Call for Papers
Mikulášská kryptobesídka

5. – 6. prosince 2024, Praha
https://mkb.tns.cz

Základní informace

Letos se uskuteční 23. 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 *5. 12.* a (b) půldne prezentací příspěvků a diskusí v pátek *6. 12. 2024*. Pro workshop jsou domluveny zvané příspěvky od:

- Peter Schwabe, Max Planck Institute for Security and Privacy (D) & Radboud University (NL).
- Jan Willemson, Cybernetica, Estonsko.
- Vasilios Mavroudis, Alan Turing Institute, Velká Británie.
- Veelasha Moonsamy, Ruhr University Bochum, Německo.
- Bohuslav Rudolf, NÚKIB & MFF UK, ČR.
- Tomáš Mráz, OpenSSL, ČR.

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: https://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: https://mkb.tns.cz. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu PDF a tak, aby přišly nejpozději do *21. června 2024*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2024 – navrh prispevku“. 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 *21. srpna*. Příspěvek pro sborník workshopu pak musí být dodán do *30. září*.

Důležité termíny

Návrhy příspěvků:	21. června 2024
Oznámení o přijetí/odmítnutí:	21. srpna 2024
Příspěvky pro sborník:	30. září 2024
Konání MKB 2024:	5.-6. prosince 2024

Programový výbor

Peter Gaži, IOG Research, SR
Jan Hajný, FEKT VUT v Brně, CZ
Ivan Homoliak, FIT VUT v Brně, CZ
Vašek Matyáš, FI MU, CZ – předseda
Bohuslav Rudolf, NÚKIB & MFF UK, CZ
Martin Stanek, UK, Bratislava, SR
Adolf Středa, MFF UK, CZ
Marek Sýs, FI MU, Brno, CZ
Petr Švenda, FI MU, Brno, CZ