
9 September

08:30 Registration

09:30 Opening remarks

10:00 Invited talk: Adrian Perrig (ETH)

11:00 Coffee break

Session 1a: Measurement and Evaluation

11:30 *Verifying Web Browser Extensions' Compliance with Private-Browsing Mode:*
B. Lerner, L. Elberty, N. Poole and S. Krishnamurthi

12:00 *A Quantitative Evaluation of Privilege Separation in Web Browser Designs:*
X. Dong, H. Hu, P. Saxena and Z. Liang

12:30 *Estimating Asset Sensitivity by Profiling Users:* Y. Park, C. Gates and S. Gates

Session 1b: Cryptography and Computation

Practical Covertly Secure MPC for Dishonest Majority – or: Breaking the SPDZ Limits: I. Damgaard, M. Keller, E. Larraia, V. Pastro, P. Scholl and N. Smart

Practical and Employable Protocols for UC-Secure Circuit Evaluation over Z_n :
J. Camenisch, R.R. Enderlein and V. Shoup

Privacy-Preserving Accountable Computation Privacy Theory Models and Methods:
M. Backes, D. Fiore and E. Mohammadi

13:00 Lunch

Session 2a: Code Analysis

14:00 *HI-CFG: Construction by Dynamic Binary Analysis, and Application to Attack Polymorphism:* D. Caselden, A. Bazhanyuk, M. Payer, S. McCamant and D. Song

14:30 *Scalable Semantics-Based Detection of Similar Android Applications:* J. Crussell, C. Gibler and H. Chen

15:00 *BISTRO: Binary Component Extraction and Embedding for Software Security Applications:* Z. Deng, X. Zhang and D. Xu

Session 2b: Applications of Cryptography

Practical Secure Logging: Seekable Sequential Key Generators: G.A. Marson and B. Poettering

Request-Based Comparable Encryption : J. Furukawa

Ensuring File Authenticity in Private DFA Evaluation on Encrypted Files in the Cloud: L. Wei and M. Reiter

15:30 Coffee break

Session 3: Network Security

16:00 *Vulnerable Delegation of DNS Resolution:* A. Herzberg and H. Shulman

16:30 *Formal Approach for Route Agility Against Persistent Attackers:* J.H. Jafarian, E. Al-Shaer and Q. Duan

17:00 *Plug-and-Play IP Security: Anonymity Infrastructure Instead of PKI:* Y. Gilad and A. Herzberg

19:00 Pre-dinner drinks

20:00 Conference dinner

10 September

08:30	Registration	
	Session 4: Formal Methods and Models	
09:00	<i>Managing the Weakest Link: A Game-Theoretic Approach for the Mitigation of Insider Threats</i> : A. Laszka, B. Johnson, P. Schöttle, J. Grossklags and R. Böhme	
09:30	<i>Automated Security Proofs for Almost-Universal Hash for MAC verification</i> : M. Gagne, P. Lafourcade and Y. Lakhnech	
10:00	<i>Bounded Memory Protocols and Progressing Collaborative Systems</i> : M. Kanovich, T. Ban Kirigin, V. Nigam and A. Scedrov	
10:30	<i>Universally Composable Key-Management</i> : S. Kremer, R. Künnemann and G. Steel	
11:00	Coffee break	
	Session 5a: Privacy Enhancing Models	Session 5b: Protocol Analysis
11:30	<i>Efficient Privacy-Enhanced Familiarity-Based Recommender System</i> : A. Jeckmans, A. Peter and P. Hartel	<i>A Cryptographic Analysis of OPACITY</i> : Ö. Dagdelen, M. Fischlin, T. Gagliardoni, G. Marson, A. Mittelbach and C. Onete
12:00	<i>Privacy-Preserving User Data Oriented Services For Groups With Dynamic Participation</i> : D. Kononchuk, Z. Erkin, J.C.A. van der Lubbe and R.L. Legendijk	<i>Symbolic Probabilistic Analysis of Off-line Guessing</i> : B. Conchinha, D. Basin and C. Caleiro
12:30	<i>Privacy-Preserving Matching of Community-Contributed Content</i> : M. Almishari, P. Gasti, E. Oguz and G. Tsudik	<i>ASICS: Authenticated Key Exchange Security Incorporating Certification Systems</i> : C. Boyd, C. Cremers, M. Feltz, K.G. Paterson, B. Poettering and D. Stebila
13:00	Lunch	
	Session 6a: Malware Detection	Session 6b: E-voting and Privacy
14:00	<i>Mining malware specifications through static reachability analysis</i> : H.D. Macedo and T. Touili	<i>Ballot secrecy and ballot independence coincide</i> : B. Smyth and D. Bernhard
14:30	<i>Patrol: Revealing Zero-day Attack Paths through Network-wide System Object Dependencies</i> : J. Dai, X. Sun and P. Liu	<i>Election Verifiability or Ballot Privacy: Do We Need to Choose?</i> : E. Cuvelier, O. Pereira and T. Peters
15:00	<i>Measuring and Detecting Malware Downloads in Live Network Traffic</i> : P. Vadrevu, B. Rahbarinia, R. Perdisci, K. Li and M. Antonakakis	<i>Enforcing Privacy in the Presence of Others: Notions, Formalisations and Relations</i> : N. Dong, H. Jonker and J. Pang
15:30	Coffee break	
16:00	Panel: Privacy in Cyberspace—Rights, Wrongs and Research	
19:00	Drinks	
20:00	Barbecue	

11 September

08:30	Registration	
09:30	Invited talk: Steven Murdoch (Cambridge University)	
10:30	Coffee break	
	Session 7a: Attacks	Session 7b: Access Control
11:00	<i>Range Extension Attacks on Contactless Smart Cards</i> : D. Schirman, Y. Oren and A. Wool	<i>Automated Certification of Authorisation Policy Resistance</i> : A. Griesmayer and C. Morisset
11:30	<i>CellFlood: Attacking Tor Onion Routers on the Cheap</i> : M.V. Barbera, V.P. Kemerlis, V. Pappas and A. Keromytis	<i>Fine-Grained Access Control System based on Outsourced Attribute-based Encryption</i> : J. Li, X. Chen, J. Ma and W. Lou
12:00	<i>Nowhere to Hide: Navigating around Privacy in Online Social Networks</i> : M. Humbert, T. Studer, M. Grossglauser and J.-P. Hubaux	<i>Purpose Restrictions on Information Use</i> : M.C. Tschantz, A. Datta and J.M. Wing
12:30	<i>Current Events: Identifying Webpages by Tapping the Electrical Outlet</i> : S. Clark, H. Mustafa, B. Ransford, J. Sorber, K. Fu and W. Xu	<i>Distributed Shuffling for Preserving Access Confidentiality</i> : S. De Capitani Di Vimercati, S. Foresti, S. Paraboschi, G. Pelosi and P. Samarati
13:00	Lunch	
	Session 8: Language-based Protection	
14:00	<i>Eliminating Cache-Based Timing Attacks with Instruction-Based Scheduling</i> : D. Stefan, P. Buiras, E. Yang, A. Levy, D. Terei, A. Russo and D. Mazieres	
14:30	<i>Data-confined HTML5 Applications</i> : D. Akhawe, F. Li, W. He, P. Saxena and D. Song	
15:00	<i>KQguard: Binary-Centric Defense against Kernel Queue Injection Attacks</i> : J. Wei, F. Zhu and C. Pu	
15:30	<i>Run-Time Enforcement of Information-Flow Properties on Android</i> : L. Jia, J. Aljuraidan, E. Fragkaki, L. Bauer, M. Stroucken, K. Fukushima, S. Kiyomoto and Y. Miyake	
16:00	Closing remarks	
