

KEYMAKER – studentská soutěž

v rámci workshopu Mikulášská kryptobesídka

2. – 3. prosinec 2010, Hotel Olympik, Praha

<http://mkb.buslab.org>

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 kryptoanalýzy.
- Tomáš Rosa (Raiffeisenbank a UK, ČR) na téma bezpečnosti RFID.
- Dan Cvrček (Apoideas, UK a VUT v Brně, ČR) na téma kryptografie v bankovníctví.
- Petr Hanáček (VUT v Brně, ČR) a Petr Švenda (MU, ČR) na téma kryptografie v bezdrátových senzorových sítích.

KEYMAKER – Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie, počítačové a komunikační bezpečnosti 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 PV rozdělí *finanční odměny v celkové výši 150 tisíc Kč*. Oceněno bude min. 3 a max. 7 příspěvků. 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://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 2010. Pro podávání příspěvků prosím použijte adresu matyas.ZAVINAC@fi.muni.cz a do předmětu zprávy uveďte „MKB 2010 – návrh příspěvku KEYMAKER“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Důležité termíny

| | |
|-------------------------------|-----------------------|
| Návrhy příspěvků: | 30. září 2010 |
| Oznámení o přijetí/odmítnutí: | 26. října 2010 |
| Konání MKB 2010: | 2. – 3. prosince 2010 |



Programový výbor

Martin Drahanský, VUT v Brně, ČR
Otokar Grošek, STU Bratislava, SR
Petr Hanáček, VUT v Brně, ČR
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

