

Seminar “Mobile Security”

winter term 2010/11

Daniel Loebenberger, Yona Raekow

b-it

25 October 2010



- ▶ Application process
- ▶ Seminar roadmap
- ▶ Grading scheme
- ▶ Description of the topics
- ▶ AOB

- ▶ Unfortunately, the seminar is overbooked.
- ▶ Please write until Wednesday, 27 October 2010, 23:59:59h an application to

`daniel@bit.uni-bonn.de`.

- ▶ The application should contain:
 - ▶ your full name with your student id,
 - ▶ your email address,
 - ▶ your aim of studies,
 - ▶ your semester,
 - ▶ all lectures related to Networks, Security or Cryptography you attended,
 - ▶ a list of three topics you are interested in,
 - ▶ a short explanation why you are interested in the seminar.

- ▶ Conference style seminar.
- ▶ Write a paper, write reviews, give a talk.
- ▶ Conference style review:
 - ▶ strong accept
 - ▶ accept
 - ▶ weak accept
 - ▶ borderline paper
 - ▶ weak reject
 - ▶ reject
 - ▶ strong reject

- ▶ 25% for the first draft of the paper,
- ▶ 25% for the reviews,
- ▶ 25% for the talk,
- ▶ 25% for the final version.

Date	Event
27 October	Application Deadline at 23:59:59h.
28 October	Distribution of the topics via email.
06 December	Deadline for submission of the paper at 23:59:59h.
08 December	You get three papers of other participants.
21 December	Due date for review I at 23:59:59h.
10 January	Due date for review II at 23:59:59h.
17 January	Due date for review III at 23:59:59h.
19 January	You obtain the reviewer comments on you paper.
31 January	Deadline for handing in your presentation.
07-08 February	Conference date (tentative dates).
21 February	Due date for the final version of your paper.

- ▶ All dates are strict. No late hand-ins will be accepted.
- ▶ Register for easychair on time.
- ▶ Do not wait for the last minute to submit your paper.
- ▶ Meet with the tutor on time.

- ▶ The paper should be 10-15 pages long.
- ▶ Content:
 - ▶ Thorough description of the topic and the security related problems.
 - ▶ Description of the proposed solution.
 - ▶ Analysis of the solution.
 - ▶ Conclusion/Outlook.
 - ▶ References.
- ▶ The content should be written by you. Copy/paste from the references, wikipedia or any other source will result in no credit.
- ▶ Prepare the paper in LaTeX.
 - ▶ Submit a PDF.
 - ▶ The first draft of the paper needs to be anonymous: Do not put your name on the submission.
 - ▶ If the first draft of the paper is rejected you will receive *no!* credit for that part.

- ▶ History and architectures of mobile networks
- ▶ Milenage and security of the UMTS network
- ▶ Denial of Service attacks on GSM and UMTS
- ▶ IMSI Catcher
- ▶ Security of Android
- ▶ Security of iPhone OS
- ▶ Car2X security
- ▶ Trusted mobile platforms
- ▶ LTE(Long Term Evolution)
- ▶ Security of sensor networks
- ▶ Security of wireless ad hoc networks/wireless mesh networks

- ▶ GSM security: Cryptanalysis of A5/1
- ▶ SIM cards
- ▶ Location based services
- ▶ Near field communication
- ▶ RFID security
- ▶ Viruses, worms and trojans on mobile phone
- ▶ Mobile phone forensics (Source Identification)
- ▶ WLAN: Breaking WEP
- ▶ WLAN: WPA and WPA2 security
- ▶ Bluetooth security

Questions?