Seminar on

Network security and privacy

(selected topics)

Prof. Dr. Dieter Hogrefe
Sviatoslav Edelev
Maimun Rizal
Hang Zhang

Course Overview

Prerequisites (Recommended)**:**
Mobile communication I
Mobile communication II

Implements Module:
M.inf.122 - Seminar Telematik I
M.Inf. 222 - Seminar Telematik II
M.Inf. 1122: Seminar Vertiefung Telematik (AI)
3.06 - Advanced Topics in Computer Networking I **(ITIS)**

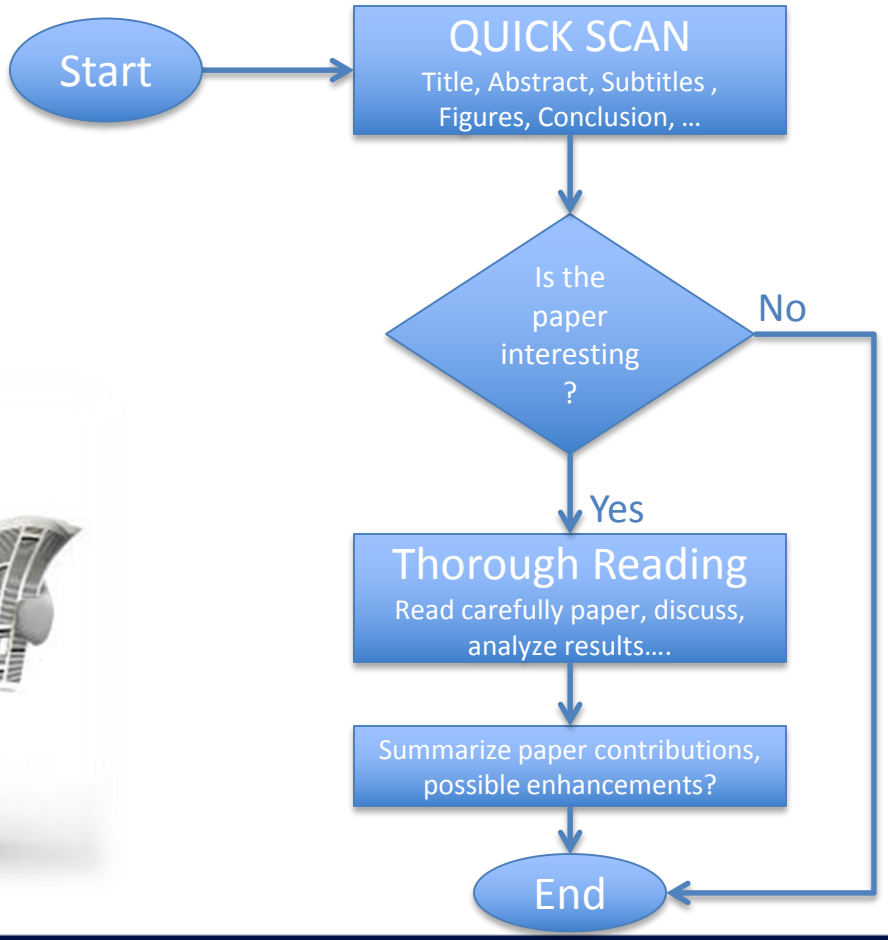
Language
English

Course Objectives

- Primary objectives:
  - Learn some fundamentals of security and privacy issues in computer and wireless networks.
  - Form the state of art on a certain topic.
  - Provide a paper form report and a professional presentation for a chosen topic.
- Secondary objectives:
  - Experience in preparing professional reports and presentations.
  - Learn how to search for papers:
    - IEEExplore, ACM, Citeseerx, whitepapers….

Hints on Reading papers

PAPER READING



Report

- Requirements:
  - In form of IEEE conference template paper [two columns, 5-8 pages]: http://www.ieee.org/conferences_events/conferences/publishing/templates.html
  - Organization:
    - Abstract,
    - Introduction
    - (Related work)
    - Main part of your topic (model, discussion, analysis, simulations, results...)
    - Conclusion
  - PDF + Editable(Latex, word...) format

Hints on Writing Scientific Papers

- Abstract: not more than 100-150 words.
- Brief Introduction*:
  - Introduce problem (why important, motivate)
  - (Related work).
  - Outline your contribution.
  - Outline paper structure.(This paper is organized as follows...)
- Body*:
  - Problem, system model/architecture, basics...
  - Discussion, anaylsis.
  - Evaluation, results.
- Summary and conclusions.
- Bibliography.

*These points might vary with the subject topic.
*Source:http://www.cs.columbia.edu/~hgs/etc/writing-style.html

Hints on Writing Scientific Papers

- Paragraphs should have a logical narrow flow.
- Avoid very long sentences.
- Clarify notations at first use.
- Write for the reader, not yourself.

- Not only show figures! Comment, Analyze and Abstract!
- Avoid spelling mistakes!!! Review several times!

Presentation

- High-quality presentation
  - Well-structured, correct spelling, professional layout.
  - Duration of each presentation ~30 minutes + ~15 minutes discussion.
  - Slides presentation (e.g. Pdf, ppt, …)

- Compliance with set deadlines.

Hints for the Presentation

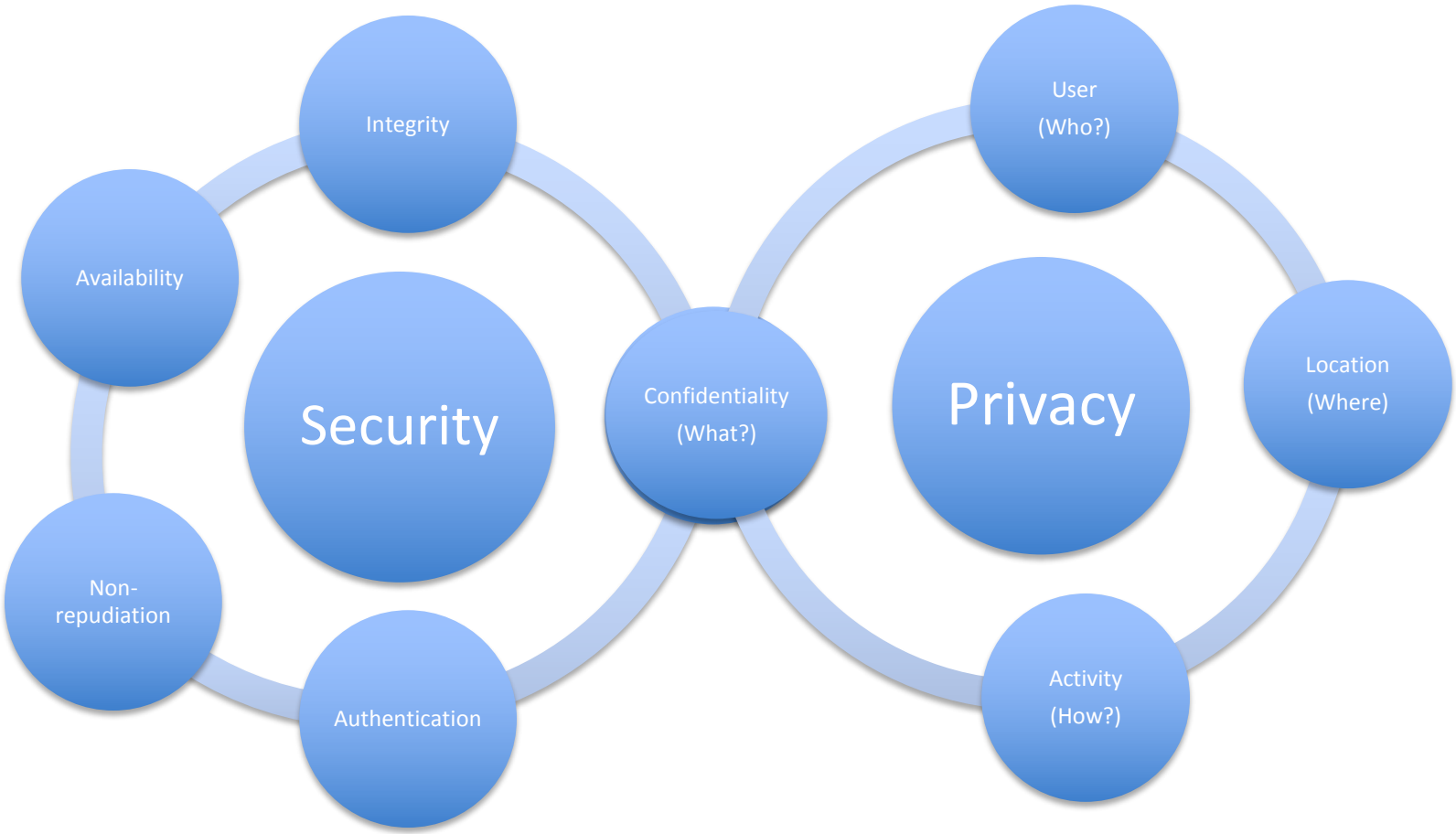
- Rule of thumb:
  - A slide containing a normal content takes about 1-2 minutes
    ➔ for 30 minutes approximately 20-26 slides.

- Basic guide
  - Welcome your audience.
  - Give an outline of the presentation.
  - Try to speak without notes, do not read out loud everything from the slides word-by-word.
  - Adjust your presentation speed so that the audience can follow.
  - **How to give a good research talk guide:**

http://research.microsoft.com/en-us/um/people/simonpj/papers/giving-a-talk/giving-a-talk.htm

http://www.ted.com/talks/nancy_duarte_the_secret_structure_of_great_talks.html

Security & Privacy Fundamentals



Applications

Internet	• Routing Protocols
WSN	• Wireless Sensor Networks
MANETs	• Mobile Ad hoc Networks
VNETs	• Vehicular Networks
WBANs	• Wireless Body Area Networks • Healthcare
VoIP	• Voice over IP
Wireless Localization	• PKE • GPS

Selected Topics

1. Survey on Distance Measurement Approaches within Bluetooth Area
2. Overview of RFID: strong and weak points, privacy and security issues, applications, open questions. Data encoding on RFID-tags.
3. DOS Attacks against IEEE 802.11
4. Intrusion-Detection Systems in Wireless Networks
5. Vulnerability Analyses and Attacks on NFC Enabled Cell Phones
6. Privacy and security issues in RFID authentication protocols
7. RFID Malware
8. Anonymity in communication systems
9. Man-in-the-Middle Attacks on VoIP
10. Authentication in Voice over Internet Protocol (VoIP)
11. Attacks of Trust and Reputation Systems
12. Key Management in Ad-hoc Networks

Available Topics

1. ~~Survey on Distance Measurement Approaches within Bluetooth Area~~
2. ~~Overview of RFID: strong and weak points, privacy and security issues, applications, open questions. Data encoding on RFID-tags.~~
3. DOS Attacks against IEEE 802.11
4. ~~Intrusion-Detection Systems in Wireless Networks~~
5. ~~Vulnerability Analyses and Attacks on NFC Enabled Cell Phones~~
6. ~~Privacy and security issues in RFID authentication protocols~~
7. ~~RFID Malware~~
8. ~~Anonymity in communication systems~~
9. ~~Man-in-the-Middle Attacks on VoIP~~
10. Authentication in Voice over Internet Protocol (VoIP)
11. ~~Attacks of Trust and Reputation Systems~~
12. Key Management in Ad-hoc Networks

References

- C. Mulliner, ''Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones '', In Proc. of International Conference on Availability, Reliability and Security, 16-19 March 2009
- L. Wang, B. Srinivasan and N. Bhattacharjee, ''Security Analysis and Improvements on WLANs'', Journal of Networks, VOL. 6, NO. 3, March 2011
- K. Finkenzeller, ''RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication'', 3rd Edition, ISBN: 978-0-470-69506-7, June 2010
- A.N. Raghavan, H. Ananthapadmanaban, M.S. Sivamurugan, B. Ravindran, ''Accurate Mobile Robot Localization in indoor environments using Bluetooth'', In Proc. of 2010 IEEE International Conference on Robotics and Automation, May 3-8, 2010, Anchorage, USA
- H. Debar, ''An Introduction to Intrusion-Detection Systems'', In Proceedings of Connect, 2000
- Marmol F G, Pérez G M. ''Security threats scenarios in trust and reputation models for distributed systems''[J]. Computers & Security, 2009, 28(7): 545-556.
- Hegland A M, Winjum E, Mjolsnes S F, et al. ''A survey of key management in ad hoc networks''[J]. IEEE Communications Surveys & Tutorials, 2006, 8(3): 48-66.

References

- A. Juels, ''RFID security and privacy: a research survey'', IEEE Journal on Selected Areas in Communications, Volume 24, Issue 2, Pages: 381 - 394, Feb. 2006
- M.R. Riebacka, P.N.D. Simpsona, B. Crispoa, A.S. Tanenbaum, ''RFID malware: Design principles and examples'', Journal on Pervasive and Mobile Computing, Volume 2, Issue 4, Pages 405-426, November 2006
- Danezis, G., et al. (2009). ''Systems for anonymous communication.'' Handbook of Financial Cryptography and Security, Cryptography and Network Security Series: 341-389.
- Ren, J. and J. Wu (2010). ''Survey on anonymous communications in computer networks.'' Computer Communications 33(4): 420-431.
- R. Zhang, X. Wang, R. Farley, X. Jiang, ''On the Feasibility of Launching the Man-in-the-Middle Attacks on VoIP from remote Attackers'', ASLACCS09, March 10-12, 2009, Sydney, NSW, Australia. ACM 978-1-60558-394-5/09/03.
- F. Wang, Y. Zhang, ''A new provably secure authentication and key agreement mechanism for SIP using certificateless public-key cryptography,'' Computer Communications, Volume 31, Issue 10, 25 June 2008, Pages 2142-2149, ISSN 0140-3664

Course Plan

No.	Course Description	Date
1	Register for the seminar by sending an email to the leading assistant. Please register as soon as possible to arrange the necessary amount of topics.	15.04.2013
2	Introduction Session (PDF)	15.04.2013
3	Finalize your topic	22.04.2013
4	Discussion of a draft of the report	21-24.05.2013
5	Register in FlexNow!. Students from ITIS should register in their examination system	**24.05.2013**
6	Submit the final report as PDF-file to the leading assistant.	10.06.2013
7	Recommended time for preparing the talk, discussion of the slides.	17.06.2013
8	Submit the slides.	20.06.2013
9	A week for discussion the slides with the leading assistant.	24-28.06.2013
10	Presentation of topics:	tba, ca. 01-05.07.2013
11	Presentation of topics:	tba

Grading points

- Report: 50%
- Presentation: 40%
- Active participation in seminar: 10%.
- Penalties may apply:
  - Incompliance with set deadlines.
  - Incomplete attendance of block seminar.

QUESTIONS ?