
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 (Chair: E. Snekkenes)11:30 *Verifying Web Browser Extensions' Compliance with Private-Browsing Mode.*
B. Lerner, L. Elbert, N. Poole and S. Krishnamurthi12:00 *A Quantitative Evaluation of Privilege Separation in Web Browser Designs.*
X. Dong, H. Hu, P. Saxena and Z. Liang12:30 *Estimating Asset Sensitivity by Profiling Users.* Y. Park, C. Gates and S. Gates**Session 1b: Cryptography and Computation (Chair: K.G. Paterson)***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.* M. Backes, D. Fiore and E. Mohammadi

13:00 Lunch

Session 2a: Code Analysis (Chair: D. Gollmann)14:00 *HI-CFG: Construction by Dynamic Binary Analysis, and Application to Attack Polymorphism.* D. Caselden, A. Bazhanyuk, M. Payer, S. McCamant and D. Song14:30 *Scalable Semantics-Based Detection of Similar Android Applications.* J. Crussell, C. Gibler and H. Chen15:00 *BISTRO: Binary Component Extraction and Embedding for Software Security Applications.* Z. Deng, X. Zhang and D. Xu**Session 2b: Applications of Cryptography (Chair: M. Kohlweiss)***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 (Chair: C. Cremers)16:00 *Vulnerable Delegation of DNS Resolution.* A. Herzberg and H. Shulman16:30 *Formal Approach for Route Agility Against Persistent Attackers.* J.H. Jafarian, E. Al-Shaer and Q. Duan17:00 *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 (Chair: P.Y.A. Ryan)

09:00 *Managing the Weakest Link: A Game-Theoretic Approach for the Mitigation of Insider Threats.* A. Laszka, B. Johnson, P. Schöttle, J. Grossklags and R. Böhme

09:30 *Automated Security Proofs for Almost-Universal Hash for MAC verification.* M. Gagne, P. Lafourcade and Y. Lakhnech

10:00 *Bounded Memory Protocols and Progressing Collaborative Systems.* M. Kanovich, T. Ban Kirigin, V. Nigam and A. Scedrov

10:30 *Universally Composable Key-Management.* S. Kremer, R. Künnemann and G. Steel

11:00 Coffee break

Session 5a: Privacy Enhancing Models (Chair: A. Herzberg)

11:30 *Efficient Privacy-Enhanced Familiarity-Based Recommender System.* A. Jeckmans, A. Peter and P. Hartel

12:00 *Privacy-Preserving User Data Oriented Services For Groups With Dynamic Participation.* D. Kononchuk, Z. Erkin, J.C.A. van der Lubbe and R.L. Legendijk

12:30 *Privacy-Preserving Matching of Community-Contributed Content.* M. Almishari, P. Gasti, E. Oguz and G. Tsudik

Session 5b: Protocol Analysis (Chair: S. Kremer)

A Cryptographic Analysis of OPACITY. Ö. Dagdelen, M. Fischlin, T. Gagliardoni, G. Marson, A. Mittelbach and C. Onete

Symbolic Probabilistic Analysis of Off-line Guessing. B. Conchinha, D. Basin and C. Caleiro

ASICS: Authenticated Key Exchange Security Incorporating Certification Systems. C. Boyd, C. Cremers, M. Feltz, K.G. Paterson, B. Poettering and D. Stebila

13:00 Lunch

Session 6a: Malware Detection (Chair: E. Al-Shaer)

14:00 *Mining malware specifications through static reachability analysis.* H.D. Macedo and T. Touili

14:30 *Patrol: Revealing Zero-day Attack Paths through Network-wide System Object Dependencies.* J. Dai, X. Sun and P. Liu

15:00 *Measuring and Detecting Malware Downloads in Live Network Traffic.* P. Vadrevu, B. Rahbarinia, R. Perdisci, K. Li and M. Antonakakis

Session 6b: E-voting and Privacy (Chair: N. Cuppens-Boulahia)

Ballot secrecy and ballot independence coincide. B. Smyth and D. Bernhard

Election Verifiability or Ballot Privacy: Do We Need to Choose?. E. Cuvelier, O. Pereira and T. Peters

Enforcing Privacy in the Presence of Others: Notions, Formalisations and Relations. N. Dong, H. Jonker and J. Pang

15:30 Coffee break

Panel: Privacy in Cyberspace—Rights, Wrongs and Research (Moderator: J. Crampton)

Rob Carolina, Lizzie Coles-Kemp, Amir Herzberg, Steven Murdoch, Adrian Perrig

19:00 Drinks

20:00 Barbecue

11 September

08:30 Registration

09:30 **Invited talk**

Security Protocols and the Law: The Case of Chip and PIN. Steven Murdoch (Cambridge University)

10:30 Coffee break

Session 7a: Attacks (Chair: L. Bauer)

11:00 *Range Extension Attacks on Contactless Smart Cards.* D. Schirman, Y. Oren and A. Wool

11:30 *CellFlood: Attacking Tor Onion Routers on the Cheap.* M.V. Barbera, V.P. Kemerlis, V. Pappas and A. Keromytis

12:00 *Nowhere to Hide: Navigating around Privacy in Online Social Networks.* M. Humbert, T. Studer, M. Grossglauer and J.-P. Hubaux

12:30 *Current Events: Identifying Webpages by Tapping the Electrical Outlet.* S. Clark, H. Mustafa, B. Ransford, J. Sorber, K. Fu and W. Xu

Session 7b: Access Control (Chair: L. Jia)

Automated Certification of Authorisation Policy Resistance. A. Griesmayer and C. Morisset

Fine-Grained Access Control System based on Outsourced Attribute-based Encryption. J. Li, X. Chen, J. Ma and W. Lou

Purpose Restrictions on Information Use. M.C. Tschantz, A. Datta and J.M. Wing

Distributed Shuffling for Preserving Access Confidentiality. S. De Capitani Di Vimercati, S. Foresti, S. Paraboschi, G. Pelosi and P. Samarati

13:00 Lunch

Session 8: Language-based Protection (Chair: F. Cuppens)

14:00 *Eliminating Cache-Based Timing Attacks with Instruction-Based Scheduling.* D. Stefan, P. Buiras, E. Yang, A. Levy, D. Terei, A. Russo and D. Mazieres

14:30 *Data-confined HTML5 Applications.* D. Akhawe, F. Li, W. He, P. Saxena and D. Song

15:00 *KQguard: Binary-Centric Defense against Kernel Queue Injection Attacks.* J. Wei, F. Zhu and C. Pu

15:30 *Run-Time Enforcement of Information-Flow Properties on Android.* L. Jia, J. Aljuraidan, E. Fragkaki, L. Bauer, M. Stroucken, K. Fukushima, S. Kiyomoto and Y. Miyake

16:00 Closing remarks
