

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: MUSIL PETR

Oponent: Hess Václav

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

Téma diplomové práce: **Ochrana proti reverznímu inženýrství zaměřeného na software běžící pod operačním systémem Android**

Hodnocení práce:

Cílem diplomové práce bylo popsat problematiku obrany proti reverznímu inženýrství zaměřeného na software běžící pod operačním systémem Android. K jeho dosažení bylo potřeba naplnit několik bodů, jejichž přesná specifikace byla součástí zadání práce.

Vypracovaná diplomová práce je členěná na několik částí na teoretickou a praktickou část, kdy každá z nich má několik dalších kapitol.

Teoretická část obsahuje informace o současném stavu řešené problematiky, kdy na vypracování této rešerše nebylo použito ani jedno literární dílo ze seznamu doporučené literatury, čímž nedošlo ke splnění bodu zadání. Názvy těchto literárních děl jsou uměle přeloženy do českého jazyka. Překlad těchto názvů působí nepřírozeně, jak kdyby bylo využito strojového překladu slovo od slova. V názvu kapitoly 1.2 nedošlo k překladu slova for do češtiny.

Následují kapitoly obsahující informace o architektuře systému Android. Je zde popsáno jádro, nativní vrstva a aplikační rámec. Tento popis by mohl být obsáhlejší, nejsou zde např. informace o bezpečnostních mechanismech Androidu, včetně oprávnění, které je následně zmiňováno v praktické části. Popis je doplněn několika obrázky, které jsou pravděpodobně stažené z internetu a nejsou, jakkoliv ozdrojované. Následuje popis aplikačního prostředí.

V dalších kapitolách jsou dobře popsány techniky manipulace apk souboru, obfuskace kódu a obrana proti dynamické analýze.

Pro splnění druhého bodu zadání bylo nutné provést analýzu současných nástrojů a postupů, které se používají pro ochranu Android aplikací. V diplomové práci bylo zběžně popsáno sedm nástrojů, bez jakýchkoliv doplňujících obrázků a podrobnějšího vysvětlení prostředí a jejich možností.

Praktická část obsahuje analýzu pěti aplikací. Jsou zde uvedena celá jména aplikací. Pro potřeby diplomové práce by bylo lepší anonymizovat jednotlivé názvy. Dále je uvedeno, jaké byly použity nástroje pro analýzu. Následuje popis jednotlivých aplikací, důvod jejich výběru a analýza. Samotná analýza neobsahuje mnoho relevantních informací, pouze u některých aplikací je uvedeno, jaká oprávnění systému Android aplikace vyžaduje a dále jsou uvedeny statistické informace jako počet DEX souborů, případný odhad, jaký nástroj mohl být použitý pro obfuskaci kódu. Chybí přehledná tabulka, která by ukázala rozdíly v analýzách jednotlivých aplikací.

V další části je popsána vytvořená aplikace s názvem ValidatorTest. Následuje popis analýzy a jednotlivé varianty jsou zběžně popsány. Chybí přehledová tabulka s přehledným shrnutím jednotlivých použitých metod. Následuje krátké zhodnocení a závěr. Na základě předchozí analýzy vybraných mobilních aplikací nedošlo k navržení metodiky ochrany proti reverznímu inženýrství. Tím nedošlo ke splnění bodu zadání.

V textu je možné nalézt mnoho překlepů a došlo i k vynechání několika slov. V některých případech nedává věta smysl. Celá diplomová práce obsahuje pouze čtyři doprovodné obrázky,

u kterých není uvedený zdroj. Z toho je zřejmé, že této diplomové práci nebylo věnováno dostatek času.

Nedošlo ke splnění všech bodů zadání, a proto nelze tuto práci doporučit k obhajobě.

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 nedoporučuji k obhajobě a navrhuji hodnocení
F - nedostatečně.**

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

Datum 21.5.2024

Podpis oponenta diplomové práce