Seminar Mobile Security

winter term 2011/12

Prof. Joachim von zur Gathen, Konstantin Ziegler

b-it

31 October 2011

Agenda today

- Application process
- Conference style
- Roadmap
- Grading scheme
- Possible topics
- Questions?

Application process

- ▶ Please write until Monday, 7 November 2011 an application to

    zieglerk@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 and these topics.

Conference style

- ▶ 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

Grading

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

Roadmap

November	
7 November	Application Deadline.
10 November	Distribution of the topics via email.
December	
12 December	Deadline for submission of the first draft of your paper.
13 December	You receive three papers for reviewing.
19 December	Due date for review I.
January 2012	
9 January	Due date for review II.
16 January	Due date for review III.
17 January	You obtain the reviewers' comments on your paper.
30 January	Deadline for handing in your presentation.
February	
6-8 February	Conference (tentative dates). Presence mandatory.
20 February	Due date for the final version of your paper.

Philosophy

- All deadlines are at midnight. No late hand-ins will be accepted.
- Register for easychair on time.
- Do not wait for the last minute to submit your paper.
- If you have general questions, ask on the mailing list.
- If you have specific topic-related questions, arrange for a meeting with Konstantin.

Paper

- ▶ 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 main part of your paper should be written by you, not just copied and pasted from the references, wikipedia or any other source.
- ▶ Do not plagiarize! The sources for any of your material must be clearly indicated, at the place where they are used.
- ▶ Prepare the paper in LATEX.
    - ▶ Submit a PDF.
    - ▶ The submission is *not* anonymous. 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
- 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
- 3GPP LTE (Long Term Evolution)
- Security of sensor networks
- Security of wireless ad hoc networks/wireless mesh networks

Topics

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

Questions?