Seminar
Selected Topics in Communication Management
Selected Topics in IT Security

Information and Advice

University of Bonn
Institute of Computer Science 4

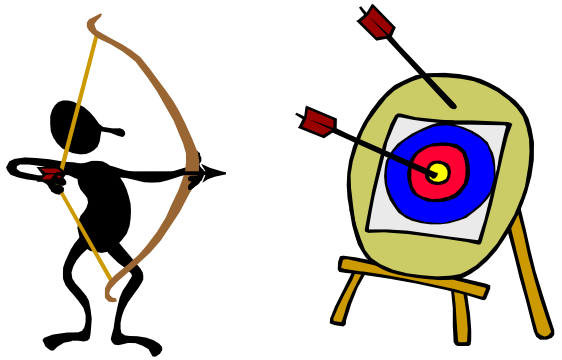
Prof. Dr. Peter Martini **Prof. Dr. Michael Meier**

winter term 2017/18

General Information

General Information 1/2

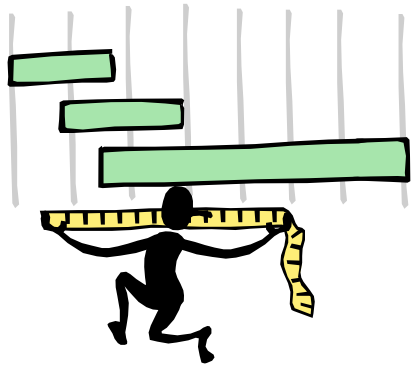
- Goals:
  - Getting familiar with a topic in a limited time frame.
  - Writing a good report.
  - Giving a good presentation to a group.



- 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.

General Information 2/2

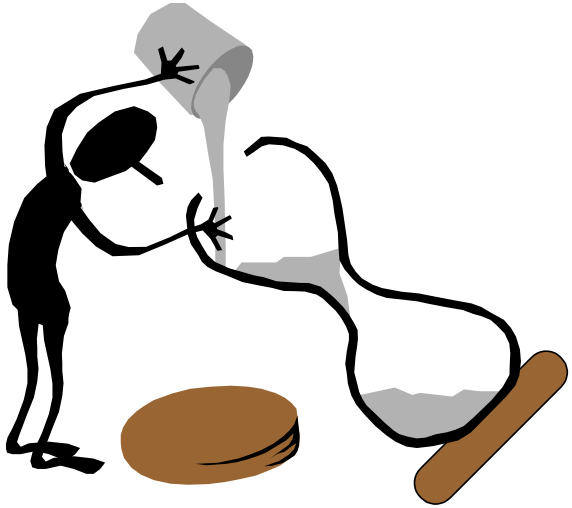
- Steps:
  - Register for the seminar (until 31 **October** in BASIS).
    This is your first important deadline! Care about the registration!
  - Initial meeting (today).
  - Structure your work, write the report, review other's reports, prepare the presentation (guided by your advisor).
  - Presentations ("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/
  - 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/

Time Schedule

Time schedule (your deadlines)



- **Today:** Introductory meeting

4w

- **31 October**: Registration in BASIS ends

4w

- **5 November:** Document outline
  - » literature research is done at this point
  - » you already know what you want to write in each section

3w

- **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

3w

- **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.

~1w

- **12 January**: Reviews done

3d

- **21 January:** Complete report, final version

5d

- **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)

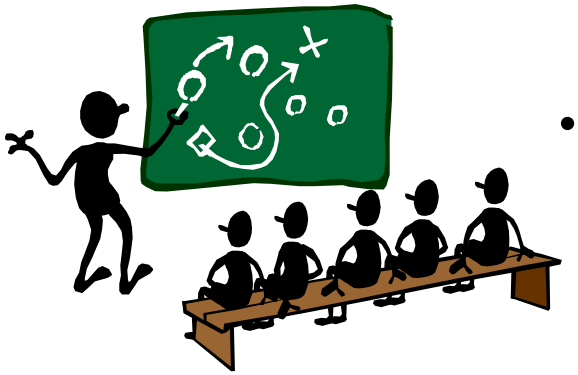
- The "Examination Rules for the Masters Degree Course in Computer Science" (i.e., the unofficial translation of the "MaPO", January 2012) say:

§ 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!

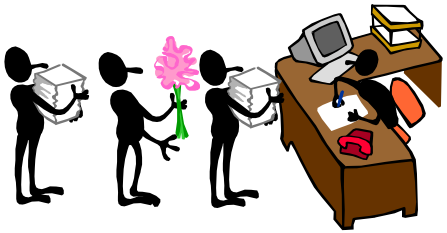
- Main literature sources:
  - Your advisor will send you an email containing further information about your topic.

Review Process

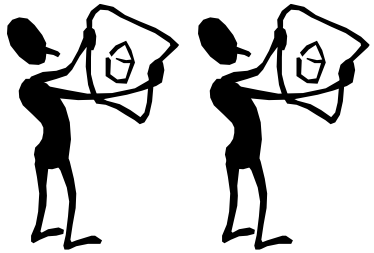
Review Process

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

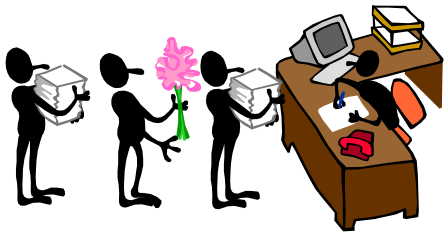
(1) Write your paper



(2) Submit paper



(3) Review other papers



(4) Submit reviews

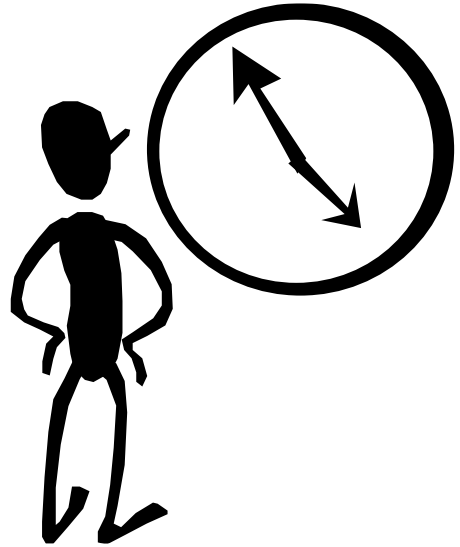
(5) Receive reviews

(6) Improve your paper

Some Advice

Advice: Deadlines

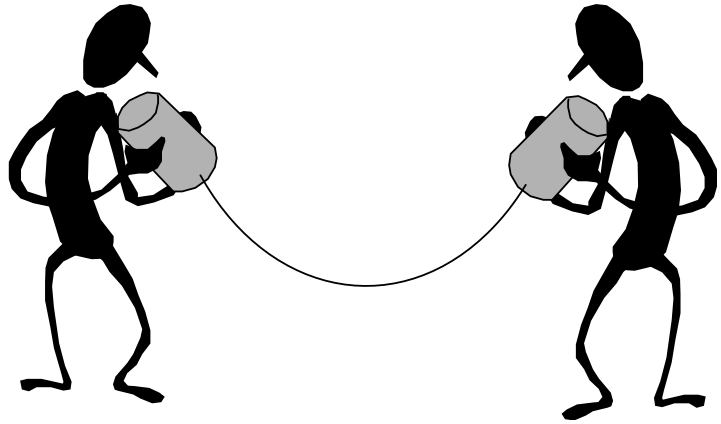
- Deadlines have to be kept!
  - Official deadlines (see previous slide on deadlines)
  - Any appointments and deadlines agreed upon with your advisor, e.g.,
    - first meeting
    - weekly meetings
    - intermediate report deadlines
  - Time management is important!



- 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.

Advice: Guidance

Guideline for the Composition of Master Theses, Seminar Papers and Lab Reports

Rheinische Friedrich-Wilhelms-Universität Bonn
Institut für Informatik IV

Prof. Dr. Peter Martini and staff

28.03.2012

1 Why?

This guideline for composing master theses, seminar papers and lab reports was inspired by the observation that, in the process of their work, students often repeat the same mistakes that could easily be avoided. On this background, the idea for this guideline was born with the intention to reduce your (and also, of course, our) time input, and provide you with a set of techniques for composing scientific texts which have proven very effective for improving the presentation of contents as well as as their comprehensibility for the reader.

1.1 The Purpose of a Lab Report

Preparing the report is an inherent part of every lab offered by our work group during the main study period. The report should give the reader a detailed picture of

- which task was tackled during the practical exercises,
- which challenges had to be coped with in order to accomplish the task,
- in what way and how well these challenges were mastered.

The report is **not a protocol of procedures**, i.e. it should not provide a detailed listing of all steps made in order to solve the problem. It is rather a documentation of

1

d solution and should also motivate why this particular solution was chosen. ppropriate to also mention other possible solutions that were tried but later on for good reasons. However, the description of the implemented solution must utweigh such references.

Purpose of a Seminar Paper

aper should summarize in short the vital aspects of a given subject. Since he text sources usually outnumbers the admitted paper volume by far, it is r the author to reduce the sources to the relevant facts. The paper should the author's own words and never be literally copied from the original text. rticularly applies to text sources in foreign languages: literal translations sy to recognize for the simple reason that they are difficult to read; apart y simply miss the point of the matter. One of the excuses for using literal that the original text could not be understood. If this is the case, rather utor for help – that is what he is there for. Other popular excuses like as so excellent, I could not have said it better" certainly do not require nments.

rpose of a Master Thesis

e MaPO (conditions of study) of 2008 [MPO08], the Master thesis is ual quotation from the German language MaPO):

Die Masterarbeit ist eine schriftliche Prüfungsarbeit, die zeigen r Prüfling in der Lage ist, innerhalb einer vorgegebenen Frist ein dem Gebiet des Studienganges selbständig nach wissenschaftlichen n bearbeiten, einer Lösung zuzuführen und diese angemessen

nglish meaning would be:

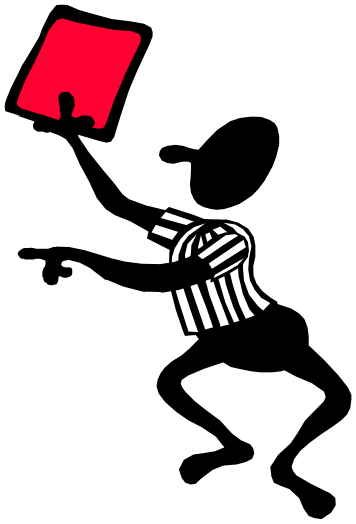
laster thesis is expected to show that the student is capable atly applying scientific methods to a problem in the field of nce within a set period of time, proving his/her aptitude for scientific work."

reviewed on the basis of the written elaboration handed in by the for the student's own benefit it is recommended to focus not only also on an appealing form of their presentation. Normally, the influenced by formal aspects of the thesis. If, however, we have to n two possible gradings, the form of presentation can be of vital

2

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!

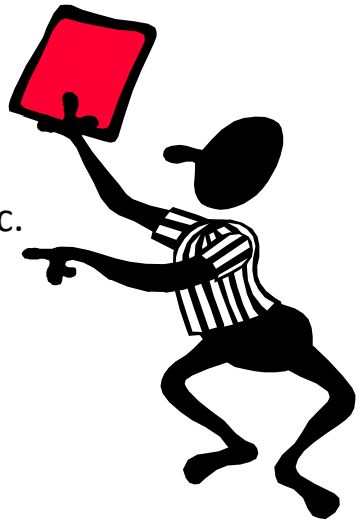


Advice: Avoid Plagiarism

- 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):

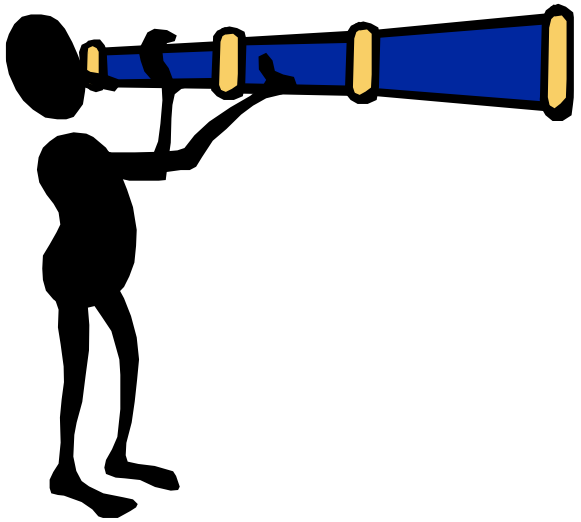


> § 13(9): „Any intentional violation of a regulation of these examination rules [...] will be regarded as an offence. Such an offence may be punished by a fine of up to 50,000 Euros."

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:

Name	Vorname	Honeypots	ICS Security	Identity Leakage	Resilience	Software Exploitation	Threat Intelligence
Bajwa	Awais			x		x	x
Hecker	Daniel	x			x	x	x
Karpienski	Marvin	x			x	x	x
Knauer	Sven			x			
Krah	Christopher					x	
Wagner	Roman		x	x		x	x
Winter	Eugen		x	x		x	x

- Each participant will choose one of the presented topics.

Topics Selection 1: Participants

Name	Vorname	Honeypots	ICS Security 2	Resilience	Threat Intelligence
Bajwa	Awais	x		X	xx
Hecker	Daniel	xx		x	xx
Karpienski	Marvin	xx		x	xx
Wagner	Roman		xx		X
Winter	Eugen		X		xx

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 -

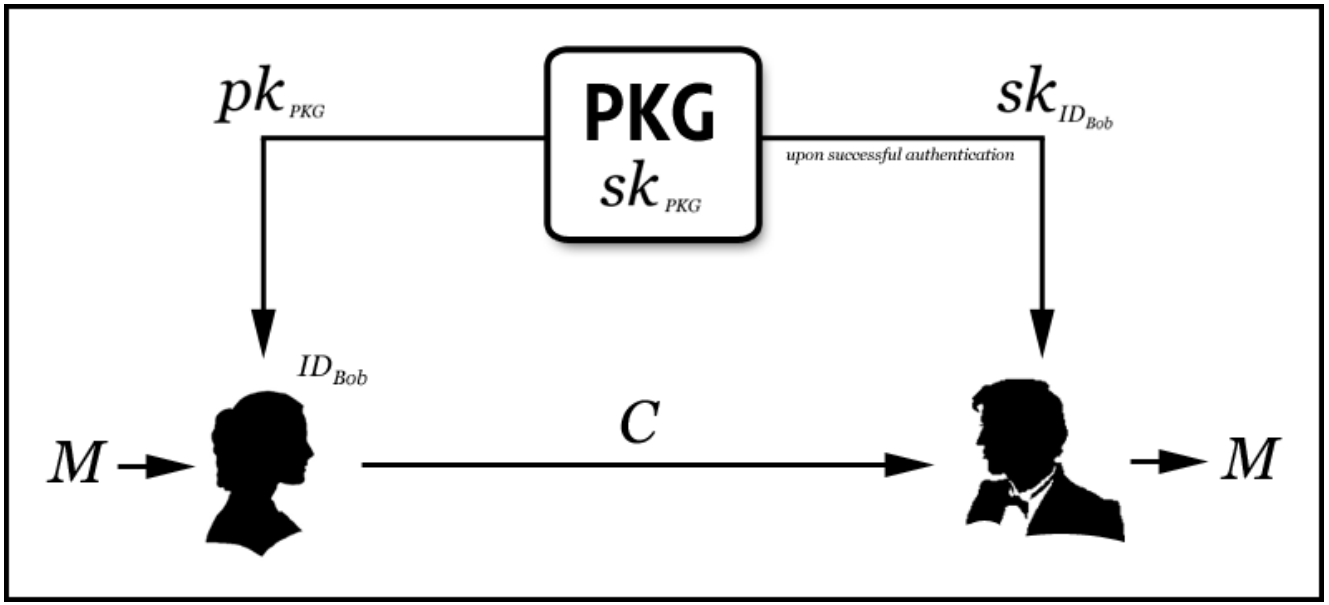
- Usability of Identity-Based Cryptography in Mobile Ad-Hoc Networks
- S. Zhao, A. Aggarwal, R. Frost, X. Bai, A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks
- Seminar objectives
  - Understand the principles of identity-based cryptography (IBC)
  - List the advantages/disadvantages 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

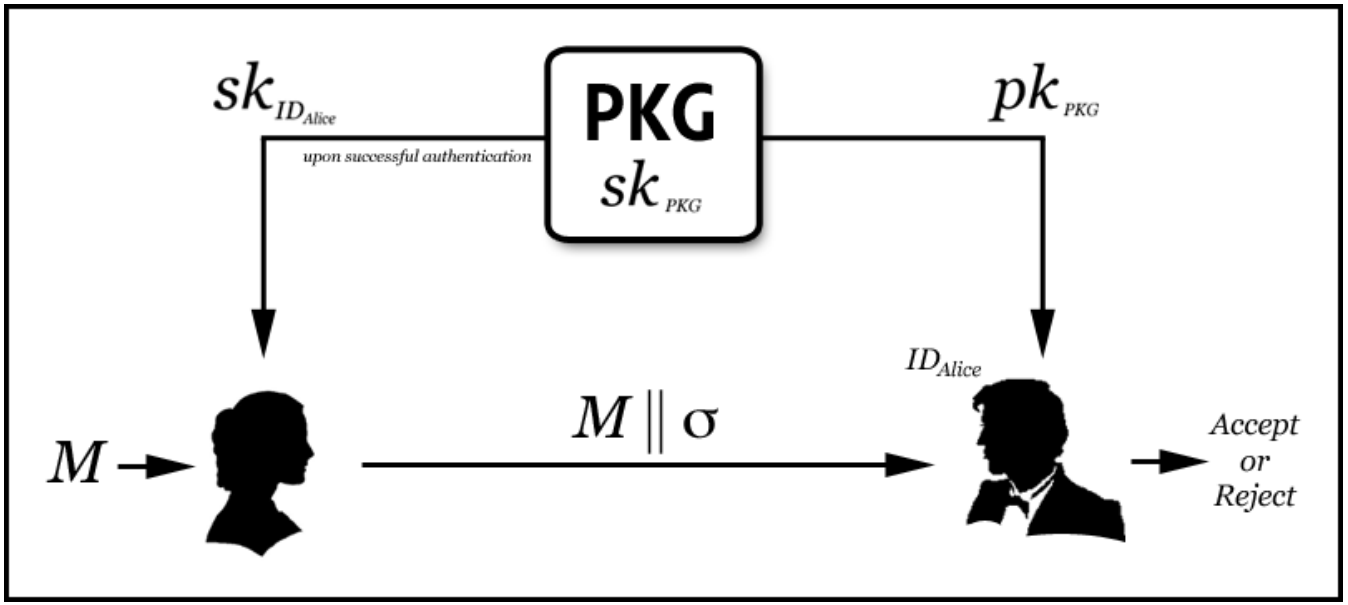
Identity-based encryption

- 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



Identity-based signature

- Alice authenticates with the PKG and receives the private key $sk_{ID_{Alice}}$ over a secure channel
- Alice generates a signature σ 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