Call for Papers
Mikulášská kryptobesídka

27. – 28. listopad 2014, Praha
http://mkb.tns.cz

Základní informace

Mikulášské kryptobesídky už letos bude dva kusy po tuctu. 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 *27. listopadu* a (b) půldne prezentací příspěvků a diskusí v pátek *28. listopadu 2014*. Pro workshop jsou domluveny zvané příspěvky od:

- Joachim Posegga: Alice in the Cloud: Insights on Security of Air Traffic Control Communication.
- Gregor Leander: Lightweight Cryptography.
- Karthik Bhargavan: Breaking and Fixing the TLS Cryptographic Protocol.
- Peter Gazi: Key-Length Extension for Block Ciphers: Plain and Randomized Cascades.

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) 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.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 *30. září 2014*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2014 – 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 *30. října*. Příspěvek pro sborník workshopu pak musí být dodán do *11. listopadu*.

Nejlepší příspěvky budou (po příp. revizi) vydány ve zvláštním vydání časopisu Infocommunications (indexovaný ve SCOPUS).

Důležité termíny

Návrhy příspěvků:	30. září 2014
Oznámení o přijetí/odmítnutí:	30. října 2014
Příspěvky pro sborník:	11. listopadu 2014
Konání MKB 2014:	27. – 28. listopadu 2014

Programový výbor

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 UK, CZ
Luděk Smolík, Siegen, DE
Martin Stanek, UK, Bratislava, SK
Pavol Zajac, STU, Bratislava, SK

Mediální partneři