

Call for Papers Mikulášská kryptobesídka

29. – 30. 11. 2018, Praha
<http://mkb.tns.cz>

Základní informace

Letos proběhne už 18. ročník workshopu Mikulášská kryptobesídka. Akce 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 29. listopadu a (b) půldne prezentací příspěvků a diskusí v pátek 30. listopadu 2018. Pro workshop jsou domluveny zvané příspěvky od:

- Pascal Paillier, CryptoExperts, Francie.
- Jan Camenisch, IBM Research, Švýcarsko.
- Werner Schindler, BSI, Německo.
- Luděk Smolík, Siegen, Německo.
- Tomáš Rosa, Raiffeisenbank & MFF UK, ČR.
- Otokar Grošek, STU v Bratislave, Slovensko.

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.

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 1. října 2018. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2018 – návrh příspěvku“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny programovým výborem workshopu a autoři budou informováni o přijetí/odmítnutí do 31. října. Příspěvek pro sborník workshopu pak musí být dodán do 13. listopadu.

Důležité termíny

Návrhy příspěvků:	1. října 2018
Oznámení o přijetí/odmítnutí:	31. října 2018
Příspěvky pro sborník:	13. listopadu 2018
Konání MKB 2018:	29. – 30. 11. 2018

Programový výbor

Peter Gaži, IOHK Research, Čína
Jan Hajný, FEKT VUT v Brně, CZ
Vašek Matyáš, FI MU, Brno, CZ – předseda
Bohuslav Rudolf, NÚKIB & MFF UK, Praha, CZ

Luděk Smolík, Siegen, SRN
Martin Stanek, UK, Bratislava, SR
Petr Švenda, FI MU, Brno, CZ

