POZVÁNKA na dvanácté setkání PRAŽSKÉHO INFORMATICKÉHO SEMINÁŘE

VÁCLAV MATYÁŠ:

Amplifikace klíčů u částečně kompromitovaných sítích

26. března 2015
16 hod.

Posluchárna E-107,
FEL ČVUT
Karlovo nám. 13,
Praha 2

po přednášce bude následovat diskuse

ANOTACE PŘEDNÁŠKY

Distribuce kryptografických klíčů je základním kamenem většiny bezpečnostních řešení v ICT. Ať již využíváme jakékoliv schéma pro distribuci klíčů, aktivní útočník může dosáhnout částečné kompromitace sítě a získat část klíčů používaných pro ochranu komunikace na jednotlivých spojích sítě. Pro obnovení bezpečnosti kompromitovaných spojů jsou navrhovány tzv. protokoly pro amplifikaci klíčů, které k dodání nových bezpečných klíčů využívají ty cesty v síti, které zůstaly zabezpečené. Návrh vhodných protokolů pro amplifikaci klíčů je stále výzvou pro scénáře, kde je třeba nalézt vhodný kompromis mezi potřebnými zdroji (např. energie potřebná pro přenos zpráv) a zlepšením bezpečnosti sítě, vyjádřeným počtem (znovu) zabezpečených spojů. V přednášce nahlédneme na nejslibnější rodiny těchto protokolů. V našem přístupu simulujeme komunikaci entit (podle dodaného nastavení) a následně analyzujeme a manuálně zpracováváme výsledky protokolů těchto simulací. Cílem je získat jednoduché, prakticky použitelné hybridní protokoly, které povedou k menší komunikační zátěži, avšak z hlediska počtu znovu zabezpečených spojů budou lepší než dříve navržené protokoly.

O PRAŽSKÉM INFORMATICKÉM SEMINÁŘI

Seminář se schází vždy 4. čtvrtek v měsíci v 16 hod. (s výjimkou letních měsíců a prosince), a to buď v budově FEL ČVUT na Karlově náměstí, nebo v budově MFF UK na Malostranském náměstí. Jeho program je tvořen hodinovou přednáškou, po níž následuje časově neomezená diskuse. Základem přednášky by mělo být něco (v mezinárodním měřítku) mimořádného nebo aspoň pozoruhodného, na co přednášející přišel a co vysvětlí způsobem srozumitelným a zajímavým i pro širší informatickou obec. Přednášky jsou standardně v angličtině.

GRAFICKÁ A MULTIMEDIÁLNÍ LABORATOŘ

Prof. RNDr. Václav Matyáš, M.Sc., Ph.D., působí na Fakultě informatiky Masarykovy univerzity, je také jejím proděkanem pro zahraničí a vnější vztahy. Věnuje se aplikované kryptografii, bezpečnosti IT a ochraně informačního soukromí. Dříve působil mj. jako Fulbright-Masaryk Visiting Scholar na Harvardově univerzitě, v Microsoft Research Cambridge, University College Dublin, ecom-monitor.com, v laboratoři Ubilab u UBS AG, u londýnské certifikační autority Uptime Commerce, a také jako Royal Society Postdoctoral Fellow na University of Cambridge. Podílel se i na vývoji Common Criteria a práci v ISO/IEC JTC1 SC27.

Kontakt: info@praguecomputerscience.cz
Informace: www.praguecomputerscience.cz