Call for Papers
Mikulášská kryptobesídka

1. – 2. prosinec 2011, Praha
http://mkb.buslab.org

Základní informace

Mikulášská kryptobesídka přichází letos již v 11. ročníku. 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 *1. prosince 2011* a (b) půldne prezentací příspěvků a diskusí v pátek *2. prosince 2011*. Pro workshop jsou domluveny zvané příspěvky:

- Chris Mitchell (Royal Holloway, UK): *New architectures for identity management - removing barriers to adoption*.
- Graham Steel (INRIA, Francie): *Attacking and Fixing PKCS#11 Security Tokens*.
- Viktor Fischer (Jean Monnet University Saint-Etienne, Francie): *Recent Advances in Random Numbers Generation for Cryptography*.
- Pavel Vondruška (Telefónica O2 Czech Republic): *Šifry používané československými osobnostmi*.
- Jozef Kollár (SvF STU v Bratislave, SR): *Československé šifry z obdobia 2. svetovej vojny*.

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 *3. října 2011*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2011 – 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 *31. října*. Příspěvek pro sborník workshopu pak musí být dodán do *14. listopadu*.

Důležité termíny

Návrhy příspěvků:	3. října 2011
Oznámení o přijetí/odmítnutí:	31. října 2011
Příspěvky pro sborník:	14. listopadu 2011
Konání MKB 2011:	1. – 2. prosince 2011

Programový výbor

Dan Cvrček, Smart Architects, UK
Vlastimil Klíma, KNZ, ČR
Vašek Matyáš, FI MU, Brno, ČR – předseda
Tomáš Rosa, Raiffeisenbank a UK, ČR
Luděk Smolík, Siegen, SRN
Martin Stanek, UK, Bratislava, SR
Petr Švenda, FI MU, Brno, ČR

Mediální partneři