CARDIS 2012 – Program

Eleventh Smart Card Research and Advanced Application Conference

Wednesday, November 28

Time	Event	
	Session/Chair	Author/Title
12:30 - 14:15	Registration & Welcome Buffet	
14:15 - 14:25	Opening Remarks	
14:25 - 15:40	Java Card Security / Berndt Gammel	Michael Lackner, Reinhard Berlach, Christian Steger, Reinhold Weiss, Johannes Loinig and Ernst Haselsteiner **Towards the Hardware Accelerated Defensive Virtual Machine - Type and Bound Checks**
		Guillaume Barbu, Philippe Andouard and Christophe Giraud **Dynamic Fault Injection Countermeasure – A New Conception of Java Card Security**
		Julien Lancia **Java Card combined attacks with localization-agnostic fault injection**
15:40 - 16:10	Coffee	
16:10 - 17:00	Protocols / Konstantinos Markantonakis	Sébastien Canard, Loïc Ferreira and Matt Robshaw **Improved (and Practical) Public-key Authentication for UHF RFID Tags**
		Jan Hajny and Lukas Malina **Unlinkable Attribute-Based Credentials with Practical Revocation on Smart-Cards**
19:00 - 22:00	Welcome Reception (Landhaus-Keller, Graz)	

Thursday, November 29

Time	Event	
	Session/Chair	Author/Title
08:30 - 09:00	Registration	
09:00 - 10:40	Side-Channel Attacks I / Hermann Drexler	Thomas Roche, Emmanuel Prouff and Jean-Sébastien Coron **On the Use of Shamir's Secret Sharing Against Side-Channel Analysis**
		Luk Bettale **Secure Multiple SBoxes Implementation with Arithmetically Masked Input**
		Cedric Murdica, Sylvain Guilley and Philippe Hoogvorst **Low-Cost Countermeasure against RPA**
		François Durvaux, Mathieu Renauld, Francois-Xavier Standaert, Loic Van Oldeneel Tot Oldenzeel and Nicolas Veyrat-Charvillon **Efficient Removal of Random Delays from Embedded Software Implementations using Hidden Markov Models**
10:40 - 11:15	Coffee	
11:15 - 12:15	Invited Talk I / Joern-Marc Schmidt	N. Asokan Mobile Platform Security
12:15 - 14:00	Lunch	
14:00 - 15:15	Implementations / Lejla Batina	Tolga Yalcin and Elif Bilge Kavun **On the Implementation Aspects of Sponge-based Authenticated Encryption for Pervasive Devices**
		Josep Balasch, Baris Ege, Thomas Eisenbarth, Benoît Gérard, Zheng Gong, Tim Güneysu, Stefan Heyse, Stéphanie Kerckhof, Francois Koeune, Thomas Plos, Thomas Poppelmann, Francesco Regazzoni, Francois-Xavier Standaert, Gilles Van Assche, Ronny Van Keer, Loic Van Oldeneel Tot Oldenzeel and Ingo von Maurich **Compact Implementation and Performance Evaluation of Hash Functions in ATtiny Devices**
		Markus Pelnar, Michael Muehlberghuber and Michael Hutter **Putting Together What Fits Together – GrAEStl**
15:15 - 15:45	Coffee	
15:45 - 16:35	Implementations for Constrainted Devices / Marcel Medwed	Yuto Nakano, Carlos Cid, Shinsaku Kiyomoto and Yutaka Miyake **Memory Access Pattern Protection for Resource-constrained Devices**
		Petr Susil and Serge Vaudenay **Multipurpose Cryptographic Primitive ARMADILLO3**
17:00 - 19:00	Guided City-Tour of Graz	
19:00 - 23:00	Gala Dinner at Restaurant SCHLOSSBERG	

Friday, November 30

Time	**Event**		
	Session/Chair	**Author/Title**	
08:30 - 09:00	Registration		
09:00 - 10:40	Side-Channel Attacks II / Francois-Xavier Standaert	David Oswald and Christof Paar **Improving Side-Channel Analysis with Optimal Pre-Processing Methods**	
		Sebastien Tiran and Philippe Maurine **SCA with Magnitude Squared Coherence**	
		Johann Heyszl, Dominik Merli, Benedikt Heinz, Fabrizio De Santis and Georg Sigl **Strengths and Limitations of High-Resolution Electromagnetic Field Measurements for Side-Channel Analysis**	
		Timo Bartkewitz **Efficient Template Attacks Based on Probabilistic Multi-class Support Vector Machines**	
10:40 - 11:15			
11:15 - 12:15	Invited Talk II / Stefan Mangard	David Naccache	Defensive Leakage Camouflage
12:15 - 12:20	Closing remarks		
12:20 - 14:00	Farewell buffet		