

Posudek oponenta diplomové práce

Student: Janeček Vít, Bc.
Téma: Modul rozšiřující funkcionalitu GDPR řešení (id 21184)
Oponent: Pluskal Jan, Ing., UIFS FIT VUT

- 1. Náročnost zadání** **obtížnější zadání**
Práce si klade za cíl vytvořit modul pro existující produkt Safetica zajišťující GDPR řešení pro malé a střední firmy. Pro úspěšné zvládnutí práce musel student nastudovat problematiku overlay sítí a kryptografických mechanismů zajišťujících bezpečnost.
- 2. Splnění požadavků zadání** **zadání splněno**
Zadání bylo splněno.
- 3. Rozsah technické zprávy** **je v obvyklém rozmezí**
Práce je v obvyklém rozsahu.
- 4. Prezentací úroveň předložené práce** **80 b. (B)**
Práce má logickou strukturu, jednotlivé kapitoly na sebe navazují. Úvodní kapitoly 2 a 3 popisující řízení přístupu a overlay sítě považují za příliš rozsáhlé a bylo by vhodnější čtenáře odkázat přímo na relevantní zdroje.
- 5. Formální úprava technické zprávy** **80 b. (B)**
V práci se vyskytuje malé množství překlepů a špatně skloňovaných slov. Místo převzetí obrázků s anglickým popisem bych v české práci ocenil jejich české alternativy v jednotném vizuálním stylu, zvláště pokud se jedná o bitmapové obrázky o nižším rozlišení.
- 6. Práce s literaturou** **70 b. (C)**
Student cituje velmi relevantní zdroje v podobě IETF standardů a RFC. Bohužel, celkový dojem z kvalitně nastudované literatury kazí její použití v textu práce. Převzaté myšlenky zejména v kapitolách 2 a 3 obsahují reference, které se objevují pouze v úvodech a ne přímo u myšlenek samotných. Čtenář takto není schopen dohledat jejich původ, pokud s nějakou myšlenkou nesouhlasí.
- 7. Realizační výstup** **95 b. (A)**
Realizovaný výstup je ve formě multiplatformního řešení v jazyce C++ za použití nejnovější normy. Program je navržen respektující objektové paradigma. Kód je dobře dokumentovaný a pochopitelný.
- 8. Využitelnost výsledků**
Výsledky budou přímo využity v produktu GDPR řešení od společnosti Safetica.
- 9. Otázky k obhajobě**
 1. Práce nestaví na matematickém modelu podkládajícím korektnost kompozice použitých kryptografických algoritmů. Jak si můžete být jist, že jste je použil korektně?
 2. Jaký je přínos v použití Vašeho řešení od klasické VPN sítě a řízení přístupu na úrovni aplikace? Případně Direct Access řešení od MS.
 3. Jaký je význam přenosu symetrického klíče již zabezpečeným kanálem?
- 10. Souhrnné hodnocení** **85 b. velmi dobře (B)**
Práce velmi detailně popisuje existující overlay sítě a úvod do kryptografických principů a metod. Dle vyjádření společnosti Safetica, pro kterou je DP realizována, student splnil požadavky nad rámec zadání a jeho programový výstup je plně integrovatelný s jejich řešením. I přes citlivost tématu bych v práci samotné ocenil větší zaměření na realizovaný výstup než obecně známé principy; obzvláště na část testování, která ukazuje funkčnost řešení, ale ne jeho bezpečnost.

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

V Brně dne: 31. května 2018

.....
podpis