

T-110.5230 Special Course in Practical Security of Information Systems

**Topic selection
Course deliverables**

29.1.2009

Outline

- Topic reservation sheet
- Course deliverables
- Topic checking

Topic reservation sheet

- The sheet will be passed around – write down
 - Group member names (and e-mail if we don't have it yet)
 - Topic title
- If your group and topic are already on the list – check info
- We'll go through the topics and groups at the end of the lecture

Course deliverables

Overview of deliverables

- Paper TOC & reference list
- Attack plans + peer reviews
- Vulnerability reports
- Paper draft + peer reviews
- Presentation slides
- Paper final

Paper TOC & reference list

- Sketch of structure
 - Section and subsection headings
 - Short explanation of (sub)section content
- Reference list should be close to final (=> BibTeX)
 - Intent is to ensure background work done properly
- References and structure are important
 - Style/language is not
- Finding references – part of the learning process
 - Remember to be critical – assess credibility and relevance carefully
 - Google, Citeseer (publications), CERT and other advisory bodies
 - IETF, RFC-Editor, www.watersprings.org, W3C (specs)

Attack plans

- Describe
 - **Target:** What you plan to attack
 - **Method:** How you plan to attack
 - **Environment:** Where you plan to attack (including environment, products, permissions...)
- Informal
 - Intent to ensure that attacks are “interesting” (relevant) and that they are implementable in practice
 - Style does not matter: text + enscript + ps2pdf is fine
- A template given on course web page
 - Please follow cover page requirements for non-LaTeX deliverables (see templates ZIP file)

Peer review of attack plans

- Review the attack plans of two other groups
 - The lists of groups you'll review will be posted to the course web page once groups & topics are clear
- Peer review is just an e-mail submission (text in body)
 - Template given on web page

Vulnerability reports

- Required parts for each vulnerability
 - Threat and Vulnerability
 - Preconditions for the Attack
 - Analysis of the Attack
 - Detection and Tracing
 - Protecting against the Attack
 - Test results
- The deliverable consists of three separate reports in one document
 - Include a cover page with topic and names
- You need to carry out the attack before submission !
- Both style / language and content matter
 - LaTeX + BibTeX strongly recommended but not mandatory
 - Please follow cover page requirements for non-LaTeX deliverables (see templates ZIP file)

Paper draft

- Stand-alone document
- Suggested structure (deviation OK if for good reason)
 - Title and authors, Abstract
 - Introduction, Background
 - Vulnerabilities explained (refer to vulnerability reports for details), include description of you attacks (plans, carrying out, results)
 - Impact
 - Protection - countermeasures, detection, etc
 - Conclusions and References
- Style and format
 - 8-10 pages, if more, confirm with staff
 - Language and style matter, LaTeX and BibTeX mandatory
 - See course page for LaTeX instructions
 - Test your LaTeX environment early if you're not familiar with LaTeX !

Presentation slides

- Content
 - Your topic and what you've done, including the vulnerability reports, the paper, etc.
 - No fixed structure – use what works best
- Grading
 - Structure
 - Style and language

Peer review of paper draft

- Review the paper draft of two other groups
 - The lists of groups you'll review will be posted to the course web page once groups & topics are clear
- Peer review is just an e-mail submission (text in body)
 - Template given on web page

Seminar presentation at HUT

- Language
 - English
- Time slots
 - 20 minutes + 5 minutes for questions
 - Schedule will be on web page well before the seminar
- Practicalities
 - Course staff brings latest PDFs you sent, these will be the primary source for presentation slides
 - No need to change laptop; send up-to-date slides early
 - But just in case...
 - Bring a USB stick/CD with your presentation (or bring your laptop)
- Grading
 - Both content and delivery will be graded

Final paper

- Address comments from peers and staff
- This is the graded submission

Topic checking

Topic checking

- Groups and topic titles
- Topic conflicts ?
 - => Backup topics
- Usually topics need scoping down for attack plans
 - Topic title may become more specific
 - If so, include the new topic in your submission (e.g. attack plans)
- If you're changing the topic (not just scoping down)
 - E-mail to confirm change

Summary

- Next steps
 - Deadlines, deadlines, ...
 - Presentations
- If something is unclear, ...
 - Use course e-mail
- Any issues with your topic at this point?
 - Don't have a topic?
 - Want to change topic?
 - Already e-mailed about topic issues?
 - Something else?
 - => Come talk to us after we finish
- Questions?