Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Vít Osička** **Oponent:** **Ing. Mojmír Přikryl**

Studijní program: **Inženýrská informatika**
Studijní obor: **Počítačové a komunikační systémy**
Akademický rok: **2019/2020**

Téma diplomové práce: **Klíčování EMV platebních terminálů podle PCI DSS normy**

Hodnocení práce:
Diplomová práce pojednává o možnostech zavedení prvotního klíče do karetních platebních terminálů. Problematika šifrování, tak i samotná PCI DSS norma je velice obsáhlá a složitá. Veškerá zařízení včetně software musí splňovat přísná kritéria a musí projít certifikací.

Oceňuji, že teoretická část začíná problematikou platebních terminálů, jejich vzniku a postupného vývoje. I když tato část přímo nesouvisí s problematikou klíčování, šifrování a PCI DSS nornou, poskytuje těmto kapitolám adekvátní úvod. Teoretická část tím získává na čtivosti, zaujme a přirozeně graduje. Shodné schéma je použito i v rozboru samotné kryptografie. Na závěr je uvedena případová studie vybraného továrního řešení. Zde bych pro doplnění uvítal i stručný seznam řešení jiných.

Praktická část se zabývá stávajícím řešením ve vybrané společnosti. Zhodnocením jeho nedostatků a limitů. Návrhem nového, univerzálnějšího, upravovatelného a efektivnějšího řešení. Za zmínku stojí například využití technologie NFC, kterou žádná jiná řešení nepodporují. Praktická část je doplněna o vizualizaci nově navrženého klíčovacího zařízení. Jsou zde zahrnuty požadavky PCI DSS normy na bezpečnost hesel, uživatelské role, počet přihlášených uživatelů, logování operací. Vizualizace jsou po grafické stránce zpracovány na úrovni, což je z praktického hlediska žádoucí při obhajobě projektu u zadavatele. Praktická část mohla být nad rámec zadání doplněna o výběr doporučeného hardware.

Předloženou diplomovou práci shledávám jako zdařilou a obsáhlou. Doporučuji ji k obhajobě a navrhuji hodnocení B – velmi dobře.

Dotazy k obhajobě:

1. Většina výrobců terminálů dodává svá řešení klíčovacích zařízení. Z jakého důvodu je navrženo vlastní? Popřípadě umožňuje přímo klíčování v továrně. Je tedy klíčovací zařízení vůbec zapotřebí?
2. Zmiňujete skutečnost, že bude v brzké době nutné přejít z 3DES na AES. Má tedy vůbec smysl vyvíjet 3DES klíčovací zařízení?

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Celkové hodnocení práce:

Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

B - velmi dobře.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 1. 9. 2020 Podpis oponenta diplomové práce