

Call for Papers Mikulášská kryptobesídka

3. – 4. prosinec 2015, Praha
<http://mkb.tns.cz>

Základní informace

Mikulášská kryptobesídka se letos bude konat už popatnácté. 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* a (b) půldne prezentací příspěvků a diskusí v pátek 4. *prosince 2015*. Pro workshop jsou domluveny zvané příspěvky od:

- Peter Schwabe (Radboud University, Nizozemí).
- Krzysztof Pietrzak (IST Austria, Rakousko).
- Pavel Vondruška (O2 Czech Republic & UK, ČR).
- Joan Daemen (STMicroelectronics, Belgie).

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: <http://mkb.tns.cz>.

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 se zajímavými finančními odměnami pro finalisty) 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. Nejlepší příspěvky z workshopu budou zařazeny do speciálního čísla časopisu Infocommunications (indexován ve SCOPUS).

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: <http://mkb.tns.cz>. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu RTF, nebo PDF a tak, aby přišly nejpozději do 29. *září 2015*. Pro podávání příspěvků prosím použijte adresu matyas.ZAVINAC@fi.muni.cz a do předmětu zprávy uveďte „MKB 2015 – 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 30. *října*. Příspěvek pro sborník workshopu pak musí být dodán do 11. *listopadu*.

Důležité termíny

| | |
|-------------------------------|-----------------------|
| Návrhy příspěvků: | 29. září 2015 |
| Oznámení o přijetí/odmítnutí: | 30. října 2015 |
| Příspěvky pro sborník: | 11. listopadu 2015 |
| Konání MKB 2015: | 3. – 4. prosince 2015 |



Programový výbor

Peter Gaži, IST Austria, AT
Michal Hojsík, Honeywell a MFF UK, Praha, CZ
Marek Kumpošt, NetSuite & FI MU, Brno, CZ

Vašek Matyáš, FI MU, Brno, CZ – předseda
Tomáš Rosa, Raiffeisenbank a MFF UK, CZ
Bohuslav Rudolf, NBÚ, CZ

Mediální partneři

