Call for Papers
Mikulášská kryptobesídka

6. – 7. prosinec 2007, Praha
http://www.buslab.cz/mkb

Základní informace

Mikulášská kryptobesídka, český a slovenský workshop, se koná letos posedmé. 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 ze (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *6. prosince 2007* a (b) půldne prezentací příspěvků a diskusí v pátek *7. prosince 2007*. Pro workshop jsou domluveny zvané příspěvky:

- Willi Meier (Fachhochschule Nordwestschweiz) o návrhu a analýze kandidátů eSTREAM,
- Claudia Diaz (KU Leuven) na téma steganografických metod a útoků proti nim,
- Vlastimil Klíma na téma hašovacích funkcí,
- Zdeněk Říha na téma kryptografických mechanismů používaných v elektronických pasech a
- Pavel Vondruška – exkurz do historie kryptologie.

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: http://mkb.buslab.org.

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). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: http://mkb.buslab.org. 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 na uvedenou adresu přišly nejpozději do *2. října 2007*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2007 – navrh prispevku“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *23. října*. Příspěvek pro sborník workshopu pak musí být dodán, společně s krátkým životopisem (50-100 slov), do *20. listopadu*.

Důležité termíny

Návrhy příspěvků:	2. října 2007
Oznámení o přijetí/odmítnutí:	23. října 2007
Příspěvky pro sborník:	20. listopadu 2007
Konání MKB 2007:	6. – 7. prosince 2007

Programový výbor

Petr Hanáček, FIT VUT v Brně
Vašek Matyáš, FI MU, Brno – předseda
Martin Stanek, FMFI UK, Bratislava
Tomáš Rosa, eBanka
Luděk Smolík, FI MU, Brno
Jiří Tůma, MFF UK, Praha
Jozef Vyskoč, VaF, Bratislava