PA168 – Postgraduate seminar on IT security and cryptography

Vašek Matyáš & Jan Staudek &
Zdeněk Říha & Petr Švenda

Email: matyas@fi.muni.cz

Typical seminar structure

- 3 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!
  - Agreed length respected (practice beforehand!)
- Time allowance is 25-35 minutes for O
  - 20-25 minutes for R and N
- ***Book your dates with Vashek Matyas by Mar 2, noon!!! (e-mail)***

“O” Talk Dates

- Mar 6 – Andriy Stetsko
- Mar 13 –
- Mar 20 – Jiri Kur
- Mar 27 – Tobias Smolka
- Apr 3 – Martin Stehlik
  - Bogdan Iakym
- Apr 10 – Adam Saleh
  - Jaromir Dobias
- Apr 17 – Matej Pristak
- Apr 24 – Stefan Miklosovic
  - Radek Janáček
- May 1 & 8 – National holidays
- May 15 – Martin Kvocka
  - Ondrej Kretek

“N” Talk Dates

- Mar 6 – Matej Pristak
- Mar 13 – Adam Saleh
  - Moderated by Filip Jurnecka
- Mar 20 –
  - Moderated by Martin Stehlik
- Mar 27 – Stefan Miklosovic
  - Moderated by Andriy Stetsko
- Apr 3 –
  - Moderated by Jiri Kur
- Apr 10 – Bogdan Iakym
  - Moderated by Vita Bukac
- Apr 17 – Martin Kvocka
  - Moderated by Jarda Dobias
- Apr 24 – Ondrej Kretek
- May 1 & 8 – National holidays
- May 15 – Radek Janáček

(R)eadings – choice for this term…

- Any paper from the 20th USENIX Security Symposium (2011)
  - All papers available from the Usenix web
    - Link in the IS

“R” Talk Dates

- Mar 6 – Adam Saleh: TRESOR Runs Encryption Securely…
- Mar 13 – Tobias Smolka: Q: Exploit Hardening Made Easy
- Mar 20 – Filip Jurnečka: Fast and Precise Sanitizer Analysis…
  - Radek Janáček: A Study of Android Application Security
- Mar 27 – Vita Bukac: Detecting Malware Domains at the…
  - Jaromir Dobias: OZZLE: Fast and Precise In-Browser…
- Apr 3 – Andriy Stetsko: Measuring Pay-per-Install…
- Apr 10 – Stefan Miklosovic: Dark Clouds on the Horizon…
- Apr 17 – Matej Pristak: SMS of Death: From Analyzing to…
  - Ondrej Kretek: Secure In-Band Wireless Pairing
- Apr 24 – Martin Kvocka: Enabling Fast Detection and Forensic
- May 1 & 8 – National holidays
- May 15 – Bogdan Iakym: Dirty Jobs: The Role of Freelance…