

# **Information Security and Cryptography**

## **Seminar offerings**

**June and July 2012  
Zurich Switzerland**

### **Organizers**

**David Basin, ETH Zurich**

**Ueli Maurer, ETH Zurich**

**ATG** **Advanced Technology Group**

Seminars in collaboration with the Department of Computer Science, ETH Zurich

# Seminar 1: Information Security and Cryptography — Fundamentals and Applications

Monday, June 11 (09:00h) – Wednesday, June 13, 2012 (17:00h)

Lecturers: David Basin and Ueli Maurer

This seminar provides an in-depth coverage of Information Security and Cryptography from both a conceptual and 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 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.

## **Information Security: An Overview**

- Information at Risk: Threats, Security Objectives, and Security Measures
- Classification of the Fundamental Information Security Problems
- Information Security as Policy Compliance
- Information Security as Risk Minimization

## **Cryptography: Basic Concepts and Terminology**

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

## **Cryptography Foundations**

- Basics of Discrete Mathematics
- 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
- Digital Signature Standard (DSS)
- Elliptic Curve Cryptography
- Modes of Operation for Cryptographic Systems
- Indistinguishability of Systems
- Simulation-based Security Definitions and Proofs
- The Constructive Cryptography Framework
- Universal Composability
- Provable Security

## **System and Network Security**

- Review of 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 Problems
- PKI Certificates, Architectures, and Standards
- Key Revocation and Recovery
- Trust Models (Direct, Cross, Hierarchical, Web of Trust)
- X.509 and PGP
- Naming and Identity
- Certificate Handling in Web Browsers

## **Nonrepudiation and Digital Evidence**

- The Digital Evidence Dilemma
- Types of Digital Evidence
- Semantics of Digital Signatures
- Certificates, Time-stamps
- Revalidation, Revocation
- Digital Signatures vs. Handwritten Signatures
- Digital Signature Legislation

## **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
- Trusted Computing

## **Advanced Topics in Cryptography**

- Cryptographic Protocols, Identification Protocols
- Zero-Knowledge Protocols
- Digital Payment Systems, E-Cash
- Secure Multi-Party Computation
- E-Voting
- Quantum Cryptography

# Seminar 2: Building Secure Software Systems

Thursday, June 14 (09:00h) – Friday, June 15, 2012 (17:00h)

Lecturers: David Basin and Torsten Lodderstedt

This seminar presents sound methods that can be used to build and evaluate security-critical software systems. The focus is on the interplay between two areas: Software Engineering and Information Security. The role of security in all phases of the software-development process is examined, including requirements analysis, risk analysis, design, implementation, and testing, as well as verification and certification. In each phase, relevant concepts, methods, and tools are covered. The material is presented in a self-contained way. However, a basic knowledge of both Information Security (e.g., from Seminar 1) and Software Engineering are assumed.

## Introduction

- Overview of Security Engineering and its Principle Challenges
- Software Engineering Activities and Where Security Fits In

## Modeling Foundations

- Role of Models in System Development
- Unified Modeling Language (UML)
- Modeling in Requirements Engineering
- Modeling in Security Design and Risk Analysis

## Requirements Engineering for Security-critical Systems

- Functional and Non-functional Requirements
- Safety and Security
- Use and Misuse Cases
- Authorization Policies based on Use Case Models
- Information Security Policies based on Domain Models
- Documenting Requirements

## Threat Modeling and Risk Analysis

- Systematic Threat Analysis using Data Pathways
- UML-based Attack Trees
- Threat and Standard Vulnerability Catalogs
- Ingredients of Risk Analysis: Assets, Threats, and Vulnerabilities
- Quantitative and Qualitative Approaches

## Security in the Design Process

- General Security Design Options
- Pattern Catalogs and Standard Counter-measures
- Modeling and Automatically Generating Security Infrastructures
- Security Design as an Iterative Process with Risk Re-evaluation

## Implementation-level Security

- Security Design Patterns for Vulnerabilities
- Typical Vulnerabilities and Countermeasures: Buffer Overflows, Format String Attacks, Injection Attacks, Cross Site Scripting, Timing Vulnerabilities, Session Handling

## Testing

- Objectives and Limitations of Testing
- Model-based Testing, Code-based Testing
- Vulnerability Testing and other Security-specific Testing Methods

## Evaluation Criteria

- Role of Standards in Evaluation
- NIST, Common Criteria, and ISO/IEC 27000-Series
- IT Baseline Protection

# Seminar 3: Wireless and Mobile Network Security

Tuesday, July 3 (09:00h) – Wednesday, July 4, 2012 (17:00h)

Lecturer: Srdjan Capkun

The seminar covers relevant security and privacy issues in contemporary and emerging wireless networks. The seminar focuses on attacks and countermeasures in different types of wireless networks and their applications. Attacks and countermeasures are first presented conceptually and then analyzed in the context of their real-world realizations. For selected attacks and countermeasures, protocols and experimental setups are presented in detail. The seminar is self-contained and accessible to a wide audience, but the knowledge of basic security and wireless networking concepts is beneficial.

## Physical-Layer Considerations

- Eavesdropping on Wireless Channels
- Insertion and Message Manipulation
- Jamming and Jamming Resistance
- Physical-layer Device Identification (Remote Device Fingerprinting)

## Link-Layer Considerations

- Medium Access Control Security
- Cooperation and Selfishness
- Denial of Service (DoS)

## Security of Contemporary Networks

- WiFi networks (WEP, WPA, WPA2)
- Cellular networks (GSM and UMTS Security Architectures)

## Security in Sensor Networks

- Efficient Cryptographic Primitives for Embedded Devices
- Key Distribution
- Efficient Authentication Mechanisms

## Modern Smartphone Platforms

- Security Architectures
- Application Security
- Access Control Mechanisms
- Privacy Considerations

## Security of RFID Systems

- HF/UHF RFID Systems
- Access Control Protocols
- Cloning Detection (Protected Memory, PUFs)
- Privacy Considerations
- Application in E-passports

## Security of Localization Systems and of Location-Based Services

- WiFi-based Localization
- Ultra-Wide-Band (UWB) and Chirp Spread Spectrum Systems
- Global Positioning System (GPS)
- Proximity-Based Access Control (e.g., to Cars and Buildings)

## Special Topics

- Passive Keyless Entry and Start Systems in Modern Cars
- Security of Implantable Medical Devices, such as Pacemakers
- GSM Spoofing Attacks
- Relay Attacks on NFC Communication
- Security of Modern Cars

# Seminar 4: Applied Information Security, Hands-on!

Thursday, July 5 (09:00h) – Friday, July 6, 2012 (17:00h)

Lecturers: David Basin and Patrick Schaller

In this seminar participants carry out hands-on experiments in Information Security. The experiments illustrate common information security problems and pitfalls arising in modern operating systems, networks, and web applications, and how to avoid or fix them. The seminar participants are introduced to the problems and afterwards carry out exploits and work through different countermeasures. In this way, they gain a detailed understanding of how vulnerabilities arise in practice and practical experience countering them.

All experiments are carried out on Linux systems, running within a virtualized networked environment. The environment runs within VirtualBox, an open source virtualization platform available for most commonly used operating systems, such as Windows, Mac OS X, and Linux. Seminar participants are expected to bring a laptop on which VirtualBox can be installed and to use their laptop for the experiments using the virtual machines provided.

## VirtualBox

- Introduction to Virtualization and VirtualBox
- Installation of Virtual Machines on Participants' Laptops

## Network Security

- Remote Access and Procedure Calls: TCP/IP, Servers, and Daemons
- Port and Vulnerability Scanners
- Network Sniffers
- Firewalls and TCP-wrappers

## Intrusion Detection

- Basic Techniques
- Integrity Checks: finding Rootkits

## Authentication and Access Control

- Securing Remote Access
- Controlling Access to Data and Programs
- Administration using Shell Scripts and its Pitfalls

## Logging and Log Analysis

- Log Mechanisms, Remote Logging
- Authenticity of Log Entries, Tamper-proof Logging
- Log Analysis

## Web Application Security

- Application Profiling: Gathering Information about Website Configurations
- Vulnerabilities and Attack Techniques: SQL Injections, Cross-Site Scripting, Remote Command Execution, Remote File Upload, Cookie Stealing, Privilege Escalation to gain Root Access, etc.
- User Authentication and Session Management
- Using SSL for Secure Web Server Access
- Identifying and Testing Potential Weaknesses: White and Blackbox Approaches

## Certificates and Public Key Cryptography using Apache

- Basics Concepts
- Creating Public and Private Keys
- Creating and Revoking Certificates
- Running a Certificate Authority
- Certificate-based Client Authentication

**NOTE:** Participants must bring their own notebook computer to the seminar.

## 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 Saarbrücken in 1996. From 1997–2002 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 2003-2011. He serves on the editorial boards of numerous journals including IEEE Transactions on Dependable and Secure Computing and Acta Informatica. He is Editor-in-Chief (together with Ueli Maurer) of Springer-Verlag's book series in Information Security and Cryptography. He serves on various management and scientific advisory boards and has consulted extensively for IT companies and government organizations.



**Ueli Maurer** is a full professor of Computer Science at ETH Zurich. He received his Ph.D. degree in electrical engineering from ETH Zurich in 1990. From 1990–1991 he was a DIMACS post-doctoral fellow at the Department of Computer Science, Princeton University. His research interests include the theory and applications of cryptography and information security. Currently he is Editor-in-Chief of the Journal of Cryptology, and Editor-in-Chief (with David Basin) of Springer Verlag's book series in Information Security and Cryptography. 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 a Fellow of the IEEE and a Fellow of the IACR.



**Srdjan Capkun** is an associate professor of Computer Science at ETH Zurich. He received his Ph.D. degree in Communication Systems from EPFL in 2004. Prior to joining ETH Zurich in 2006 he was a postdoctoral researcher at the University of California Los Angeles and an assistant professor at the Technical University of Denmark. He is the director of the Zurich Information Security Center since 2011 and a member of the RFID Consortium for Security and Privacy. He is an associate editor of the IEEE Transactions on Mobile Computing and was a program chair of the ACM Conference on Wireless Network Security in 2009. He coauthored several patents in secure localization and location-based access control and with his group discovered numerous vulnerabilities in commercial localization and physical access-control systems.



**Torsten Lodderstedt** is a Senior Expert in Identity Management Services and a System Architect with Deutsche Telekom AG. In his previous positions as consultant and IT architect, he has helped customers since 1996 in various sectors (e.g. government, finance, railway, tele-communication) to build large-scale, security-critical IT systems. He received his Ph.D. in Computer Science from the University of Freiburg in Germany in 2004. His areas of expertise are Information Security, identity management, software engineering methods and tools, and software architectures.



**Patrick Schaller** received his masters in mathematics in 1999 and his Ph.D. in Computer Science in 2010, both from ETH Zurich. He has worked in numerous industry positions related to Information Security, including as an information security officer for a major Internet service provider and as a software engineer for the finance industry. He currently works for Avaloq as a software engineer developing security-critical software components for the banking industry.

## Seminar goals

Information Security and Cryptography are of vital importance today, with applications in communication and information systems, electronic commerce, and more generally, in the emerging Information Society. Our 2012 seminars cover complementary topics and are aimed at different target audiences.

**Seminar 1** presents the foundations of Information Security and Cryptography. It 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 seminar provides an excellent basis for the other three seminars.

**Seminar 2** explains concepts, methods, and tools for building secure systems. It is aimed at all professionals who develop, analyze, or manage security-critical systems. This includes system designers and engineers, programmers, project managers and consultants, as well as instructors in this area.

**Seminar 3** covers relevant security and privacy issues in contemporary and emerging wireless networks. The seminar focuses on attacks and countermeasures in different types of wireless networks and their applications. Attacks and countermeasures are first presented conceptually and then analyzed in the context of their real-world realizations. For selected attacks and countermeasures, protocols and experimental setups are presented in detail. The seminar is self-contained and accessible to a wide audience, but a knowledge of basic security and wireless networking is beneficial.

**Seminar 4** provides a hands-on experimental counterpart to the other seminars. It helps participants better understand the principles of securing systems, by seeing how vulnerabilities arise in modern operating systems, networks, and Web applications and gaining practical experience in employing countermeasures. The seminar presumes basic knowledge of Information Security and some experience using Unix-like systems. It is aimed at system designers and administrators, as well as IT professionals who want hands-on experience in applied information security.

## Venue

All four seminars will take place at

Courtyard Zurich North  
Max-Bill-Platz 1  
CH-8050 Zurich  
Switzerland

The hotel is located between downtown Zurich and the airport, easily accessible in a few minutes with public transportation.

**ATG** Advanced Technology Group

[www.infsec.ch](http://www.infsec.ch)

## Seminar enrollment 2012

Venue: Courtyard Zurich Nord  
Max-Bill-Platz 1, CH-8050 Zurich, Switzerland

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

Last name / first name: .....

Business address: .....

.....

.....

Phone: .....

Fax: .....

Email: .....

Seminar 1 "Information Security and Cryptography" on June 11-13, 2012  
Early registration before February 29, 2012: CHF 3,500  
Standard registration as from March 1, 2012: CHF 3,800

Seminar 2 "Building Secure Software Systems" on June 14-15, 2012  
Early registration before February 29, 2012: CHF 2,400  
Standard registration as from March 1, 2012: CHF 2,600

Seminar 3 "Wireless and Mobile Network Security" on July 3-4, 2012  
Early registration before March 30, 2012: CHF 2,400  
Standard registration as from April 1, 2012: CHF 2,600

Seminar 4 "Applied Information Security, Hands-on!" on July 5-6, 2012  
Early registration before March 30, 2012: CHF 2,400  
Standard registration as from April 1, 2012: CHF 2,600  
*Participants must bring their own notebook computer to Seminar 4.*

Price includes course material, lunches, coffee breaks, and beverages during the seminar.  
If you register for two or more seminars this year, we offer a discount of 5%.

Check enclosed payable to ATG Advanced Technology Group GmbH, Wil

Payment will be made upon receipt of invoice

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

**Hotel reservation 2012**

Venue: Courtyard Zurich Nord  
Max-Bill-Platz 1, CH-8050 Zurich, Switzerland

Reference: ATG seminars 2012 "Information Security and Cryptography"

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 seminars on a first-come first-serve basis. Please reserve your room at your earliest convenience. The block reservation cut-off date is May 11, 2012 for Seminars 1 and 2, and June 3 for Seminars 3 and 4.

- Single room
- Double room

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

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

Last name / first name: .....

Business address: .....  
.....  
.....

Phone: .....

Fax: .....

Email: .....

Credit card number: .....

Expiration date: .....

Name on card: .....

Type of card: .....

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