

Call for Papers Mikulášská kryptobesídka

4. – 5. prosinec 2008, Praha
<http://www.buslab.cz/mkb>

Základní informace

Mikulášská kryptobesídka se koná letos již poosmé. 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 4. prosince 2008 a (b) půldne prezentací příspěvků a diskusí v pátek 5. prosince 2008. Pro workshop jsou domluveny zvané příspěvky:

- Eli Biham (Technion, Haifa, Israel): *On the (In)security of the Ciphers and Protocols of GSM.*
- Richard Clayton (University of Cambridge, UK): *Can cryptography secure the Internet?*
- Jozef Gruska & Jan Bouda (MU, Brno): *New directions in quantum cryptography*
- Martin Hlaváč & Tomáš Rosa (UK, Praha & e-banka): *Towards Disclosing the RSA Private Key of an e-Passport*
- Zdeněk Říha (MU, Brno): *On security and crypto issues of e-passports*

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 2008. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2008 – návrh příspěvku“. Přijem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do 21. října. Příspěvek pro sborník workshopu pak musí být dodán do 18. listopadu.

Důležité termíny

Návrhy příspěvků:	30. září 2008
Oznámení o přijetí/odmítnutí:	21. října 2008
Příspěvky pro sborník:	18. listopadu 2008
Konání MKB 2008:	4. – 5. prosince 2008



Programový výbor

Dan Cvrček, VUT v Brně & MU, Brno
Vlastimil Klíma, nezávislý kryptolog
Vašek Matyáš, MU, Brno – předseda
Zdeněk Říha, MU, Brno & JRC Ispra, Itálie

Martin Stanek, UK, Bratislava
Luděk Smolík, MU, Brno
Pavel Vondruška, Telefónica O2 & UK, Praha

Mediální partneři

