

# PA168 – Postgraduate seminar on IT security and cryptography

Vašek Matyáš & Jan Staudek

Email: [matyas@fi.muni.cz](mailto:matyas@fi.muni.cz)

Office hours: Mon, Tue, Thu 12:22-13:33 (B415)

# All presentations

- Well structured
  - Slides (projector care – Honza Krhovjak)
  - Agreed length respected (practice beforehand!)
- Time allowance is 30-35 minutes for O, R
  - 20-40 minutes for N 😊
- ***Book your dates with me by March 9!!!***

# “O” Talk Dates

- March 5 – ?
- March 12 – guest talk of Martin Drahansky
- March 19 – none (2 R talks)
- March 26 – Petr Svenda
- April 2 – Marek Kumpost
- April 9 – Easter Monday – no class
- April 16 – Vasek Lorenc
- April 23 –
- April 30 –
- May 7 –
- May 14 –

# “R” Talk Dates

- Today – Vasek Lorenc – A Comparison of Commercial and Military Computer Security Policies (Clark & Wilson)
- March 5 – Petr Svenda – The Economics of Information Security: A Survey and Open Questions (Anderson, Moore)
- March 12 – ??? – Privacy Preserving Multi-Factor Authentication with Biometrics (ACM DIM 2006)
- March 19 – ??? – Towards an Open, Trusted Digital Rights Management Platform (ACM DRM 2006)
- March 19 – ??? – Towards a Secure and Interoperable DRM Architecture (ACM DRM 2006)
- April 2 – ??? – Search Worms (ACM WORM 2006, Niels Provos et al.)
- April 9 – Easter Monday – no class
- April 16 –
- April 23 –
- April 30 –
- May 7 –
- May 14 –

# “N” Talk Dates

- Today – Vasek Lorenc
- March 12 – Petr Svenda
- March 19 –
- March 26 –
- April 2 –
- April 9 – Easter Monday – no class
- April 16 –
- April 23 –
- April 30 –
- May 7 –
- May 14 –