10-14 September 2012 - CNR Research Area of Pisa, Italy

17th European Symposium on Research in Computer Security

MONDAY, SEPTEMBER 10TH

09:00-10:15
AUDITORIUM
• Welcome and opening
• Invited Talk: Mind the gap: Smart phone security and privacy in Theory and Practice by Ann-Kristin Salsgiver

10:45-12:15
AUDITORIUM
Session 2A: Security and privacy in mobile and wireless networks (chair: Roberto Di Pietro)

• A Probabilistic Framework for Localization of Attackers in MANETs by Maximilien Attaran, Alessandra De Santis, Sashi Apanda and Paul Slatorke
• Robust Protocable Files Packet Injection for Receiver-Locality Privacy in Wi-Fi by Ruben Rios, Jorge Casella and Javier Lopez
• Privacy-Aware Messages Exchange for Geographically Roamed Human Movement Networks by Adam Atre, Mihal Sherm, Matt Blaize and Jonathan Smith

16:15-17:45
Session 6A: Identity-based encryption and group signature (chair: Joachim Possgage)

• Identity-Based Trapdoor with Short Private Key and Short Collusion-Proof Multi-secret by Kaufman Sun, Yi Mu and Willy Susilo
• Third-Party DFA Evaluation on Encrypted Files in the Cloud by Li Wei and Michael Reller
• New Algorithms for Secure Outsourcing of Modular Exponentiations by Xiaoliang Chen, Jin-Zhi Jiang, Qiang Teng and Wenyong Liu

TUESDAY, SEPTEMBER 11TH

09:00-10:15
AUDITORIUM
• Invited Talk: Integrity of storage and computations in the cloud by Christian Cachin

10:45-12:15
AUDITORIUM
Session 7: Encryption key and password security (chair: Josep Garcia-Alans)

• Evaluation of Standardized Password-Based Key Derivation against Parallel Processing Platforms by Markus Dürmuth, Tim Golle, Martin Kasper, Christof Paar, Tolga Yalcin and Ralf Zimmermann
• Beyond-KC: Perfect Forward Security under Active Compromise and Ephemeral Key Reuse by Cao Crenos and Michelle Fraz
• Bitcoin’s atomicSwap: Breaking P2PSegW 1.5 and The Verge by Trevor Golder and Andrew Miller
• On the Security of Password Manager Database Formats by Paola Salsi and Krzysztof Riedmaier

14:15-15:45
UDITORIUM
Session 8: Malware and phishing (chair: Friederic Cuppens)

• Malware Taxonomy Classification for Automated Malware Detection by Jason Stotts, John Paul, Helen Weng, Zhe Fan, Jonathan, Rekey, Mady Hamzeh, and Marco Ghidoni
• Address-based Malware Analysis Using Random Testing and Model Checking by Philipp Beauchamp, Satchui Sridhar and Jean-Yves Marion
• Detection of Malicious Phantom-Driven Emailing the Natural Language Way by Francesco Vanini, Svetlana Dzhdovskaia, and Natalia Dzhdovskaia

16:15-17:45
UDITORIUM
Session 9: Software security (chair: Dieter Gollmann)

• JAVAPortal Sanitizing Java Native Libraries by Mengfei Sun and Gang Tan
• Automated Analysis of Source Code for Vulnerability in Java Using a Trust Program Interaction by Sicheng Wu, Sotiris Stravdos, Volker Stekel, Roland Ne and Zhenwei Li
• Socialimpact: Systematic Analysis of Underground Social Dynamics by Zining Zhang, Gai-Joon Ahn, Hongxin Hu and David Markos