PA168 – Postgraduate seminar on IT security and cryptography

Vašek Matyáš & Jan Staudek

Email: matyas@fi.muni.cz
Office hours: Mon 15:05-55 & Tue 9:05-55 (B415)

Typical seminar structure

- 2-3 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
    - Detailed review of the paper with discussion (might involve reading some of the related/referenced work!)

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 (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 me by Feb 28, noon!!!***

“O” Talk Dates

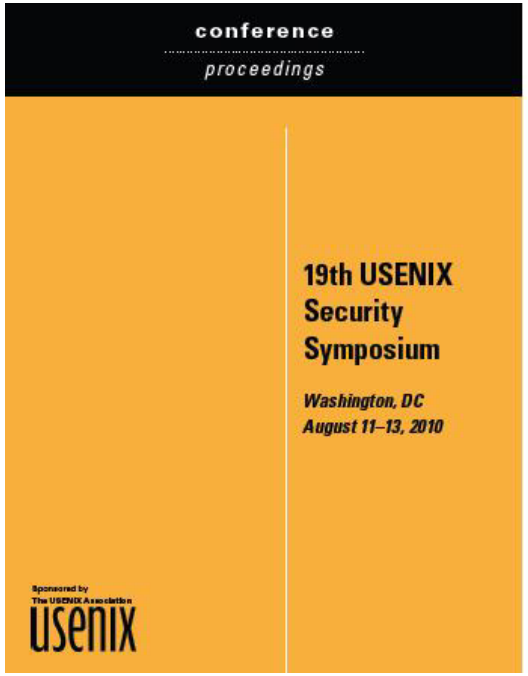
- Mar 7 – Tomas Vymetal
- Mar 14 – Maroš Barabas
- Mar 21 – Andriy Stetsko (& Jirka Kur)
- Mar 28 – Filip Jurnecka
- Apr 4 – Martin Malina
- Apr 11 – Tobias Smolka, Pavel Tucek
- Apr 18 – Vít Bukač, Roman Zilka
- Apr 25 – *Easter*
- May 2 – Richard Baranyi, Martin Tehan
- May 9 – Martin Stehlik, Alexandr Kuckir
- May 16 – Marek Čermák, Richard Nossek

“N” Talk Dates

- Mar 7 – Peter Jurnečka
- Mar 14 – Tobias Smolka
  - Moderated by Jiri Kur
- Mar 21 – Richard Baranyi
  - Moderated by Filip Jurnecka
- Mar 28 – Martin Stehlik
  - Moderated by Andriy Stetsko
- Apr 4 – Vít Bukač
  - Moderated by Tomas Vymetal
- Apr 11 – Richard Nossek
  - Moderated by Roman Zilka
- Apr 18 – Marek Čermák
  - Moderated by Pavel Tucek
- Apr 25 – *Easter*
- May 2 – Alexandr Kuckir
- May 9 – Martin Tehan
- May 16 – Martin Malina

(R)eadings – choice for this term…

- Any paper from the USENIX Security '10 Symposium
  - Washington, DC, August 11-13, 2010
  - All papers available from the Usenix web
    - Link in the IS



“R” Talk Dates

- Presented - Toward Automated Detection…
- Mar 7 – Richard Baranyi: An Analysis of Private Browsing…
- Mar 14 – Martin Henzl
  - Pavel Tucek: The case for ubiquitous transport-level…
- Mar 21 – Martin Malina: Understanding CAPTCHA-Solving…
  - Tomáš Vymětal: Searching the Searchers with SearchAudit
- Mar 28 – Vít Bukač: Idle Port Scanning and Non-interference..
  - Peter Jurnečka
- Apr 4 – Martin Stehlik: Building a Dynamic Reputation...
  - Roman Zilka: Making Linux Protection Mechanisms Egal…
- Apr 11 – Andriy Stetsko: Dude, Where's That IP? Circumv…
- Apr 18 – Jiri Kur: Security and Privacy Vulnerabilities of…
- Martin Tehan: Baaz: A System for Detecting Access…
- Apr 25 – *Easter*
- May 2 – Marek Čermák: BotGrep: Finding P2P Bots with…
- May 9 – Richard Nossek: Securing Script-Based Extensibility..
- May 16 – Alexandr Kuckir: Acoustic Side-Channel Attacks…