# T-110.5190

## Seminar on Internetworking

# Presenting Papers

Sanna Liimatainen and Antti Ylä-Jääski

**http://www.tml.hut.fi/Opinnot/T-110.5190/**

# Contents

- Conference
- Presentation
- Opponing and grading

# Conference

- Traveling to the site
- Registration: proceedings, name tag, other material
- Presentations: papers, posters, invited talks
- Breaks and social events
- Conference staff: session chair

# Presentation

- Length of the presentation
- Audience
- Technical equipment and visual aids
- Presenting your work

# LENGTH OF THE PRESENTATION

- T-110.5190 Papers: 20 min for talk and 5 min for questions
- Follow the instructions of the session chair
- Do not exceed your time, it is not polite
- Changing the speaker is included in the time given

# Audience

- The audience knows much and wants to know more
- Here: computer science students, post-graduate students and professor
- Respect your audience: keep the timetable
- No marketing talk

# Conference Room and Technical Equipments

- If possible, check the room beforehand
- Find out what are the technical equipments available
- Contact your session chair beforehand
- T-110.5190: upload your slides to Optima latest: 3rd May 2006 Midday either in .pdf or .ppt

# SLIDES

- Use large font: less than 10 lines per slide
- Use few slides: presenting a slide will take at least one or two minutes, often much more
- Dark text on light background is usually best

## Slides - What to Avoid

- Animations and fancy slide transitions
- Unnecessary and irrelevatn clip art
- Company logos
- Incoherence of markings

# BAD EXAMPLE

The IPsec architecture has several parts. Some of them are part of the protocol stack of the Internet, and some of them are used otherwise.

- The IPsec architecture consists of two types of protection headers, the concept of security association (SA), protocols for negotiating the security associations, and two storages, one for acceptable security associations and another for used security associations.
- **A Security association (SA)** defines used modes (i.e. transport or tunnel mode), method (i.e. AH or/and ESP protection header), cryptographic algorithms and keys etc [RFC2401]. When a protected session is created, security associations are negotiated for both ways of the connection. That is, there exist two security associations for every connection: one for one direction and another for the other direction. These SAs can define, for example, different encryption keys for different directions of the traffic. I give examples later in this presentation.
- *The Internet Key Exchange (IKE) protocol* [RFC2409] is used for SA negotiations. It is based on Internet Security Association and Key Management Protocol (ISAKMP) [RFC2408] but defines in more detail how security associations are created. Before a session can be established between two endpoints, these two endpoints have to agree on how the session will be protected.
- *The Domain of Interpretation for IPsec is defined in [RFC2407]*. This RFC tells abbreviation numbers for all protocols and algorithms used in IPsec, and these abbreviation numbers are used in security association negotiation messages to shorten the messages and to ease the computer decoding of the messages.
- The IPsec framework defines use of two databases: one for security associations that are in use in a session and another for the rules to form these SAs. The first database is Security Association Database (SAD). After the SA negotiation, the endpoint stores the information about the used SA into this database. It uses a Security Parameter Index (SPI) as an identifier for SAs. The second database used in IPsec is the Security Policy Database (SPD). It gives instructions on what kind of SAs are acceptable according to the security policy of the organization. For example, the policy can state that all the connections must be encrypted. The SPD database is used during the SA establishing negotiation. IPsec does not define how these databases are implemented. However, this does not affect the interworking of different implementations since the message format is still same and databases are only used internally.

# Content of the Slides

- Main points, not all what your paper consists
- E.g. Your own contribution
- Not for yourself but for the audience

# Content of the Presentation

- Main results
- The big picture
- Avoid long introduction
- Adapt your presentation to previous ones (hard)

# The Most Important Parts of the Presentation

Beginning

- Your research question that you tried to answer
- Why the topic is interesting

Ending

- Main conclusions
- What we should remember

# QUESTIONS

- Questions and discussions give valuable feedback for your work
- “I do not know”
- “That was out of scope of this work”
- Not argueing back without justifications

# Before the Presentation

- Practice the presentation
- Upload your slides to Optima either on .pdf or .ppt: deadline 3rd May 2006 at midday
- Discuss with your session chair before the presentation
- Check that the slides work on the presentation computer

# OPPONING

- Prepare some questions and ask them
- If someone else has questions, give him/her time to ask, too
- Do not present your opponent raport verbally
- Written feedback aftewards: deadline 11th May at midday (paper, presentation, answering to questions) good, must be improved, wrong, and grade

# GRADING

- Normal grading: 1=poor, 2=something to correct, 3=good work, 4=clearly consist own thinking, 5=brilliant
- Paper: 60%
- Presenting: 25%
- Opponing at the seminar: 10%
- First phase of the opponing: 5%