Mikulášská kryptobesídka 2005

1. - 2. prosinec 2005
Praha
Hotel Olympic

Kdy & kde

Intro

Mikulášská kryptobesídka, český a slovenský workshop, se koná letos popáté. Je zaměřena na podporu úzké spolupráce odborníků se zájmem o teoretickou a aplikovanou kryptografii a další příbuzné oblasti informační bezpečnosti. Hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez obchodních vlivů, starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Registrace

Do 4. 11. 2005	základní	*1904,- Kč*
Do 4. 11. 2005	předplatitelé DSM a studenti	*1666,- Kč*
Od 5. 11. 2005	jednotná	*2261,- Kč*
sborník workshopu (včetně vstupu)		*2261,- Kč*

Zvané přednášky

Dieter Gollmann (Technical University Hamburg-Harburg)
Protocol Design: Coming Down from the Cloud
George Danezis (Katholieke Universiteit Leuven)
An Introduction to Traffic Analysis
Christian Rechberger (Technical University Graz)
Recent results on SHA-1 and SHA-256
Luboš Brim (Masarykova univerzita Brno)
Automated Formal Verification

Vybrané příspěvky

Bypassing personal firewalls under Windows NT or: feel free to fix them on your own (Petr Matoušek)
One-Time HNP or Attacks on a Flawed El Gamal Revisited (Tomáš Rosa)
Využitie zložitosti súborových formátov na vytváranie zmysluplných MD5 kolizií (Ondrej Mikle)
Slabiny šifrovacieho algoritmu Puzzle (Martin Stanek, L. Staneková)
Srovnání protokolů pro "Remotely Keyed Encryption" (Petr Švenda)

Bonus

Panelová diskuse
Vyhlášení soutěže KEYMAKER 2005 o nejlepší studentskou práci v oblasti informační bezpečnosti a kryptologie

Pořádáno za podpory

GiTy — LOOK LISTEN & COMMUNICATE

eracom TECHNOLOGIES

Mediální partneři

Více na stránkách http://www.buslab.org/mkb/