Mikulášská kryptobesídka 2004

http://www.tns.cz/kryptobesidka

Mikulášská kryptobesídka – workshop o kryptografii a příbuzných oborech se letos koná počtvrté. Programový výbor už vybral příspěvky, které budou letošní rok prezentovány a stanovené je i téma panelové diskuse. Pokud máte zájem se tento rok zúčastnit, je třeba se zaregistrovat. S platbou do 12. listopadu je možné využít levnější registrační poplatek – podrobné informace naleznete na našich www stránkách.

Mikulášskou kryptobesídku pořádá TNS, a.s., za podpory

RSA SECURITY Confidence Inspired™ — Confidence inspired

ICZ — Vaše jistota na trhu IT

GiTy LOOK LISTEN & COMMUNICATE — Look, Listen & Communicate

Předběžný program

6. prosince 2004 (pondělí)

14:30 - 15:30	*Registrace*
15:30 - 15:45	*Zahájení workshopu*
15:45 -	*zvaný příspěvek*
	Karthik Bhargavan – Verifying Security of Web Service Configurations
- 17:30	minipanel – Provable Security – Future or Myth
18:00	večeře

Následuje série neformálních diskuzí v prostorách centra vyhrazených pouze pro účastníky kryptobesídky.

7. prosince 2004 (úterý)

U každého příspěvku je min. 5 minut pro dotazy a diskuzi k tématu

9:00 - 9:15	Zahájení druhého dne workshopu
9:15 - 10:05	*zvaný příspěvek*
	Peter Hellekalek – A Concise Introduction to Random Number Generators
10:05 - 10:40	Klonowski, Kutylowski, Lauks, Zagorski – Universal Re-Encryption of Signatures and Controlling Anonymous Information Flow
10:40 - 11:15	Petr Švenda – Implementace kryptografického protokolu s využitím mobilní kryptografie
11:15 - 12:05	*zvaný příspěvek*
	Alexandre Stervinou – Digital Rights Management Work in Open Mobile Environment

do 13:30 *Oběd*

13:30 - 14:05 Vlastimil Klíma – Útoky na šifru Hiji-bij-bij (HBB)
14:05 - 14:40 Krhovják, Cvrček – Útoky na a přes API: PIN Recovery Attacks

do 15:15 *Přestávka na kávu*

Krátké příspěvky a panelová diskuse
15:15 - 15:30 Frank Schindler – Remarks on Security in Programming

15:30 - 17:30 Panelová diskuse – Archivace dokumentů – bezpečnost a kryptografie

Závěr workshopu