Mikulášská kryptobesídka / SantaCrypt 2017

http://mkb.tns.cz/

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

Programme

30. listopadu 2017 (čtvrtek) / November 30, 2017 (Thursday)

9:00 –	*Registrace / Registration*
9:25 – 9:30	*Zahájení workshopu / Workshop opening*
9:30 – 10:30	*Keynote* Mike Just: Secure and usable authentication
10:30 – 12:00	*KEYMAKER I* Martin Ukrop: Why Johnny the Developer Can't Work with Public Key Certificates: An Experimental Study of OpenSSL Usability Peter Spacek: McEliece Engine for TLS Handshake Adolf Středa: Attacking Zero Added Equations (Hidden Field Equations)
12:00 – 13:15	*Oběd / Lunch*
13:15 – 14:15	*Keynote* Timo Kasper: Security Nightmares in the Internet of Things: Electronic Locks and More
14:15 – 14:45	*KEYMAKER II* Valdemar Švábenský: Challenges Arising from Prerequisite Testing in Cybersecurity Games
14:45 – 15:15	*Přestávka na kávu a čaj / Coffee & tea break*
15:15 – 16:15	*Keynote* Juraj Somorovsky: Systematic Fuzzing and Testing of TLS Libraries
16:15 – 17:00	Matúš Nemec: Looking at RSA Public Keys from Close and Far Distances
17:00 – 17:22	*Rump session*
17:30 –	*Večeře / Dinner*

Mikulášská kryptobesídka / SantaCrypt 2017

http://mkb.tns.cz/

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

1. prosince 2017 (pátek) / December 1, 2017 (Friday)

9:00 – 9:05	*Zahájení druhého dne workshopu / Opening of the second day of the workshop*
9:05 – 10:05	*Keynote* Pavel Vondruška: eIDAS a hodnocení služeb důvěry
10:05 – 10:35	*Přestávka na kávu a čaj / Coffee & tea break*
10:35 – 11:25	David Smékal: Vysokorychlostní šifrování se silnou autentizací na platformě FPGA
11:25 – 11:55	*KEYMAKER III* Martin Eliáš: Lúštenie historických šifier na GRIDe pomocou GA a PGA Martin Očenáš: Analyzujeme Bitcoin blockchain
11:55 –	*Mikuláš / Santa*

Závěr workshopu... / Workshop ends...