Information Security and Cryptography

Fundamentals and Applications

June 11–13, 2018

Lecturers:
Prof. David Basin, ETH Zurich
Prof. Ueli Maurer, ETH Zurich

Zurich, Switzerland

ATG Advanced Technology Group
www.infsec.ch

Program
Starting 09:00 on Monday June 11 and ending at 17:00 on June 13

Information Security: An Overview
- Information at Risk: Threats, Security Objectives, and Security Measures
- Classification of the Fundamental Information Security Problems
- Course Overview

Cryptography: Basic Concepts
- Some History
- Types and Models of Cryptographic Systems
- Cryptographic Functions, Hash Functions
- Secrecy, Authenticity, and their Duality and Independence
- Symmetric Cryptography: Block Ciphers, Stream Ciphers, MACs, etc.
- Randomness and Pseudo-Randomness
- Cryptanalytic Attacks, Assumptions, Security Definitions
- Public-Key Encryption and Secret-Key Agreement
- Digital Signatures, Certificates

Cryptography Foundations
- Discrete Mathematics Basics, Groups, Fields
- Theoretical Foundations of Cryptography
- Discrete Logarithms, Factoring, and other Hard Problems
- Design and Analysis of Cryptographic Systems
- RSA: Workings and Security Analysis
- Diffie-Hellman Protocol: Workings and Security Analysis
- Elliptic Curve Cryptography
- Modes of Operation for Cryptographic Systems
- Security Proofs, Indistinguishability, Reductions
- Constructive Cryptography and Universal Composability

System and Network Security
- Networking Essentials
- Trade-offs in Securing Network Layers
- Security Protocols including Kerberos, SSL, IPsec
- Security Architectures
- Firewalls and Intrusion Detection

PKI and Key Management

- Key Management Challenges
- PKI Certificates, Architectures, and Standards
- Key Revocation and Recovery
- Trust Models (Direct, Cross, Hierarchical, Web of Trust)
- X.509 and PGP
- Alternative PKIs: Client, CA, and Domain-Centric Options
- Certificate Handling in Web Browsers

Authentication, Authorization, and Access Control

- AAA Architectures: Authentication, Authorization, and Access Control
- Authentication: Passwords, Biometrics, and Token-based
- Policies and Models
- Access Control Matrix Model
- DAC and MAC Models
- BLP, Biba, and Chinese Wall Models
- RBAC, XACML
- Single Sign-on
- Identity Management

Privacy and Usage Control

- Data Protection and Control of Intellectual Property
- Anonymity and Privacy-enhancing Technologies
- Proxies, Mix Networks, and other Anonymity Approaches
- Usage Control Architectures
- Digital Rights Management and Trusted Computing

Security Engineering and Web-Application Security

- Security Engineering in the Software Engineering Life Cycle
- Common Vulnerability Classes including: Session Management, Injection Attacks, Cross-Site Scripting, and Race Conditions.
- Security Standards and Certification

Advanced Topics in Cryptography

- Cryptographic Protocols
- Zero-Knowledge Protocols
- Secure Multi-Party Computation
- E-Voting
- Digital Payment Systems, E-Cash
- Block-chains, Smart Contracts
- Crypto-Currencies, Bitcoin
- Quantum Cryptography

ATG Advanced Technology Group

www.infsec.ch

Lecturers

David Basin is a full professor of Computer Science at ETH Zurich. He received his Ph.D. in Computer Science from Cornell University in 1989 and his Habilitation in Computer Science from the University of Saarbrucken in 1996. From 1997 to 2002 he held the chair of Software Engineering at the University of Freiburg in Germany. His research areas are Information Security and Software Engineering. He is the founding director of the ZISC, the Zurich Information Security Center, which he led from 2003 to 2011. He is Editor-in-Chief of the ACM Transactions on Privacy and Security and of Springer-Verlag's book series on Information Security and Cryptography. He serves on various management and scientific advisory boards, co-founded three security companies, and has consulted extensively for IT companies and government organizations.

Ueli Maurer is a full professor of Computer Science at ETH Zurich. His research interests include the theory and applications of cryptography and information security. He served as the Editor-in-Chief of the Journal of Cryptology from 2001 to 2010, and Editor-in-Chief of Springer Verlag's book series in Information Security and Cryptography from 1997 to 2012. Maurer holds several patents for cryptographic systems. He serves on several management and scientific advisory boards, has consulted extensively for the financial industry, the IT industry, and government organisations, and has co-founded the Zurich-based security-software company Visonys AG. He is an IEEE Fellow, an ACM Fellow, an IACR Fellow, and recipient of the 2013 Vodafone Innovation Award for Mobile Communications and the 2016 RSA Award for Excellence in the Field of Mathematics.

Seminar goals

Information Security and Cryptography are of vital importance today, with applications in communication and information systems, cyberphysical systems, and more generally, in the digitalization of businesses and services. Our 2018 seminar covers complementary topics and is aimed at different target audiences, providing an in-depth coverage of Information Security and Cryptography from both a conceptual and an application-oriented viewpoint. At the same time, the mathematical, algorithmic, protocol-specific, and system-oriented aspects are explained in a way understandable to a wide audience. This includes the foundations needed to understand the different approaches, a critical look at the state-of-the-art, and a perspective on future security technologies.

The seminar is aimed at all professionals who need up-to-date knowledge and expertise in this area. This includes system designers and engineers, security experts, IT-professionals, instructors, project managers, consultants, law enforcement professionals, and professional cryptographers.

The material is presented at three different levels. At the *highest level*, the basic concepts are presented in detail, but abstractly (e.g., as black boxes), without mathematics. No background is required to follow at this level. At an *intermediate level*, the most important concrete schemes, models, algorithms, and protocols are presented as well as their applications. Here some minimal mathematical and systems background is assumed. At the *deepest level*, which is not required to understand the higher levels, different special topics, requiring some mathematical background, are discussed.

Venue

The seminar will take place at the Marriott Courtyard Zurich North, Max-Bill-Platz 19, CH-8050 Zurich, Switzerland. The seminar hotel is conveniently located between downtown Zurich and the airport, easily accessible from both with public transportation.

ATG Advanced Technology Group

Seminar enrollment 2018

Venue: Hotel Marriott Courtyard Zurich Nord
Max-Bill-Platz 19, CH-8050 Zurich, Switzerland

❒ Ms. ❒ Mr. ❒ Dr. ❒ Prof. ❒ Other: .....

Last name: .....

First name: .....

Company name: .....

Business address: .....

.....

Invoice address: .....

.....

Your ref-no for invoice.: .....

Phone: .....

Fax: .....

Email: .....

"Information Security and Cryptography" on June 11-13, 2018 in Zurich, Switzerland

Early registration before February 28, 2018: CHF 3,500

Standard registration as from March 1, 2018: CHF 3,900

Payment to be made upon receipt of invoice by means of bank transfer.

Price includes course material, lunches, coffee breaks, and beverages during the seminar.

Date: ..... Signature: .....

Send to: ATG Advanced Technology Group GmbH – Grundgasse 13 – CH-9500 Wil
info@infsec.ch – www.infsec.ch
Fax +41-(0)44-632 1172

ATG **Advanced Technology Group**

Hotel reservation 2018

Venue: Hotel Marriott Courtyard Zurich Nord
Max-Bill-Platz 19, CH-8050 Zurich, Switzerland

Please reserve your hotel room for the seminars directly with the hotel (and with payment to the hotel). Note that there are a limited number of discounted rooms available for the seminar on a first-come first-serve basis. Please reserve your room at your earliest convenience. The block reservation cut-off date is May 1, 2018.

❒ Single room (CHF 279 including breakfast and WLAN)

❒ Double room (CHF 299 including breakfast and WLAN)

Arrival date: ..... Departure date: .....

❒ Ms. ❒ Mr. ❒ Dr. ❒ Prof. ❒ Other: .....

Last name / first name: .....

Company name: .....

Business address: .....

.....

Phone: .....

Fax: .....

Email: .....

Credit card number: .....

Expiration date: .....

Name on card: .....

Type of card: .....

Date: ..... Signature: .....

Send to: Marriott Courtyard Zurich North – Max-Bill-Platz 19 – CH-8050 Zurich – Switzerland
Fax +41-(0)44-564 0400