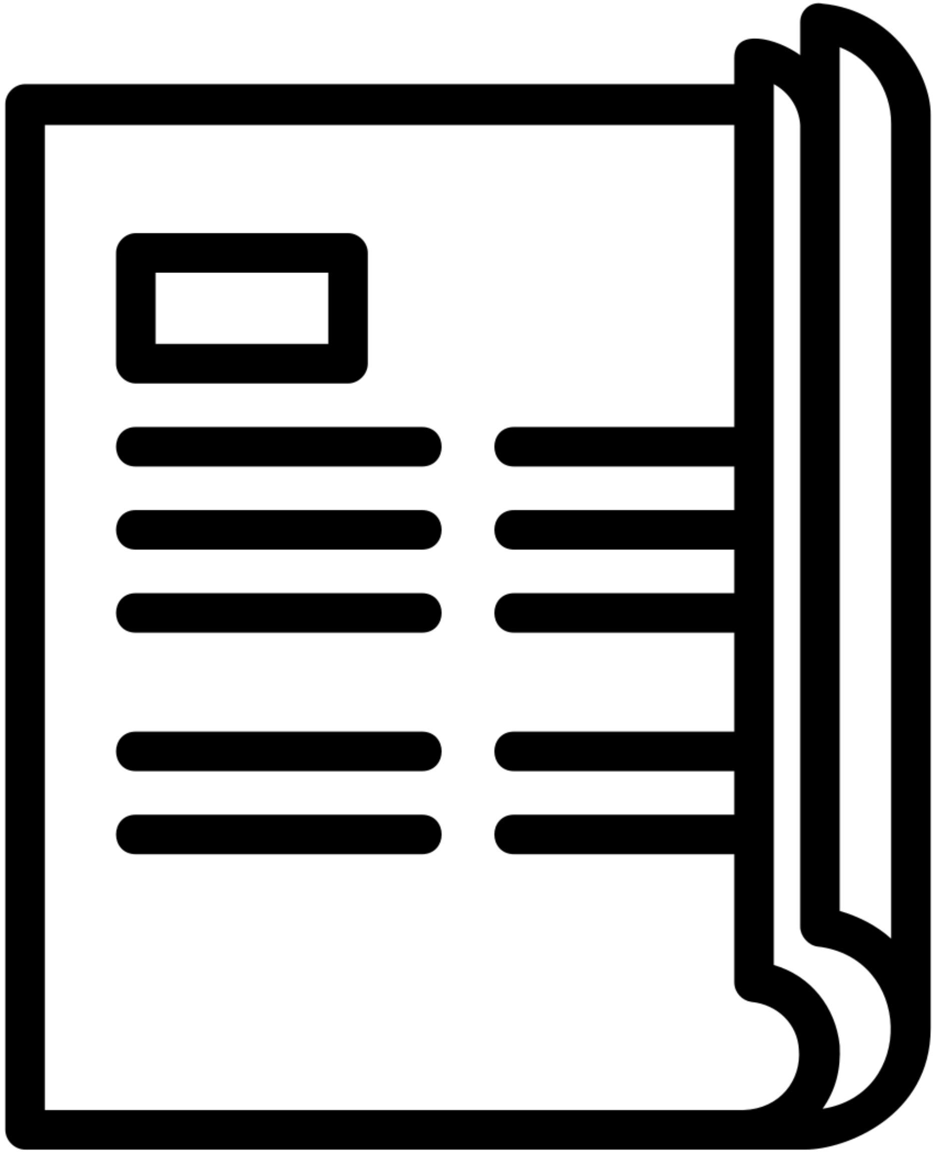


SWS2 - OVERVIEW

Prof. Dr. Bernhard Tellenbach

Module Software and System Security 2 (SWS2-EN)

- Team
  - Prof. Dr. Bernhard Tellenbach
    Head of Research Area, Information Security
    tebe@zhaw.ch, Office TG 210, 058 934 6568
  - Wissem Soussi
    Research Assistant, PhD Student
    sous@zhaw.ch

- You want to work in security? Don’t hesitate to contact us!
  - Consider a Master of Science in Engineering (MSE) with focus on Information Security – We offer a co-operative program of work and study (part-time positions)
  - Consider working for us as a research assistant!
- Teaching platform: Moodle, https://moodle.zhaw.ch
  - Course SWS2 – FS2022
  - Primary source of information, timetable, material

Goals

- Students receive a sound introduction to system security. The focus of the module is set on "Modern Attack Techniques & Ethical Hacking", "Modern Defense Techniques", "Mobile Security" and "The Human Factor in Information (In)Security".
- You know and understand modern techniques and methods to attack and defend IT infrastructures, and you are familiar with their strengths and weaknesses.
- You know the basic procedure of a penetration test and can carry out key elements of such a test on your own.
- You can implement methods and techniques for monitoring networks and systems in lab settings and assess their suitability for detecting a compromise of the monitored system.
- You know important security concepts of mobile platforms and common mistakes made when developing applications for them. You can apply this know-how to improve the security of your own mobile applications
- You know about awareness measures that can help to address the human risk factor and you can judge their effectiveness

Course Overview (1)

Part I

- Introduction to Securing Information Systems (2)
  - Overview on how to secure information systems (high-level)
- Threat Landscape (2)
  - Overview and how and where to get information about threats
- Penetration Testing and Exploitation (8)
  - Procedure, Phases and Tools – How to do a penetration test
- Malware / Botnets / Anti-Virus (3)
  - Malware types, concepts and technology
- Security Controls: Monitoring / SIEM Systems (3)
  - Overview and discussion of strengths and weaknesses of these systems

Course Overview (2)

Part II

- Security of Mobile Platforms (4)
  - iOS and Android security architecture and security testing

Part III

- Human Factor (2)
  - A glance at the importance of this factor for security and (some of) the challenges faced when trying to manage it

Lab Topics (1)

- Hacking-Lab – Getting started (2)
  - Experiment with the Hacking-Lab and revisit some of your skills from IS and SWS1 to solve some simple hacking challenges.
- Analysis of the ENISA threat landscape report (2)
  - Get an overview of the current threat landscape
- Penetration-Testing (4)
  - Flex your fingers and do intelligence gathering and vulnerability analysis in the Hacking-Lab and use the Metasploit Framework to hack into vulnerable systems.

Lab Topics (2)

- Exploitation I, II and III (2+2+2)
  - Exploit buffer overflow vulnerabilities despite protections like DEP, ASLR or Stack Canaries. Apply Return-Oriented Programming (ROP) to execute arbitrary code without having to inject any code. Learn what you can do to on the defender’s side to make the life of attackers hard.
- SIEM-Lab (4)
  - Introduction to Security Information and Event Management systems. Discover attacks, write monitoring rules and do some simple event correlation and attack detection tasks.
- Finding and Exploiting Vulnerabilities in Android Apps (4)
- Identify and fix problems in mobile apps (2) [4]

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

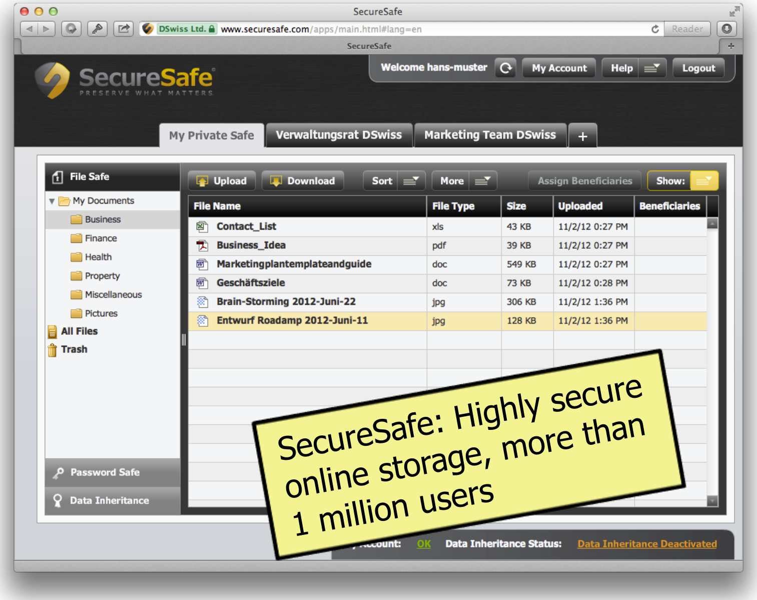
- Analysis of software systems by means of (automated) security testing
- Improving the quality, efficiency and reproducibility of security testing
- R&D of novel security mechanisms and protocols with focus on domain-specific functionality

Cyber Attacks and Defense

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

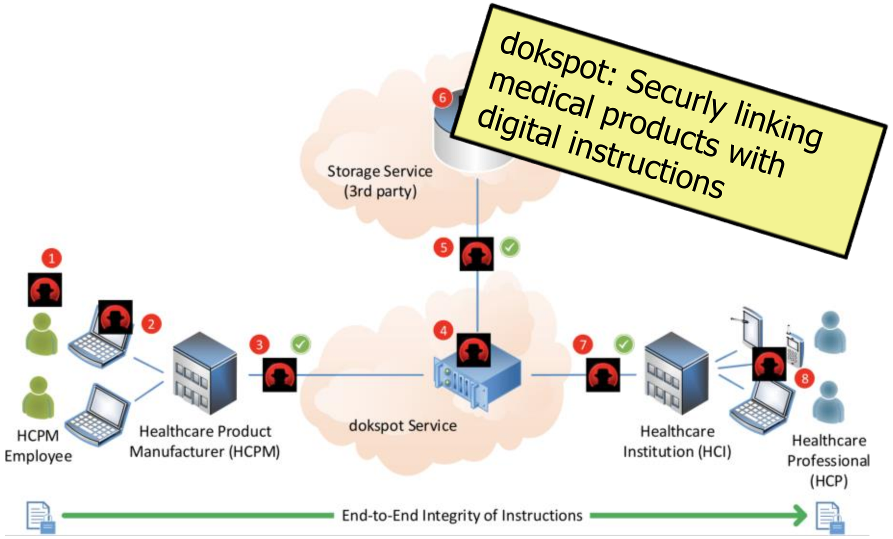
- Threats related to the introduction and use of new technologies (e.g., 5G/6G)
- Improvement of the defense posture (e.g., using OSINT)
- Applications of machine learning for cyber defense
- Understanding and mitigating the human factor

The Information Security Research Group – Project Examples

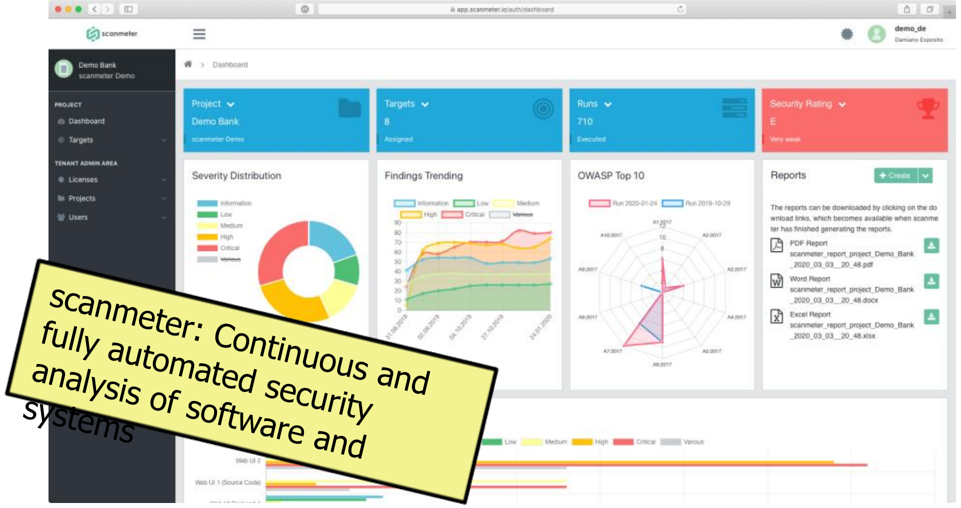


File Name	File Type	Size	Uploaded	Beneficiaries
Contact_List	xls	43 KB	11/2/12 0:27 PM	
Business_Idea	pdf	39 KB	11/2/12 0:27 PM	
Marketingplantemplateandguide	doc	549 KB	11/2/12 0:27 PM	
Geschäftsziele	doc	73 KB	11/2/12 0:28 PM	
Brain-Storming 2012-Juni-22	jpg	306 KB	11/2/12 1:36 PM	
Entwurf Roadamp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

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



dokspot: Securly linking medical products with digital instructions

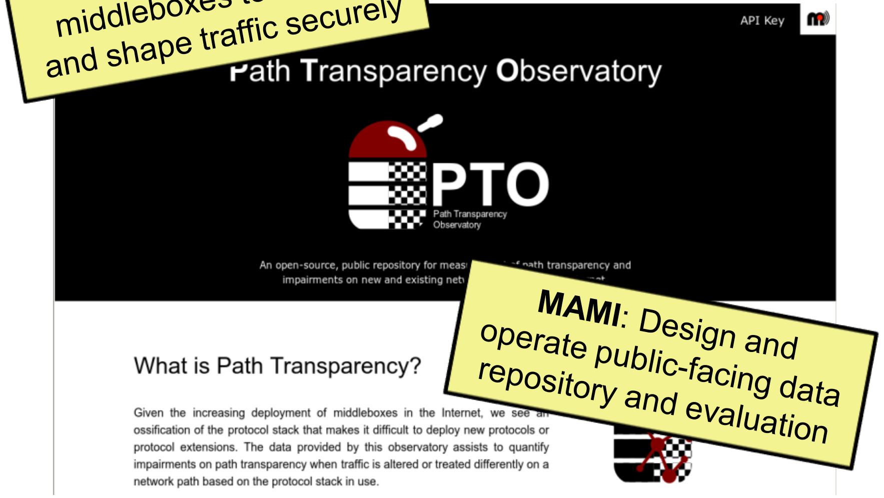


scanmeter: Continuous and fully automated security analysis of software and systems

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

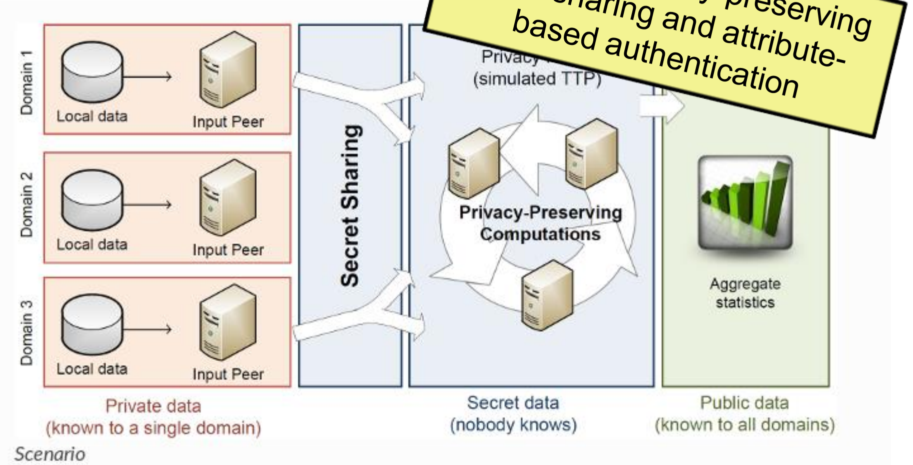


An open-source, public repository for meas… of path transparency and impairments on new and existing netw…

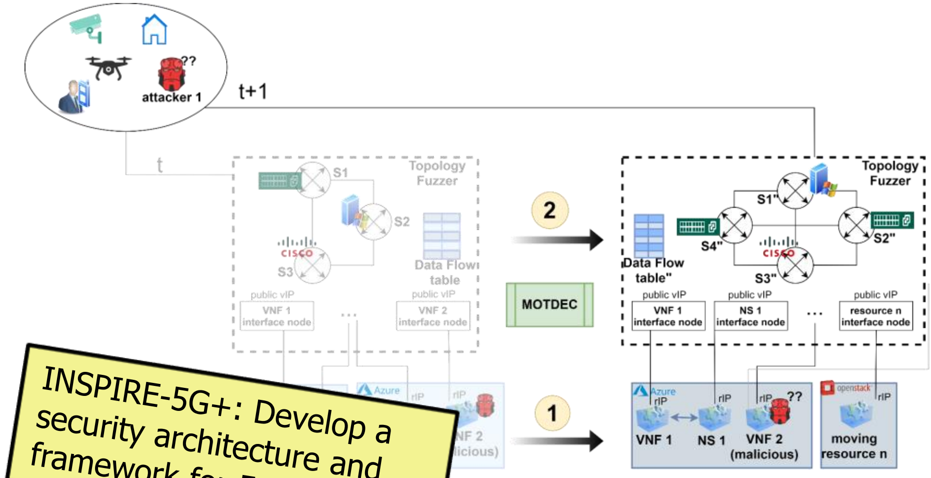
What is Path Transparency?

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.

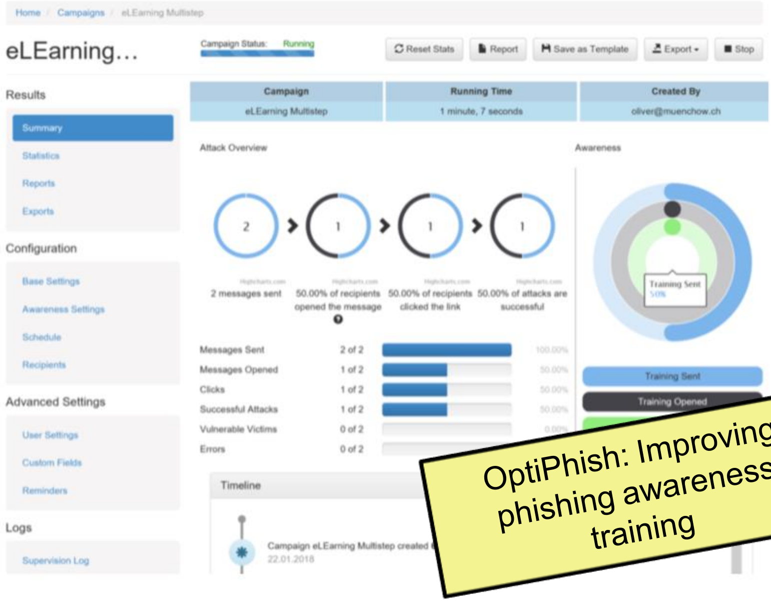
MAMI: Design and operate public-facing data repository and evaluation



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



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



eLEarning…

Campaign Status: Running

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

Attack Overview

2 › 1 › 1 › 1

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	

Awareness

Training Sent 50%

Timeline

Campaign eLEarning Multistep created
22.01.2018

OptiPhish: Improving phishing awareness training