Florian Tramèr

720 Serra Street, Apt. 516, Stanford, CA 94305
✉ tramer@cs.stanford.edu
http://www.floriantramer.com
http://www.linkedin.com/in/floriantramer
https://scholar.google.com/citations?user=ijH0-a8AAAAJ&hl=en
☎ +1-650-250-6336

Education

Sep. 2016 - Today	**PhD in Computer Science** - Stanford University, Stanford CA, USA Advised by Prof. Dan Boneh
Sep. 2013 - Aug. 2015	**Master in Computer Science** - EPFL, Lausanne, Switzerland Thesis: "Algorithmic Fairness Revisited", supervised by Prof. Jean-Pierre Hubaux Specialization in *Internet Computing* GPA: 5.9/6.0
Sep. 2009 - Aug. 2012	**Bachelor in Computer Science** - EPFL, Lausanne, Switzerland Exchange year (2011-2012) - Carnegie Mellon University, Pittsburgh PA, USA GPA: 5.8/6.0

Professional Experience

Jun. 2017 - Sep. 2017	**IBM Research** - *Research Intern*, Yorktown Heights, NY, USA Supervised by Dr. Evelyn Duesterwald • Study of *adversarial examples* for speech recognition systems.
Sep. 2015 - Aug. 2016	**EPFL** - *Scientific Assistant*, Lausanne, Switzerland • Study of *extraction attacks* on Machine-Learning-as-a-Service platforms [TZJ+16]. • Formal analysis of *trusted execution environments* [PST17], in particular for *transparent enclaves*, a model of trusted hardware with arbitrary side-channel leakage [TZL+17]. • Design of formal methodologies and a tool, *FairTest*, for the discovery of "discrimination bugs" in data-driven algorithms [TAG+17]. • Research on privacy-preserving ride-hailing [PDJ+17] and genomic studies [THH+15]. Supervised by Prof. J-P. Hubaux, Laboratory for Communications and Applications.
Sep. 2013 - Feb. 2015	**EPFL** - *Research Assistant*, Lausanne, Switzerland Implementation and complexity analysis of algorithms for solving hard learning problems such as Learning Parity with Noise [BTV16], Learning with Errors and Learning with Rounding [DTV15]. Supervised by Prof. S. Vaudenay, Laboratory for Cryptography and Security.
Mar. 2013 - Aug. 2013	**ELCA** - *Security Intern*, Lausanne, Switzerland Design, proof of concept and implementation of a proxy web-application integrating the Elcard strong-authentication mechanism with the Saml 2.0 standard. Acquired experience with federated identity solutions, strong authentication methods, J2ee web development and software testing (unit, integration, regression). The new functionality is to be added to the next Elcard release.

Professional Service

Organizing committee.

- Workshop on Security in Machine Learning (co-located with NIPS), 2018 (**Co-chair**)

Program committee.

- Deep Learning and Security Workshop (co-located with IEEE S&P), 2019
- Machine Learning and Computer Security Workshop (co-located with NIPS), 2017

Peer reviewer.

- Neural Information Processing Systems (NIPS), 2018
- International Conference on Machine Learning (ICML), 2018, 2019
- Financial Cryptography and Data Security (FC), 2018
- IEEE Symposium on Security & Privacy (IEEE S&P), 2017
- Privacy Enhancing Technologies Symposium (PETS), 2016

Awards and Scholarships

2018	**Gift from the Open Philanthropy Project**
2018	**DOC.Mobility Fellowship (Swiss National Science Foundation)**
2016	**Zdenek and Michaela Bakala Foundation Fellowship**
2015	**EPFL Master Award** (Highest GPA for complete Master studies at EPFL) **SIA Vaudoise Award** (Highest GPA in Engineering) **ELCA Award** (Highest GPA in Computer Science)
2013-2015	**EPFL Excellence Fellowship** (Awarded for outstanding academic records)
2013-2015	**EPFL Research Scholars MSc Program**

Languages

French	Native language
English	Fluent - Cefr level C2, Certificate in Advanced English - Esol (2009)
German	Fluent - Cefr level C2

Technical Skills

Programming	Java, Scala, C, Python	very good skills
	Matlab, x86 Assembly, J2EE, Web Development	good skills
Machine Learning	TensorFlow, Theano, Keras, Scikit-Learn	
Systems	Unix, Windows, OS X environments Tomcat, Apache Httpd, Adfs 2.0, SQL, Hadoop, HBase, Svn, Git	

Publications

Journal Articles

[RTJ+17] Jean Louis Raisaro, **Florian Tramèr**, Zhanglong Ji, Diyue Bu, Yongan Zhao, Knox Carey, et al. "Addressing Beacon Re-Identification Attacks: Quantification and Mitigation of Privacy Risks". *Journal of the American Medical Informatics Association (JAMIA)* (Feb. 2017).

[BTV16] Sonia Bogos, **Florian Tramèr**, and Serge Vaudenay. "On Solving LPN using BKW and Variants". *Cryptography and Communications* 8.3 (July 2016), pp. 331–369.

Conference Proceedings

[TB19] **Florian Tramèr** and Dan Boneh. "Slalom: Fast, Verifiable and Private Execution of Neural Networks in Trusted Hardware". In *International Conference on Learning Representations (ICLR)*. **Oral Presentation**. May 2019.

[BDT+18] Lorenz Breidenbach, Phil Daian, **Florian Tramèr**, and Ari Juels. "Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts". In *USENIX Security Symposium*. **Invited to appear in IEEE Security and Privacy Magazine**. Aug. 2018.

[TKP+18] **Florian Tramèr**, Alexey Kurakin, Nicolas Papernot, Ian Goodfellow, Dan Boneh, and Patrick McDaniel. "Ensemble Adversarial Training: Attacks and Defenses". In *International Conference on Learning Representations (ICLR)*. Apr. 2018.

[PDJ+17] Anh Pham, Italo Dacosta, Bastien Jacot-Guillarmod, Kévin Huguenin, Taha Hajar, **Florian Tramèr**, and Jean-Pierre Hubaux. "PrivateRide: A Privacy-Preserving and Secure Ride-Hailing Service". In *Privacy Enhancing Technologies Symposium (PETS)*. July 2017.

[PST17] Rafael Pass, Elaine Shi, and **Florian Tramèr**. "Formal Abstractions for Attested Execution Secure Processors". In *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. Apr. 2017.

[TAG+17] **Florian Tramèr**, Vaggelis Atlidakis, Roxana Geambasu, Daniel Hsu, Jean-Pierre Hubaux, Mathias Humbert, Ari Juels, and Huang Lin. "FairTest: Discovering Unwarranted Associations in Data-Driven Applications". In *IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE. Apr. 2017.

[TZL+17] **Florian Tramèr**, Fan Zhang, Huang Lin, Jean-Pierre Hubaux, Ari Juels, and Elaine Shi. "Sealed-Glass Proofs: Using Transparent Enclaves to Prove and Sell Knowledge". In *IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE. Apr. 2017.

[TZJ+16] **Florian Tramèr**, Fan Zhang, Ari Juels, Michael Reiter, and Thomas Ristenpart. "Stealing Machine Learning Models via Prediction APIs". In *USENIX Security Symposium*. Aug. 2016.

[THH+15] **Florian Tramèr**, Zhicong Huang, Jean-Pierre Hubaux, and Erman Ayday. "Differential Privacy with Bounded Priors: Reconciling Utility and Privacy in Genome-Wide Association Studies". In *ACM Conference on Computer and Communications Security (CCS)*. ACM. Oct. 2015, pp. 1286–1297.

[DTV15] Alexandre Duc, **Florian Tramèr**, and Serge Vaudenay. "Better Algorithms for LWE and LWR". In *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. Springer, Apr. 2015, pp. 173–202.

Workshops

[EEF+18] Kevin Eykholt, Ivan Evtimov, Earlence Fernandes, Bo Li, Amir Rahmati, **Florian Tramèr**, Atul Prakash, Tadayoshi Kohno, and Dawn Song. "Physical Adversarial Examples for Object Detectors". In *USENIX Workshop on Offensive Technologies (WOOT)*. June 2018.

Manuscripts

[TDR+18] **Florian Tramèr**, Pascal Dupré, Gili Rusak, Giancarlo Pellegrino, and Dan Boneh. *Ad-versarial: Defeating Perceptual Ad-Blocking*. arXiv preprint arXiv:1811:03194. Nov. 2018. URL: http://arxiv.org/abs/1811.03194.

[TPG+17] **Florian Tramèr**, Nicolas Papernot, Ian Goodfellow, Dan Boneh, and Patrick McDaniel. *The Space of Transferable Adversarial Examples*. arXiv preprint arXiv:1704.03453. Apr. 2017. URL: https://arxiv.org/abs/1704.03453.