Posudek vedoucího na bakalářskou práci

Jan Kučera, **Courtoisův útok na MIFARE**

Práce se zabývá nedávno publikovanými útoky na bezkontaktní čipové karty typu MIFARE Classic. Tyto karty využívají RFID technologii jsou velmi rozšířené v nejrůznějších oblastech.

Kapitola s názvem **RFID** obsahuje velmi detailní a precizní úvod do problematiky RFID, standardů, které se v této oblasti používají, a fyzikální realizace komunikace mezi transpondérem a terminálem.

V následující stručné kapitole jsou popsány detaily a zvláštnosti karty MIFARE Standard 1K a protokol pro autentizaci terminálu, který je na této kartě použit.

Jádro práce je v posledních dvou kapitolách číslo 4 a 5. Čtvrtá kapitola obsahuje popis proudové šifry Crypto 1, která je na kartě používána. Tato kapitola vychází z publikovaných popisů, které různé skupiny ziskaly pomocí reverse-engineering, výrobce karet algoritmy sám nezveřejnil.

Poslední pátá kapitola obsahuje popis tří různých útoků, které využívají slabin šifry Crypto 1, a pomocí kterých lze odhalit tajné klíče na kartě. První dva útoky publikoval F.D. Garcia se spolupracovníky, třetí a nejrychlejší z těchto útoků pak pochází od N. Courtoise. Implementace Courtoisova útoku je na přiloženém CD spolu se zdrojovým souborem. Při implementaci autor mohl vycházet pouze ze stručného a nepříliš úplného popisu algoritmu v Courtoisově článku. Jeho vlastní popis je také dosti stručný, autor ale problematiku plně pochopil jak vyplývá z úspěšné implementace. Uvedené popisy útoků autor doplnil vlastními výpočty pravděpodobnostmi různých vlastností nelineární funkce, kterou algoritmus Crypto 1 používá ke generování proudu klíče pro proudovou šifru.

Jinak lze práci sotva co vytknout. Autora problematika RFID čipů zjevně zajímá, vyhledal si spoustu informací z literatury zcela nad rámec zadání práce a všechny dostupné informace zpracoval do přehledného a čtivého textu. Kapitolu **RFID** lze bez jakýchkoliv úprav použít jako základní text o problematice. Stejně tak bude možné využít při výuce grafickou vizualizaci šifry Crypto 1, kterou autor rovněž vytvořil.

Jakkoliv problematika není matematicky příliš složitá, autor téma plně pochopil a přehledně zpracoval. Ocenění si také zaslouží jeho osobní komunikace s autory základních prací o této kartě a vyjasnění některých nepřesností z originálních prací. Celkově lze shrnout, že jde o bakalářskou práci mimořádně kvalitní a proto navrhuji hodnotit ji známkou *výborně*.

V Praze 20.6.2010

Doc. RNDr. Jiří Tůma, DrSc.

Oponentský posudek bakalářské práce

# Jan Kučera: Courtoisův útok na MIFARE

Práce uvádí čtenáře do problematiky RFID (identifikace na rádiových frekvencích) a zaměřuje se na popis a softwarovou implementaci útoku na konkrétní typ pasivního transpodéru od firmy NXP Semiconductors. Po úvodu se stručným historickým přehledem následuje popis relevantních průmyslových standardů pro fyzickou a transportní vrstvu komunikace na radiových vlnách a popis antikolizního protokolu. Dále práce pokračuje kapitolami s popisem aplikační vrstvy rodiny transpodérů MIFARE od firmy NXP a implementace proudové šifry Crypto1 a generátoru náhodných čísel zabudovaného do dotčených transpodérů.

Konečně nejobsáhlejší kapitola se věnuje slabinám zabezpečení transpodérů a útokům. Je zde popsáná role nešťastné volby výpočtu paritních bitů a pseudonáhodných čísel. Dále jsou analyzovány a formálně dokazovány vlastnosti booleovských funkcí použitých v šifře Crypto1. Nakonec jsou podrobně popsány Garciovy útoky i nejrychlejší známý útok od Courtoise, jehož softwarová část je na přiloženém CD implementována.

Práce je velice pěkně a precizně napsána a popisuje problematiku z mnoha hledisek, od fyzických parametrů rádiové komunikace přes vrstvy protokolů až po implementační detaily útoků a použitá matematická tvrzení. Je patrné dobré porozumění a zájem o problematiku. Vytknout by bylo možné poněkud stručné zpracování kapitoly o Courtoisově útoku, zvláště v porovnání s podrobným popisem útoků Garciových. Speciálně pak není z popisu zcela jasné, jak byla určena pravděpodobnost selhání útoku a tedy předpokládaný nutný počet jeho opakování.

Předloženou práci **doporučuji k obhajobě** a navrhuji ohodnotit stupněm **výborně**.

V Praze dne 18. 6. 2010

RNDr. Jan Šťovíček, Ph.D.