Software and System Security 1 – Overview

Prof. Dr. Marc Rennhard, Dr. Stephan Neuhaus
Institut für angewandte Informationstechnologie InIT
ZHAW School of Engineering
rema | neut @zhaw.ch

Module Software and System Security 1 (SWS1-EN)

- Lecturers
  - Prof. Dr. Marc Rennhard, rema@zhaw.ch,
    Office TD O3.01, 058 934 7245

  - Dr. Stephan Neuhaus, neut@zhaw.ch,
    Office TG 203, 058 934 4767
  - We are part of the Information Security Research Group at the Institute of Applied Information Technology (InIT, www.zhaw.ch/init)
    → If you are interested in doing further work in information security, don't hesitate to contact us
    - E.g., bachelor thesis, MSE positions, research positions,...
    - For details, see the final three slides of this slide set and the InIT website
- Learning platform: Moodle, moodle.zhaw.ch
  - Primary source of information, schedule, module materials

Goals

The overall goal of this module is that you learn to develop secure software and systems. In particular, you will acquire the following skills:

- You understand the overall secure software development lifecycle and the security activities that must be employed during the different phases; and you can apply these activities to any given software development process.
- You are capable of designing secure systems by defining appropriate security requirements and by integrating suitable security controls into a system design.
- You are capable of developing secure systems. For this, Java will be used as the example language and technology, but most what you learn can directly be applied to other languages and technologies.
- You know methods and tools to detect security vulnerabilities in implemented systems and you can apply these methods and tools to find and exploit vulnerabilities on your own. This is called penetration testing.
- You know methods to analyze the security of a system design and you can apply these methods to uncover conceptual security vulnerabilities. This is often identified as threat modeling.

Lecture Topics (1)

1. Introduction to Software Security
   - Motivation, examples, terminology
2. Secure Development Lifecycle
   - Security activities during a secure software development lifecycle
3. Software Security Errors
   - Overview of security-relevant software errors and detailed discussion of some typical examples such as buffer overflows
4. Java Security
   - Components of the Java library to implement cryptographic operations and secure communication in Java programs (JCA, JSSE)
5. Fundamental Security Principles
   - General but very important security guidelines you should always keep in mind when thinking about security during software development

Lecture Topics (2)

6. Web Application Security Testing
    - How to find and exploit vulnerabilities in web applications
7. Developing Secure Traditional Web Applications
    - How to design and develop secure web applications that follow a traditional architecture (i.e., monolithic, code mainly runs server-side)
8. Developing Secure Modern Web Applications
    - How to design and develop secure web applications that follow a modern architecture (i.e., single page applications that use REST based microservices and lots of JavaScript code in the browser)
9. Security Requirements Engineering and Threat Modeling
    - Methods to define the right security requirements and to uncover conceptual security vulnerabilities in a security architecture / design
10. Security Risk Analysis
    - Methods to rate the risk (severity) of vulnerabilities

Lab Topics (1)

1. Secure File Storage Service
   - Analyze and fix a simple but very insecure file storage service program to see how even simple programs can easily contain serious vulnerabilities

2. Buffer Overflow Attacks
   - Find and exploit different types of buffer overflow vulnerabilities in C programs

3. Cryptography in Java
   - Develop a program to authenticate, integrity-protect and encrypt files using various cryptographic algorithms

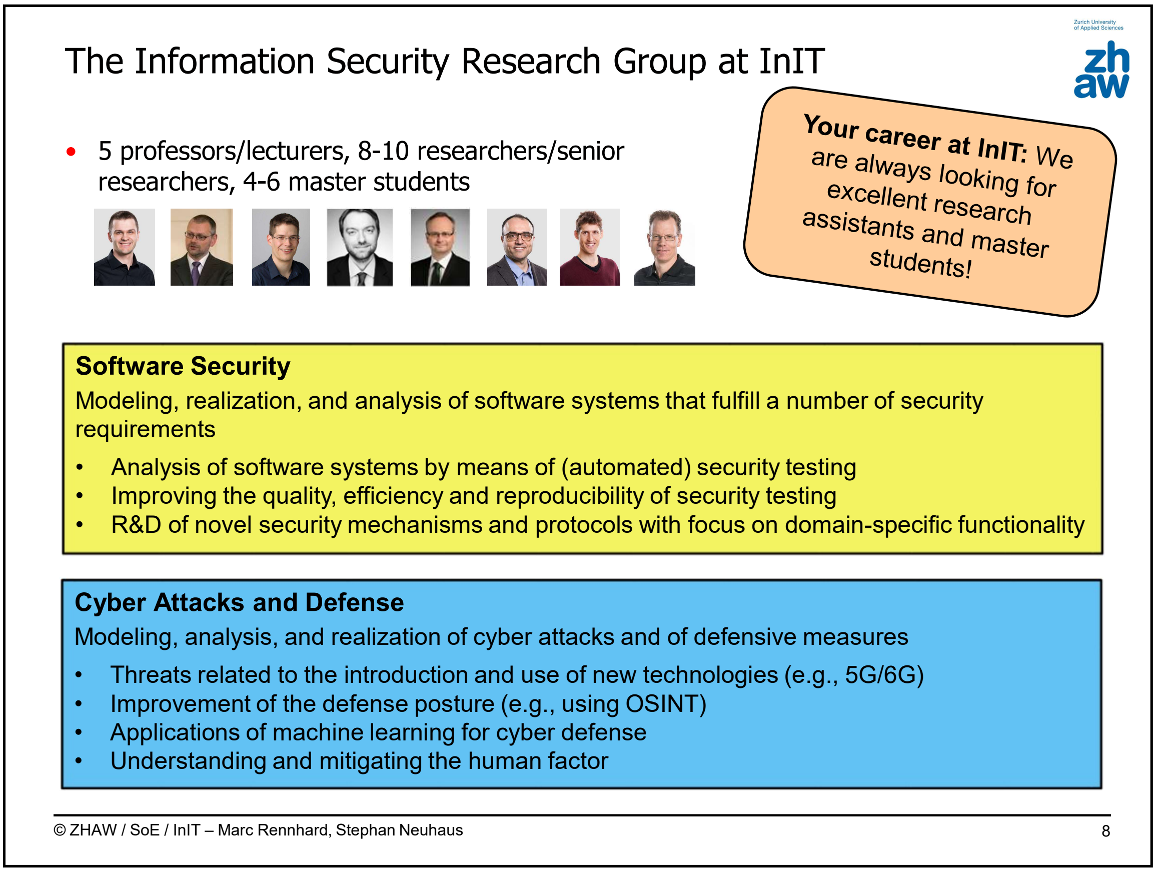
4. Security Testing a Webshop Application
   - Find and exploit vulnerabilities in an e-shop web application that was developed by security-unaware students

Lab Topics (2)

5. Security Testing Tools
   - Experiment with a static code analysis tool and a vulnerability scanner to learn about the possibilities and limitations of automated testing tools

6. Developing Secure Web Applications and RESTful Web Services: Extending Marketplace
   - Extend a Jakarta EE application discussed in the lecture with additional functions and implement the right security measures

7. Security Requirements Engineering and Threat Modeling
   - Analyze a given scenario for conceptual security vulnerabilities and propose appropriate security requirements



The Information Security Research Group at InIT

- 5 professors/lecturers, 8-10 researchers/senior researchers, 4-6 master students

Your career at InIT: We are always looking for excellent research assistants and master students!

Software Security

Modeling, realization, and analysis of software systems that fulfill a number of security requirements

- Analysis of software systems by means of (automated) security testing
- Improving the quality, efficiency and reproducibility of security testing
- R&D of novel security mechanisms and protocols with focus on domain-specific functionality

Cyber Attacks and Defense

Modeling, analysis, and realization of cyber attacks and of defensive measures

- Threats related to the introduction and use of new technologies (e.g., 5G/6G)
- Improvement of the defense posture (e.g., using OSINT)
- Applications of machine learning for cyber defense
- Understanding and mitigating the human factor

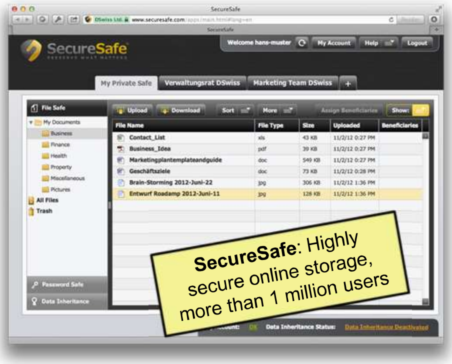
Contact Information of Professors/Lecturers in the Information Security Research Group:

- Dr. Peter Berlich, berp@zhaw.ch (lecturer)
- Dr. Stephan Neuhaus, neut@zhaw.ch (lecturer)
- Tobias Ospelt, ospe@zhaw.ch (part time lecturer)
- Prof. Dr. Marc Rennhard, rema@zhaw.ch (head of institute InIT)
- Prof. Dr. Bernhard Tellenbach, tebe@zhaw.ch (head of information security research group)

Websites of InIT and Information Security Research Group:

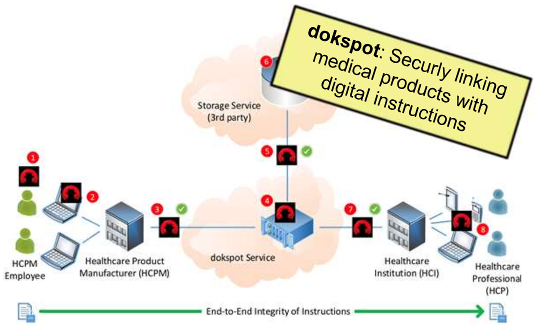
- InIT: www.zhaw.ch/init
- Information Security Research Group: www.zhaw.ch/de/engineering/institute-zentren/init/information-security/

The Information Security Research Group – Project Examples



File Name	File Type	Size	Uploaded	Beneficiaries
Contact_List	xls	43 KB	11/2/12 0:27 PM	
Business_Idea	pdf	39 KB	11/2/12 0:27 PM	
Marketingplantemplateandguide	doc	549 KB	11/2/12 0:27 PM	
Geschäftsziele	doc	73 KB	11/2/12 0:28 PM	
Brain-Storming 2012-Juni-22	jpg	306 KB	11/2/12 1:36 PM	
Entwurf Roadamp 2012-Juni-11	jpg	128 KB	11/2/12 1:36 PM	

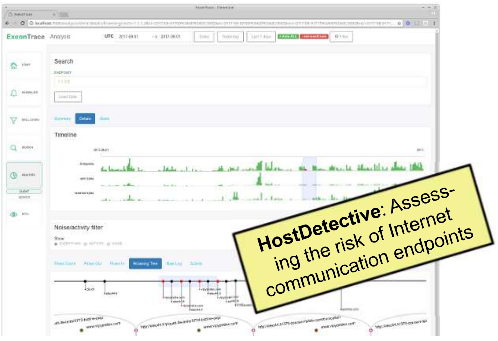
SecureSafe: Highly secure online storage, more than 1 million users



Storage Service (3rd party)
HCPM Employee
Healthcare Product Manufacturer (HCPM)
dokspot Service
Healthcare Institution (HCI)
Healthcare Professional (HCP)
End-to-End Integrity of Instructions
1
2
3
4
5
6
7
8

dokspot: Securly linking medical products with digital instructions

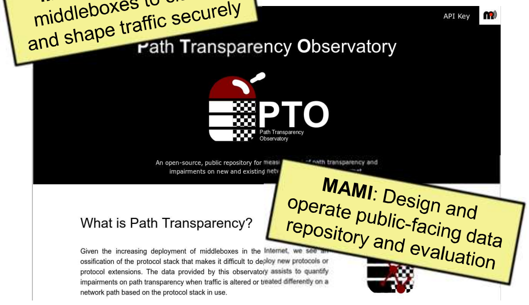
scanmeter: Continuous and fully automated security analysis of software and systems



HostDetective: Assessing the risk of Internet communication endpoints

The Information Security Research Group – Project Examples

MAMI: Allow Internet middleboxes to classify and shape traffic securely



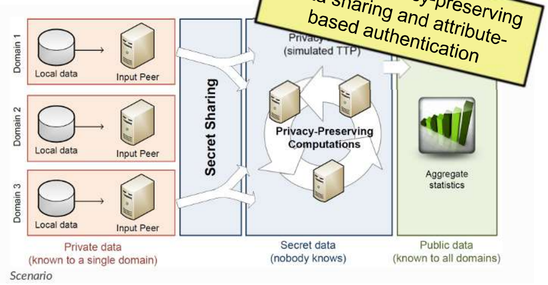
An open-source, public repository for meas… …f path transparency and impairments on new and existing netv…

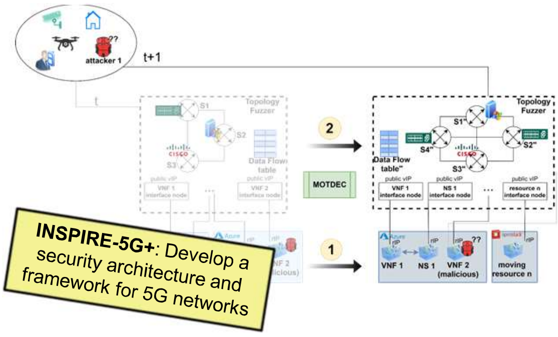
What is Path Transparency?

Given the increasing deployment of middleboxes in the Internet, we see an ossification of the protocol stack that makes it difficult to deploy new protocols or protocol extensions. The data provided by this observatory assists to quantify impairments on path transparency when traffic is altered or treated differently on a network path based on the protocol stack in use.

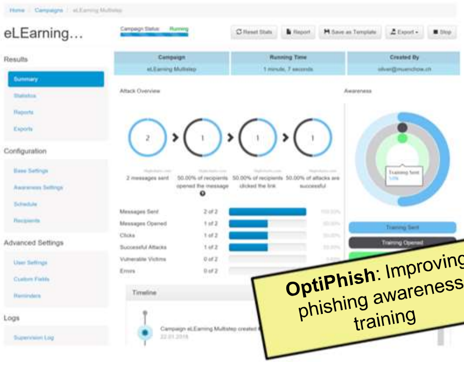
MAMI: Design and operate public-facing data repository and evaluation

FIWARE: Privacy-preserving data sharing and attribute-based authentication





INSPIRE-5G+: Develop a security architecture and framework for 5G networks



Campaign	Running Time	Created By
eLEarning Multistep	1 minute, 7 seconds	oliver@muenchow.ch

2 messages sent · 50.00% of recipients opened the message · 50.00% of recipients clicked the link · 50.00% of attacks are successful

Messages Sent	2 of 2	100.00%
Messages Opened	1 of 2	50.00%
Clicks	1 of 2	50.00%
Successful Attacks	1 of 2	50.00%
Vulnerable Victims	0 of 2	0.00%
Errors	0 of 2	

Campaign eLEarning Multistep created
22.01.2018

OptiPhish: Improving phishing awareness training