

Oponentní posudek disertační práce

Autor: Ing. Zdeněk Martinásek

Název: Kryptoanalýza postranními kanály

Vydavatel: Fakulta elektrotechniky a komunikačních technologií, Vysoké učení technické v Brně, 2013

Zpracovatel posudku: doc. Ing. Jaroslav Dočkal, CSc., ředitel Ústavu aplikované informatiky, Vysoká škola Karla Engliše, a.s.

Disertace plně odpovídá oboru disertace a dané téma je velmi aktuální z hlediska současného stavu vědy. Téma práce je velmi náročné, protože jde o novou oblast vědního výzkumu, v České republice se jí málokdo zabývá a výzkum v této oblasti vyžaduje samostatně získat přehled o řadě řešení v zahraničí. Autor s přehledem vyřešil dva základní úkoly – vytvořil si dostatečný přehled o metodách proudové analýzy a našel si vlastní „parketu“ pro řešení.

Cíle práce jsou uvedeny v kapitole 2 na str. 30. Jde o čtyři cíle, z nichž jeden je dominantní (návrh a implementace nové metody proudové analýzy využívající neuronové sítě), ostatní tři cíle jsou podpůrné a vyplývají z logiky řešení hlavního cíle. Všechny cíle byly beze zbytku splněny. Metoda je opravdu originální a líbí se mi, že jí (jak se někdy stává) není autor uhranut, nýbrž velmi objektivně na straně 97 práce s přehledem hodnotí výhody a nevýhody své metody v porovnání s dosud používanými dalšími metodami.

Co na práci zvláště pozitivně oceňuji je, že autor ve velké míře předkládá výsledky měření v přehledné grafické podobě. Rovněž oceňuji, že na řešený problém nenahlíží staticky, ale ve vývoji souboje mezi útokem na šifru a obrannými opatřeními (viz podkapitola 3.3.4).

Co mi trochu vadí, je, že se disertant rozepisuje příliš a zbytečně zešíroka, např. k čemu je vzhledem k zaměření práce výčet bezpečnostních služeb v úvodu práce? A tak než se čtenář dobere k vlastnímu seznámení s řešením autora, musí se probrat čtyřiceti stránkami, na kterých se prolíná nezbytný a užitečný text s textem, který lze snadno postrádat. A když se k tomu přidá poněkud těžkopádný způsob vyjadřování autora, práce ztrácí na čtivosti. Autor rovněž s oblibou používá zkratky – na str. 114 je sice jejich přehled (neuspořádaný), ale ne všechny v práci použité zkratky jsou v něm uvedeny.

Práce je zpracována v jazyce českém (v posledních letech je předkládána řada prací v angličtině), což já osobně vítám. Až na dvě výjimky v práci nejsou větší gramatické chyby, sem tam je překlep (str. 70) a chybí čárka. Často píše o kapitole, ale míní podkapitolu. Autor má i jisté problémy v oblasti typografie (pomlčku si plete s rozdělovníkem či spojovníkem, často píše chybně procenta, trojtečku atd.). U bibliografických odkazů se implicitně předpokládá dodržování ČSN ISO 690 (01 0197), pokud dal autor přednost jiné normě, bylo by dobré uvést které.

Jádro práce bylo dostatečně publikováno. Ing. Zdeněk Martinásek je potřebně publikačně aktivní. Na str. 112 práce je seznam vybraných dvanácti publikací autora, protože ale je ve všech případech spoluautorem, bylo by vhodné vždy uvést svůj autorský podíl.

Pro Ing. Martinásku mám tyto dotazy k obhajobě:

- Popište vybranou reálnou situaci, ve které by se uplatnily přednosti vašeho řešení ve srovnání s konkurenčními.

- Co ve vámi uvedeném vztahu pro permutaci s opakováním označuje m_i .
- Po obhajobě hodláte ve výzkumu metod proudových postranních kanálů pokračovat? Pokud ano, kterým směrem?

Závěrem Disertační práce Ing. Zdeňka Martináska plně odpovídá obecně uznávaným požadavkům k dělení titulu Ph.D. Doporučuji práci předložit k obhajobě.

A handwritten signature in black ink, appearing to read "J. Šochel". The signature is stylized with a large initial "J" and a long horizontal stroke extending to the right.

V Brně 20. června 2013