Posudek oponenta bakalářské práce

Student: Bobčík Martin
Téma: Bezpečnostní analýza karet Mifare Classic (id 21980)
Oponent: Hellebrandt Lukáš, Ing., UITS FIT VUT

1. Náročnost zadání **méně obtížné zadání**

Jde o nastudování problematiky a demonstraci již popsaných útoků, které si autor měl sám zvolit.

2. Splnění požadavků zadání **zadání splněno s drobnými výhradami**

Student si zvolil tři útoky k demonstraci. Jeden z nich úspěšně provedl, zbylé dva se nepodařily. Důvody jsou korektně popsány v práci, společně s možnými řešeními, o která už se ovšem autor nepokusil. Pro provedení úspěšného útoku vůbec nebyla potřeba implementační část práce.

3. Rozsah technické zprávy **splňuje pouze minimální požadavky**

Práce má asi 43 normostran a rozsah není uměle zvyšován zbytečným obsahem.

4. Prezentační úroveň předložené práce **75 b. (C)**

Práce má logickou strukturu a její obsah je vhodně podaný a pochopitelný. Některé věty jsou mluvnicky špatně až nedávají smysl, není to ale časté a je to způsobené nejspíš jen nedostatečnou korekturou. Některé pojmy nejsou dostatečně vysvětlené (klíčování, backscatter modulace, volné vázání...). V práci se vyskytují některá tvrzení, která budí pochyby a nejsou ozdrojována, nicméně jde o tvrzení pro smysl práce nevýznamná. Chybí popis rovnic 3.1 až 3.6, popis proměnných v nich a jejich souvislostí. Některé rovnice, tabulky a obrázky vůbec nejsou zmíněny v textu.

Kapitola o útocích by měla být výrazně delší. Většinu práce zabírá teorie, vlastní práce je v dosti malém rozsahu.

5. Formální úprava technické zprávy **75 b. (C)**

Práce je v češtině. Obsahuje drobné typografické chyby. Časté chyby v interpunkci a místy překlepy, které by odhalil spellcheck. Nedokonalá angličtina v anglickém abstraktu. Žádná z chyb ovšem nepůsobí při čtení práce rušivě a nejde o hrubé chyby.

6. Práce s literaturou **75 b. (C)**

Citovaná literatura je k tématu a kvalitní. Často je citována práce o UHF RFID, přestože podle autora chytré karty používají HF. Některá tvrzení nejsou citována a některá citovaná tvrzení jsou sporná (vizte otázky k obhajobě). Teorie je nastudována a popsána vhodně.

7. Realizační výstup **55 b. (E)**

Žádný z útoků, které využívají implementační část práce, nebyl úspěšný. Důvody jsou v práci korektně popsány, nastíněny jsou i možnosti řešení, o ty už se ovšem autor nepokusil. Implementační část práce tedy slouží jen k demonstraci, že a proč daný postup nefunguje.

Po technické stránce nemám výhrady, jen si myslím, že bylo vhodné se pokusit o úpravu firmware zařízení Chameleon Mini. Dokumentace je v textu práce a kromě pokynů k instalaci je dostatečná.

8. Využitelnost výsledků

Jde o nastudování problematiky a praktickou demonstraci již popsaných útoků.

9. Otázky k obhajobě

Šlo by opakování výzev zneužít k replay útoku?

V článku tvrdíte, že nová generace karet Mifare Classic nepoužívá pseudonáhodná čísla, ale náhodná. Vysvětlete.

Pokus o časovou kryptoanalýzu se nezdařil kvůli technickým omezením. Kdyby se zdařil, k čemu by šlo výsledky použít? Bylo by možné ho provést pomocí úpravy firmware zařízení Chameleon Mini a tedy s přesnějším časováním?

Lze zabránit útoku s klonováním karty beze změny karty, tedy jen úpravou software ve čtecích zařízeních?

Proč není možné mít při relay útoku Proxy přepnuté do módu čtečky a pro skutečnou čtečku aktivně emulovat chování karty nastavením vhodné frekvence a modulace?

10. Souhrnné hodnocení

65 b. uspokojivě (D)

Zadání bylo spíše jednoduché. Práce je po formální a logické stránce v pořádku. Teorie byla popsána kvalitně. Většinu práce zabírá teorie, vlastní práce je v dosti malém rozsahu. Přínos není velký, jelikož šlo o demonstraci známých útoků. Ze tří zvolených útoků se povedl jeden a ten vůbec nevyžadoval implementační část práce. Příčiny neúspěchu dalších dvou útoků jsou korektně popsány a je nastíněno jejich řešení, to už ovšem nebylo realizováno.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 3. června 2019

Hellebrandt Lukáš, Ing.
oponent