

PA168 – Postgraduate seminar on IT security and cryptography

Vašek Matyáš & Jan Staudek

Email: 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 😊
- ***All dates set...*** 😊

“O” Talk Dates

- Today – ? guest talk of Martin Drahanaky
- March 19 – none (2 R talks)
- March 26 – Petr Svenda
- April 2 – Marek Kumpost
- April 9 – Easter Monday – no class
- April 16 – Vasek Lorenc & Petr Sveda
- April 23 – Ondrej Vyborny & Honza Krhovjak
- April 30 – Ondrej Bitto & Andriy Stetsko

“R” Talk Dates

- Today – Honza Krhovjak – Privacy Preserving Multi-Factor Authentication with Biometrics (ACM DIM 2006)
- March 19 – Andriy Stetsko – Towards an Open, Trusted Digital Rights Management Platform (ACM DRM 2006)
- March 19 – Ondrej Vyborny – Towards a Secure and Interoperable DRM Architecture (ACM DRM 2006)
- April 2 – Ondrej Bitto – Search Worms (ACM WORM 2006)
- April 23 – Petr Sveda – The unbearable lightness of PIN cracking (Berkman & Ostrovsky)

“N” Talk Dates

- Today – Petr Svenda
- March 19 – Ondrej Bitto
- March 26 –
- April 2 – Ondrej Vyborny
- April 9 – Easter Monday – no class
- April 16 – Andriy Stetsko
- April 23 –
- April 30 – Petr Sveda