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.