universität
innsbruck

Information Security II – Proseminar

Introduction and Topics

Dr. Pascal Schöttle

Preliminaries

There are no stupid questions.

- Please interrupt me at any time.
- Be (more) polite when students are presenting.

English as a second language

- Ask for clarification.
- Correct me if I'm wrong.

Illustrations: xkcd.com

Team

Professor

Univ.-Prof. Dr.-Ing.
Rainer Böhme

Secretary

Jenifer
Payr

Technician

Manuel
Knoflach-Schrott

Scientific Staff

Dr. Cecilia
Pasquini

Dr. Markus
Riek

Dr. Pascal
Schöttle

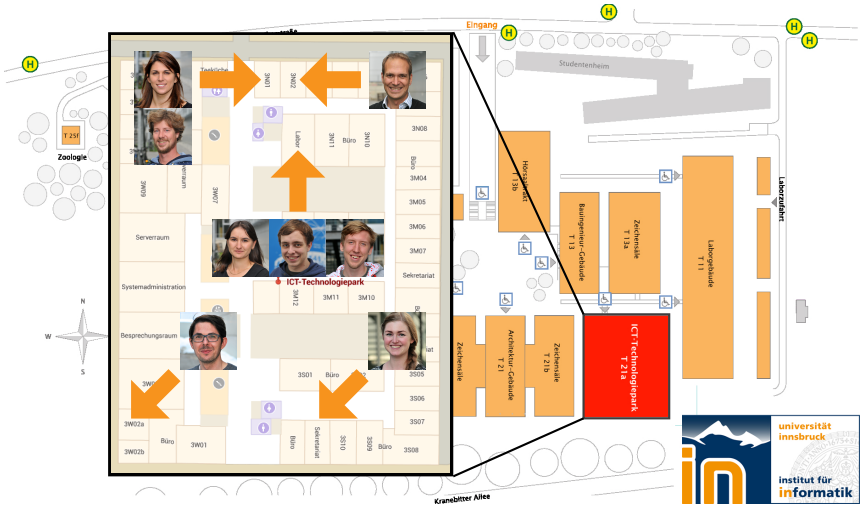
Svetlana
Abramova

Maximilian
Hils

Olaf Markus
Köhler

Michael
Fröwis

Where to Find Us



Tentative Schedule – Summer Term 2018

08.03.18	1.	Introduction, topic presentation
15.03.18	2.	Topic assignment
22.03.18	3.	Presentation of expected outcome (starting at 2pm, Room SR 2)
12.04.18	4.	Exercise sheet distribution
19.04.18	5.	Presentation of related work
26.04.18	6.	Exercise sheet discussion
03.05.18	7.	Introduction to game theory
17.05.18	8.	Homework assignment
24.05.18	9.	Homework discussion
07.06.18	10.	Lecture
14.06.18	11.	**Final presentations** (+ 60 min.)
21.06.18		No seminar
28.06.18	12.	Reserved

Learning Goals (Proseminar)

- Deepen the topics from the lecture
- Broaden your horizon on security techniques
- Fully understand the principles and limits of one technique
- Learn to present formal arguments in talk and thesis

Organization

- Seven elements for grading:
  1. state your preferences for the seminar project
  2. present your topic and the expected outcome to students of UNITN
  3. present related work to your fellow students
  4. write up the most important related work
  5. one graded exercise sheet
  6. final presentation incl. demonstration
  7. seminar thesis
- Form teams of two students
- Everything but the exercise sheet will be graded **per team**
- 08 July 2018: Deadline for all seminar papers

Organization – The Seminar Project

1. Preferences for the seminar project:
   - choose exactly three topics (priority 1 to 3)
   - write two sentences for each of the three topics, why you chose it
   - send an email to `pascal.schoettle@uibk.ac.at`, stating the members of your team and the preferences and if you join the dinner with UNITN students on 22 March.
2. Presentation of expected outcome:
   - state in a 5 minute presentation
     - why your topic is practically relevant
     - what you expect to be the outcome at the end of the semester
   - the audience will include students visiting from University of Trento (UNITN)
   - we do **not** hold you liable if you do not reach that outcome in the end
3. Presentation of related work:
   - present the initial source(s) as well as the most important related work
   - clearly state how and why these sources are important for your topic
   - plan about 10 minutes for the talk

Organization – The Seminar Project (cont'd)

4. Related work write-up:
   - elaborate on why the sources are important
   - be careful when formatting the bibliography
   - write up to two pages, excluding the bibliography
5. Final presentation and demonstration:
   - introduce why your topic is relevant
   - first, give the theoretical background
   - then, give a small demonstration
   - ideally, conclude with an outlook
   - plan about 20 minutes for the talk/demonstration and additional 10 minutes for Q&A
6. Seminar thesis:
   - present your arguments in a scientific manner
   - write up to 20 pages, including figures and bibliography
   - take care about formatting the bibliography
   - add contribution statement

Example Contribution Statement

“This is joint work of Alice and Bob. Alice did the literature research and contacted Eve for test data. Bob implemented the experimental code which was later optimized together. Bob ran the main experiment and prepared tables and figures. Alice wrote most of the initial draft, which was then edited jointly. We thank Charlie for the idea to use non-linear optimization and Eve for making available her data.”

Expected Outcome Presentation

Purpose: Present why your topic is practically relevant and what you expect to demonstrate at the end of the semester. This presentation helps us to see if your expectations might be overly ambitious.

Target Audience: Students from UNITN

Present your topic in a structured way, accessible for students with a general CS background, but not the content of Information Security I & II.

- Support your talk with two or three slides, preferably including a visualization.
- Duration: 5 minutes
- We communicate the detailed agenda for 22 March next week in the proseminar.
- You can join the UNITN students (and us) for dinner that evening.
  (Please state in your *topic preference email* if you want to join the dinner.)

Seminar Presentations

Purpose: Study one specific application of information security, explain the main ideas, and related work in a comprehensible fashion.

Target Audience: Your Fellow Students

Assume lectures Information Security I & II as background. Recall concepts, terminology and notation from the lecture, but do not spend too much time on repetition.

- Support your talk with a set of clear and precise slides.
- Smart use of formalisms, preference for visualization
- Duration: initial: 10 minutes; final: 20 minutes + 10 minutes Q&A

Seminar Theses

Purpose: Learn to present formal arguments in a scientific seminar paper. Present the contents of your presentation in greater detail and take up comments and questions from the discussion in class.

- Write a comprehensive and accessible overview
- Structure and notation of your seminar thesis should harmonize the approaches in the literature.
- Explain

Quality vs Quantity

Demonstrate your academic drafting skills, not your ability to “fill paper”. Twelve very readable and concise pages are much more welcome than 20 or more pages of mixed quality.

More Hints

- Carefully back all statements and claims with references to the academic literature.
- A typical seminar thesis has 15–30 references, meaning you skim 25–50 papers and study 10–20 of them in detail.
- If you find errors or can formulate an outright critique, then do it, but double-check with the adviser to rule out that you just misunderstood.
- We offer every student to send us a draft structure and up to two pages (until 24 June) to proof-read, respectively. The page limit is strictly enforced. You'll get detailed comments which you can extrapolate to the rest of the paper.

Overall Grading

We grade every submission. The combined mark is the weighted average followed by unbiased rounding:

	%
Submission 1: Topic preferences	5
Submission 2: Expected outcome presentation (5 min)	5
Submission 3: Related work presentation (10 min)	10
Submission 4: Related work write-up (∼2 pages)	10
Submission 5: Homework	20
Submission 6: Final presentation (20 + 10 min)	25
Submission 7: Final write-up (∼20 pages)	25

A fail in one component leads to failure of the entire proseminar.

Important Dates

Deadlines are strict. All submissions (except the topic preferences) must be submitted in OLAT before 23:59 on the day of the deadline. Delayed submissions lead to a lower grade for this submission, two delayed submissions lead to a fail of the overall course.

	Deadline
Submission 1: Topic preferences	14.03.2018
Submission 2: Expected outcome presentation	22.03.2018
Submission 3: Related work presentation	19.04.2018
Submission 4: Related work write-up	20.04.2018
Submission 5: Homework due	24.05.2018
Submission 6: Final presentation	14.06.2018
Submission 7: Final write-up	08.07.2018

Topic 1: Attacking DH Key Exchange in Practice

A recently proposed man-in-the-middle attack on Diffie–Hellman key exchange, termed Logjam, allows an attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography. The attacker can read and modify any data passed over the connection.

The students who work on this project will report what *export-grade* cryptography is (for) and reproduce the setup in the given paper. Then, they will show how the Logjam attack works and, ideally, demonstrate how to successfully break a DH key exchange (note: this needs some precomputation effort).

- Adrian, D., Bhargavan, K., et al. (2015): Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. In *Proc. ACM SIGSAC Conference on Computer and Communications Security*, ACM Press, New York, p. 5–17.

Topic 2: Key Reinstallation Attack against WPA2

In a key reinstallation attack, an attacker tricks a victim into reinstalling an already-in-use key. This kind of attack was first published in 2017 and it was shown that the popular Wi-Fi encryption standard WPA2 is vulnerable to it.

The students who work on that topic will explain why installing an already-in-use key is a security threat and how severe it is. Furthermore, they will reimplement and demonstrate the original attack and talk about possible countermeasures.

- Vanhoef, M., Piessens, F. (2017): Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In *Proc. ACM SIGSAC Conference on Computer and Communications Security*, ACM Press, New York, p. 1313–1328.

Topic 3: Vulnerabilities of Out-of-order Execution

In early 2018, two hardware vulnerabilities affecting a huge proportion of modern microprocessors shocked not only the security community but almost everyone in the IT sector. The vulnerabilities, termed *Meltdown* and *Spectre*, allow an attacker to access memory she is not authorized to access via a timing side channel.

The students who work on that topic will explain both vulnerabilities and at least implement a successful attack leveraging the Meltdown vulnerability. Furthermore, they will present countermeasures and talk about their impact on peformance.

- Lipp, M., Schwarz, M., et al. (2018): Meltdown. In *arXiv:1801.01207*, `https://arxiv.org/abs/1801.01207`.
- Kocher, P., Genkin, D., et al. (2018): Spectre Attacks: Exploiting Speculative Execution. In *arXiv:1801.01203*, `https://arxiv.org/abs/1801.01203`.

Topic 4: Countermeasures Against DPA

In the lecture about side channel attacks we will show you how naive implementations of security relevant algorithms can be broken with Simple Power Analysis (SPA) and how to defend against it. Furthermore, we will show you how the more advanced Differential Power Analysis (DPA) works.

The students who work on this topic will implement a countermeasure for AES against DPA and show that the countermeasure complicates the DPA attack. For this, they will get access to our working group's oscilloscope and picoscope.

- Itoh, K., Takenaka, M., Torii, N. (2001): DPA Countermeasure Based on the "Masking Method". In *Proc. Information Security and Cryptology*, Springer, Berlin, p. 440–456.

Topic 5: IoT Light Bulb Covert Channel

The prevalence of IoT devices opens space for a whole bunch of new attacks.

The students who work on this topic will present a taxonomy of attacks against IoT devices and demonstrate a so-called *functionality extension attack*. Here, existing functionalities of IoT devices are used to achieve a totally different effect, i. e., a smart light bulb can be used to create a covert communication channel.

- Ronen E., Shamir A. (2016): Extended Functionality Attacks on IoT Devices: The Case of Smart Lights. In *IEEE European Symposium on Security and Privacy*, IEEE, p. 3–12.

Topic 6: Security of the Signal Messaging Protocol

The Signal messaging protocol is a recently proposed open source protocol for end-to-end encrypted instant messaging. It is claimed that the Signal protocol provides, among others, backward secrecy, message repudiation, and participation repudiation.

The students working on this topic will detail how the Signal protocol achieves these *uncommon* protection goals and set up their own Signal server and show the security properties of Signal communications practically.

- Cohn-Gordon K., Cremers C., Dowling B., Garratt L., Stebila D. (2017): A Formal Security Analysis of the Signal Messaging Protocol. In *IEEE European Symposium on Security and Privacy*, IEEE, p. 451–466.

Topic 7: Robustness of Deep Learning Approaches

Deep learning subsumes all machine learning approaches that are based on deep neural networks (DNN). Deep learning approaches achieve stat-of-the-art results in several classification tasks. Recent developments suggest that DNNs are vulnerable to so-called *adversarial examples*, specifically crafted inputs that get misclassified by the DNN with a very high probability and confidence.

The students who work on this project will set up and train their own DNN and examine its robustness to adversarial examples. Ideally, they will furthermore implement methods to harden the DNN against naively crafted adversarial examples.

- Szegedy C., Zaremba W., Sutskever I., Bruna J., Erhan D., Goodfellow I., Fergus R. (2014): Intriguing properties of neural networks. In *International Conference on Learning Representations*, `https://arxiv.org/abs/1312.6199`.

Topic 8: Shedding Light into an Obscure Cryptocurrency

With a market value of USD 4.1 billon, IOTA is currently the cryptocurrency ranked 11th in terms of market capitalization[1]. At least since it was discovered that IOTA's underlying hash function Curl was seriously flawed, the community is very skeptical about IOTA.

The students working on this topic will explain what is reliably known about IOTA, how it is supposed to work, and will collect and demonstrate known security flaws and concerns from public sources. The presentation can include a quantitative analysis of market reactions to discovered security issues.

- Popov S. (2017): The Tangle. In *IOTA - Whitepaper*, `https://iota.org/IOTA_Whitepaper.pdf`.
- Heilman E., Narula N., Dryja T., and Virza M. (2017): IOTA Vulnerability Report: Cryptanalysis of the Curl Hash Function Enabling Practical Signature Forgery Attacks on the IOTA Cryptocurrency. In *Vulnerability report on IOTA and colliding bundles*, `https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md`.

[1] `https://coinmarketcap.com/`

Topic 9: Your Project Idea

If you have an idea for another project with a similar effort as the proposed ones, feel free to include it into your 3 topic preferences. Please describe your idea in up to 5 sentences and give a scientific paper as starting point. Keep in mind that you have to convince us that your idea is **relevant**, has a **security aspect** and is **feasible** in the timeframe of the proseminar.

List of Topics

1. Attacking DH Key Exchange in Practice
2. Key Reinstallation Attack against WPA2
3. Vulnerabilities of Out-of-order Execution
4. Countermeasures Against Differential Power Analysis
5. IoT Light Bulb Covert Channel
6. Security of the Signal Messaging Protocol
7. Robustness of Deep Learning Approaches
8. Shedding Light into an Obscure Cryptocurrency
9. **Your project idea**

Tentative Schedule – Summer Term 2018

08.03.18	1.	Introduction, topic presentation
15.03.18	2.	Topic assignment
22.03.18	3.	Presentation of expected outcome (starting at 2pm, Room SR 2)
12.04.18	4.	Exercise sheet distribution
19.04.18	5.	Presentation of related work
26.04.18	6.	Exercise sheet discussion
03.05.18	7.	Introduction to game theory
17.05.18	8.	Homework assignment
24.05.18	9.	Homework discussion
07.06.18	10.	Lecture
14.06.18	11.	**Final presentations** (+ 60 min.)
21.06.18		No seminar
28.06.18	12.	Reserved