Posudek na disertační práci

Martin Henzl, *Security of Contactless Smart Card Protocols*

Jan Staudek, oponent disertační práce *

2. června 2016

Předmět disertační práce spadá do širokého oboru obvykle nazývaného *informační bezpečnost*. Výzkumné činnosti doktoranda, jejichž výsledky mj. ilustruje hodnocená disertační práce (mimo tuto práci jsou předmětem i dalších publikací) se orientují do oblasti prověřování bezpečnosti systémů vybudovaných na bázi používání bezkontaktních čipových karet. Inovativní charakter výzkumu v této oblasti bezpečnosti takových systémů spočívá ve výzkumu a zavádění nových metod cílených na ověřování bezpečnosti těchto systémů jako celku. Dosavadní formy zajištění bezpečnosti těchto systémů se orientovaly buď to na certifikaci jejich komponent nebo na formální verifikace protokolů zajišťujících jejich chod. Martin Henzl tyto dva směry spojuje. Jím navržená metoda přispívá k minimalizaci zbytkového rizika, že karta i protokol budou samostatně považované za dostatečně bezpečné komponenty, ale nevhodným použitím příkazů karty nebo nesprávnou implementaci protokolu vznikne zranitelné místo v systému. Inspiracemi výzkumných prací Martina Henzla byly zřejmě publikace řešící automatické hledání zranitelných míst v *security tokenech* implementujících standard $PKCS\#11$ pomoci metod souhrně označovaných jako *model checking*.

Původním přínosem disertační práce Martina Henzla v širším slova smyslu je možnost obohacení formální verifikace bezpečnostních protokolů o příkazy a vlastnosti konkrétní karty, které jsou důležité pro to, aby byl protokol jako celek bezpečný.

Konkrétním vlastním přínosem prací Martina Henzla je pak vypracování metody pro poloautomatické hledání zranitelných míst v určitém protokolu, který používá nějaké konkrétní příkazy na nějaké konkrétní kartě, tedy příkazy, jejichž implementace je přesně definována.

Metoda navržená Martinem Henzlem využívá již existující nástroje pro formální verifikaci (tj. pro modelování protokolu a následnou verifikaci takového modelu – *model checking*). Vlastní přínosy Martina Henzla spočívají především:

*Doc. Ing. Jan Staudek, CSc., FI MU Brno, tel.: 549 497 047, e-mail: staudek@fi.muni.cz

- ve vypracování a ověření metodiky vytváření modelu tak, aby se co nejpřesněji reprezentovala jak konkrétní karta, tak i modelovaný bezpečnostní protokol,
- v navržení celého procesu poloautomatického hledání zranitelnosti,
- a konečně v zahrnutí fází postupného zpřesňování modelu na základě dat získaných z výstupů verifikací prováděných ve fázi *model checking*

Výše popsaný hlavní výsledek výzkumné činnosti Martin Henzl v disertační práci doplňuje dalším konkrétním vlastním výsledkem v oblasti bezpečnosti bezkontaktních čipových karet – řešením ochran proti *relay* útoku. Na zajištění bezpečnosti opatření proti tomuto typu útoku, podobně jako proti fyzickým útokům nebo proti útokům na postranní kanály, se metoda formální verifikace nedá použít (což správně zmiňuje Martin Henzl ve své práci). Tento výsledek je dobrou ilustrací velmi širokého a přitom důkladného záběru výzkumných činností Martina Henzla v oblasti bezpečnosti bezkontaktních kartových systémů. Skutečnost, že se mu věnuje až v závěru disertační práce a v rozsahu menším než verifikaci protokolů nijak nesnižuje jeho hodnotu a přínos pro zajištění potřebné úrovně bezpečnosti protokolu bezkontaktních čipových karet.

Výsledky výzkumných prací Martina Henzla jsou publikované, publikace mají dostatečnou referenční úroveň.

Publikacemi, formou a obsahem disertační práce Martin Henzl prokázal velmi dobrou vědeckou erudici. A to nejen vědeckou. Měl jsem možnost se seznámit s velmi prakticky a aplikačně orientovanými výsledky analýzy rizik konkretního bezkontaktního platebního systému v jedné zahraniční bance s širokou mezinárodní působností provedené Martinem Henzlem. Byly přesvědčivé, pro sponzora auditu přínosné a sponzorem auditu vysoce kladně hodnocené.

Hodnocená disertační práce Martina Henzla podle názoru oponenta odpovídá obecně uznávaným požadavkům k udělení akademického titulu PhD.

Jan Staudek