PA168 – Postgraduate seminar on IT security and cryptography

Vašek Matyáš & Jan Staudek

Email: matyas@fi.muni.cz
Office hours: Tue 8:30-30 & Thu 15:00-16:00 (B415)

Typical seminar structure

- 2 presentations for the start
- Discussion related to above
- News/developments update
  - Recent news
    - New results/achievements (no attack stats!)
    - Crypto-Gram (B. Schneier), comp.risk,
    - http://www.lightbluetouchpaper.org/
    - http://www.theregister.co.uk/
  - *Own insight / analysis / view*

Your presentations

- O (Own work)
  - On the topic of your current research / interest
  - Ideally as a training for your needs
    - Presentation for a conference/workshop, thesis, etc.
- N (News)
  - Presentation of news from the last week (or so)
- R (Reading)
  - Presentation of a recent paper
    - Papers proposed during the term
    - Detailed review of the paper with discussion

Marking & Language

- The course primary language is English!!!
  - In Czech only when the ultimate target for your presentation requires this
    - M.Sc. thesis presentation
    - Czech conference presentation
- Mark comprises:
  - O presentation 40%
  - R & N presentation 30% each
  - Resulting P(ass) for 75% or more
- Other activities (conference report, etc.) can yield up to 10% bonus

All presentations

- Well structured
  - Slides (projector care – Pavel Tucek; laptop care is upon your mutual agreement!)
  - Agreed length respected (practice beforehand!)
- Time allowance is 30-35 minutes for O
  - 20-25 minutes for R and N
- ***Book your dates with me by Feb 25, noon!!!***

“O” Talk Dates

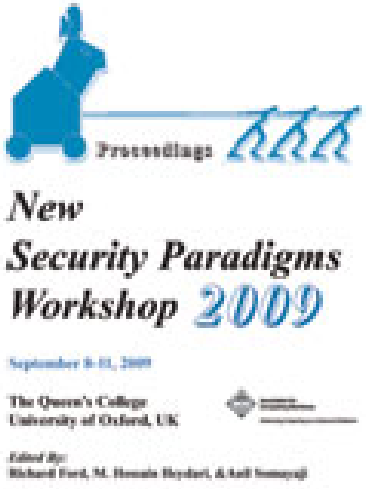
- Mar 1 –
- Mar 8 –
- Mar 15 – Zbynek Ondrak, Jiří Vomáčka
- Mar 22 – Shkodran Gerguri
- Mar 29 – Andriy Stetsko
- Apr 5 – *Easter*
- Apr 12 – Richard Barányi, Tobias Smolka
- Apr 19 – Rastislav Rusinko, Pavel Tuček
- Apr 26 – Jakub Breier, Juraj Ďaďo
- May 3 – Luboš Ptáček
- May 10 – Jirka Kur
- May 17 – Michal Růžička

“N” Talk Dates

- Mar 1 – Pavel Tucek
- Mar 8 – Andriy Stetsko
- Mar 15 – Jiří Vomáčka
- Mar 22 – Richard Barányi
- Mar 29 – Jirka Kur
- Apr 5 – *Easter*
- Apr 12 – Jakub Breier
- Apr 19 – Luboš Ptáček
- Apr 26 – Zbynek Ondrak
- May 3 – Juraj Ďaďo, bonus talk Tobias Smolka
- May 10 – Michal Růžička
- May 17 – Rastislav Rusinko

(R)eadings – choice for this term…

- Any paper from the Proceedings of the 2009 New security paradigms workshop
  - Oxford, United Kingdom, September 8-11, 2009
  - All papers available in the ACM Digital Library
    - Link in the IS



“R” Talk Dates

- Mar 1 – Vasek Lorenc
- Mar 8 – Pavel Tuček,
  - Tobias Smolka – Fluid information systems
- Mar 15 – Jirka Kur – So long, and no thanks for the extern…
- Mar 22 – Juraj Ďaďo
- Mar 29 – Richard Barányi – Server-Side Detection of Malware
- Apr 5 – *Easter*
- Apr 12 – Luboš Ptáček – Musipass: authenticating me softly…
- Apr 19 – Jakub Breier
- Apr 26 – Rastislav Rusinko
- May 3 – Michal Růžička – Generative usability: security and…
- May 10 – Jiří Vomáčka
- May 17 – Zbynek Ondrak – Securing data through avoidance…