Mikulášská kryptobesídka / SantaCrypt 2010

http://mkb.buslab.org/

Pořádá TNS, a.s., a BUSLab za podpory / Organized by TNS, a.s. and BUSLab with support of

Program

2. prosince 2010 (čtvrtek) / December 2, 2010 (Thursday)

8:45 –	*Registrace / Registration*
9:30 – 9:40	*Zahájení workshopu / Workshop opening*
9:40 – 10:40	*Keynote* Danilo Gligoroski – Why narrow-pipe cryptographic hash functions are not a match to wide-pipe cryptographic hash functions?
10:40 – 11:40	*Keynote* Paul Leyland – Experiences with GPUs for Cryptography
11:40 – 12:25	Michal Rjaško, Martin Stanek – On Designated Verifier Signature Schemes
12:30 – 13:30	*Oběd / Lunch*
13:30 – 14:30	*Keynote* Dan Cvrček – Thoughts On Cryptography in Banking
14:30 – 15:00	*KEYMAKER I* Kamil Malinka – Evaluation of Flash VEP Usability as Behavioural Characteristics for Biometric Authentication
15:00 – 15:30	*Přestávka na kávu a čaj / Coffee & tea break*
15:30 – 17:00	*KEYMAKER II* Bedřich Hovorka – Search for S-boxes with evolutionary computing Peter Vagánek – Alternative elliptic curves for cryptography Tobiáš Smolka – Strengthening applications by automatic transformations
17:00 – 17:25	*Rump session*
17:30 –	*Večeře / Dinner*

Následují neformální diskuze v prostorách vyhrazených pouze pro účastníky kryptobesídky. / Followed by informal discussions in the hall available only to the workshop participants.

Mikulášská kryptobesídka / SantaCrypt 2010

http://mkb.buslab.org/

Pořádá TNS, a.s., a BUSLab za podpory / Organized by TNS, a.s. and BUSLab with support of

3. prosince 2010 (pátek) / December 3, 2010 (Friday)

8:55 – 9:00 *Zahájení druhého dne workshopu / Opening of the second day of the workshop*

9:00 – 10:00 *Keynote*
Tomáš Rosa – Unleashing EMV Cards for Security Research

10:00 – 10:30 *Přestávka na kávu a čaj / Coffee & tea break*

10:30 – 11:30 *Keynote*
Petr Hanáček, Petr Švenda – Cryptography for Resource-limited Network Nodes

11:30 – 12:10 *KEYMAKER III*
Eugen Antal – Porovnanie rotorových šifrátorov Enigma a Fialka M-125
Juraj Varga, Eugen Antal – Zodiac

12:11 – *Mikuláš / Santa*

Závěr workshopu... / Workshop ends...