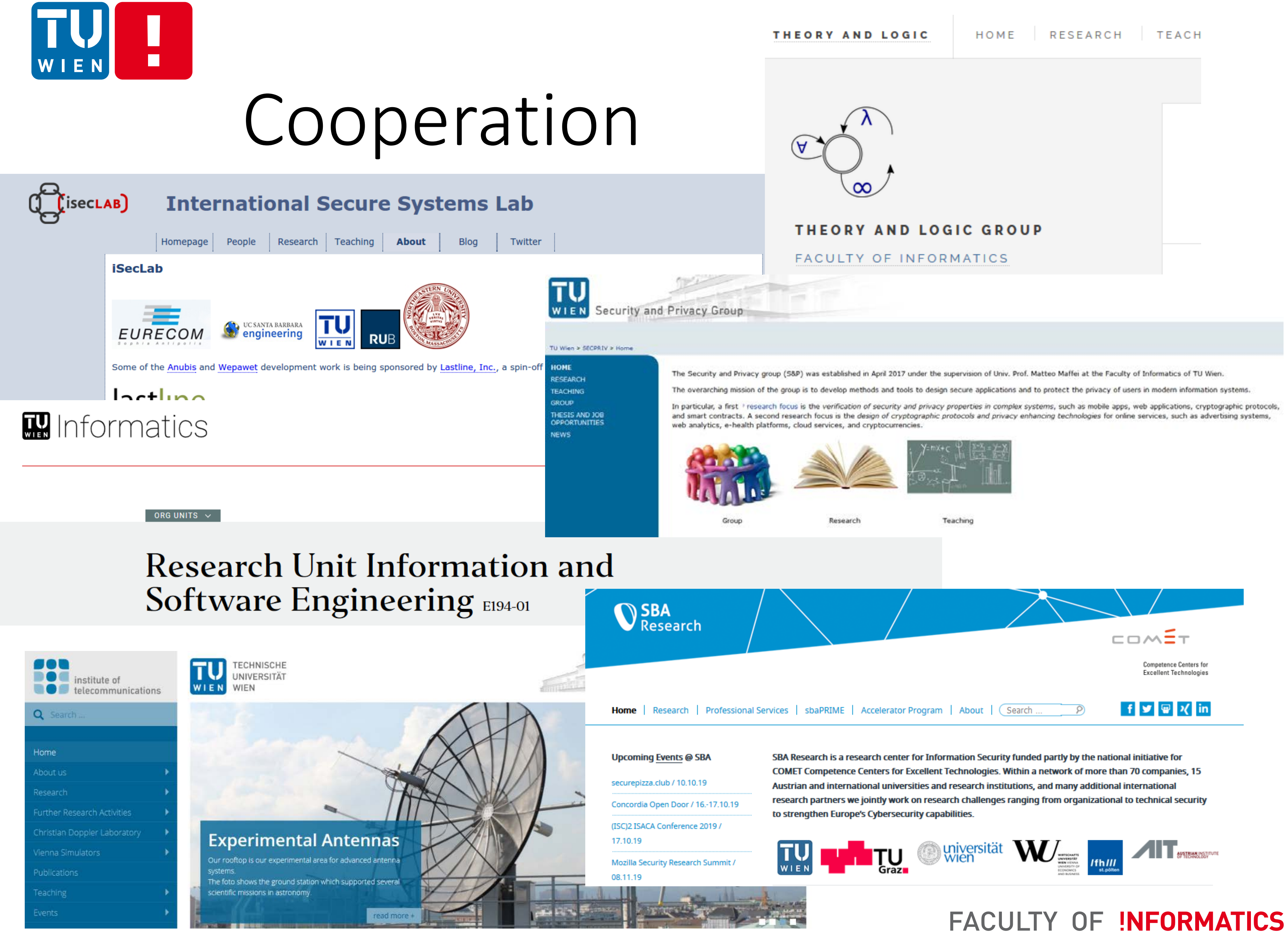
FAKULTÄT
FÜR !NFORMATIK

Faculty of Informatics

Organizational Details
Winter 2019

This presentation contains the organizational details of (most) **courses on information security** offered by 191-03, 192-05, 192-06, 194-01, 389 and SBA Research

Cooperation



THEORY AND LOGIC | HOME | RESEARCH | TEACH

THEORY AND LOGIC GROUP

FACULTY OF INFORMATICS

International Secure Systems Lab

Homepage | People | Research | Teaching | **About** | Blog | Twitter

iSecLab

Some of the Anubis and Wepawet development work is being sponsored by Lastline, Inc., a spin-off

Informatics

ORG UNITS

Research Unit Information and Software Engineering E194-01

Security and Privacy Group

TU Wien > SECPRIV > Home

HOME
RESEARCH
TEACHING
GROUP
THESIS AND JOB OPPORTUNITIES
NEWS

The Security and Privacy group (S&P) was established in April 2017 under the supervision of Univ. Prof. Matteo Maffei at the Faculty of Informatics of TU Wien.

The overarching mission of the group is to develop methods and tools to design secure applications and to protect the privacy of users in modern information systems.

In particular, a first research focus is the *verification of security and privacy properties in complex systems*, such as mobile apps, web applications, cryptographic protocols, and smart contracts. A second research focus is the *design of cryptographic protocols and privacy enhancing technologies* for online services, such as advertising systems, web analytics, e-health platforms, cloud services, and cryptocurrencies.

Group | Research | Teaching

institute of telecommunications

TECHNISCHE UNIVERSITÄT WIEN

Search ...

Home
About us
Research
Further Research Activities
Christian Doppler Laboratory
Vienna Simulators
Publications
Teaching
Events

Experimental Antennas

Our rooftop is our experimental area for advanced antenna systems.
The foto shows the ground station which supported several scientific missions in astronomy.

read more +

SBA Research

COMET
Competence Centers for Excellent Technologies

Home | Research | Professional Services | sbaPRIME | Accelerator Program | About | Search ...

Upcoming Events @ SBA

securepizza.club / 10.10.19

Concordia Open Door / 16.-17.10.19

(ISC)2 ISACA Conference 2019 / 17.10.19

Mozilla Security Research Summit / 08.11.19

SBA Research is a research center for Information Security funded partly by the national initiative for COMET Competence Centers for Excellent Technologies. Within a network of more than 70 companies, 15 Austrian and international universities and research institutions, and many additional international research partners we jointly work on research challenges ranging from organizational to technical security to strengthen Europe's Cybersecurity capabilities.

Cooperation

183/1-ISecLab, 191-03, 192-05, 192-06, 194-01, 389
and SBA Research teach together

Dr. Martina Lindorfer
(192-06)

Prof. Matteo Maffei
(192-06)

Prof. Gernot Salzer
(192-05)

Prof. Tanja Zseby
(389)

PD Edgar Weippl
(194-01, SBA)

Overview

- 188.312 Organizational Aspects of IT-Security
- 188.982 Privacy Enhancing Technologies
- 188.922 Digital Forensics
- 192.062/063 Introduction to Modern Cryptography and Tutorial on Introduction to Modern Cryptogr.
- 192.065 Cryptocurrencies
- 192.091 Advanced Internet Security
- 192.092 Capture The Flag
- 192.075/192.076 Project in Computer Science 1/2
- 192.093 Seminar aus Security (Systems)
- 389.159/160/161 Network Security Module

188.312
Organizational Aspects of IT-Security

Overview

- TUWEL as central point of information
  - all material, Forum
  - Email only for personal questions
    - Edgar Weippl (edgar.weippl@tuwien.ac.at)
    - Michael Stephanitsch (Michael.Stephanitsch@itsv.at)
- Lecture in two parts:
  - Part 1 – CISSP:
    - Lecture and group arrangement on Oct 18
    - Lecture on Nov 19
  - Part 2 – ISMS:
    - CISA, CISM, BCM
    - Lecture on Nov 8
    - Presentation on Dec 6

Grading

- Grading:
  - 2 presentations
  - 1 written assignment

  - 50 - 64pt . . . 4 (Genügend)
  - 65 - 79pt . . . 3 (Befriedigend)
  - 80 - 91pt . . . 2 (Gut)
  - 92 -100pt . . . 1 (Sehr gut)

188.982
Privacy Enhancing Technologies

Content

- Online privacy
- Anonymity
- Tor
- Online Censorship
- Tracking
- Fingerprinting
- TLS reloaded
- Signal, PGP, OTR, …

Speakers

Lecture is (mostly) Thursday 17:00-19:00, FH5

Lecturetube will be available!

Lecture by:

- Markus Donko-Huber markus.donko.huber@tuwien.ac.at
- Wilfried Mayer wilfried.mayer@tuwien.ac.at
- Martin Schmiedecker martin.schmiedecker@tuwien.ac.at
- TA: Lukas Anzinger
- Guest lecturer: TBD

Grading

4 Assignments:

- Submission via TUWEL
- Deadlines in TUWEL

Exams:

- Midterm exam, 8.11.2019
- Final exam, 13.12.2019
- (+ optional Retake exam, 14.01.2020):
  possibility to retake either midterm or final, last result counts.

- **Exam registration in TISS!** Room assignment will be announced before exams

Grading Scheme

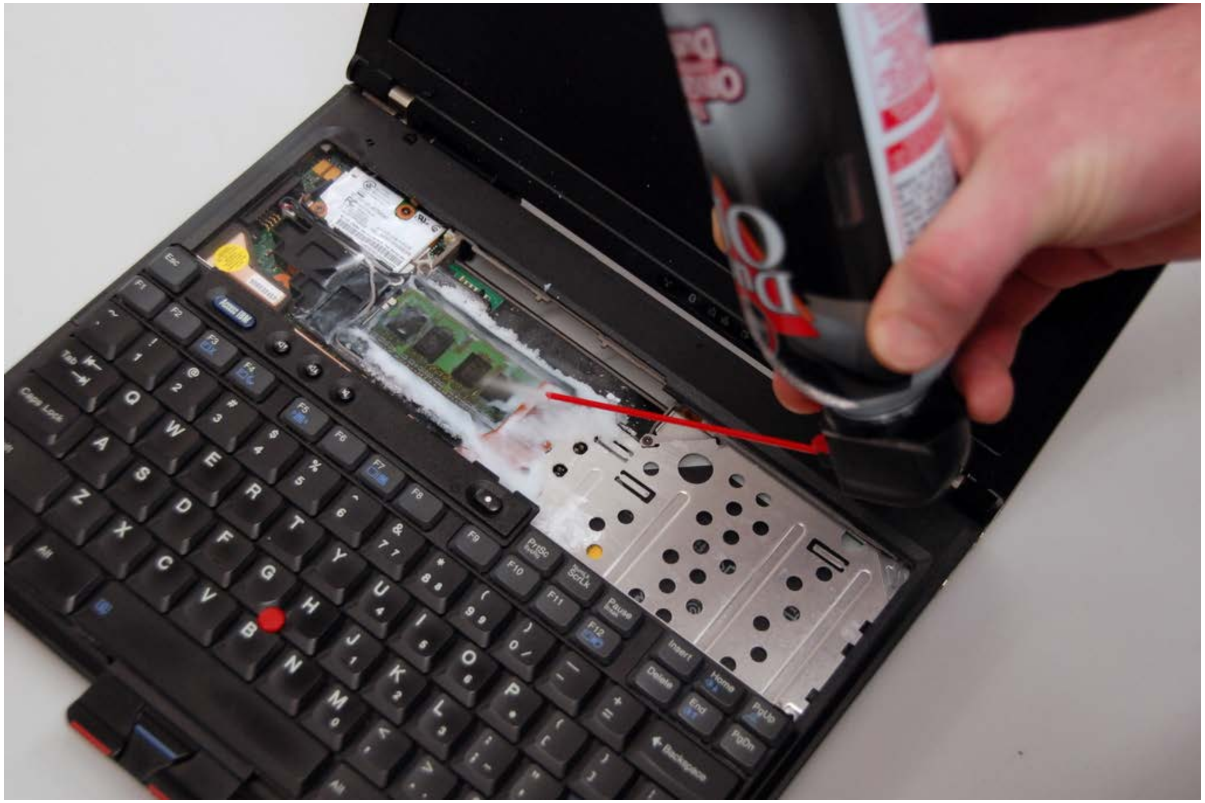
Total 100 points:

- 50 pt assignments (min. 25 to pass)
- 50 pt written exams (25 pt each, min. 12.5 each to pass)

Grades:

- 50 – 64 pt … 4 (Genügend)
- 65 – 79 pt … 3 (Befriedigend)
- 80 – 91 pt … 2 (Gut)
- 92 – 100 pt … 1 (Sehr Gut)

188.922
Digital Forensics



source: https://www.usenix.org/legacy/events/sec08/tech/full_papers/halderman/halderman_html/images/memory_2.jpg

Content

- Focus on post-incident analysis
- Understanding artefacts
- Operating systems
- File systems
- Memory forensics
- Reporting
- Smartphones

Lecture

- Lecture is (mostly) on Tuesdays, 17:00-19:00, EI 9 Hlawka
- Lecturetube will be available!

Lectures by:

- Martin Schmiedecker
  martin.schmiedecker@gmail.com
- Karsten Theiner
  karsten.theiner@t3k-forensics.com
- Guest lecturer: TBA
- TA: Regina Hofer

Grading

4 Assignments:

- Submission via TUWEL

2 Exams:

- Midterm exam, 12.11.2018
- Final exam, 16.12.2018
- (+ optional Retake exam, 23.01.2019):
  possibility to retake either midterm or final, last result counts.

- **Exam registration in TISS!**

Grading Scheme

Total 100 points:

- 50 pt assignments (min. 25 to pass)
- 50 pt written exams (25 pt each, min. 12.5 each to pass)

Grades:

- 50 – 64 pts … 4 (Genügend)
- 65 – 79 pts … 3 (Befriedigend)
- 80 – 91 pts … 2 (Gut)
- 92 – 100 pts … 1 (Sehr Gut)

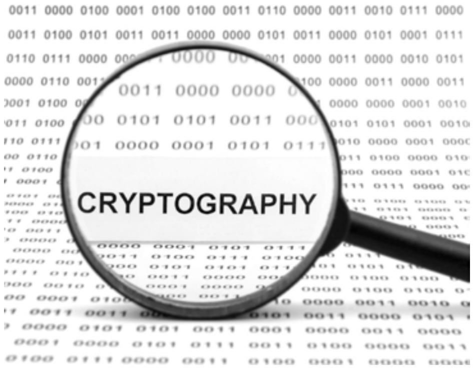
192.062
Introduction to Modern Cryptography

192.063
Tutorial on Introduction to Modern Cryptography

3 + 3 ECTS

Content

- Foundations of Cryptography
  - Information-theoretic security
  - Computational security
  - Private key encryption
  - Message authentication codes
  - Hash functions
  - Public key cryptography
  - Digital signature schemes



- You will learn the theory underlying cryptographic schemes
  - What does it mean for a crypto scheme to be secure?
  - How do we prove a crypto scheme secure?

Lecture

- 12 lectures, Tuesday, 16-18
- 12 tutorials, Thursday, 15-17

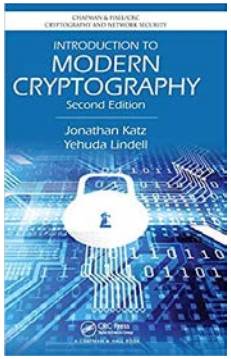
Lecturers:

Krzysztof Pietrazk

Daniel Slamanig

Material

- Textbook



Krzysztof Pietrazk
(IST Austria)

Daniel Slamanig
(AIT)

Organization

Exams:

- Midterm exam and final exam
- Retake exam: possibility to retake both
- **Exam registration in TISS!** Room assignment will be announced before exams

Grading:

- Final grade: 50% midterm + 50% final
- Minimal requirements to pass:
  - 50% midterm exam
  - 50% final exam

FAKULTÄT
FÜR !NFORMATIK

Faculty of Informatics

192.065
Cryptocurrencies

6 ECTS

Content

- Bitcoin
  - Blockchain
  - Consensus
  - Mining (proofs of work)
  - Privacy (Coinjoin, Coinshuffle, etc.)
  - Scalability (Lightning network)
- Alternative mining (proofs of space, stake, etc.)
- Alternative privacy techniques (Monero, Zcash, Mimblewimble)
- Alternative scripting
  - Ethereum and smart contracts

Lecture

- 14 lectures, Tuesday, 9-11, Hörsaal 6

Lecturer:

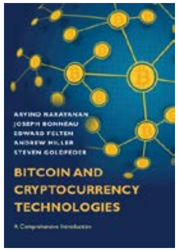
Matteo Maffei (matteo.maffei@tuwien.ac.at)
Aljosha Judmayer (ajudmayer@sba-research.org)

Teaching assistant

Erkan Tairi (erkan.tairi@tuwien.ac.at)
Lukas Aumayr (lukas.aumayr@tuwien.ac.at)

Material

- Textbook
- Slides
- Suggested reading



Organization

2 Projects (Bitcoin, Ethereum) and Final Exam

- **Exam registration in TISS!** Room assignment will be announced before exams

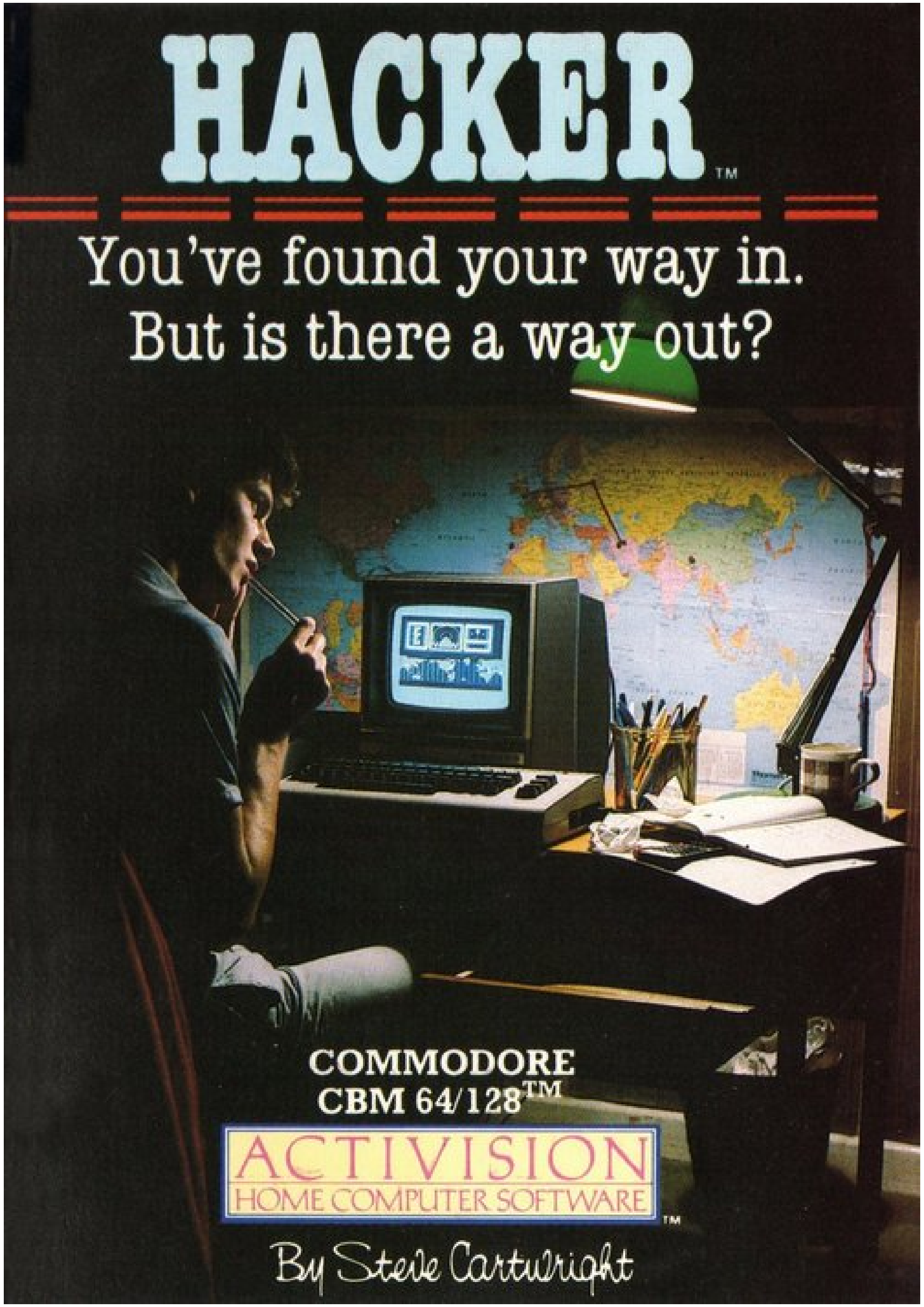
Grading:

- Final grade: 50% exam and 50% project
- Minimal requirements to pass:
  - 50% exam
  - 50% projects

FAKULTÄT FÜR !NFORMATIK

Faculty of Informatics

192.091
Advanced Internet Security


HACKER™
You've found your way in.
But is there a way out?
COMMODORE
CBM 64/128™
ACTIVISION
HOME COMPUTER SOFTWARE™
By Steve Cartwright

Advanced Internet Security

- Cooperation between SBA and e192/S&P (SecLab)
- Internet Security in summer term
  Advanced Internet Security in winter term
- Mode
  - Weekly lectures,
    - Wednesday 18:00-20:00
    - EI 8
  - Lab: Seven “Challenges”
    - Break things!!!!111
- Grading: 30% final exam, 70% challenges

Advanced Internet Security

- Lecture (preliminary)
  - Malware
  - Binary Analysis
  - Memory Corruption
  - Meltdown/Spectre/…
  - IoT Security
  - Hardware Security
  - Mobile Security
  - Advanced Web Security
- Lab Challenges (preliminary)
  - Virus, Trojan, Worm
  - Android
  - Binary
  - …

Advanced Internet Security

- Who should do AInetSec?
  - If you like to become “security guru”
    - We also take part in Capture-the-Flag contests
  - People who are technically oriented
    - Somewhat familiar with C and Linux, Assembler and a scripting language helps.
  - You should be interested in solving technical problems

Advanced Internet Security

- At a glance
  - Wednesday 18:00
  - EI 8
- Register via TISS
  - Until October 9
- Final Exam
  - January 22

- https://secenv.appsec.at/inetsec2
  - The homepage is currently still “under construction”
- inetsec@appsec.at

192.092
Capture The Flag
(SE, 6 EC)

Capture The Flag!

IT Security Exercise:

- Solve Challenges, Exploit Services
- Get the Flag

  `CTFNAME{this_is_a_flag}`
- Get points

Gain Experience

Concept

- Elective course, organized like a “hack meeting”
- Collaboration between S&P Group and SBA research
- Learn by… competing on the world’s stage!
  - Train with DEF CON CTF, RUCTF finalists
  - Take part to the best CTFs with We_0wn_Y0u
  - Practice with bleeding edge attack and defense techniques
- Share your knowledge with your teammates and challenge them!
- HACK THE PLANET!

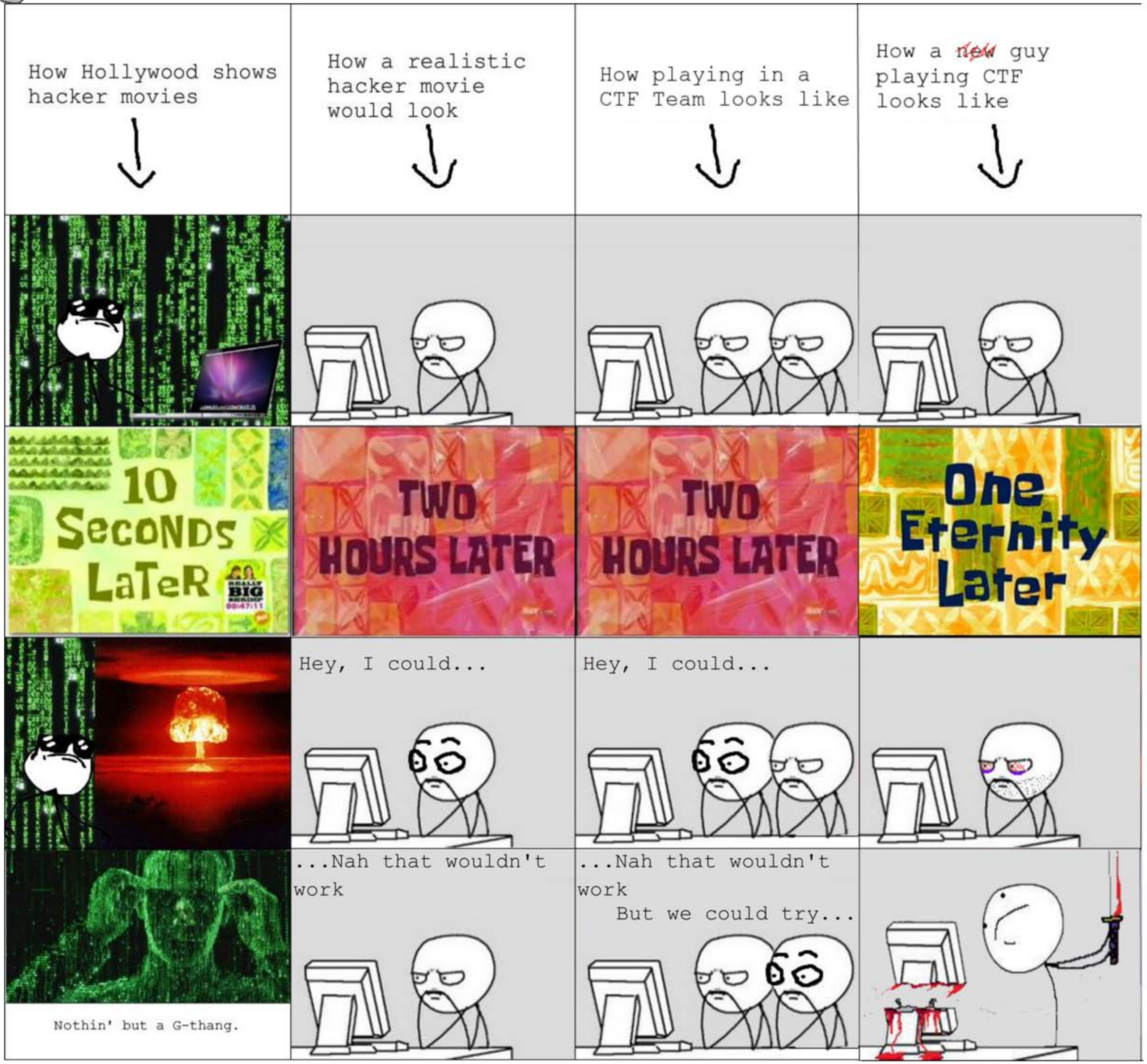
Modalities

- Organisers: Marco Squarcina, Georg Merzdovnik

  20 years of CTF experience
  3 DEF CON CTF finals

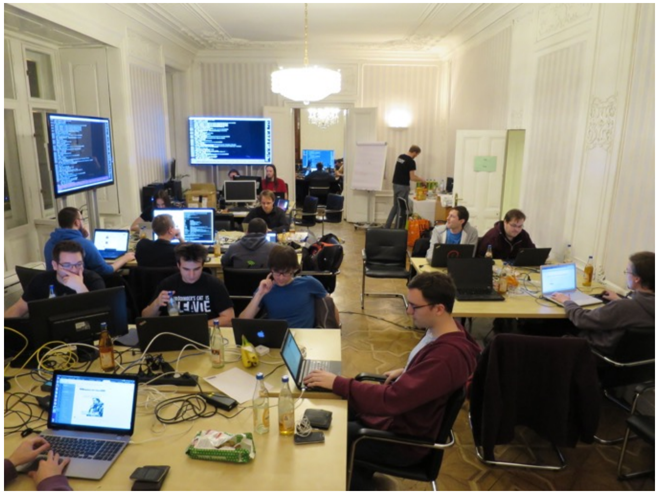
  } combined

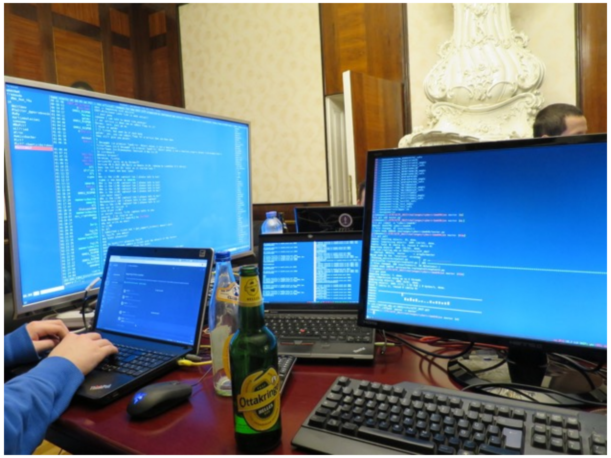
- 6 ECTS
- 5 on-site meetings
- Mandatory attendance to international CTF competitions (can be either remote or on-site)
- Evaluation based on a presentation of a security challenge from a high-profile security contest
- Registration and further information via TISS


How Hollywood shows hacker movies
How a realistic hacker movie would look
How playing in a CTF Team looks like
How a ~~new~~ guy playing CTF looks like
10 SecONDs LaTeR
TWO HOURS LATER
TWO HOURS LATER
One Eternity Later
Hey, I could...
Hey, I could...
...Nah that wouldn't work
...Nah that wouldn't work
But we could try...
Nothin' but a G-thang.

We_0wn_Y0u

- Our CTF Team
  - Around since 2004 (First international iCTF)





WE OWN YOU
二進忍術
DEFCON
CTF
DDTEK PRESENTS CAPTURE THE FLAG 2012

Interested?

- What you should bring:
  - Interest in Security
  - Self motivation to learn new stuff
    - You don’t need to know everything already!

- What you will get:
  - Chance to hack stuff ;)
  - Learn new things
  - Skillz and knowledge

- Want more infos?
  - https://w0y.at
  - @We_0wn_Y0u
  - contact@w0y.at

FAKULTÄT FÜR !NFORMATIK

Faculty of Informatics

192.075/192.076 Project in Computer Science 1/2

Imagine a project about magic internet money*

* Discover Cryptocurrencies, Blockchains, and Distributed Ledgers with Spongeblock Squarechain

Project in Computer Science 1/2

- **At a glance**
  - 4.0 SWS / 6.0 ECTS
  - Select topics from information security
  - Ask other speakers about the projects they can offer to you
- **What are we interested in?**
  - Analysis and improvement of different Blockchain Protocols (PoW,PoS,BFT,DAGs etc.)
  - Empirical Analysis of Distributed Ledgers and assets (e.g Smart Contracts)
  - (Bribing) Attacks/Security under Rational Players
  - Distributed Randomness/Distributed Key Generation
  - Basically anything related to Blockchains/Cryptocurrencies ;-)
  - Implementation of Cryptographic Protocols and Primitives
- **A Great opportunity to look into topics for your upcoming thesis**
- blockchain@sba-research.org

192.093
Seminar aus Security (Systems)

Overview

Lecturers:

Martina Lindorfer (martina.lindorfer@tuwien.ac.at)
Edgar Weippl (edgar.weippl@tuwien.ac.at)
Georg Merzdovnik (georg@seclab.tuwien.ac.at)

Content:

- State-of-the-art system security research from „top 4“ conferences
- Discussion of
  - technical contribution
  - potential future work
  - methodology, evaluation, paper structure, ...

Grading:

- Presentation and discussion lead of at least one research paper
- Participation in other paper discussions
- Attendance of ≥ 80% of discussions

389.159/160/161
Network Security Module

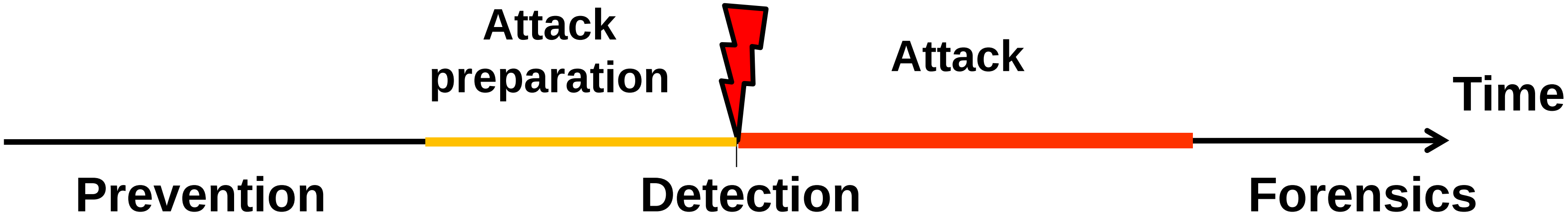
E389 Network Security Module

Tanja Zseby

Institute of Telecommunications (E389)

Faculty of Electrical Engineering and Information Technology (ETIT)

E389 Communication Networks: Research Focus



- **Network Security**
  - Malware Communication, Network Steganography
  - Digital Signatures in Protocols
- **Anomaly Detection Methods**
  - Network Supervision
  - Statistical Detection Methods
  - Machine Learning, Clustering
- **Secure Communication in Cyber Physical Systems**
  - Smart Grid Communication (synchrophasor measurements, secure clock sync)
  - Cyber Physical Production Systems

Module Network Security (E389)

- VU Network Security (389.159)
  - SS, 2 SWS, 3.0 ECTS
- VU Network Security Advanced (389.160)
  - WS, 2 SWS, 3.0 ECTS
- SE Communication Networks Seminar (389.161)
  - SS, 2SWS, 3.0 ECTS

Prerequisites:

- Knowledge about communication networks, especially TCP/IP networks (e.g., VO Communication Networks 1)

VU Concept

- Lectures and Exercises
  - Theory lectures (6 weeks) ➔ written test
  - Lab exercises ➔ lab report and oral exam
- Focus on **Network** Security
  - Network and Transport Layer Security
  - Attack Detection, Network Traffic Analysis
  - Not in scope: software or applications

- Lab Exercises
  - Teams of 2 students
  - NetSec: Attack Detection in Network Traffic
  - NetSec Advanced: Network Steganography

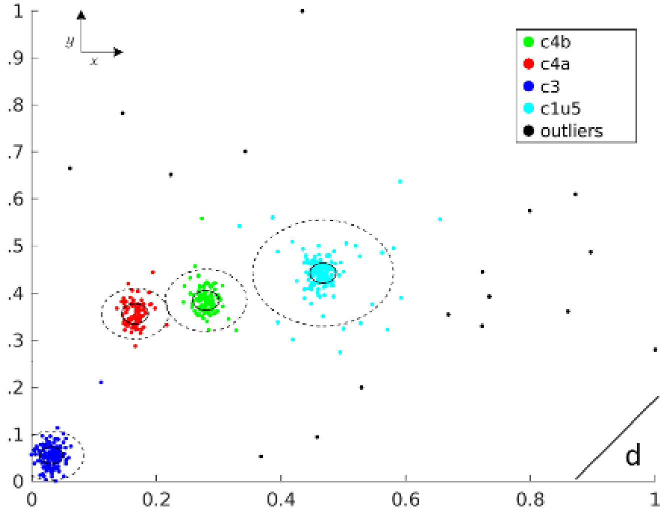
Network Security – Theory Part

- Security Basics (Attacks, Security Objectives)
- Cryptography - Basics
  - Block and stream ciphers (AES, DES, RC4)
  - Message Authentication Codes (MAC)
  - Digital Signatures
- Cryptography - Methods
  - RSA, Elgamal
  - Diffie-Hellman Key Exchange
  - Elliptic Curve Cryptography (ECC)
- Security Protocols (IPsec, TLS)
- Network Supervision Techniques
- Anomaly Detection Methods

Network Security – Lab Exercises

- Lab Exercises: **Attack Detection**
  - – Analysis of Network Traffic collected at UCSD
  - – IP Darkspace Data (attacks, unsolicited traffic)
  - – Traffic analysis methods
  - – Attack detection methods

- Tools
  - – Wireshark
  - – silk
  - – Matlab
  - – RapidMiner
  - – Own tools, scripts, programs

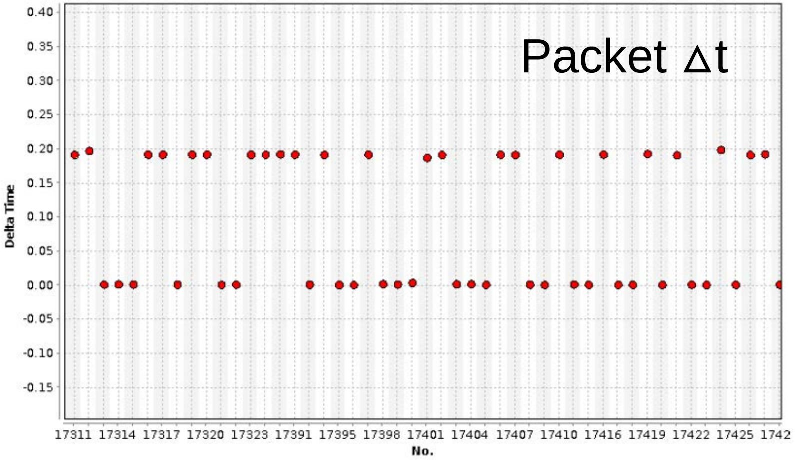


Network Security Advanced – Theory Part

- IPv6 Security Concepts
  - Secure Neighbor Discovery (SEND)
  - Cryptographically Generated Addresses (CGA)
- Routing Security
  - BGP Security (Attacks, AS Path Validation, Route Origin Authorization, RPKI)
  - Security in Mobile Ad Hoc Networks (MANETs)
- Group Communication Security
- Smart Grid Security
- Network Steganography
  - Covert Channels in TCP/IP
  - Subliminal Channels in Signatures

Network Security Advanced – Lab Exercises

- Lab Exercises: **Network Steganography**
  - Detection of covert communication in TCP/IP traffic
  - Analysis of different covert communication methods
  - Creation of own covert channels
- Tools
  - wireshark
  - silk
  - Matlab
  - RapidMiner
  - Own tools, scripts, programs



CN Seminar: Selected Security Topics

- Focus on selected topics in Network Security Research such as:
  - Network anomaly detection methods (statistics, machine learning, data mining concepts)
  - Smart grid security concepts
  - Modern digital signatures
  - Attacks on clock synchronization
- Each students presents a topic based on recent papers
- Grading based on
  - Scientific understanding of the topic
  - Presentation of the topic

Thank you!

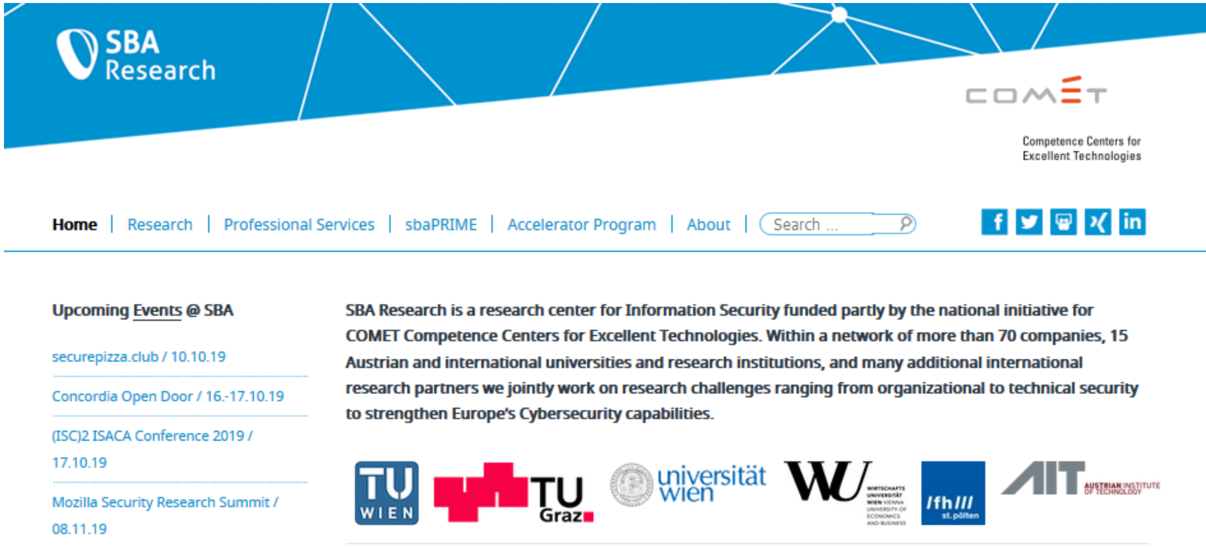
Contact: tanja.zseby@tuwien.ac.at

General Information

Information Security

Additionally we can offer:

- Praktikum (PR)
- Bachelor Thesis
- Master Thesis
- PhD Thesis


SBA Research
COMET
Competence Centers for Excellent Technologies
Home | Research | Professional Services | sbaPRIME | Accelerator Program | About | Search ...

Upcoming Events @ SBA

securepizza.club / 10.10.19

Concordia Open Door / 16.-17.10.19

(ISC)2 ISACA Conference 2019 / 17.10.19

Mozilla Security Research Summit / 08.11.19

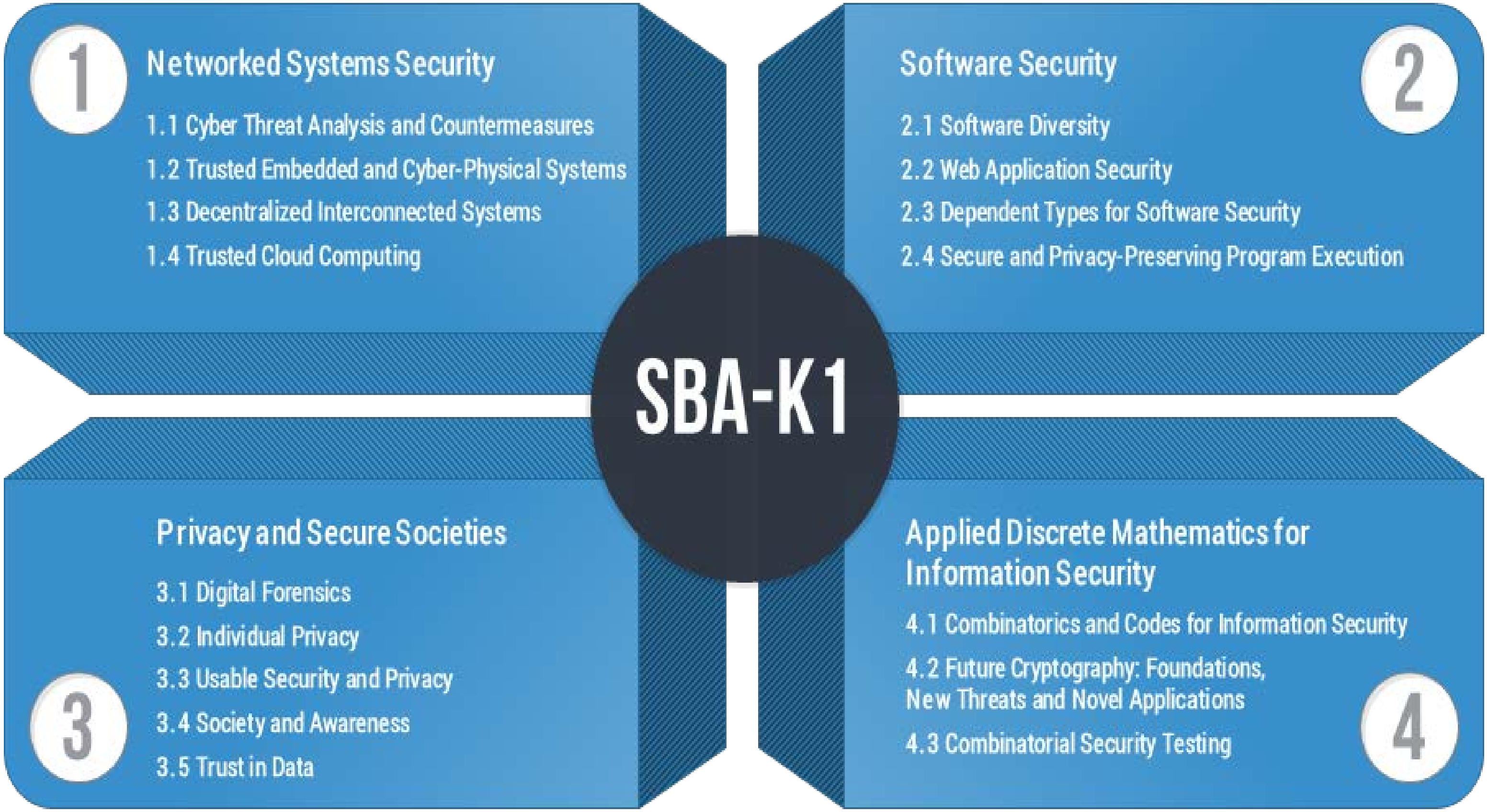
SBA Research is a research center for Information Security funded partly by the national initiative for COMET Competence Centers for Excellent Technologies. Within a network of more than 70 companies, 15 Austrian and international universities and research institutions, and many additional international research partners we jointly work on research challenges ranging from organizational to technical security to strengthen Europe's Cybersecurity capabilities.

Research assistant

Industry projects

https://www.sba-research.org/research/bachelor-master-phd-thesis-supervision/

SBA Research



SBA-K1

1 Networked Systems Security

- 1.1 Cyber Threat Analysis and Countermeasures
- 1.2 Trusted Embedded and Cyber-Physical Systems
- 1.3 Decentralized Interconnected Systems
- 1.4 Trusted Cloud Computing

2 Software Security

- 2.1 Software Diversity
- 2.2 Web Application Security
- 2.3 Dependent Types for Software Security
- 2.4 Secure and Privacy-Preserving Program Execution

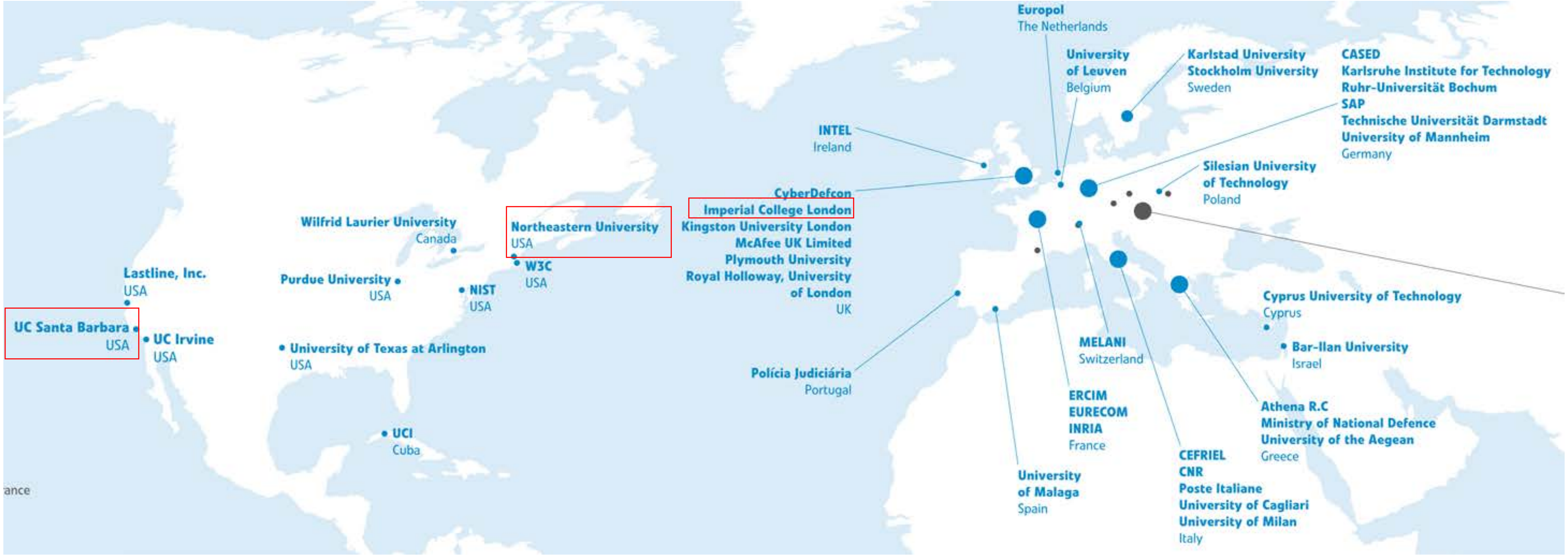
3 Privacy and Secure Societies

- 3.1 Digital Forensics
- 3.2 Individual Privacy
- 3.3 Usable Security and Privacy
- 3.4 Society and Awareness
- 3.5 Trust in Data

4 Applied Discrete Mathematics for Information Security

- 4.1 Combinatorics and Codes for Information Security
- 4.2 Future Cryptography: Foundations, New Threats and Novel Applications
- 4.3 Combinatorial Security Testing

International Cooperation



Research at the Security & Privacy Group

S&P

Topics:

- Formal methods for security and privacy
- Cryptocurrencies
- Applied cryptography and privacy-enhancing technologies
- Web security
- Software security
- (Mobile) Systems security and privacy

We offer:

- Praktikum (PR)
- Bachelor, Master & PhD Thesis (with Research Assistant positions)

https://secpriv.tuwien.ac.at/thesis_and_job_opportunities