BUSLab

KEYMAKER – studentská soutěž

v rámci workhopu Mikulášská kryptobesídka

3. – 4. prosinec 2009, Praha
http://mkb.buslab.org

Mikulášská kryptobesídka se koná letos již podeváté. 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 *3. prosince 2009* a (b) půldne prezentací příspěvků a diskusí v pátek *4. prosince 2009*. Pro workshop jsou domluveny zvané příspěvky:

- Kenny Paterson (Royal Holloway, UK): *Cryptography and secure channels*.
- Paul Leyland (Cepia Technologies, ČR): *Use of Graphics Processing Units in cryptography*.
- Otokar Grošek (Slovak University of Technology): *Latin squares and cryptography.*
- Vlastimil Klíma (nezávislý kryptolog, ČR): *Hašovací funkce SHA-3, BMW a EDON-R.*.
- Pavel Vondruška (Telefónica O2 Czech Republic): *Vývoj kryptografických zařízení v ČS(S)R.*

KEYMAKER – 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. Příspěvek pro KEYMAKER má 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. Přijímány jsou články, bakalářské či diplomové práce, nebo jiná kvalitní ucelená díla, kde v případě rozsahu nad 15 stran požadujeme výtah podstatného obsahu v max. rozsahu 8 stran, s vlastní prací jako přílohou.

Mezi autory nejlepších příspěvků, kde oceněno bude min. 3 a max. 7 příspěvků, budou rozděleny *finanční odměny v celkové výši 125 tisíc Kč*. Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *30. října*. Příspěvek pak musí být prezentován na workshopu.

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 PDF, příp. RTF a to tak, aby na uvedenou adresu přišly nejpozději do *30. září 2009*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2009 – navrh prispevku KEYMAKER“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Důležité termíny

Návrhy příspěvků:	30. září 2009
Oznámení o přijetí/odmítnutí:	30. října 2009
Konání MKB 2009:	3. – 4. prosince 2009

Programový výbor

Jan Bouda, FI MU, Brno, ČR
Petr Hanáček, FIT VUT v Brně, ČR
Vašek Matyáš, FI MU, Brno, ČR – předseda
Štefan Porubský, ÚI AV ČR, Praha, ČR
Zdeněk Říha, FI MU, Brno, ČR
Luděk Smolík, Siegen, SRN
Jiří Tůma, MFF UK, Praha, ČR
Jozef Vyskoč, VaF, Rovinka, SR