Seminar
Selected Topics in Communication Management
Selected Topics in IT Security

Information and Advice

University of Bonn
Institute of Computer Science 4

Prof. Dr. Peter Martini  Prof. Dr. Michael Meier

winter term 2017/18
General Information
General Information 1/2

• Goals:
  – Getting familiar with a topic in a limited time frame.
  – Writing a good report.
  – Giving a good presentation to a group.

• Components:
  – Written report of approx. 10 pages (a template will be provided)
  – Review of ~two other reports. For this part you will use a conference management system. We will inform you on time via e-mail.
  – Presentation (~30-minute talk, 15-minute discussion).
  – Lots of interaction with your advisor and fellow students.
• **Steps:**
  – Register for the seminar (until 31 October in BASIS).
    *This is your first important deadline! Care about the registration!*
  – Initial meeting (today).
  – Structure your work, write the report, review other’s reports, prepare the presentation (guided by your advisor).
  – Presentations (“Blockseminar”, all presentations are given within one day: 29 January 2018 in room II.27; exact time will be announced timely).

• **Seminar Websites:**
  – Seminar MA-INF 3209 “Selected Topics in Communication Management”  
    [https://net.cs.uni-bonn.de/wg/cs/teaching/wt-201718/sticm/](https://net.cs.uni-bonn.de/wg/cs/teaching/wt-201718/sticm/)
  – Seminar MA-INF 3317 “Selected Topics in IT Security”  
    [https://net.cs.uni-bonn.de/wg/itsec/teaching/wt-201718/selected-topics-in-it-security/](https://net.cs.uni-bonn.de/wg/itsec/teaching/wt-201718/selected-topics-in-it-security/)
Time Schedule
Time schedule (your deadlines)

- **Today:** Introductory meeting
- **31 October:** Registration in BASIS ends
- **5 November:** Document outline
  - literature research is done at this point
  - you already know what you want to write in each section
- **3 December:** Complete report draft
  - final report, as you would want it to be graded
  - correct citation/referencing, no grammar or spelling mistakes
- **10 December:** You receive comments on your report from your advisor
- **22 December:** Complete report, ready for peer-review
  - you read, understand and comment on two other reports
  - You receive reviews from your classmates and your supervisor.
- **12 January:** Reviews done
- **21 January:** Complete report, final version
- **24 January:** Slide set for your presentation
- **29 January:** Final presentation
Regulations and Marks

• You will receive a mark for the seminar based on:
  – the written report (substance, presentation, language, ...)
  – the reviews (understanding, quality of comments, ...)
  – the presentation (scientific presentation, reduction to main aspects, understanding, ...)
  – the discussion (ability to explain, understanding)

• The “Examination Rules for the Masters Degree Course in Computer Science” (i.e., the unofficial translation of the “MaPO”, January 2012) say:

  § 11(5): “Examination results in seminars will relate, as a rule, to written papers and oral discourses relating to partial areas of the subject matter dealt with in the seminar.”

  § 16(3): “Seminar discourses document the candidates’ ability to present scientific results in a comprehensible manner and to explain them in a discussion.”
Seminar Summer Term 2017

• Questions?
  – Organizational: Saffija Kasem-Madani
cs4-seminars-labs@lists.iai.uni-bonn.de
  – About your topic: Your advisor

• Dates:
  – Presentations: Monday, 29 January 2018, exact time t.b.a.
  – Submission of written report (final): Sunday, 21 January 2018
   These are firm dates!

• Main literature sources:
  – Your advisor will send you an email containing further information about your topic.
Review Process
**Review Process**

**Peer review** is the evaluation of papers by other researchers to the writer of the work to maintain quality (and improve the paper).

1. Write your paper
2. Submit paper
3. Review other papers
4. Submit reviews
5. Receive reviews
6. Improve your paper
Some Advice
Advice: Deadlines

• Deadlines have to be kept!
  – Official deadlines (see previous slide on deadlines)
  – Any appointments and deadlines agreed upon with your advisor, e.g.,
    • first meeting
    • weekly meetings
    • intermediate report deadlines
  – Time management is important!

• A complete version is meant to be complete!
  – Submit a complete report without empty sections or paragraphs.
  – Include a full list of proper references and sources.
  – Make sure your text is free of spelling and grammar mistakes.
Advice: Guidance

• Contact your advisor:
  – Let your advisor approve your work.
  – Discuss the structure of the report with your advisor.
  – Discuss your presentation slides with your advisor.
  – Ask your advisor for help if you have questions or want to improve your understanding of the topic or you are unsure about proper citing/referencing.

• Consider the feedback you receive:
  – Take notes during the meetings with your advisor.
  – The suggestions by your advisor are meant to improve your work. However, in general only you are responsible for your work.
  – Exception: change request by your advisor. Ignoring a change request may result in a failed seminar.
Guideline for the Composition of Master Theses, Seminar Papers and Lab Reports

Friedrich-Wilhelms-Universität Bonn
Institut für Informatik IV
Prof. Dr. Peter Martin and staff

1. Why?

The guidelines for preparing master theses, seminar papers and lab reports were inspired by the external examiner, Dr. HP Freese of the same institute, during his report on the exam process. Our institute is the only institute for computer science in the region, and we have been asked to help students with their projects. The guidelines are not intended to replace the teaching staff, but they are meant to help students with their projects and provide additional guidance for students preparing for the exam.

1.1. The Purpose of a Lab Report

A lab report is a description of what one has done during the practical session. It is divided into different sections, such as:
- Introduction: describes the purpose of the experiment.
- Methods: explains the procedures used.
- Results: presents the findings of the experiment.
- Conclusion: summarizes the results and draws conclusions.

The purpose of a lab report is to provide a detailed account of what one has learned during the practical session. It should be written in a clear and concise manner.

---

Advice: Guidance

Purpose of a Seminar Paper

A seminar paper is a short, informal, and informal paper, which is submitted in the form of a seminar. The seminar paper is intended to provide an overview of the main ideas presented in the seminar and to give the reader an understanding of the main ideas presented. The seminar paper should be written in a clear and concise manner, and it should be submitted in the form of a seminar.

Purpose of a Master Thesis

A master thesis is a formal written report that is submitted to the doctoral committee as part of the requirements for the degree. The master thesis should be written in a clear and concise manner, and it should be submitted in the form of a seminar.
Advice: Citing and Copying

• Goal of the seminar:
  – Describe a topic in your own words, based on existing sources.

• Citations and figures:
  – Clearly indicate citations, e.g., when you cite opinions of others or results obtained by others.
  – Do not cite excessively!
  – When “citing” figures:
    • reference the original work,
    • draw the figures yourself, and
    • include only relevant parts

• Work scientifically or fail the course:
  – Copying (even if slightly modified or rearranged) without citing the original work leads to a failed seminar.
  – Simply translating from other works is equal to copying.
  – Excessive citing may lead to a failed seminar.
  – Know the difference between citing and referencing.
    • If you don’t: ask your advisor!
Advice: Avoid Plagiarism

• What is plagiarism?
  – To steal and pass off the ideas or words of another as one's own.
  – Use another's production without crediting the source.
  – To commit literary theft.
  – Present as new and original an idea or product derived from an existing source.

  – Merriam-Webster Online Dictionary

• How do I avoid it?
  – Do not copy, paraphrase, translate, or summarize from any source without documenting adequately and truthfully.
  – Do not quote excessively, such that the quoted material makes up significant portions of your work. This applies even if you give credit!

• Consequences
  – If plagiarism is in evidence, you fail the lecture, seminar, thesis, etc.
  – Plagiarism may become expensive (see MaPO):

  § 13(9): „Any intentional violation of a regulation of these examination rules [...] will be regarded as an offence. Such an offence may be punished by a fine of up to 50,000 Euros.“
Advice: Sources, References and Style

• **Use the LNCS document class for the final report.**
  – Downloadable from the seminars’ websites.

• **List of references:**
  – Give a complete list of all sources used.
    • Author and title.
    • Type of publication.
    • Date.
    • For online sources: state when you last checked the contents.
  – When in doubt, ask your advisor!

• **Choose sources carefully:**
  – Use the sources indicated by your advisor, and look for further sources yourself.
  – Be aware that some sources may be unreliable or change frequently (common example: to cite or not to cite a Wikipedia article).
  – When in doubt, again, ask your advisor!
Conclusions
Your “Take-Home” Message

• Read your e-mails regularly
  – We advise you to use your @cs.uni-bonn.de address.
  – Use another ➔ you are responsible that e-mails really reach you.

• Keep dates and deadlines in mind
  – Don’t miss deadlines!

• Problems? Contact your advisor
  – In time!

• Do proper time management
  – Start early!

• Don’t plagiarize
  – We will find out …
Topics Selection
Topics Selection 1: Participants

• Participants:
  – Awais Bajwa
  – Daniel Hecker
  – Marvin Karpienski
  – Sven Knauer
  – Christopher Krah
  – Roman Wagner
  – Eugen Winter

• Each participant will choose one of the presented topics.
### Topics Selection 1: Participants

- **Your preferences:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Vorname</th>
<th>Honeypots</th>
<th>ICS Security</th>
<th>Identity Leakage</th>
<th>Resilience</th>
<th>Software Exploitation</th>
<th>Threat Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bajwa</td>
<td>Awais</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Hecker</td>
<td>Daniel</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Karpienski</td>
<td>Marvin</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Knauer</td>
<td>Sven</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Krah</td>
<td>Christopher</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Wagner</td>
<td>Roman</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Winter</td>
<td>Eugen</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

- **Each participant will choose one of the presented topics.**
### Topics Selection 1: Participants

<table>
<thead>
<tr>
<th>Name</th>
<th>Vorname</th>
<th>Honeypots</th>
<th>ICS Security 2</th>
<th>Resilience</th>
<th>Threat Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bajwa</td>
<td>Awais</td>
<td>x</td>
<td></td>
<td>x</td>
<td>xx</td>
</tr>
<tr>
<td>Hecker</td>
<td>Daniel</td>
<td>xx</td>
<td></td>
<td>x</td>
<td>xx</td>
</tr>
<tr>
<td>Karpienski</td>
<td>Marvin</td>
<td>xx</td>
<td></td>
<td>x</td>
<td>xx</td>
</tr>
<tr>
<td>Wagner</td>
<td>Roman</td>
<td>xx</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Winter</td>
<td>Eugen</td>
<td>x</td>
<td></td>
<td></td>
<td>xx</td>
</tr>
</tbody>
</table>
Topics Selection 2: Topics

• Honeypots
  – 1 Place
  – Supervisor: Mohammad Qasem

• Identity Leakage
  – 1 place
  – Supervisor: Timo Malderle

• Industrial Control Systems’ Security
  – 2 places
  – Supervisors: Piotr Pausztelo and Christian Hemminghaus

• Resilience OR Secure Group Communication
  – 1 place
  – Supervisor: Dr. Thorsten Aurisch

• Software Exploitation
  – 1 place
  – Supervisor: Thomas Barabosch

• Threat Intelligence
  – 1 place
  – Supervisor: Marc Ohm
Honeypots
Mohammad Qasem
Identity Leakage
Timo Malderle
reserved for Sven Knauer
ICS Security 1
Piotr Pauksztelo
ICS Security 2
Christian Hemminghaus
Resilience OR Secure Group Communication
Dr. Thorsten Aurisch
Seminar Selected Topics in IT Security
- Autonomous security mechanisms to enable cyber resilience -

Thorsten Aurisch

Bonn, den 06.10.2017
Autonomous security mechanisms to enable cyber resilience
- Identity-Based Cryptography -

- Usability of Identity-Based Cryptography in Mobile Ad-Hoc Networks
- S. Zhao, A. Aggarwal, R. Frost, X. Bai, A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks

- Seminar objectives
  - Understand the principles of identity-based cryptography (IBC)
  - List the advantages/disadvantages of IBC
  - Understand the main applications
  - Identify future research
Main characteristics of identity-based cryptography

- Cryptography for unprepared users
- Public keys are some attribute of a user’s identity (e.g. email address, phone number, biometric data)
- Sender only needs to know recipient’s identity attribute in order to send an encrypted message
- Recipient needs to interact with a trusted third party (Private Key Generator, PKG) after receiving an encrypted message
Identity-based encryption

- Alice prepares the message $M$ for Bob using $ID_{Bob}$ and a master public key $pk_{PKG}$.
- Bob receives the encrypted message $C$ from Alice, authenticates with the PKG and retrieves the private key $sk_{ID_{Bob}}$ over a secure channel.
- Bob decrypts $C$ using his private key to recover the message $M$. 

![Diagram of identity-based encryption](image)
Identity-based signature

- Alice authenticates with the PKG and receives the private key $sk_{ID_{Alice}}$ over a secure channel
- Alice generates a signature $\sigma$ and transmits it to Bob along with the message $M$
- Bob checks the signature on $M$ using Alice’s identity $ID_{Alice}$ and $pk_{PKG}$
Software Exploitation
Thomas Barabosch
reserved for Christopher Krah
Threat Intelligence
Marc Ohm