RSA SECURITY

TRUSTED NETWORK SOLUTIONS

GiTy

ECOM-MONITOR.COM

Mikulášská kryptobesídka

8. prosince 2003 (Pondělí)

Kongresové centrum IKEM, Vídeňská 1958/9, 140 21 Praha 4

15:30 - 16:20 Registrace
16:20 - 16:30 Zahájení workshopu
16:30 - 17:30 Ross Anderson - The New Research Frontier – API Security
Prostor pro diskuzi k tématu

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

9. prosince 2003 (Úterý)

Kongresové centrum IKEM, Vídeňská 1958/9, 140 21 Praha 4

9:00 - 9:25 Registrace
9:25 - 9:30 Zahájení druhého dne workshopu
9:30 - 10:30 Serge Vaudenay - Matsui's Attack and Beyond: On Measuring Resistance to Linear Cryptanalysis
Prostor pro diskuzi k tématu
asi 10:35 - 11:05 Milan Vojvoda - On One Hash Function Based on Quasigroup
Prostor pro diskuzi k tématu
asi 11:10 - 11:40 Martin Drahanský, Luděk Smolík, Filip Orsag - Biometric Security Systems
Prostor pro diskuzi k tématu
asi 11:45 - 12:00 David C. Hájíček, Ivo Studenský - Ověření času a služby elektronického notáře
Prostor pro diskuzi k tématu

do 13:30 Oběd

Mediální partneři:

Crypto-World

RSA SECURITY

TRUSTED NETWORK SOLUTIONS

GiTy

ECOM-MONITOR.COM

13:30 - 14:15 Alexandre Stervinou - Standards for Federated Network Identity: The Liberty Alliance

Prostor pro diskuzi k tématu

14:20 - 14:50 Daniel Cvrček - Using Evidence for Trust Computation

Prostor pro diskuzi k tématu

do 15:30 Přestávka na kávu

15:30 - 16:00 Jan Bouda - Úvod do kvantové kryptografie

Prostor pro diskuzi k tématu

16:05 - 17:30 Panelová diskuse - Kryptografie v praxi a teorii: jedno a totéž, či nikoliv?

Nosné otázky:
- proč se prakticky používané systémy příliš neblíží všem teoriím, které se probírají na kryptologických workshopech a konferencích;
- je teorie v době svého vzniku příliš vzdálená od praxe, nebo praxe nestačí teorii, nebo je to úplně jinak;
- máme s tím něco dělat a když, tak co?

Panelisté:
Jaroslav Dočkal
Otokar Grošek
Petr Hanáček
Tomáš Rosa - moderátor
Bohuslav Rudolf

Závěr workshopu

Mediální partneři:

Crypto-World