Quality and Security Program Tirol

ANNUAL REPORT
2016/2017

STUDY
NETWORK
GET AHEAD!

CONTENTS

About QSP

The Quality and Security Program Tirol is an initiative of the Institute of Computer Science at the University of Innsbruck to foster application-oriented education in the area of software engineering, information security and IT management.

QSP Tirol offers series of events such as Labs, Talks and Lectures given by renown experts and is dedicated to students enrolled in Tyrolean Universities.

QSP was inaugurated in November 2014 and since then the events held within the initiative have gained a lively interest from the university students. In the third QSP year, 13 QSP Labs have had arround 180 participations of Bachelor and Master students and have been positively evaluated being perceived as an opportunity to get an insight into practice.

QSP Sponsoring Partners

www.arz.at

www.barracuda.com

www.egger.com

www.mils.com

QSP Supporting Partners

The Supporting Partners of Quality and Security Program Tirol support the initiative by leading the QSP Labs and giving the QSP Talks.

www.av-comparatives.org   **www.anecon.com**   **www.cisco.com**

www.finleap.com   **www.gruender-consulting.com**   **www.itestra.de**

www.lean42.com/de   **www.kaspersky.com**   Wir machen Software. Sicher.   **www.mgm-sp.com**
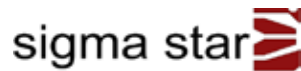
www.seppmed.de   **www.sigma-star.at**   **www.simula.no**

QSP Labs

The Quality and Security Program Tirol offers a broad selection of one to three half day labs with renown experts and hands-on knowledge transfer addressing students at Bachelor and Master level.

Since October 2016 until June 2017 the students have had the possibility to attend 13 Labs and benefit from the knowledge of experienced experts from ANECON, ARM, Barracuda Networks, Cisco Systems, FinLeap, Free University of Bolzano, Graz University of Technology, Gründer Consulting, mgm security partners, sigma star, Simula Research Laboratory and University of Trento.

QSP Labs: October 2016 - June 2017

21.10.2016	**Daniel Gruss, Graz University of Technology** *Oh my Cache! - Introduction to having fun with your Cache*
04.11.2016	**Richard Weinberger, sigma star** *A Journey to Filesystem Lands*
11.11.2016	**Michael Gredler, Christian Pumberger, Unternehmensberatung** *Cybercrime verhindern - Schwachstellen und Angriffe erkennen*
02.12.2016 **16-17.12.2016**	**Hannes Tschofenig, ARM** *Internet of Things (IoT) with Microcontrollers from ARM*
13.01.2017	**Tomas Pevny, Cisco Systems** *Analyzing traffic of infected machines*
20.01.2017	**Benjamin Kellermann, mgm security partners** *Web Application Security*
27.01.2017	**David Gstir, sigma star** *Transport Layer (In?)Security*
10.03.2017	**Dominic Breuker, FinLeap** *The Tech behind Chatbots*

31.03.2017-01.04.2017	**Torsten Gründer, Gründer Consulting** *IT-Outsourcing Management*
07-08.04.2017	**Thomas Bucsics, Roland Germ, ANECON** *Software development through quality*
18-19.05.2017	**Andrea Janes, Free University of Bolzano** **Katsiaryna Labunets, University of Trento** **Michael Felderer, University of Innsbruck** *Joint Seminar on Empirical Software Engineering*
19.05.2017	**Gregor Koenig, Martin Ortner, Barracuda Networks** *Workshop Internet Security - Breaking TLS for fun and profit*
09-10.06.2017	**Magne Jørgensen, Simula Research Laboratory** *Evidence-based software engineering*

» **Daniel Gruss, Graz University of Technology**
Oh my Cache! - Introduction to having fun with your Cache

Almost everything the CPU processes passes the cache. Luckily the cache cannot just be read from a process. However, side-channel attacks allow to deduce information in a fine granularity. In this lab students learn how to do micro-measurements, basic attack techniques, and run our attacks on real-world applications. After the lab, participants can perform cache side-channel attacks and other related attacks. They have a basic understanding of what leaks through cache side-channels and can use this understanding to write better, more secure software.

Daniel Gruss is a PhD Student at Graz University of Technology. He has done his master's thesis on identifying and minimizing architecture dependent code in operating system kernels. Daniel's research focuses on software-based side-channel attacks that exploit timing differences in hardware and operating system. In July 2015, he and his colleagues demonstrated the first hardware fault attack performed through a remote website, known as Rowhammer.js.

» **Richard Weinberger, sigma star**
A Journey to Filesystem Lands

In this lab an introduction to filesystem design and development is given. Students learn what constraints a filesystem designer has to consider and what concepts current filesystems, such as ext4, NTFS, or btrfs use. One of the filesystems is examined in detail such that students gain the basics to implement a minimal filesystem driver.

Richard Weinberger is a co-founder of sigma star GmbH and offers Linux kernel consulting services. He's been working with Linux for 10 years and works on the Linux kernel for more than five years. Besides of the kernel he has a strong focus on various low level components of Linux including virtualization techniques and networking security. Upstream he currently maintains UBI and UserModeLinux.

» **Michael Gredler, Christian Pumberger, Unternehmensberatung**
Cybercrime verhindern - Schwachstellen und Angriffe erkennen

In diesem Workshop lernen die TeilnehmerInnen Motive und Methoden von Cyber-Kriminellen kennen und wie man sich dagegen wappnet.

» Angreiferprofile von Script kiddies bis zur NSA (Motive, Ziele, Methoden)
» Schwachstellen, Angriffe und Sicherheitsvorfälle
» ID-Klau, Social Engineering und andere Einfallstore
» Sichere Kennwörter und Alternativen
» Schwachstellen erkennen und eliminieren bzw. reduzieren
» Angriffsmuster identifizieren und Angriffe wirksam abwehren

Mag. phil. Michael Gredler, ISO-27001 Auditor, seit 1989 als Unternehmensberater in Innsbruck tätig. Beratungsschwerpunkte sind u.a. Informationssicherheit, Security-Awarenessbildung und proaktive Verhinderung von Online-Wirtschaftskriminalität.

Ing. Christian Pumberger, MBA, seit über 20 Jahren in der IT-Sicherheit und im Notfallmanagement tätig und Experte für technische sowie organisatorische IT-Sicherheit. Langjähriger IT-Sicherheitsbeauftragter einer Bank. Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für die Fachgebiete IT-Sicherheit, IT-Systeme und Nachrichtentechnik.

» **Hannes Tschofenig, ARM**
Internet of Things (IoT) with Microcontrollers from ARM

In this course students learn:

» about ARM-based microprocessors (and the Cortex M family in particular),
» how to develop programs for these microcontrollers,
» to connect IoT devices to the Internet, and
» how to incorporate security to these IoT devices.

This course combines theoretical know-how with hands-on experience. The necessary hardware is provided by ARM.

Hannes Tschofenig is employed by ARM Ltd. His work life focused on developing standards to make the Internet work better. He has been active in the Internet Engineering Task Force (IETF) for the past 15+ years and has contributed to more than 70 technical specifications on security, privacy, and emergency services. Prior employers include the European Data Protection Supervisor, Nokia and Siemens.

» **Tomas Pevny, Cisco Systems**
Analyzing traffic of infected machines

In this course the participants take a role of a security researcher, who investigates the traffic of a malware captured in a sandbox (or other machine where full packet capture is possible). Participants learn basics about malware, what are their communication with command server, what are their monitization schemes, and how the modules and schemes can be inferred from the network traffic.

Tomas Pevny holds the position of researcher at CTU in Prague and Technical Lead at Cisco Systems, Inc. He has received his Ph.D. in Computer Science from SUNY, Binghamton (2008) and MS in CS at CTU, Prague (2003). In years: 2008-2009, he has spent one year as a post-doc in Gipsa-lab in Grenoble, France. His reseach focuses on machine learning in security domains.

» **Benjamin Kellermann, mgm security partners**
Web Application Security

In diesem Lab werden die Grundlagen der Sicherheit von Webapplikationen vorgestellt. Es werden die vom Open Web Application Security Project (OWASP) herausgegebenen 10 häufigsten Schwachstellen der Sicherheit von Webapplikationen diskutiert. Die Teilnehmer sind während des Seminars aufgefordert, selbst Schwachstellen in einer bereitgestellten Beispielapplikation zu finden.

Benjamin Kellermann ist Informationssicherheitsberater sowie Penetrationstester bei der mgm security partners in Dresden. Seit 2004 beschäftigt er sich intensiv mit Informationssicherheit und forschte zu sicheren Webanwendungen am Lehrstuhl Datenschutz und Datensicherheit bei Prof. Andreas Pfitzmann. Mehrere Jahre unterrichtete er im Gebiet der Informationsicherheit und ist Sprecher auf zahlreichen Fachkonferenzen.

» **David Gstir, sigma star**
Transport Layer (In?)Security

In recent years researchers discovered multiple flaws in the Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) when it is used in practice. This lab introduces the concepts of TLS/SSL and explain recent attacks like CRIME or POODLE. It also includes a look at commonly used implementations of the protocols.

David Gstir studied Computer Science at TU Graz with a focus on IT-Security. He analyzed attacks on the AES encryption algorithm, security and privacy aspects, smart meters and software developed for the LHC Computing Grid. Since 2013 he is a member of the Linux and Security Team at sigma star GmbH.

» **Dominic Breuker, FinLeap**
The Tech behind Chatbots

If you follow startup scene news regularly, you probably could not avoid noticing the current hype around conversational interfaces. What you see is a gold rush toward creating a new market similar to the app economy that emerged in 2008 when smartphones began appearing in stores. Investments into chatbot technology are surging, not least due to the general optimism with respect to AI (bloom. bg/2cjjQoT). In this lab, some notable examples of conversational interface technology are introduced. Students dive into chatbot software architecture and look into relevant parts of NLP (sentence classification / named entity regocnition) along with state-of-the-art solutions for that.

Dominic Breuker works at FinLeap GmbH, a Berlin-based FinTech company builder, where he is responsible for building up new FinTech ventures as well as facilitating the growth of FinLeap's exiting portfolio. Prior to joining FinLeap, Dominic received his Ph.D. in Information Systems from the University of Münster for his work on applying machine learning in the field of business process management.

» **Torsten Gründer, GRÜNDER Consulting**
IT-Outsourcing Management

Konkretes Praxiswissen zur strategischen Gestaltung und praktischen Umsetzung von Outsourcing-Vorhaben. Anhand typische Szenarien lernen die Teilnehmer häufige Fehler zu vermeiden, Risiken zu beherrschen und die sich mit Outsourcing bietenden Vorteile gezielt zu nutzen. Zentrale Aspekte im ersten Teil sind u.a.: Projektorganisation und -management, Ausschreibung, Leistungsbeschreibung, Vertragsgestaltung, Preismodelle, Transition, Dienstleistersteuerung, Beendigungsmanagement - im zweiten Teil: Fallstudien und Erfahrungen aus mehr als 120 Outsourcing-Projekten.

Torsten Gründer ist Outsourcing-Experte, Fachbuchautor und Hochschuldozent. Seit über 15 Jahren berät er Anwenderunternehmen im Bereich IT-Services/ IT-Outsourcing als Geschäftsführer der Spezialberatung GRÜNDER Consulting GmbH. Mit dem OMIT-Referenzmodell hat er die Projektmanagementmethode zur erfolgreichen Outsourcing-Umsetzung entwickelt.

» **Thomas Bucsics, Roland Germ, ANECON Software Design und Beratung**
Software development through quality

Creating high-quality software has always been a challenge. Quality assurance and testing methods have developed in parallel to constructive software engineering practices. The introduction of increasing demands on quality, and the trend of agile software development have made quality and testing a primary concern in all phases of software development. In this lab, students focus on Test Driven Development and Acceptance Test Driven Development, to show how these crucial techniques work - in theory and practice.

Thomas Bucsics studied Computational Intelligence and Media Computer Sciences at the TU Vienna. He specializes at ANECON in test automation approaches & architecture. He is author of the German-language standard literature on the topic, „Basiswissen Testautomatisierung" (d.punkt, 2012, 2. ed. in 2015).

Roland Germ studied Computer Science at the TU Vienna. He started as a software architect at ANECON's Java group, and specializes in agile practices and Software Craftmanship. He has more then 20 years experience in software development and he likes to train developers how-to develop Clean Code.

» **Andrea Janes (Free University of Bolzano)**
Katsiaryna Labunets (University of Trento)
Michael Felderer (University of Innsbruck)
Joint Seminar on Empirical Software Engineering

The lab attendants learn how to make use of modern statistical and machine learning methods to support decisions in software and security engineering, to develop and apply models to predict vulnerabilities in software and to compare the results with those of professional tools. This knowledge enables to analyze modern estimation and prediction approaches and to investigate and develop such approaches and to successfully apply them in a software projects and products.

Dr. Andrea Janes is a researcher at the Free University of Bolzano, Italy. His research interests include Lean and Agile software development, value-based software engineering, and empirical software engineering. He received the Master in Computer Science from the Technical University of Vienna, Austria and the doctorate in Computer Science from the University of Klagenfurt, Austria.

Dr. Katsiaryna Lobunets works in the Security Research Group under the supervision of Prof. Fabio Massacci at the University of Trento. Her research interests include empirical research methods, security requirements engineering, security methodologies validation, risk model comprehension and data analysis.

PD Dr. Michael Felderer is a senior researcher in the Institute of Computer Science at the University of Innsbruck. He holds a PhD and habilitation degree in Computer Science. His research interests are in the areas of software and security engineering. The research has a strong empirical focus also using methods of data science and is directed towards development and evaluation of efficient and effective methods to facilitate and measure quality of software systems and processes. Dr. Felderer works in close collaboration with industry and transfers his research results into practice as a consultant and a speaker on industrial conferences.

» **Gregor Koenig, Martin Ortner, Barracuda Networks**
Workshop Internet Security - Breaking TLS for fun and profit

The main purpose of Transport Layer Security (TLS) is to transmit data in a secure and confidential way over an unsecured network. It is the de-facto standard for secured communication in the internet. This workshop explains the technical background of the cryptographic algorithms used in TLS as well as the existing attacks in a profound but understandable and practical way. Famous examples are BEAST, CRIME, BREACH and the Padding Oracle Attack Lucky 13. Lab experts discuss the attacks and elaborate strategies to prevent them with the active participation of the students. This workshop aims to transfer profound knowledge and understanding of TLS to avoid known pitfalls and weaknesses.

Dr. Gregor Koenig's professional focus lies on the research and development of secure communication and safety-critical systems and their application in different fields. Since 2013 Dr. Koenig works for Barracuda Networks AG and develops products for secure internet communication. This involves the design and development of Linux kernel modules for the Barracuda NG Firewall and the management of international projects in the same technical field. Before joining Barracuda Networks Dr. Koenig was a scientist at the Austrian Institute of Technology in the field of bio-signal processing for medical devices, a lecturer at the Technical University of Vienna, worked for Frequentis AG in the research and development of safety-critical communication systems for air-traffic security and did projects for Skidata AG in Salzburg. He wrote his PhD thesis at the Medical University of Vienna.

Martin Ortner is a full-time security enthusiast that joined Barracuda Networks AG in 2011 as a Software Developer Quality Assurance creating network security products by taking apart hard- and software in order to make sure the quality goals are met. Prior to joining Barracuda Networks AG, Martin graduated with a master's degree from the department of Secure Information Systems at the University of Applied Sciences Upper Austria. During these years Martin worked with worldwide leading companies in the industrial sector focusing on computer emergency response coordination, penetration testing and holding security awareness workshops in order to open eyes for the beauty and constraints of software development. Being an independent security researcher for more than ten years with a passion for reverse engineering and the art of exploitation Martin actively searches for security relevant defects in order to disclose them.

> » **Magne Joergensen, Simula Research Laboratory**
> *Evidence-based software engineering*

Important judgments, decisions and choices in software engineering should be based on critical collection and evaluation of best evidence from research and practise. In this course lab expert introduces evidence-based software engineering and explains how this approach can be used to improve decisions. Topics that are covered include: how to disclose myths and fashion in software engineering, empirical research methods, collection of practise-based evidence, and challenges related to learning from experience. The goal is that the participants, as researchers and software practitioners, are able to better formulate precise problems, collect and evaluate relevant and valid evidence, summarise the evidence and apply the knowledge properly.

Magne Jørgensen works as a chief research scientist at Simula Research Laboratory, professor at University of Oslo, guest professor at the University of Kathmandu and as an advisor for Scienta. He is promoting the principles and process of evidence-based decisions to software professionals and students.

QSP TALKS

Beside the QSP Labs, university students have also the opportunity to attend evening events with presentations given by experts from industry and academia.

QSP Talks: Oktober 2016 - June 2017

12.10.2016 **Bernd Guggenberger, CHG Rechtsanwälte**
Die EU-Datenschutz-Grundverordnung - Datenschutz neu?

Mit Inkrafttreten der EU-Datenschutz-Grundverordnung im Mai 2018 gibt es erstmals ein in der ganzen EU geltendes, einheitliches Datenschutzrecht. Ziel der Verordnung ist es, ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und gleichzeitig Hemmnisse für den Verkehr mit personenbezogenen Daten in der Union zu beseitigen. Das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten soll in allen Mitgliedsstaaten der EU gleichwertig sein. Freilich stellt sich die Frage, ob die Verordnung diesen Zielen tatsächlich gerecht wird? Was ändert sich konkret - sowohl für den Betroffenen einer Datenverarbeitung, als auch für den Datenverarbeiter im Vergleich zum derzeit noch geltenden Recht?

Dr. Bernd Guggenberger ist Rechtsanwalt in Innsbruck und Partner der Kanzlei CHG Rechtsanwälte. Er ist seit vielen Jahren im IT-Recht tätig und ist dabei laufend mit Fragen des Datenschutzrechts befasst und als Vortragender tätig.

17.05.2017 **Martina Vogel, Hauptabteilungsleiterin VKB, München**
Digital Insurance – Künstliche Intelligenz in der Versicherungs Branche

Die VKB hat begonnen, kognitive Systeme im Rahmen des Beschwerdemanagements einzusetzen und hat damit den Grundstein für den Einsatz künstlicher Intelligenz in der Versicherungsbranche gelegt. Ziel dabei ist es, große Mengen unstrukturierter Daten mit Hilfe von kognitiven Systemen zu strukturieren und dadurch automatisiert Kundenanliegen zu erkennen und schnellstmöglich zu bearbeiten. Frau Vogel wird über das Projekt berichten, erste Ergebnisse vorstellen und Zukunftsperspektiven aufzeigen.

19.06.2017   **Marion Lanaro, Mitglied der Geschäftsleitung Creditreform Boniversum, Neuss**
Martin Schmid, CSO FinTecSystems, München
Kay Wossidlo, Partner Senacor Technologies AG, München
FinTechs - Disruptive Innovation oder Digitaler Hype?

FinTechs wird aktuell das Potenzial zugeschrieben, die Finanzdienstleistungsbranche zu revolutionieren. Jedoch ist bis heute unklar, ob es sich dabei tatsächlich um eine sogenannte, „disruptive Innovation" handelt, die klassische Geschäftsmodelle in der Finanzdienstleistungsbranche verdrängt. Viele Experten vertreten auch die Meinung, dass FinTechs einen neuen - durch die Euphorie um Social Media und die Sharing Economy ausgelösten - digitalen Hype darstellen und lediglich einen zusätzlichen digitalen Vertriebskanal für klassische Finanzdienstleister anbieten. Diese und weitere Standpunkte werden auf dieser Veranstaltung von hochkarätigen Referenten aus verschiedenen Bereichen der FinTech-Branche beleuchtet und diskutiert.

INDAY STUDENTS 2016

The third issue of inDay students took place on November 24th, 2016. The mission of inDay students is to gather together students of Computer Science and present them the research groups, collaborating industry partners and spin-offs. QSP co-sponsored this event.

Presentation of the research results at inDay students

The winners of the Students' Project Slam with the jury members and the sponsors

Keynotes: Prof. Dr. Nassir Navab, Technical University of Munich and Prof. Dr. Vittorio Ferrari, Google Zürich and University of Edingburgh

Contact:

Prof. Dr. Ruth Breu
Quality Engineering Research Group
Institute of Computer Science
University of Innsbruck
Technikerstrasse 21a
6020 Innsbruck
Tel: +43 (0)512-507-53203
Fax: +43 (0)512-507-53029

Prof. Dr. Rainer Böhme
Security and Privacy Lab
Institute of Computer Science
University of Innsbruck
Technikerstrasse 21a
6020 Innsbruck
Tel: +43 (0)512-507-53202
Fax: +43 (0)512-507-53018