Call for Papers
Mikulášská kryptobesídka

6. – 7. prosinec 2004, Praha
http://www.tns.cz/kryptobesidka

Základní informace

Mikulášská kryptobesídka, český a slovenský workshop, se koná letos počtvrté. 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. ;-)

Workshop se skládá z (a) půldne prezentací příspěvků, diskusí a neformálního setkání v pondělí *6. prosince 2004* a (b) dne prezentací příspěvků a diskusí v úterý *7. prosince 2004*. Na workshopu opět zazní zvané příspěvky:

- **Karthik Bhargavan** (Microsoft Research, Cambridge)
  Verifying Security of Web Service Configurations
- **Peter Hellekalek** (pLab, University of Salzburg)
  A Concise Introduction to Random Number Generators
- **Alexandre Stervinou** (RSA Security, Europe)
  Digital Rights Management work in the Open Mobile Aliance

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: http://www.tns.cz/kryptobesidka.

Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie a dalších souvisejících oblastí. Návrhy příspěvků (5-15 stran A4) připravené pro anonymní hodnocení (bez jmen autorů a zjevných odkazů), budou mít oddělenou stranu textu s emailovou adresou pro korespondenci, telefonním číslem a poštovní adresou.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: http://www.tns.cz/kryptobesidka. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu RTF, nebo LaTeX a to tak, aby je programový výbor (dále jen PV) obdržel nejpozději do *11. října 2004*. Elektronická podání jsou preferována; papírová podání je nutno předem dohodnout.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *29. října*. Příspěvek pro sborník workshopu pak musí být dodán, společně s krátkým životopisem (50-100 slov), do *22. listopadu*.

Zasílání příspěvků

Preferujeme elektronické podání příspěvků.
E-mail: *dc@workshop.tns.cz*
Předmět pro email: "MKB2004"
Poštovní adresa: *MKB2004*
TNS, a.s.
Žižkova 600
664 01 Bílovice nad Svitavou

Důležité termíny

Návrhy příspěvků:	11. října 2004
Oznámení o přijetí/odmítnutí:	29. října 2004
Příspěvky pro sborník:	22. listopadu 2004
Konání MKB 2004:	6. – 7. prosince 2004

Programový výbor

Dan Cvrček, University of Cambridge – předseda
Petr Hanáček, FIT VUT
Vlastimil Klíma, LEC, spol. s r.o.
Vašek Matyáš, FI MU a Microsoft Research Ltd.
Zdeněk Říha, FI MU
Luděk Smolík, seculab s.r.o.
Jaroslav Šmíd, NBÚ
Pavel Vondruška, ČESKÝ TELECOM, a.s.

Organizační výbor

Zdeněk Burda, FIT VUT a TNS a.s. – předseda
Jan Krhovják, FI MU
Marek Kumpošt, FI MU
Roman Pavlík, TNS a.s.
Magda Procházková, TNS, a.s.
Eva Špatná, TNS a.s. – tajemník
Petr Švenda, FI MU