Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Jan Němec** **Oponent:** **Ing. Kamil Halouzka, Ph.D.**

Studijní program: **Bezpečnostní technologie, systémy a management**
Studijní obor/Specializace: **Bezpečnostní technologie**
Akademický rok: **2021/2022**

Téma diplomové práce: **Systém pro sběr entropie z okolního elektromagnetického šumu**

Hodnocení práce:
Zde vložte Vaše vlastní hodnocení předložené práce. V posudku se zaměřte především na
- úplnost vypracování, aktuálnost a obtížnost řešeného úkolu,
- způsob a úroveň pojetí řešeného úkolu,
- úroveň zpracování tématu, přínos diplomanta,
- formální náležitosti práce, chyby a omyly v technické zprávě,
- dotazy k obhajobě.
- v závěru zhodnoťte celkově předloženou diplomovou práci a klasifikujte dle klasifikační stupnice uvedené v závěru tohoto formuláře.

Hodnocení může přesahovat na další strany.

Úplnost vypracování, aktuálnost a obtížnost řešeného úkolu

Cílem diplomové práce Bc. Jana Němce „**Systém pro sběr entropie z okolního elektromagnetického šumu**“ bylo vypracovat rešerši z oblasti antén, vytvořit prototyp sběru signálu SW definovaného rádia s následným generováním náhodných čísel, aplikovat prototyp do vybraného kryptografického systému, navrhnout metodu testování funkčnosti prototypu a otestovat a optimalizovat prototyp.

Problematiku lze z hlediska tématu hodnotit jako aktuální. Po stránce rozsahu a obtížnosti předloženou diplomovou práci hodnotím jako velmi dobrou.

Metodika řešení diplomové práce

Diplomová práce je členěna na teoretickou a praktickou část. V teoretické části se diplomant zaměřil na rozdělení antén, kterou zakončil výběrem vhodné teleskopické prutové antény pro sběr entropie. Zvolená anténa byla vhodně použita s HackRF One SDR, které je vhodně popsáno v další kapitole. V popisu diplomant chybně zmiňuje Shannon-Kotělníkovou teorém (v textu je uveden Kotelník). Následně student vhodně rozpracoval generátory náhodných čísel s možnostmi jejich využití. V části využití v kryptografii student nastínil využití v symetrické a asymetrické kryptografii, ale již nevysvětlil rozdíl mezi uvedenými způsoby šifrování.

V praktické části diplomant vhodně popsal linuxovou aplikaci GNU Radio Companion, která slouží pro ovládání SDR. Kladně hodnotím zpracování transformace entropie v časové a frekvenční

doméně a jejich kombinaci. Velmi názorným způsobem je zpracováno ověření náhodnosti, kde student sledoval a vyhodnotil tři základní charakteristiky generovaných čísel a to: frekvence výskytu symbolů, průměrná hodnota symbolů závislá na pozici čísla a entropie čísla (dle frekvence a dle délky antény). V poslední kapitole se student zaměřil na využitelnost v praxi, kde jim navržené metody vhodně implementoval do náhodného generátoru k vytvoření grafického prostředí a pro implementaci v kryptografickém systému.

Úroveň zpracování tématu, přínos práce

Diplomová práce je přehledná a je systematicky členěna do kapitol a podkapitol. Za přínos DP považuji návrh způsobu pro sběr elektromagnetického šumu s následným ověřením náhodnosti.

Formální náležitosti práce

Po formální stránce je diplomová práce napsaná správně. Z hlediska písemného vyjadřování a jazykové stránky splňuje stanovená kritéria.

DOTAZY K OBHAJOBĚ

1. Ve své DP zmiňujte hashovací algoritmy. Objasněte pojem hashovací funkce a vysvětlete jejich důležitost v kryptografii.

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

A - výborně.

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

Datum 1. 6. 2022 Podpis oponenta diplomové práce