Mikulášská kryptobesídka / SantaCrypt 2012

http://mkb.buslab.org/

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

Program

29. listopadu 2012 (čtvrtek) / November 29, 2012 (Thursday)

8:45 –	*Registrace / Registration*
9:30 – 9:40	*Zahájení workshopu / Workshop opening*
9:40 – 10:40	*Keynote* Michal Šrámka – Achieving Privacy of Shared Information: Crypto & Beyond
10:40 – 11:40	*Keynote* Andreas Uhl – Watermarking in Biometrics
11:40 – 12:10	Martin Stanek – Attacking Scrambled Burrows-Wheeler Transform
12:15 – 13:45	*Oběd / Lunch*
13:45 – 14:45	*Keynote* Klaus Schmeh – Cracking Enigma Messages from WW2
14:45 – 15:15	*KEYMAKER I* Jiří Kůr – Two Improvements of Random Key Predistribution for Wireless Sensor Networks
15:15 – 15:45	*Přestávka na kávu a čaj / Coffee & tea break*
15:45 – 16:45	*KEYMAKER II* Marcel Šebek – Deniable Encryption Ondřej Koutský – On power analysis of RSA smartcard implementations Milan Boháček – On security analysis of the Skype VOIP software
16:45 – 17:22	*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 2012
http://mkb.buslab.org/

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

30. listopadu 2012 (pátek) / November 30, 2012 (Friday)

8:55 – 9:00	*Zahájení druhého dne workshopu / Opening of the second day of the workshop*
9:00 – 10:00	*Keynote* Vlastimil Klíma – SHA-3 a lehká kryptografie
10:00 – 10:20	*KEYMAKER III* Veronika Půlpánová – SymPC
10:20 – 10:50	*Přestávka na kávu a čaj / Coffee & tea break*
10:50 – 11:50	*Keynote* David Naccache & Zdeněk Říha – Statistical Speedups for Biometric Identification
11:55 –	*Mikuláš / Santa*

Závěr workshopu... / Workshop ends...