Call for Papers
Mikulášská kryptobesídka

29. – 30. listopad 2012, Praha
http://mkb.buslab.org

Základní informace

Mikulášská kryptobesídka přichází už podvanácté. 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 *29. listopadu* a (b) půldne prezentací příspěvků a diskusí v pátek *30. listopadu 2012*. Pro workshop jsou domluveny zvané příspěvky:

- David Naccache (ENS, Francie) & Zdeněk Říha (FI MU): *Statistická zrychlení pro biometriky.*
- Karsten Nohl (nezávislý výzkumník, SRN): *Téma je domlouváno*.
- Andreas Uhl (Univerzita Salzburg): *Watermarking in Biometrics*.
- Vlastimil Klíma (KNZ): *SHA-3 a lehká kryptografie*.
- Michal Šrámka (STU Bratislava): *Achieving Privacy of Shared Information: Crypto & Beyond*.
- Klaus Schmeh (spisovatel, SRN): *Lámání zpráv Enigmy z 2. světové války*.

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 se přijímají odděleně pro sekci KEYMAKER (studentská soutěž) a pro hlavní program workshopu. Oba druhy návrhů mají požadovaný rozsah 5-15 stran A4 a připravenost pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou a jasným označením KEYMAKER, nebo STANDARD TRACK.

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 PDF a tak, aby přišly nejpozději do *1. října 2012*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2012 – 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 *29. října*. Příspěvek pro sborník workshopu pak musí být dodán do *12. listopadu*.

Důležité termíny

Návrhy příspěvků:	1. října 2012
Oznámení o přijetí/odmítnutí:	29. října 2012
Příspěvky pro sborník:	12. listopadu 2012
Konání MKB 2012:	29. – 30. listopadu 2012

Programový výbor

Dan Cvrček, Smart Architects, UK
Otokar Grošek, STU, Bratislava , SK
Jan Krhovják, Cepia Technologies, CZ
Vašek Matyáš, FI MU, Brno, CZ – předseda
Zdeněk Říha, FI MU, Brno, CZ
Luděk Smolík, Siegen, DE
Martin Stanek, UK, Bratislava, SK
Pavel Vondruška, Telefónica O2 & UK, CZ

Mediální partneři