Mikulášská kryptobesídka / SantaCrypt 2018

http://mkb.tns.cz/

Pořádá TNS, a.s., a CROCS FI MU za podpory / Organized by TNS, a.s. and CROCS FI MU with support of

Programme

29. listopadu 2018 (čtvrtek) / November 29, 2018 (Thursday)

9:00 –	*Registrace / Registration*
9:25 – 9:30	*Zahájení workshopu / Workshop opening*
9:30 – 10:30	*Keynote* Jan Camenisch: Modular cryptographic protocol design
10:30 – 12:00	*KEYMAKER I* Ján Jančár: Security of Elliptic Curves: domain parameters & Implementations Jakub Klemsa: VeraGreg – A Framework for Verifiable Privacy-Preserving Data Aggregation Miloslav Homer: A Chosen Plaintext Attack on Offset Public Permutation Mode
12:00 – 13:30	*Oběd / Lunch*
13:30 – 14:30	*Keynote* Pascal Paillier: Homomorphic encryption for deep learning: a revolution in the making
14:30 – 15:00	*Přestávka na kávu a čaj / Coffee & tea break*
15:00 – 16:00	*Keynote* Werner Schindler: Security evaluation of physical RNGs
16:00 – 16:30	*KEYMAKER II* Adam Janovský: Bringing kleptography to real-world TLS
16:30 – 17:15	*Rump session*
17:15 –	*Večeře / Dinner*

Mikulášská kryptobesídka / SantaCrypt 2018

http://mkb.tns.cz/

Pořádá TNS, a.s., a CROCS FI MU za podpory / Organized by TNS, a.s. and CROCS FI MU with support of

30. listopadu 2018 (pátek) / November 30, 2018 (Friday)

9:00 – 9:05	*Zahájení druhého dne workshopu / Opening of the second day of the workshop*
9:05 – 10:05	*Keynote* Tomáš Rosa: 101 RF Hacking with SDR - From Beautiful Equations to Real Threats
10:05 – 10:35	*Přestávka na kávu a čaj / Coffee & tea break*
10:35 – 11:35	*Keynote* Otokar Grošek: O histórii ruských šifier od Cyrila a Metoda až 2. sv. v.
11:35 – 12:15	*KEYMAKER III* Tomas Hliboky: Meta-heuristiky a ohodnocovanie textu pri lúštení transpozičných šifier Tomáš Gerlich: Analýza filtračních schopností linuxových nástrojů
12:15 –	*Mikuláš / Santa*

Závěr workshopu... / Workshop ends...