

PA168 – Postgraduate seminar on IT security and cryptography

Vašek Matyáš & Jan Staudek

Email: matyas@fi.muni.cz

Office hours: Mon & Tue 3:05-3:55pm (B415)

Typical seminar structure

- About 2 presentations for the start
- Discussion related to above
- News/developments update
 - Recent news
 - Crypto-Gram (B. Schneier),
 - comp.risk,
 - www.buslab.cz,
 - <http://swordfish.buslab.org/>
 - <http://www.lightbluetouchpaper.org/>
 - New results/achievements (no attack stats!)
 - 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.
- R (Reading)
 - Presentation of a recent paper
 - Papers proposed during the term
 - Detailed review of the paper with discussion
- N (News)
 - Presentation of news from the last week (or so)

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 & R presentations 40% each, N presentation 20%
 - P for 75% or more
- Other activities (conference report, etc.) can yield up to 10% bonus

All presentations

- Well structured
 - Slides (projector care – Vasek Lorenc)
 - Agreed length respected (practice beforehand!)
- Time allowance is 30-35 minutes for O, R
 - 15-25 minutes for N 😊
- ***Book your dates with me by September 29, noon!!!***

“O” Talk Dates

- Today – Vasek Lorenc
 - Honza Samek: Using Multiple-Context Trust Model in Wireless Sensor Networks
- Oct 12 – Shkodran Gerguri: Biometric RNG
- Oct 19 – Martin Drašar
- Oct 26 – Roman Zilka
 - Tomáš Pyszko: Implementation of OpenVPN with crypto tokens
- Nov 2 – Karol Kubanda
- Nov 9 – Jiri Kur
- Nov 16 – *before national holidays?*
- Nov 23 – Lukáš Folkman
- Nov 30 – Pavel Tucek
- Dec 7 – Vit Bukac
 - Peter Puskar
- Dec 14 – Jakub Dobrovolny
 - Pavel Piskac

(R)eadings – choice for this term...

- Almost any paper from the 18th USENIX Security Symposium
 - August 10–14, Montreal, Canada
 - All papers (and video or audio!) available at <http://www.usenix.org/events/sec09/tech/>



“R” Talk Dates

- Today – Jirka Kur: Security Engineering (book)
- Oct 12 – Andriy Stetsko: ENISA report "ATM Crime..."
 - Roman Zilka: Protecting Confidential Data on Personal...
- Oct 19 – Pavel Tucek: Compromising Electromagnetic...
- Oct 26 – Lukáš Folkman: xBook: Redesigning Privacy Con...
- Nov 2 – Pavel Piskac: Compression, Correction, Confid...
- Nov 9 – Vit Bukac: Crying Wolf: An Empirical Study of SSL...
 - Shkodran Gerguri: CCCP: Secure Remote Storage...
- Nov 16 – *before national holidays?*
- Nov 23 – Jakub Dobrovolny: Vanish: Increasing Data Priv...
 - Peter Puskar: VPriv: Protecting Privacy in Location-Bas...
- Nov 30 – Martin Drašar:
- Dec 7 – Karol Kubanda
- Dec 14 – Tomáš Pyszko: Improving Tor using a TCP...

“N” Talk Dates

- Oct 5 – Roman Zilka
- Oct 12 – Pavel Piskac
- Oct 19 – Vit Bukac
- Oct 26 – Jakub Dobrovolny
- Nov 2 – Jiri Kur
- Nov 9 – Shkodran Gerguri
- Nov 16 – *before national holidays?*
- Nov 23 – Karol Kubanda
- Nov 30 – Peter Puskar
- Dec 7 – Pavel Tucek
- Dec 14 – Lukáš Folkman