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,
    - 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 – Honza & Marek)
  - Agreed length respected (practice beforehand!)
- Time allowance is 30-40 minutes for O, R
  - 15-25 minutes for N ☺
- ***Book your R-talk topics with me by October 13, noon!!!***

(R)eadings – choice for this term…

- Almost any paper from the 2008 IEEE Symposium on Security and Privacy
  - May 18-21, 2008, Oakland, California, USA
  - All papers available in the IEEE Computer Society Digital Library
    - Link in the IS

“R” Talk Dates

- Oct 6 – Andriy Stetsko: SybilLimit: A Near-Optimal Social…
  - Ludek Svoboda: A Language for Enforcing User-…
- Oct 13 – Jiri Zizkovsky: Civitas: Toward a Secure Voting…
  - Jan Krhovjak: Thinking Inside the Box: System-level
- Oct 20 – Jirka Kur: Secure Web Browsing with the OP Web...
- Nov 3 – Ondrej Malek: Compromising Reflections – How to…
  - Honza Vykopal: Casting out Demons: Sanitizing…
- Nov 10 – Roman Zilka: Defeating Encrypted and Deniable…
  - Khalid Ibrahim Al Khatib:
- Nov 24 – Richard Benkovský: Anonymous Networking with…
- Dec 1 – Jaromir Dobias
- Dec 8 – Martin Synak: Pacemakers and Implantable Cardiac
- Dec 15 – Marek Kumpost: Robust De-anonymization of Large
  - Marek Hulan

“O” Talk Dates

- Oct 6 – Josef Sprojcar
- Oct 13 – Honza Vykopal
  – Vasek Lorenc
- Oct 20 – Marek Hulan
  – Jaromir Dobias
- Nov 3 – Jan Krhovjak
- Nov 10 – Jirka Kur
  – Khalid Ibrahim Al Khatib
- Nov 24 – Andriy Stetsko
  – Ludek Svoboda
- Dec 1 – Roman Zilka
  – Martin Synak
- Dec 8 – Richard Benkovský
  – Ondrej Malek
- Dec 15 – Jiri Zizkovsky

“N” Talk Dates

- Oct 6 – Ondrej Malek
- Oct 13 – Jirka Kur
- Oct 20 – Jiri Zizkovsky
  - Ludek Svoboda – short reading talk
- Nov 3 – Roman Zilka
- Nov 10 – Richard Benkovský
- Nov 17 – *national holidays*
- Nov 24 – Jaromir Dobias
- Dec 1 – Honza Vykopal
- Dec 8 – Marek Hulan
- Dec 15 – Martin Synak
  - Khalid Ibrahim Al Khatib – short reading talk