Call for Papers
Mikulášská kryptobesídka

1. – 2. prosinec 2005, Praha
http://www.buslab.cz/mkb

Základní informace

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. ;-)

Workshop se skládá z (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *1. prosince 2005* a (b) půldne prezentací příspěvků a diskusí v úterý *2. prosince 2005*. Na workshopu opět zazní tři zvané příspěvky:

- Dieter Gollmann, Technische Universität Hamburg,
- George Danezis, Katholieke Universiteit Leuven,
- Luboš Brim, Masaryk University in Brno.

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

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 vyplňte při registraci v našem konferenčním systému.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: http://www.buslab.cz/mkb. 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 *12. září 2005*. Pro podávání příspěvků prosím použijte konferenční systém https://www.buslab.cz/conftool.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *17. října*. Příspěvek pro sborník workshopu pak musí být dodán, společně s krátkým životopisem (50-100 slov), do *14. listopadu*.

Zasílání příspěvků

Letos poprvé používáme konferenční systém. Pro odevzdání příspěvku je třeba se zaregistrovat na
https://www.buslab.cz/conftool
Na stejném místě pak podávejte příspěvky.

Důležité termíny

Návrhy příspěvků:	12. září 2005
Oznámení o přijetí/odmítnutí:	17. října 2005
Příspěvky pro sborník:	14. listopadu 2005
Konání MKB 2005:	1. – 2. prosince 2005

Programový výbor

Dan Cvrček, FIT VUT v Brně – předseda
Vlastimil Klíma, nezávislý kryptolog
Tomáš Rosa, eBanka
Zdeněk Říha, FI MU v Brně
Martin Stanek, FMFI UK, Bratislava
Jan Staudek, FI MU v Brně
Jiří Tůma, MFF UK, Praha
Jozef Vyskoč, VaF