

PA168 – Postgraduate seminar on IT security and cryptography

Vašek Matyáš & Jan Staudek

Email: matyas@fi.muni.cz

Office hours: Mon 15:00-55 & Tue 9:00-9:55 (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)
 - This talk can be replaced by your service as a seminar chair/moderator (recommended to PhD students!)
- R (Reading)
 - Presentation of a recent paper
 - Papers proposed during the term
 - Detailed review of the paper with discussion

Marking & Language

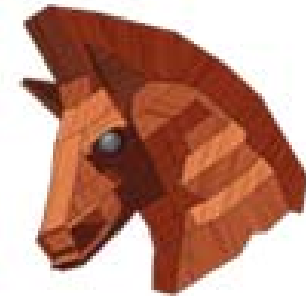
- The course primary language is English!!!
 - In Czech only when the ultimate target for your presentation requires this
 - M.Sc. thesis presentation
 - Czech conference presentation
- Mark comprises:
 - O presentation 40%
 - R & N presentation 30% each
 - Resulting P(ass) for 75% or more
- Other activities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

All presentations

- Well structured
 - Slides (projector care – Jirka Kur; 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 Vashek Matyas by Oct 1, noon!!! (e-mail)***

(R)eadings – choice for this term...

- Any paper from the Proceedings 2010 IEEE Symposium on Security and Privacy
 - Berkeley, California, USA
 - May 16-19, 2010
 - ISBN: 978-0-7695-4035-1
 - All papers available in the IEEE Computer Society Digital Library



“O” Talk Dates

- Oct 11 – Jan Michelfeit
 - Tomas Vymetal
- Oct 18 – Michal Trunecka
- Oct 25 – Shkodran Gerguri
 - Ladislav Tkac
- Nov 1 – Antonín Víteček
 - Lukas Jakubik
- Nov 8 – Jirka Kur
 - Martin Stehlik
- Nov 15 – Jiří Vomáčka
 - Richard Barányi
- Nov 22 – Tobias Smolka
- Nov 29 – Stefan Koepsell (guest)
 - Vita Bukac
- Dec 6 – Miroslav Buda – Australian Internet censorship system
- Dec 13 – Marián Novotný (guest): Design and analysis of a data integrity protocol for Wireless Sensor Networks

“N” Talk Dates

- Oct 11 –
 - Moderator – Tobias Smolka
- Oct 18 – Jiří Vomáčka
 - Moderator – Andriy Stetsko
- Oct 25 – Miroslav Buda
 - Pavel Tucek
- Nov 1 – Michal Trunecka
- Nov 8 – Jan Michelfeit
- Nov 15 – Vita Bukac
- Nov 22 – Lukas Jakubik
- Nov 29 – Martin Stehlik
- Dec 6 – Ladislav Tkac
- Dec 13 – Tomas Vymetal

“R” Talk Dates

- Oct 11 – Vita Bukac
- Oct 18 – Jirka Kur – A Practical Attack to De-Anonymize Soc...
 - Pavel Tucek – The password thicket:...
- Oct 25 – Tobias Smolka - Inspector Gadget: Automated Extr...
- Nov 1 – Jiří Vomáčka – Side-Channel Leaks in Web Apps...
- Nov 8 – Miroslav Buda – How Good Are Humans at Solving...
- Nov 15 – Michal Trunecka – Outside the Closed World: On...
- Nov 22 – Antonín Víteček –
 - Martin Stehlik
- Nov 29 – Jan Michelfeit – SCiFI - A System for Secure Face...
- Dec 6 – Lukas Jakubik – Overcoming an Untrusted Comp...
 - Tomas Vymetal
- Dec 13 – Richard Barányi – Identifying Dormant Functionality..