Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **BC. ALEŠ RYŠKA** **Oponent:** **Ing. Ladislav Vyskočil**

Studijní program: **Informační technologie**
Studijní obor/Specializace: **Kybernetická bezpečnost**
Akademický rok: **2023/2024**

Téma diplomové práce: **Application of Machine Learning in the Domain of Side-Channel Attacks (Využití strojového učení při útocích postranním kanálem)**

Hodnocení práce:

Cílem diplomové práce bylo popsat problematiku využití strojového učení v oblasti útoků postranními kanály, k jehož dosažení bylo třeba naplnit několik bodů, jejichž přesná specifikace byla součástí zásad uvedených v zadání práce. Diplomová práce je napsána v anglickém jazyce, je přehledně strukturována a jednotlivé části na sebe logicky navazují. Text práce je zpracován odborně a srozumitelně. Po jazykové stránce nebyly nalezeny žádné pravopisné, nebo stylistické chyby. Po formální stránce je práce vhodně doplněna komentáři i odkazy na odpovídající literární či elektronické zdroje. Diplomová práce obsahuje přiměřené množství obrázků, tabulek a příloh.

V teoretické části byl nejdříve popsán vývoj útoků vedlejšími kanály, zahrnující EMI útoky, akustické útoky, historické špionážní techniky, AES útoky, jejich analýzy, důsledky a vývoj protiopatření. V další kapitole je popsán současný stav a výzkum v oblasti analýzy útoků postranními kanály, kryptografická řešení a hardwarové zranitelnosti. Dále je popsána výkonová analýzy se zaměřením na korelační analýzu výkonu (CPA) a diferenciální analýzu výkonu (DPA), popis fází, výhod a nevýhod DPA a HD a HW model. Poslední kapitola v této části se zabývá proudovou šifrou TRIVIUM, její strukturou, generováním proudu klíčů, nastavením a HW implementací. Popsány byly i bezpečnostní aspekty.

Úvod praktické části práce je zaměřen na útoky vedlejším kanálem podporované strojovým učením - nástroj SCAAML, jeho architekturu, provádění útoků, jeho potenciál a datové sady a modely. Dále byl popsán třístupňový přístup k obnově stavu/klíče, popis funkce Frameworku, praktické hodnocení a výsledky. V poslední kapitole praktické části je provedeno celkové vyhodnocení, jak tříkrokového útoku na šifru TRIVIUM, tak i SCAAML. Dále jsou zde shrnuty hlavní poznatky a porovnání praktických výsledků celého výzkumu.

Diplomová práce se zabývá v praxi mnohdy opomíjeným tématem. Přínos práce vidím v odborném popisu této problematiky včetně praktických postupů, kdy může sloužit jako zdroj užitečných informací pro další výzkum. Všechny body zadání diplomové práce byly splněny v plném rozsahu. Diplomant popisované problematice dobře rozumí. Diplomová práce se jeví jako splňující svůj cíl, a proto ji doporučuji předložit k obhajobě.

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

A - výborně.

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

Datum 16. 5. 2024 Podpis oponenta diplomové práce