PA168 – Postgraduate seminar on IT security and cryptography

Vašek Matyáš & Jan Staudek

Email: matyas@fi.muni.cz

Office hours: Mon, Tue, Thu 9:00-9:55 (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

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 – myself)
  - 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 October 1, noon!!!***

Datakon 2007

- Kind offer of organizers (Jan Staudek)
- Attending the Sun morning tutorial on ISO 2700x standards (9-12am)
- Attending the Mon afternoon session on security (partly) and evening security panel, dinner included (3:30-9:30am)

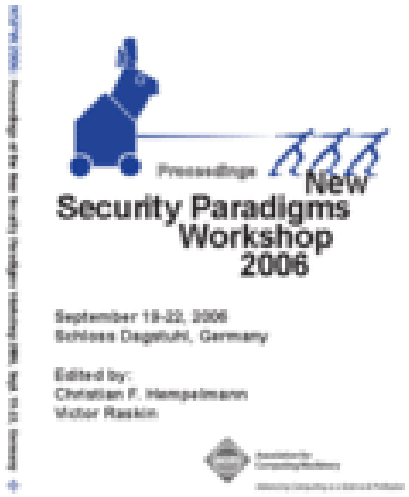
- If interested, mailto:staudek@fi.muni.cz and specify which day(s) you wish to come

“O” Talk Dates

- Sep 24 – Marek Kumpost
- Oct 1 – Petr Svenda
- Oct 8 – Kamil Malinka
- Oct 15 – guest talk of Ludek Novak
- Oct 22 – *Datakon*
- Oct 29 – Geraint Price: Client puzzle attacks
- Nov 5 –
- Nov 12 –
- Nov 19 – Jiri Zizkovsky – Impl. PRNG on Symbian
- Nov 26 –
- Dec 3 – Jakub Ferenc
- Dec 10 – Hana Kleinova
- Dec 17 – Jirka Kur

(R)eadings – choice for this term…

- Almost any paper from the New Security Paradigms Workshop 2006
  - Not the Bond & Danezis paper (read last term)
  - Proceedings of the 2006 workshop on New security paradigms, Germany, *Sep 19 - 22, 2006*
  - ACM Digital Library



“R” Talk Dates

- Sep 24 –
- Oct 1 –
- Oct 8 – Jiri Zizkovsky – *Googling Considered Harmful*
- Oct 15 – guest talk of Ludek Novak
- Oct 22 – *Datakon* ?Hana Kleinova
- Oct 29 – guest talk of Geraint Price
- Nov 5 – Kamil Malinka
- Nov 12 – ?Hana Kleinova / ?Marek Kumpost
- Nov 19 – Jakub Ferenc – *Cent, five cent, ten cent, dollar…*
- Nov 26 –
- Dec 3 –
- Dec 10 – Jirka Kur
- Dec 17 –

“N” Talk Dates

- Sep 24 –
- Oct 1 –
- Oct 8 –
- Oct 15 –
- Oct 22 – *Datakon*
- Oct 29 – Kamil Malinka
- Nov 5 – Hana Kleinova
- Nov 12 – Marek Kumpost
- Nov 19 –
- Nov 26 – Jiri Zizkovsky
- Dec 3 – Jirka Kur
- Dec 10 – Jakub Ferenc
- Dec 17 –