Call for Papers
Mikulášská kryptobesídka

2. – 3. prosinec 2010, Praha
http://mkb.buslab.org

Základní informace

Mikulášská kryptobesídka se koná letos již podesáté. 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 *2. prosince 2010* a (b) půldne prezentací příspěvků a diskusí v pátek *3. prosince 2010*. Pro workshop jsou domluveny zvané příspěvky:

- Danilo Gligoroski (NTNU, Norsko) na téma SHA-3 a BMW.
- Paul Leyland (Cepia Technologies, ČR) na téma GPU a kryptanalýzy.
- Tomáš Rosa (Raiffeisenbank a UK, ČR) na téma bezpečnosti RFID.
- Dan Cvrček (Apoideas, UK a VUT v Brně, ČR) na téma kryptografie v bankovnictví.
- Petr Hanáček (VUT v Brně, ČR) a Petr Švenda (MU, ČR) na téma kryptografie v bezdrátových senzorových sítích.

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 to tak, aby na uvedenou adresu přišly nejpozději do *30. září 2010*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2010 – 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 *26. října*. Příspěvek pro sborník workshopu pak musí být dodán do *18. listopadu*.

Důležité termíny

Návrhy příspěvků:	30. září 2010
Oznámení o přijetí/odmítnutí:	26. října 2010
Příspěvky pro sborník:	18. listopadu 2010
Konání MKB 2010:	2. – 3. prosince 2010

Programový výbor

Otokar Grošek, STU Bratislava, SR
Vlastimil Klíma, KNZ, ČR
Jan Krhovják, Cepia Technologies, ČR
Vašek Matyáš, FI MU, Brno, ČR – předseda
Luděk Smolík, Siegen, SRN
Martin Stanek, UK, Bratislava, SR
Pavel Vondruška, Telefónica O2 & UK, ČR

Mediální partneři