PEDRO MORENO-SANCHEZ

pmorenos@purdue.edu – www.cs.purdue.edu/homes/pmorenos/
Department of Computer Science, Purdue University
305 N. University Street, West Lafayette, IN 47907, USA

EDUCATION

Department of Computer Science - Purdue University — West Lafayette, USA
PhD Student. Cryptographic Systems Research Group — Aug 2015-*Present*

Cluster of Excellence - Saarland University — Saarbrucken, Germany
PhD Student. Cryptographic Systems Research Group — Apr 2013-Jul 2015

University of Murcia — Murcia, Spain
M.Sc. in New Technologies in Computer Science — Oct 2011-Feb 2013

B.Sc. in Computer Science — Sep 2007-Sep 2011

RESEARCH INTEREST

My work aims at developing and evaluating cryptographic solutions for secure, privacy-preserving network systems. My current research focuses on emerging online payment networks such as credit networks (e.g., Ripple, Stellar) and cryptocurrencies (e.g., Bitcoin and Ethereum).

RESEARCH INTERNSHIPS

IBM Research — Zurich, Switzerland
Intern with Christian Cachin — Jun 2017-Aug 2017

Ripple Inc. — San Francisco, USA
Intern with Stefan Thomas, and Evan Schwartz — Jun 2016-Aug 2016

Philips Research Europe — Eindhoven, Netherlands
Intern with Oscar Garcia-Morchon, Sye Loong Keoh and Sandeep Kumar — Jun 2012-Dec 2012

SELECTED PROJECTS

- **Security and Privacy of Cryptocurrencies and Credit Networks** — Aug 2013-*Present*
  We aim at applying cryptographic protocols and privacy solutions to the most widely deployed cryptocurrencies (e.g., Bitcoin) and credit networks (e.g., Ripple). Results published at HotPETs'14, ESORICS'14, NDSS'15, PETS'16, HotPETs'16, BITCOIN'17, PETS'17 and NDSS'17.
- **Security of Network Access Control** — Jun 2010-Jul 2013
  We design, implement and evaluate systems to securely enforce network access control in many different scenarios such as NAT systems (PCP), constrained environments (Internet of Things), and multicast networks. Results published at IETF86, WiSec'13, Sensors Journal and IEEE Network Magazine.

REFEREED PUBLICATIONS

1. **Pedro Moreno-Sanchez**, Tim Ruffing and Aniket Kate: "PathShuffle: Credit Mixing and Anonymous Payments for Ripple". *Privacy Enhancing Technologies Symposium (PETS'17)*, July 2017 (To appear).
2. Tim Ruffing and **Pedro Moreno-Sanchez**: "Mixing Confidential Transactions: Comprehensive Transaction Privacy for Bitcoin". *Workshop on Bitcoin and Blockchain Research (BITCOIN'17)*, April 2017.
3. Giulio Malavolta*, **Pedro Moreno-Sanchez***, Aniket Kate and Matteo Maffei: "SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks". *Network and Distributed System Security (NDSS'17) Symposium*, February 2017. * Both authors contributed equally and are considered to be co-first authors
4. Tim Ruffing, **Pedro Moreno-Sanchez** and Aniket Kate: "P2P Mixing and Unlinkable Bitcoin Transactions". *Network and Distributed System Security (NDSS'17) Symposium*, February 2017.
5. **Pedro Moreno-Sanchez**, Muhammad Bilal Zafar and Aniket Kate: "Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network". *Privacy Enhancing Technologies Symposium (PETS'16)*, July 2016.
6. **Pedro Moreno-Sanchez**, Aniket Kate, Matteo Maffei and Kim Pecina: "Privacy Preserving Payments in Credit Networks". *Network and Distributed System Security (NDSS'15) Symposium*, February 2015.
7. Tim Ruffing, **Pedro Moreno-Sanchez** and Aniket Kate: "CoinShuffle: Practical Decrentralized Coin Mixing for Bitcoin". *European Symposium on Research in Computer Security (ESORICS'14)*, September 2014.
8. **Pedro Moreno-Sanchez**, Rafa Marin-Lopez and Francisco Vidal-Meca: "An Open Source Implementation of the Protocol for Carrying Authentication Network Access: OpenPANA". *IEEE Network Magazine; Special Issue: Open Source for Networking: Development and Experimentation*, April 2014.
9. **Pedro Moreno-Sanchez**, Rafa Marin-Lopez and Antonio F. Gomez-Skarmeta: "PANATIKI: A Network Access Control Implementation based on PANA for IoT devices". *Sensors 2013*, October 2013.
10. Oscar Garcia-Morchon, Sye Loong Keoh, Sandeep S. Kumar, **Pedro Moreno-Sanchez**, Francisco Vidal-Meca and Jan Henrik Ziegeldorf: "Securing the IP-based Internet of Things with HIP and DTLS". *6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'13)*, April 2013.

SCIENTIFIC SERVICE

I have served as a member of the Student Program Committee of IEEE S&P (2017).

I have served as an external reviewer for the following conferences: ICDCS (2017), ACNS (2016), EUROCRYPT (2016), CCS (2015), WPES (2015).

AWARDS AND SCHOLARSHIPS

- **Emil Stefanov Fellowship in Computer Science** for the academic achievements specializing in security, Purdue. USA — April 2017
- **CERIAS/Intel Research Scholarship** as research assistant in the Department of Computer Science, Purdue. USA — Jan 2017-May 2017
- **Research Scholarship** as research assistant in the Department of Information and Communication Engineering (DIIC) - Computer Science Department. Murcia, Spain — Oct 2011-May 2012
- **Extraordinary Prize "End of Bachelor"**
  (Student with the highest average grade in the class of 2011) — Jul 2011
- **Scholarship from Spanish Ministry of Education** for the the first year in the University of Murcia, Spain. (Student with the highest average grade in the class 2007). — Sep 2007

SELECTED TALKS

- "Listening to and Silencing the Whispers of Ripple: Study and Solutions for Privacy in IOweYou Credit Networks" at *George Mason University.* Host: Prof. Foteini Baldimtsi, USA, April 2017.
- "SilentWhispers: En- forcing Security and Privacy in Decentralized Credit Networks" at *Network Distributed System Security (NDSS'17) Symposium*, USA, February 2017.
- "Listening to and Silencing the Whispers of Ripple: Study and Solutions for Privacy in IOweYou Credit Networks" at *Real World Cryptography Conference (RWC'17)*, USA, January 2017.
- "Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network" at *Privacy Enhancing Technologies Symposium (PETS'16)*, Germany, July 2016.
- "Whispers: A Distributed Architecture for Enforcing Privacy in Credit Networks" at *Hot Topics in Privacy Enhancing Technologies (HotPETs'16)*, Germany, July 2016.
- "Privacy Preserving Payments in Credit Networks" at *Network Distributed System Security (NDSS'15) Symposium*, USA, February 2015.
- "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" at *Hot Topics in Privacy Enhancing Technologies (HotPETs'14)*, Netherlands, July 2014.

TEACHING EXPERIENCE

Privacy Enhancing Technologies Summer Semester 2014, 2015
Teaching Assistant

Security Winter Semester 2014/15
Tutor

BIOGRAPHICAL INFORMATION

I am a Spanish citizen. I speak fluent English and native Spanish.

ACADEMIC REFERENCES

Aniket Kate Purdue University, USA
Assistant Professor at the Computer Science Department
e-mail: *aniket@purdue.edu*

Matteo Maffei TU Vienna, Austria
Professor at the Computer Science Department.
e-mail: *matteo.maffei@tuwien.ac.at*

Rafa Marin-Lopez University of Murcia, Spain
Professor at the Computer Science Department.
e-mail: *rafa@um.es*