14] R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and JP. Hubaux. "Hiding in the Mobile Crowd: Location Privacy through Collaboration". *In IEEE Transactions on Dependable and Secure Computing (***TDSC***) 2014.*

[STT+12] R. Shokri, G. Theodorakopoulos, C. Troncoso, JP. Hubaux, and JY. Le Boudec. "Protecting Location Privacy: Optimal Strategy against Localization Attacks". *In ACM Conference on Computer and Communications Security (***CCS***) 2012.*

[STLH11] R. Shokri, G. Theodorakopoulos, JY. Le Boudec, and JP. Hubaux. "Quantifying Location Privacy". *In IEEE Symposium on Security and Privacy (***S &P, Oakland***) 2011.*

[STD+11] R. Shokri, G. Theodorakopoulos, G. Danezis, JP. Hubaux, and JY. Le Boudec. "Quantifying Location Privacy: The Case of Sporadic Location Exposure". *In Privacy Enhancing Technologies Symposium (***PETS***) 2011.*

[FSH09] J. Freudiger, R. Shokri, and JP. Hubaux. "On the Optimal Placement of Mix Zones". *In Privacy Enhancement Technologies Symposium (***PETS***) 2009.*

[SPTH09] R. Shokri, P. Pedarsani, G. Theodorakopoulos, and JP. Hubaux. "Preserving Privacy in Collaborative Filtering through Distributed Aggregation of Offline Profiles". *In ACM Conference on Recommender Systems (***RecSys***) 2009.*

[SPR+09] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and JP. Hubaux. "A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks". *In ACM Conference on Wireless Network Security (***WiSec***) 2009.*

Bibliometrics

Citations: 1860 *h-index*: 20

Software Tools

Location Privacy and Mobility Meter (based on [STLH11]): *an open-source tool to train mobility models from potentially noisy location traces with missing data, and to quantify location privacy of mobile users against inference attacks such as identification, tracking and localization.*

Web-Search Privacy Quantification Tool (based on [GSS+15]): *an open-source tool to model users' web search behavior, and to quantify their privacy against inference attacks.*

Synthetic Location Traces Generator Tool (based on [BS16]): *an open-source tool to generate synthetic yet plausible location traces which are semantically similar to real traces in a seed dataset, however do not leak significantly about locations visited in the real traces.*

Teaching

Cornell Tech

Guest lecturer: "Security and Privacy: Practice and Case Studies" 2016

Guest lecturer: "Security and Privacy Technologies" 2015

Guest lecturer: "Privacy in the Digital Age" 2015

ETH Zurich

Guest lecturer: "Computer Security" 2014

EPFL

Teaching assistant: "Mobile Networks" 2009 — 2013

Teaching assistant: "Security and Cooperation in Wireless Networks" 2009 — 2012

University of Tehran

Lecturer: "Operating System Laboratory: Linux kernel programming" 2005 — 2006

Supervised Student Research Projects

Cornell Tech

Richard McPherson (PhD student), *Evaluating Privacy of Obfuscated Images* 2016

Vincent Bindschaedler (PhD intern), *Generating Privacy-Preserving Synthetic Data* 2016

ETH Zurich

Arthur Gervais (PhD student), *Quantifying Web-Search Privacy* 2014

EPFL

Nauman Shahid (PhD student), *Data Sharing: User Behavior Modeling and Analysis* 2013

Alexandra M. Olteanu (PhD student), *Social aspects of Location Privacy* 2013

Pierre Pfister (MSc student), *Impact of Human Mobility on Location Privacy* 2012

Vincent Bindschaedler (MSc student), *Impact of Human Mobility on Location Privacy* (Thesis) 2012

Saeid Sahraei (MSc student), *Lower Bounds on Location Privacy* 2012

Ypatia Tsavliri & Vasileios Agrafiotis (MSc students), *Analyzing Location Sharing in Facebook* 2011

David Freiburghaus (MSc student), *Theoretical Location Privacy* 2011

Quentin Hounkpatin (BSc student), *Evaluating Location Obfuscation Mechanisms* 2011
Arun Mallya (MSc intern), *Reconstructing Noisy Trajectories* 2011
Vincent Bindschaedler (MSc student), *Developing the Location-Privacy Meter Tool* 2011
Ehsan Kazemi (PhD student), *Location Privacy in Peer-to-Peer Wireless Networks* 2011
Francisco Santos (MSc student), *Game Theoretic Analysis of MobiCrowd* 2011
Jean Biollay (MSc student), *Privacy-Preserving Mobile Recommender Systems* 2010
Selma Chouaki (PhD student), *Privacy vs. Trust in Participatory Sensing Systems* 2010
Acacio Martins & Emanuel Cino (MSc students), *Privacy-Preserving Friend-Finder* 2010
Hai Ly Hoang (MSc student), *Evaluating Location-Privacy Preserving Mechanisms* 2009
Loic Pfister (MSc student), *Implementing A Collaborative Privacy Protection Method* 2009
Frederico Venturieri (BSc student), *Wireless Communication Helps Privacy* 2009
Antoine Parisod (MSc student), *Privacy Preserving Recommender Systems* 2009
Laurent Bindschaedler & Marc Bailly (BSc students), *Secure SMS Communication* 2009
Hai Ly Hoang (MSc student), *Trust in Mobile Networks* 2009
Nawfal Cherqui (BSc student), *Secure Communication in Ad-hoc Networks* 2009
Hasan Mirjalili (PhD student), *Privacy-Preserving People-centric Sensing* 2008
Loic Pfister (BSc student), *Wormhole Attack Prevention in Sensor Networks* 2008
Gael Ravot (MSc intern), *Secure Neighbor-Verification in Sensor Networks* 2008

Invited Talks on various topics in data privacy

Computer Science Department at EPFL 2017
Computer Science Department at ETH Zurich 2017
ECE Department at the University of Texas at Austin 2017
Computer Science Department at Caltech 2017
Computer Science Department at University of Southern California 2017
The U.S. Census Bureau 2017
College of Information and Computer Sciences, at UMass, Amherst 2016
Electrical Engineering Department at Princeton University 2016
Computer Science Department at University of Maryland 2015
Information Trust Institute, ECE Department at UIUC 2015
Inria Saclay, Paris 2014
GI-Dissertationspreis 2013 Kolloquium, Dagstuhl, Germany 2014
TDW Conference: Enabling the Economics of Trust, Vienna 2014
Computer Science Department at Luxembourg University 2014
School of Information Studies at McGill University 2014

Computer Science Department at the University of Waterloo	2014
Computer Science Department at the University of Toronto	2014
NEC Germany	2014
LIX, Ecole Polytechnique, Paris	2013
Microsoft Research at Cambridge, UK	2013
Palo Alto Research Center (PARC), CA	2011
Information Trust Institute, ECE Department at UIUC	2011
COSIC, K.U.Leuven, Belgium	2010
WINLAB, ECE Department at Rutgers University, NJ	2009

Selected Media Coverage

MIT Technology Review *Microsoft and Google Want to Let Artificial Intelligence Loose on Our Most Private Data.*

WIRED *AI Can Recognize Your Face Even If You're Pixelated.*

BBC *De-blurring Obscured Online Images.*

The Register *Pixellation popped: AI can ID you, even after PhotoShop phuzzing.*

The Telegraph *Pixelated photos and licence plates can be unblurred using artificial intelligence.*

Hacker News *Defeating Image Obfuscation with Deep Learning.*

Quartz *Nothing pixelated will stay safe on the internet.*

Popular Science *Researchers Train AI To Defeat Face Blurring Technologies.*

Popular Mechanics *Nowhere to Hide: Algorithms Are Learning to ID Pixelated Faces.*

Inverse *A.I. Can Identify Pixelated, Blurred Faces When Humans Can't.*

Biometric Update *Researchers train software to recognize pixelated faces.*

Digital Trends *Hiding a person by pixelating their face? Computer system says don't bother.*

RT *AI that identifies pixelated & blurred faces easy for hackers to exploit - researchers.*

KCBS *Pixelated Images That Conceal Identities Undone With New Technology.*

Daily Mail *Forget trying to blur your pictures: Artificial intelligence can recognise your face even in pixelated images.*

Tech Emergence *Google and Microsoft Invest in "Privacy-Preserving" Deep Learning.*