TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky
a mezioborových studií

# OPONENTNÍ POSUDEK ZÁVĚREČNÉ KVALIFIKAČNÍ PRÁCE

**Autor závěrečné práce:** Bc. Jan Petřvalský

**Název práce:** Zranitelnost technologie Mifare Classic

**Oponent práce** Ing. Ondřej Zelinka, Ph. D.

**Pracoviště oponenta** Lumena s.r.o.

| | |
|---|---|
| A. Kvalita abstraktu, klíčová slova odpovídají náplni práce | Výborně (1) |
| B. Rozsah a zpracování rešerše | Velmi dobře (2) |
| C. Řešení práce po teoretické stránce | Výborně (1) |
| D. Vhodnost, přiměřenost použité metodiky | Výborně mínus (1-) |
| E. Úroveň zpracování výsledků a diskuse | Velmi dobře (2) |
| F. Vlastní přínos k řešené problematice | Velmi dobře (2) |
| G. Formulace závěru práce | Výborně (1) |
| H. Splnění zadání (cílů) práce | Splněno |
| I. Skladba, správnost a úplnost citací literárních údajů | Výborně (1) |
| J. Typografická a jazyková úroveň (vč. pravopisu) | Výborně mínus (1-) |
| K. Formální náležitosti práce (struktura textu, řazení kapitol, přehlednost ilustrací) | Výborně mínus (1-) |

Komentáře či připomínky:

Úvodní kapitola práce je poměrně stručná. Autor práce již na těchto prvních dvou stránkách respektuje zvolené tématické zaměření, tedy otázku bezpečnosti RFID technologie. Z mého pohledu by bylo vhodné pojmout tuto úvodní kapitolu obecněji. Například se alespoň stručně zmínit o základních fyzikálních principech, popsat rozdělení transpondérů na pasivní a aktivní, uvést možné vzdálenosti dosahu s ohledem na použité frekvence, atd.
Ve druhé kapitole je přehledně popsán aplikační protokol Mifare Classic včetně struktury datové paměti. Třetí kapitola již kombinuje rešeršní text spolu s vlastními přínosy autora. V jejím začátku je popsán šifrovací algoritmus Crypto1 vyvinutý společností NXP Semiconductors. V podkapitole nazvané "Zranitelnosti" potom autor rozebírá šest konkrétních bezpečnostních nedostatků. U třech slabin je dále navržena metodika testování.
Ve čtvrté kapitole je popsán samotný návrh SW nástroje pro testování zranitelností. Jak sám autor zmiňuje, je odstranění popisovaných bezpečnostních slabin v reálném nasazení prakticky neřešitelné (především z důvodů kompatibility). Proto je do práce zařazena pátá kapitola, která obsahuje soupis doporučení, jak alespoň minimalizovat bezpočnostní rizika.
V Závěru jsou stručně shrnuty klíčové části práce a zhodnoceny dosažené výsledky.

*...pokračuje na straně 2*

Celkové zhodnocení:

Po formální stránce, je tato diplomová práce zpracována pěčlivě. Chyby se v textu vyskytují pouze velmi ojediněle. Práce je dobře čitelná, až na několik málo vět, které nemají pro čtenáře bez popsání širších souvislostí význam (např. strana 15 "Kolize je detekována jako vysoká úroveň po celou dobu hodinového taktu.").
Z odborného hlediska je práce na velice dobré úrovni. Diplomant prokázal jak velké množství znalostí v oblasti kryptografie, tak schopnost dobře se orientovat v odborné literatuře týkající se této problematiky. V praktické části práce bych uvítal konkrétnější popis provedených testů.

Závěrem mohu konstatovat, že zadání diplomové práce bylo bezezbytku splněno.

Otázky k obhajobě:

V kapitole 3.4.1 na straně 26 řešíte problém nízké entropie generátoru náhodných čísel určených pro autentizaci bloku. Konkretizujte časovou náročnost operací potřebných pro dosažení konstantní vygenerované hodnoty ve 35% případů s Vámi použitým HW. Na blokovém schématu ukažte vhodnější HW sestavu pro minimalizaci potřebného času. Jakého zlepšení by mohlo být dosaženo?

Pro tři diskutovaná slabá místa testované technologie jste navrhoval a realizoval testovací algoritmus. Stručně popište/shrňte, co je reálným výsledkem těchto navržených testů. Jaké odlišnosti, rozpoznatelné navrženými testy, se mohou v různých implementacích této technologie vyskytovat.

**Celková klasifikace:**

Práce splňuje požadavky na udělení akademického titulu, a proto ji doporučuji k obhajobě

Navrhuji tuto práci klasifikovat stupněm Výborně mínus (1-)

V Liberci

dne 19.5.2014

Podpisem současně potvrzuji, že nejsem v žádném osobním vztahu k autorovi práce

. . . . . .

podpis oponenta