Mikulášská kryptobesídka / SantaCrypt 2013

http://mkb.tns.cz/

Pořádá TNS, a.s., a CROCS MU / Organized by TNS, a.s. and CROCS MU

Program

28. listopadu 2013 (čtvrtek) / November 28, 2013 (Thursday)

8:45 –	*Registrace / Registration*
9:25 – 9:30	*Zahájení workshopu / Workshop opening*
9:30 – 10:20	*Keynote* David Naccache: Using Hamiltonian Totems as Passwords
10:20 – 11:10	*Keynote* Riccardo Foccardi: Practical Padding Oracle Attacks on RSA
11:10 – 12:00	Dan Cvrček: How to Forget Passwords
12:00 – 13:00	*Oběd / Lunch*
13:00 – 13:50	*Keynote* Flaminia Luccio: Cracking bank PINs by playing a Mastermind Game
13:50 – 14:35	*KEYMAKER I* Lukáš Pohanka: Serpent optimization for ARM processors Tomáš Dragoun: Covert channels in IPv6 Dušan Klinec: Whitebox attack resistant cryptography
14:35 – 15:05	*Přestávka na kávu a čaj / Coffee & tea break*
15:05 – 15:35	*KEYMAKER II* Martin Ukrop: The Evolution of Randomness Testing Jiří Kůr: An adaptive security architecture for location privacy sensitive…
15:35 – 16:25	Michal Rjaško: Compression function reducibility
16:25 – 16:55	*Rump session*
17:00 –	*Večeře / Dinner*

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

Mikulášská kryptobesídka / SantaCrypt 2013

http://mkb.tns.cz/

Pořádá TNS, a.s., a CROCS MU / Organized by TNS, a.s. and CROCS MU

29. listopadu 2013 (pátek) / November 29, 2013 (Friday)

8:55 – 9:00	*Zahájení druhého dne workshopu / Opening of the second day of the workshop*
9:00 – 9:50	Luděk Smolík: Je jen jedno správné vnímání kvantové kryptografie?
9:50 – 10:20	Richard Ostertág: Entropy Assessment of Windows OS Performance Counters
10:20 – 10:50	*Přestávka na kávu a čaj / Coffee & tea break*
10:50 – 11:20	*KEYMAKER III* Filip Machovec: Adaptívna steganografia a metóda ABCDE Karel Koranda: Hardwarová akcelerace AES-GCM pro protokol SSH
11:20 – 12:10	*Keynote* Tomáš Rosa: Bit Commitment Adventures in Wi-Fi and Bluetooth
12:11 –	*Mikuláš / Santa*

Závěr workshopu... / Workshop ends...