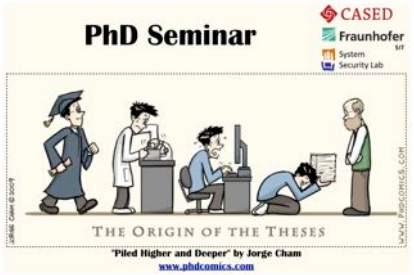
PhD Seminar 2011

Prof. Dr.-Ing. Ahmad-Reza Sadeghi
Dr.-Ing. Thomas Schneider
Prof. Dr. rer. nat. Michael Waidner



http://www.trust.cased.de/teaching/seminars/phd-seminar/

Recap: The Organizers

Prof. Dr.-Ing. Ahmad-Reza Sadeghi
Head of System Security Lab, TU Darmstadt
Director for Science, Fraunhofer SIT Darmstadt
http://trust.cased.de

Dr.-Ing. Thomas Schneider
Postdoctoral Researcher,
System Security Lab, TU Darmstadt
http://trust.cased.de

Prof. Dr. rer. nat. Michael Waidner
Head of SIT Research Group, TU Darmstadt
Director of Fraunhofer SIT Darmstadt
http://www.sit.cased.de

Recap: Our Goals for the PhD Seminar

Your successful PhD in IT Security:

- **Background Information**
- **Required Skills**
- **Goals**
- **Best Practices**
- **Learning-by-Doing**

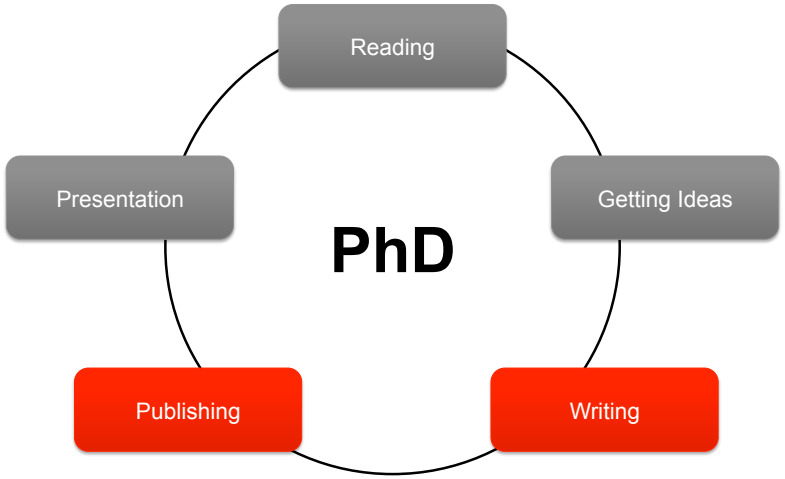
Recap: Methods

- **Interactive !**
- **Some Slides**
- **Exchange of Experiences + Best Practices**
- **Learning-by-doing**
- **Feedback**
- **Invited Talks (speakers to be announced)**

Contents of the Seminar

- **What is Research?**
  - Roles, Areas, Funding
- **Obtaining a PhD**
  - Motivation, Goals, Tips & Tricks
- **Research Skills**
  - Getting Ideas
  - Scientific Writing / Publishing / Presentation

Research Skills



Homework of last PhD seminar

- **If your research idea has been discussed today:**
  - Rethink your idea according to the feedback you got
- **Otherwise:**
  - Revise your presentation with feedback you got today
- **Write the abstract of your research paper!**
  - Max. [illegible] words
  - Structure:
    - Problem description
    - Related work & what's missing
    - Contribution
  - Send the abstract per email by Monday, June [illegible]

Always use the feedback you got to improve on what you did ! (in this case also your presentation)

Today's Schedule

Your Presentations	14:00 – 15:30	90min
Coffee Break	15:30 – 15:35	5min
Scientific Publishing	15:35 – 15:55	20min
Coffee Break	15:55 – 16:00	5min
Scientific Writing	16:00 – 17:00	60min

Today's Schedule

Your Presentations	14:00 – 15:30	90min
Coffee Break	15:30 – 15:35	5min
Scientific Publishing	15:35 – 15:55	20min
Coffee Break	15:55 – 16:00	5min
Scientific Writing	16:00 – 17:00	60min

YOUR PRESENTATIONS

Homework of last PhD seminar

- **If your research idea has been discussed today:**
  - Rethink your idea according to the feedback you got
- **Otherwise:**
  - Revise your presentation w.r.t. what you've learned today
- **Write the abstract of your research paper:**
  - Max. 1 page + 1 page references
  - Structure:
    - Problem description
    - Related work & what's missing
    - Contribution
  - Send the abstract per email by Monday, June 13

Homework of first PhD Seminar

- **Summarize most important research idea you are currently doing and present this within 15 minutes.**
- **Presentation Guidelines:**
  - 2 minutes per slide
  - Structure:
    - First 1/3 for undergraduate students
    - Second 1/3 for people in security area
    - Third 1/3 for experts in your area

Today's Schedule

CASED

Your Presentations	14:00 – 15:30	90min
Coffee Break	15:30 – 15:35	5min
Scientific Publishing	15:35 – 15:55	20min
Coffee Break	15:55 – 16:00	5min
Scientific Writing	16:00 – 17:00	60min

CASED

SCIENTIFIC PUBLISHING (PART 1)

Where to submit?

CASED

- **Your advisor will help you to decide !**
- **Shoot for best conferences & journals with reasonable chance to be accepted**
  - approximately same work, "who dares wins"
- **"Time-to-market":**
  - papers (few months)
  - journals (about a year)

http://www.cs.unc.edu/~azuma/hitch4.html

Conference Rankings

CASED

- **Do not rely on them too much**
- **Some links on PhD Seminar homepage**
  http://www.trust.informatik.tu-darmstadt.de/teaching/seminars/phd-seminar/

Example Top 20

CASED

Rank	Conference	Full Name
	Conference:	
13	CCS	ACM Conference on Computer and Communications Security
28	USENIX Security Symposium	USENIX Security Symposium
30	NDSS	Network and Distributed System Security Symposium
33	CSFW	Computer Security Foundations Workshop
35	CRYPTO	International Cryptology Conference
63	PET	Privacy Enhancing Technologies
74	S&P	IEEE Symposium on Security and Privacy
79	RAID	International Symposium On Recent Advances in Intrusion Detection
88	PKC	Public Key Cryptography
96	EUROCRYPT	Theory and Application of Cryptographic Techniques
125	ESORICS	European Symposium on Research in Computer Security
131	ASIACRYPT	The Annual International Conference on the Theory and Application of Cryptology & Information Security
139	SACMAT	Symposium on Access Control Models and Technologies
160	Financial Cryptography	Financial Cryptography
186	Information Hiding	Information Hiding
224	DSN	Dependable Systems and Networks
225	ACSAC	Annual Computer Security Applications Conference
276	FSE	Fast Software Encryption
279	ACISP	Australasian Conference on Information Security and Privacy
283	CHES	Cryptographic Hardware and Embedded Systems

http://www.arnetminer.net/page/conference-rank/html/Security,Privacy.html

Other Example Top 20

Here we first define the Conference Impact Factor (CIF) as follows:

CIF = 1 / (AR+PR+CR), where
AR = No. accepted papers / No. of submissions
PR = No. accepted papers / No. of registered participants
CR = No. accepted papers / No. of citations

Conference	CIF [2010]	AR	PR	CR [2010]
1. Usenix Sec	4.39	**14%** (25.6 / 182.8) [2006-2010]	**6.2%** (25.6 / 411.4) [2006-2010]	**2.6%**
2. IEEE S&P	4.15	**11.3%** (25.1 / 222) [2003-2010]	**10%** (25.1 / 250.8) [2003-2010]	**2.8%**
3. Crypto	3.38	17.5% (35.2 / 201.2) [2006-2010]	**9%** (35.2 / 389.6) [2006-2010]	**3.1%**
4. Eurocrypt	3.24	18.7% (32.6 / 174.6) [2006-2010]	**7.9%** (32.6 / 411) [2006-2010]	**4.3%**
5. ACM CCS	2.87	18% (54.8 / 304.3) [2007-2010]	**12.1%** (54.8 / 454.5) [2007-2010]	4.7%
6. Asiacrypt	2.69	**13.8%** (34.4 / 250) [2006-2010]	15.5% (34.4 / 221.8) [2006-2010]	7.9%
7. NDSS	2.60	**14.6%** (20.8 / 142.5) [2007-2010]	20.5% (20.8 / 101.5) [2007-2010]	**3.4%**
8. RAID	2.20	21.9% (19 / 86.8) [2006-2010]	15.3% (19 / 123.8) [2006-2010]	8.2%
9. CHES	2.09	27.9% (31.6 / 113.2) [2002-2010]	12.5% (31.6 / 253.1) [2002-2010]	7.5%
10. PET	1.95	25.6% (16.6 / 64.8) [2006-2010]	16.5% (16.6 / 100.8) [2006-2010]	9.3%
11. IEEE CSF	1.85	23.8% (23.2 / 98.4) [2006-2010]	25% (23.2 / 92.8) [2006-2010]	5.2%
12. ACSAC	1.82	25.3% (39.5 / 156.3) [2000-2010]	18.8% (39.5 / 210.3) [2000-2010]	10.8%
13. FSE	1.80	31.3% (26.2 / 83.8) [2006-2010]	15.8% (26.2 / 166) [2006-2010]	8.5%
14. DSN	1.74	23% (68.9 / 300) [2004-2010]	23.6% (68.9 / 291.6) [2004-2010]	11%
15. CT-RSA	1.59	30.2% (25.8 / 85.4) [2006-2010]	22.7% (25.8 / 113.8) [2006-2010]	9.9%
16. PKC	1.50	26.2% (30 / 114.6) [2004-2010]	30.3% (30 / 99) [2004-2010]	10.2%
17. TCC	1.48	32.3% (32.2 / 99.8) [2006-2010]	24.4% (32.2 / 131.8) [2006-2010]	10.9%
18. ESORICS	1.45	21% (38.4 / 182.6) [2006-2010]	36.5% (38.4 / 105.2) [2006-2010]	11.6%
19. ACNS	1.44	**16.5%** (32.6 / 197.9) [2003-2010]	33.4% (32.6 / 97.5) [2003-2010]	19.5%
20. DIMVA	1.42	29.6% (13.1 / 44.3) [2004-2010]	15.8% (13.1 / 82.7) [2004-2010]	25%

http://icsd.i2r.a-star.edu.sg/staff/jianying/conference-ranking.html

Upcoming Calls for Papers

CASED

- **See list on PhD Seminar homepage:**
  - IACR Calendar of Events in Cryptology
    http://www.iacr.org/events/eventsbysubmission.php4
  - UCL Crypto Group: Call for Papers
    http://www.uclouvain.be/crypto/callforpapers/forthcoming
  - IEEE Security: Call for Papers
    http://www.ieee-security.org/CFP/Cipher-Call-for-Papers.html

Call for Papers

- **What are the important dates?**
  - Make sure at least one author can present !
- **Who is in the Program Committee?**
  - Know & cite their previous works !
- **Formatting restrictions?**
- **Anonymous or non-anonymous submission?**

Submission Deadlines

- **Start to write as early as possible !**
- **You won't sleep the night of the submission anyways ☺**
- **Note: Top conferences <u>never</u> extend the deadline !!!**

Today's Schedule

Your Presentations	14:00 – 15:30	90min
Coffee Break	15:30 – 15:35	5min
Scientific Publishing	15:35 – 15:55	20min
Coffee Break	15:55 – 16:00	5min
Scientific Writing	16:00 – 17:00	60min

SCIENTIFIC WRITING

References

(see PhD seminar webpage for links)

- **How to write a great research paper**
  by Simon Peyton Jones
- **How to write a security paper**
  by Patrick McDaniel
- **How to write a good systems paper**
  by Roy Levin & David D. Redell
- **Writing clear conference submissions**
  by Shai Halevi
- **How to write a paper**
  by Oded Goldreich

General ideas on writing

(taken & combined from references on previous slide)

- **The goal of your paper is to convey your idea(s) from your head into your reader's head (who may find it useful).**
- **Start writing a paper and give a talk already about preliminary ideas:**

  - Forces us to be clear & focused
  - Crystallises what we don't understand
  - Allows dialogue: reality check, critique, and collaboration

How to write a good paper

- **Writing good papers requires long experience**
  - Read papers from good writers (e.g., Mike Reiter)
  - Respect and learn from the feedback of senior researchers (they are the best representatives for the reviewers)
- **Always keep the reviewers/readers in mind**
  - You must convince both, non-experts and experts
  - Write top-down:
    - always give the high-level idea first (to convince non-experts)
    - before diving into technical details (to convince experts)
  - Structure your text as good as possible (no continuous text !)
  - A good picture often says more than thousand words !

Possible Structure of a Paper

CASED

Abstract (4 sentences)
Introduction (1 page)
The problem (1 page)
My idea (2 pages)
The details (5 pages)
Related work (1-2 pages)
Conclusions and further work (0.5 pages)

(from Simon Peyton Jones: "How to write a great research paper")

The Abstract

CASED

- **High-level description of your paper**
- **Might be all that some readers can access**
  - Self-contained: no links to rest of paper (e.g., references)
  - Informative and not too cumbersome or too long
- **Used by PC members to decide which papers to read**
  - Make (the right) people interested in reading your paper
- **Four sentences (or at least parts) [Kent Beck]**
  1. State the problem
  2. Say why it's an interesting problem
  3. Say what your solution achieves
  4. Say what follows from your solution

Example:

CASED

Problem	1.	Many papers are badly written and hard to understand
Relevance	2.	This is a pity, because their good ideas may go unappreciated
Solution	3.	Following simple guidelines can dramatically improve the quality of your papers
Impact	4.	Your work will be used more, and the feedback you get from others will in turn improve your research

(from Simon Peyton Jones: "How to write a great research paper")

Homework of last PhD seminar

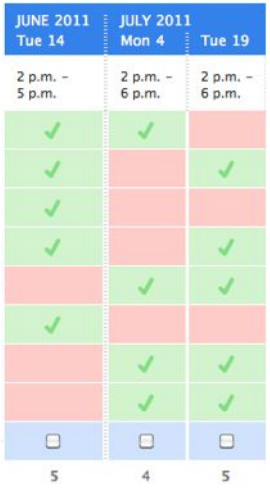
CASED

- **If your research idea has been discussed today:**
  - Rethink your idea according to the feedback you got
- **Otherwise:**
  - Revise your presentation w.r.t. what you've learned today
- **Write the abstract of your research paper:**
  - Max. 1 page + 1 page references
  - Structure:
    - Problem description
    - Related work & what's missing
    - Contribution
  - Send the abstract per email by Monday, June 13

Your Extended Abstract

- **Pick a first partner**
  - Exchange the abstracts you prepared and give feedback (first by writing notes on the abstract, then talk about it)
- **Use the feedback to improve your abstract**
- **Pick a second partner**
  - Exchange your improved abstracts and give feedback again
- **Improve your abstract again**

Date for next PhD Seminar



July 19 was planned originally.
➪ but Dan Wallach will visit CASED and give a talk.

July 4 is not possible as well.
➪ **we are looking for the next date and announce it soon**

Homework until next PhD seminar

- **Use the feedback you got on your extended abstract**
- **Split/extend your extended abstract into the following parts of your paper:**
  - Abstract
  - Introduction
  - Related Work
  - References (use Bibtex & compact+consistent references: “In Computer and Communications Security (CCS’09)” but not “In Proceedings of 12th International Conference on …”)
- **Print your paper 12 times & bring it to next seminar**