PA168 – Postgraduate seminar on IT security and cryptography

Vašek Matyáš & Jan Staudek

Email: matyas@fi.muni.cz

Office hours: Mon 3:00-3:55pm & Tue 1:00-1:55pm (B415)

Typical seminar structure

- 1-2 presentations for the start
- Discussion related to above
- News/developments update
  - Recent news
    - Crypto-Gram (B. Schneier), comp.risk,
    - http://www.lightbluetouchpaper.org/
    - www.buslab.cz,
      - http://swordfish.buslab.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 – Honza & Marek)
  - – Agreed length respected (practice beforehand!)
- Time allowance is 30-40 minutes for O, R
  - – 15-25 minutes for N ☺
- ***Book your dates with me by March 2, noon!!!***

“O” Talk Dates

- Mar 9 – Petr Svenda
- Mar 16 – none, two R talks
- Mar 23 – Tomáš Homola
- Mar 30 – Andriy Stetsko
- Apr 6 – Jaromir Dobias
- Apr 13 – *Easter*
- Apr 20 – Martin Drašar
- Apr 27 – Lumir Honus
- May 4 – Roman Zilka
  - Martin Henzl
- May 11 – Lukáš Folkman
  - Dušan Halabica

(R)eadings – choice for this term…

- Any paper from the 2008 (15th) ACM Conference on Computer and Communications Security
  - October 27-31, 2008, Alexandria, Virginia, USA
  - All papers available in the ACM Digital Library
    - Link in the IS

“R” Talk Dates

- Mar 9 – Tomáš Homola – Constructions of truly practical…
- Mar 16 – Roman Zilka – Rootkit-Resistant Disks
  – Martin Henzl – ???
- Mar 23 – Martin Drašar – Information leaks in structured…
- Mar 30 – Lumir Honus – RFIDs and secret handshakes…
- Apr 6 – Dusan Halabica – A Low-cost Attack on M. CAPTCHA
- Apr 13 – *Easter*
- Apr 20 – Jaromir Dobias – OMash: Enabling Secure Web…
- Apr 27 – Lukáš Folkman – Identity-based encryption…
- May 4 – none, two O talks
- May 11 – none, two O talks

“N” Talk Dates

- Mar 9 – Dusan Halabica
- Mar 16 –
- Mar 23 – Lukáš Folkman
- Mar 30 – Roman Zilka
- Apr 6 – Tomáš Homola
- Apr 13 – *Easter*
- Apr 20 – Lumir Honus
- Apr 27 – Vasek Lorenc
- May 4 – Martin Drašar
- May 11 – Martin Henzl