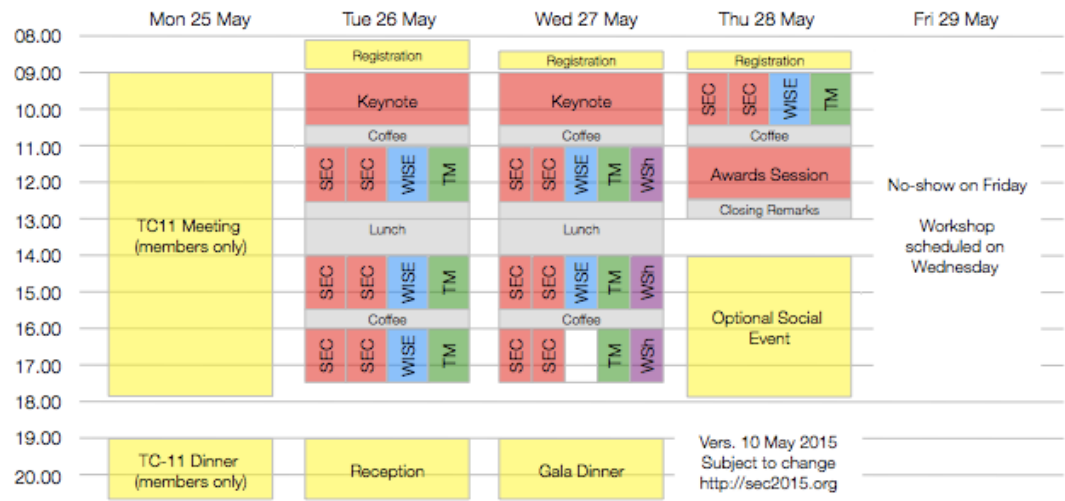# IFIP SEC 2015

International Conference on ICT Systems Security and Privacy Protection, May 26–28, 2015 in Hamburg, Germany

Conference Program

IFIP SEC 2015, IFIPTM 2015, WISE 9, Workshop on Assurance & Control, Workshop on Information Security Management

Presenters should prepare their talk to last a maximum of 20 minutes to allow sufficient time for discussion. Short papers will have 10-15 minutes for presentation.

25 May 2015 (Monday)

09:00	TC-11 Meeting (IFIP TC-11 members only)	121W
12:30	Lunch Break	
14:00	TC-11 Meeting	
18:00	TC-11 Meeting End	
19:00	TC-11 Dinner (IFIP TC-11 members only)	

26 May 2015 (Tuesday)

08:00	Registration	First Floor
09:00	**IFIP SEC 2015 Opening**	221W

IFIP SEC Invited Talk
The SCION Next-generation Secure Internet Architecture
Adrian Perrig (ETH Zürich, Switzerland) – **download slides of talk (PDF) (files/invited-talk-sec2015-adrian-perrig.pdf)**

10:30	Coffee Break	Ground Floor
11:00	**Parallel Session 1a: IFIP SEC (Privacy I, Chair: Jaap-Henk Hoepman)**	121W

O-PSI: Delegated Private Set Intersection on Outsourced Datasets
    Aydin Abadi, Sotirios Terzis and Changyu Dong
Flexible and Robust Privacy-Preserving Implicit Authentication
    Josep Domingo-Ferrer, Qianhong Wu and Alberto Blanco-Justicia
Towards Relations between the Hitting-Set Attack and the Statistical Disclosure Attack
    Dang Vinh Pham and Dogan Kesdogan

| 11:00 | **Parallel Session 1b: IFIP SEC (Web Security, Chair: Carlos Rieder)** | 221W |

Cache Timing Attacks revisited: efficient and repeatable browser history, OS and network sniffing
Chetan Bansal, Sören Preibusch and Natasa Milic-Frayling

Enforcing Usage Constraints on Credentials for Web Applications
Jinwei Hu, Heiko Mantel and Sebastian Ruhleder

A Survey of Alerting Websites: Risks and Solutions
Amrit Kumar and Cedric Lauradoux

| 11:00 | **Parallel Session 1c: WISE (Tools and Applications for Teaching, Chair: Matt Bishop)** | 220W |

Welcome by IFIP WG 11.8 Chair – Lynn Futcher

Learn To Spot Phishing URLs with the Android NoPhish App
Gamze Canova, Melanie Volkamer, Clemens Bergmann, Roland Borza, Benjamin Reinheimer, Simon Stockhardt and Ralf Tenberg

An Innovative Approach in Digital Forensic Education and Training: the EduFors Tool
Primoz Cigoj and Borka Jerman-Blazic

On Experience of Using Distance Learning Technologies for Teaching Cryptology
Sergey Zapechnikov, Natalia Miloslavskaya and Vladimir Budzko

| 11:00 | **Parallel Session 1d: IFIPTM (Short Papers)** | 120W |

1,2, pause: Lets start by meaningfully navigating the current online authentication solutions space
Ijlal Loumi and Audun Jøsang

Data Confidentiality in Cloud Storage Protocol based on Secret Sharing Scheme: A brute force ajack evaluation
Alexandru Butoi, Mircea Moca and Nicolae Tomai

The Detail of Trusted Messages: Retweets in a Context of Health and Fitness
Natasha Dwyer and Stephen Marsh

Reusable Defense Components for Online Reputation Systems
Johannes Sänger, Christian Richthammer, Artur Räsch and Günther Pernul

Continuous Context-Aware Device Comfort Evaluation Method
Jingjing Guo, Christian Damsgaard Jensen and Jianfeng Ma

| 12:30 | Lunch Break | Ground Floor |

| 13:30 | IFIP WG 11.11 Meeting | 120W |

| 14:00 | **Parallel Session 2a: IFIP SEC (Privacy II, Chair: Bart De Decker)** | 121W |

POSN: A Personal Online Social Network
Esra Erdin, Eric Klukovich, Mehmet Gunes and Gurhan Gunduz

Strategic Noninterference
Wojciech Jamroga and Masoud Tabatabaei

Verifying Observational Determinism
Jaber Karimpour, Ayaz Isazadeh and Ali A. Noroozi

| 14:00 | **Parallel Session 2b: IFIP SEC (Mobile and Cloud Services Security I, Chair: Nathan Clarke)** | 221W |

ApkCombiner: Combining Multiple Android Apps to Support Inter-AppAnalysis
Li Li, Alexandre Bartel, Tegawendé F. Bissyandé, Jacques Klein and Yves Le Traon

Assessment of the Susceptibility to Data Manipulation of Android Games with In-app Purchases
Francisco Vigário, Miguel Neto, Diogo Fonseca, Mário M. Freire and Pedro R. M. Inácio

An Empirical Study on Android for Saving Non-shared Data on Public Storage
Xiangyu Liu, Zhe Zhou, Wenrui Diao, Zhou Li and Kehuan Zhang

| 14:00 | **Parallel Session 2c: WISE** | 220W |

Panel Discussion: **Building National Cybersecurity Workforces**

| 14:30 | **Parallel Session 2d: IFIPTM** | 120W |

IFIPTM Keynote on **Data Protection** by *Marit Hansen* (ULD Kiel)

| 15:30 | Coffee Break | Ground Floor |

| 16:00 | **Parallel Session 3a: IFIP SEC (Security Management and Human Aspects of Security I, Chair: Ingrid Schaumüller-Bichl)** | 121W |

Social groupings and information security obedience within organizations
Teodor Sommestad

Attack Trees with Sequential Conjunction
Ravi Jhawar, Barbara Kordy, Sjouke Mauw, Sasa Radomirovic and Rolando Trujillo-Rasua

Enhancing the Security of Image CAPTCHAs through Noise Addition
David Lorenzi, Emre Uzun, Jaideep Vaidya, Shamik Sural and Vijay Atluri

| 16:00 | **Parallel Session 3b: IFIP SEC (Mobile and Cloud Services Security II, Chair: Leon Strous)** | 221W |

The Dual-Execution-Environment Approach: Analysis and Comparative Evaluation
Mohamed Sabt, Mohammed Achemlal and Abdelmadjid Bouabdallah

On the Privacy, Security and Safety of Blood Pressure and Diabetes Apps
Konstantin Knorr, David Aspinall and Maria Wolters

A Cloud-based eHealth Architecture for Privacy Preserving Data Integration
Alevtina Dubovitskaya, Visara Urovi, Matteo Vasirani, Karl Aberer and Michael I. Schumacher

| 16:00 | **Parallel Session 3c: WISE (Software Security Education, Chair: Erik Moore)** | 220W |

Cybersecurity through Secure Software Development
Audun Jøsang, Marte Ødegaard and Erlend Oftedal

Security Injections 2.0: Increasing Engagement and Faculty Adoption using Enhanced Secure Coding Modules for Lower-level Programming Courses
Sagar Raina, Blair Taylor and Siddharth Kaza

The Use of Software Design Patterns to Teach Secure Software Design: an Integrated approach
Johan van Niekerk and Lynn Futcher

| 16:00 | **Parallel Session 3d: IFIPTM** | 120W |

Tutorial / Panel on **Data Protection**

| 18:15 | Bus transfer from Dammtor (Shell gas station, REISERING buses) to Reception at Town Hall. Alternatively, you can walk or use public transport. See the program book in your conference bag for instructions. |

| 19:00 | Reception ("Senatsempfang") with drinks and Finger Food: Hamburg Town Hall, Rathausmarkt 1, 20095 Hamburg Appropriate attire (business formal or business casual) expected, but not enforced strictly. **Please remember to bring your invitation card and passport with you.** |

27 May 2015 (Wednesday)

| 08:30 | Registration | First Floor |

| 09:00 | **IFIP SEC Invited Talk**
Advances in Privacy Aware Authentication
Miroslaw Kutylowski (Wroclaw University of Technology) – **download slides of talk (PDF) (files/invited-talk-sec2015-miroslaw-kutylowski.pdf)** | 221W |

| 10:30 | Coffee Break | Ground Floor |

| 11:00 | **Parallel Session 4a: IFIP SEC (Applied Cryptography, Chair: Dominik Herrmann)** | 121W |

Fast Revocation of Attribute-Based Credentials for Both Users and Verifiers
Wouter Lueks, Gergely Alpar, Jaap-Henk Hoepman and Pim Vullers

Chaotic Chebyshev polynomials based remote user authentication scheme in client-server environment
Toan-Thinh Truong, Minh-Triet Tran, Anh-Duc Duong and Isao Echizen

A Secure Exam Protocol Without Trusted Parties
Giampaolo Bella, Rosario Giustolisi, Gabriele Lenzini and P. Y. A. Ryan

| 11:00 | **Parallel Session 4b: IFIP SEC (Software Security I, Chair: André Zúquete)** | 221W |

SHRIFT System-wide HybRid Information Flow Tracking
Enrico Lovat, Alexander Fromm, Martin Mohr and Alexander Pretschner

ISboxing: an Instruction Substitution based Data Sandboxing for x86 Untrusted Libraries
Liang Deng, Qingkai Zeng and Yao Liu

Exploit Generation for Information Flow Leaks in Object-Oriented Programs
Quoc Huy Do, Richard Bubel and Reiner Hähnle

| 11:00 | **Parallel Session 4c: WISE (Innovative Methods, Chair: Natalia Miloslavskaya)** | 220W |

Realism in Teaching Cybersecurity Research: The Agile Research Process
Melissa Dark, Matt Bishop and Rick Linger

Assurance Cases as a Didactic Tool for Information Security
Roberto Gallo and Ricardo Dahab

Cognitive Task Analysis Based Training for Cyber Situation Awareness
Zequn Huang, Chien-Chung Shen, Sheetal Doshi, Nimmi Thomas and Ha Duong

A Cyber Security Multi Agency Collaboration for Rapid Response That Uses AGILE Methods on an Education Infrastructure
Erik Moore and Daniel Likarish

11:00	**Parallel Session 4d: IFIPTM (Authentication)**	120W

Mathematical Modeling of Trust Issues in Federated Idenity Management
Md. Sadek Ferdous, Gethin Norman, Audun Jøsang and Ron Poet

Simple and Practical Integrity Models for Binaries and Files
Yongzheng Wu and Roland H.C. Yap

Enabling NAME-based security and trust
Nikos Fotiou and George C. Polyzos

11:00	**Parallel Session 4e: Workshop on Assurance & Control / Workshop on Information Security Management**	223W

Welcome by Workshop co-chairs - Abbas Shahim / Gurpreet Dhillon and Karen Hedstrom

Information assurance
Ronald Paans

Keynote on Audit & Trust in cloud environments
Abbas Shahim

12:30	Lunch Break	Ground Floor

14:00	**Parallel Session 5a: IFIP SEC (Access Control, Trust and Identity Management I, Chair: Dogan Kesdogan)**	121W

A Generalization of ISO/IEC 24761 to Enhance Remote Authentication with Trusted Product at Claimant
Asahiko Yamada

Enhancing Passwords Security using Deceptive Covert Communication
Mohammed Almeshekah, Mikhail Atallah and Eugene Spafford

Information Sharing and User Privacy in the Third-party Identity Management Landscape
Anna Vapen, Niklas Carlsson, Anirban Mahanti and Nahid Shahmehri

14:00	**Parallel Session 5b: IFIP SEC (Software Security II, Chair: Hannes Federrath)**	221W

Memoized Semantics-Based Binary Diffing with Application to Malware Lineage Inference
Jiang Ming, Dongpeng Xu and Dinghao Wu

Mitigating Code-Reuse Attacks on CISC Architectures in a Hardware Approach
Zhijiao Zhang, Yashuai Lü, Yu Chen, Yongqiang Lü and Yuanchun Shi

Integrity for Approximate Joins on Untrusted Computational Servers
Sabrina De Capitani Di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi and Pierangela Samarati

14:00	**Parallel Session 5c: WISE (Syllabus Design, Chair: Lynn Futcher)**	220W

Reflections on the Ethical Content of the IT honours Program Project Module
Lynette Drevin and Gunther Drevin

Professional Competencies Level Assessment for Training of Masters in Information Security
Natalia Miloslavskaya and Alexander Tolstoy

History of Cryptography in Syllabus on Information Security Training
Sergey Zapechnikov, Alexander Tolstoy and Sergey Nagibin

14:00	**Parallel Session 5d: IFIPTM (Privacy)**	120W

Trust Driven Strategies for Privacy by Design
Thibaud Antignac and Daniel Le Métayer

Lightweight practical private one-way anonymous messaging
Anirban Basu, Juan Camilo Corena, Jaideep Vaidya, Jon Crowcrog, Shinsaku Kiyomoto, Stephen Marsh, Yung Shin Van Der Sype and Toru Nakamura

Privacy-Preserving Reputation Mechanism: A Usable Solution Handling Negative Ratings
Paul Lajoie-Mazenc, Emmanuelle Anceaume, Gilles Gueje, Thomas Sirvent and Valérie Viet Triem Tong

14:00	**Parallel Session 5e: Workshop on Assurance & Control / Workshop on Information Security Management**	223W

Security Operations Center
Stef Schinagl and Keith Schoon

Investigating Cloud Storage Security Requirements and Critical Controls
Farashazillah Yahya, Robert Walters and Gary Wills

End user development and information security culture
Fredrik Karlsson and Karin Hedström

15:30	Coffee Break	Ground Floor

16:00	**Parallel Session 6a: IFIP SEC (Access Control, Trust and Identity Management II, Chair: Simone Fischer-Hübner)**	121W

An Iterative Algorithm for Reputation Aggregation in Multi-dimensional and Multinomial Rating Systems
Mohsen Rezvani, Mohammad Allahbakhsh, Lorenzo Vigentini, Aleksandar Ignjatovic and Sanjay Jha

A Comparison of PHY-Based Fingerprinting Methods Used to Enhance Network Access Control
Timothy Carbino, Michael Temple and Juan Lopez Jr.

Model-driven Integration and Analysis of Access-control Policies in Multi-layer Information Systems
Salvador Martínez, Joaquin Garcia-Alfaro, Frédéric Cuppens, Nora Cuppens-Boulahia and Jordi Cabot

| 16:00 | **Parallel Session 6b: IFIP SEC (Network Security, Chair: Kai Rannenberg)** | 221W |

Authenticated File Broadcast Protocol
> *Simão Reis, André Zúquete, Carlos Faneca and José Vieira*

Automated Classification of C&C Connections through Malware URL Clustering
> *Nizar Kheir, Gregory Blanc, Hervé Debar, Joaquin Garcia-Alfaro and Dingqi Yang*

B.Hive: A Zero Configuration Forms Honeypot for Productive Web Applications
> *Christoph Pohl, Alf Zugenmaier, Michael Meier and Hans-Joachim Hof*

| 16:00 | **Parallel Session 6d: IFIPTM (Trust in Online Collaboration)** | 120W |

Obscuring Provenance Confidential Information via Graph Transformation
> *Jamal Hussein, Luc Moreau and Vladimiro Sassone*

Social Network Culture Needs the Lens of Critical Trust Research
> *Natasha Dwyer and Stephen Marsh*

Predicting Quality of Crowdsourced Annotations using Graph Kernels
> *Archana Nojamkandath, Jasper Oosterman, Davide Ceolin, Gerben Klaas Dirk de Vries and Wan Fokkink*

An Architecture for Trustworthy Open Data Services
> *Andrew Wong, Vivky Liu, William Caelli and Tony Sahama*

| 16:00 | **Parallel Session 6e: Workshop on Assurance & Control / Workshop on Information Security Management** | 223W |

IT audit and financial statement review
> *Andre Sanders*

Secure and Privacy Focused Customer Device Management in a Smart Household Environment
> *Vinh Pham, Hartmut Richthammer and Dogan Kesdogan*

| 18:15 | Bus transfer from Dammtor (Shell gas station, REISERING buses) to Gala Dinner. Alternatively, you can use public transport. See the program book in your conference bag for instructions. |

| 19:00 | Gala Dinner: **Lutter & Wegner (http://www.l-w-hamburg.de/location/)**, Große Elbstraße 49, 22767 Hamburg
Bring your badge / dinner ticket! |

| 21:30 | Early Bus from Restaurant back to Dammtor |

| 22:30 | Late Bus from Restaurant back to Dammtor |

| 23:00 | End of Gala Dinner; you can use public transport (Bus 112) from **Hafentreppe** or **Fischmarkt** bus stops to get back to Dammtor station. |

28 May 2015 (Thursday)

| 08:30 | Registration | First Floor |

| 09:00 | **Parallel Session 7a: IFIP SEC (Security Management and Human Aspects of Security II, Chair: Philippos Peleties)** | 121W |

Investigation of Employee Security Behaviour: A Grounded Theory Approach
> *Lena Connolly, Michael Lang and Doug J. Tygar*

Practice-Based Discourse Analysis of InfoSec Policies
> *Fredrik Karlsson, Goran Goldkuhl and Karin Hedström*

Understanding Collaborative Challenges in IT Security Preparedness Exercises
> *Maria B. Line and Nils Brede Moe*

| 09:00 | **Parallel Session 7b: IFIP SEC (Cyber-physical Systems and Critical Infrastructures Security, Chair: Peter Lambert)** | 221W |

Application of a Game Theoretic Approach in Smart Sensor Data Trustworthiness Problems
> *Konstantinos Maraslis, Theodoros Spyridopoulos, George Oikonomou, Theo Tryfonas and Mo Haghighi*

Securing BACnet's Pitfalls
> *Jaspreet Kaur, Jernej Tonejc, Steffen Wendzel and Michael Meier*

On the secure distribution of vendor-specific keys in deployment scenarios
> *Nicolai Kuntze and Carsten Rudolph*

| 09:00 | **Parallel Session 7c: WISE** | 220W |

WG 11.8 meeting (All IFIP WG 11.8 members) and WISE9 Closing

| 09:00 | **Parallel Session 7d: IFIPTM (Towards Trustworthy Cloud Infrastructures)** | 120W |

A Cloud Orchestrator for deploying public services on the cloud — the case of STRATEGIC project

> *Panagiotis Gouvas, Konstantinos Kalaboukas, Giannis Ledakis, Theo Dimitrakos, Joshua Daniel, Géry Ducatel and Nuria Rodriguez Dominguez*

Integrating Security Services in Cloud Service Stores

> *Joshua Daniel, Fadi El-Moussa, Géry Ducatel, Pramod Pawar, Ali Sajjad, Robert Rowlingson and Theo Dimitrakos*

Building an Eco-System of Trusted Services via user Control and Transparency on Personal Data

> *Michele Vescovi, Corrado Moiso, Mapa Pasolli, Lorenzo Cordin and Fabrizio Antonelli*

Security-as-a-Service in Multi-cloud and Federated Cloud Environments

> *Pramod S. Pawar, Ali Sajjad, Theo Dimitrakos and David W. Chadwick*

The role of SLAs in building a Trusted Cloud for Europe

> *Ana Juan Ferrer and Enric Pages i Montanera*

| 10:30 | Coffee Break | Ground Floor |

| 11:00 | **IFIP SEC 2015 Awards Session** | 221W |

Video message from the Kristian Beckman Award 2015 winner **(download MOV file, 575 MB) (files/Ian_Brown_May2015.mov)**

> *Ian Brown, Professor of Information Security and Privacy at the Oxford Internet Institute of the University of Oxford*

IFIP SEC 2015 Best Student Paper Award

Reputation – from Social Perception to Internet Security

> *Ehud Gudes, Ben-Gurion University of the Negev, William Winsborough Award Winner*

| 12:30 | **IFIP SEC 2015 Closing Remarks** | 221W |

| 12:30 | **IFIPTM 2015 Closing Remarks** | 221W |

| 14:30 | Optional Social Event: **Waterways trip "Fleetfahrt" (http://www.alstertouristik.de/English/classics/waterways-trip.html?)** |

Boat departs from Jungfernstieg at the waterfront (pier number will be announced on Wednesday at the registration desk).
Important notes: You have to sign up for the social event at the registration desk. There is no organized transfer from SEC venue. There is no lunch on the boat and no space for large pieces of luggage.

| 16:30 | End of optional Social Event |

Boat returns to Jungfernstieg.

29 May 2015 (Friday)

Important note: The Workshop on Information Security Management is now scheduled on 27 May 2015 (Wednesday) 16:00-17:30.