Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Šimo Filip** **Oponent:** **Ing. Bibiána Magáthová, PhD.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Informační technologie**
Akademický rok: **2019/2020**

Téma diplomové práce: **Ověření bezpečnosti open source aplikace Signal**

Hodnocení práce:

Predložená diplomová práca svojou témou aktuálne reflektuje na súčasné potreby zabezpečenia mobilných zariadení a ich aplikácií voči útokom. Denne sú medializované informácie o zneužití mobilného zariadenia rôznymi sofistikovanými útokmi, o ktorých vlastník zariadenia nemá ani tušenia. Aplikácia Signál je laickou verejnosťou považovaná za bezpečnú, preto je často využívaná. Analýza zdrojového kódu, identifikácia kryptografických algoritmov, zabezpečovacích mechanizmov, prevedenie útokov a návrh riešení na zvýšenie bezpečnosti na mobilných zariadeniach s operačným systémom Android predstavuje komplexné riešenie danej témy, čo hodnotím vysoko pozitívne. Realizáciu praktickej časti práce považujem za pomerne obtiažnu vzhľadom na potrebu nasadenia viacerých nástrojov, ktoré bolo potrebné vhodne nakonfigurovať a upraviť za účelom vykonania útokov.

Ako som už uviedla, diplomant pristúpil k riešeniu témy komplexne, oceňujem výber spôsobu vykonania útoku, nakoľko modifikácia a rekompilácia zdrojového kódu predstavuje relatívne sofistikované prevedenie útoku vzhľadom na zachovanie všetkých užívateľsky využívaných funkcionalít pôvodnej aplikácie. Rovnako pozitívne hodnotím zámer diplomanta poskytnúť užívateľovi návod na lepšie zabezpečenie svojho mobilného zariadenia.

Diplomová práca v teoretickej časti obsahuje popis operačného systému Android so zameraním na bezpečnostné funkcie, popisuje aplikáciu Signal a jej analýzu zdrojového kódu, ktorou sa identifikovali použité kryptografické algoritmy a iné zabezpečovacie mechanizmy. Praktická časť práce prehľadne a detailne popisuje prípravu a spôsob vykonania útoku na aplikáciu.

Hlavným prínosom práce je praktická ukážka útoku na moderné mobilné zariadenia postavené na báze operačného systému Android. Vysoko pozitívne hodnotím aj popis navrhovaných riešení, ktoré majú reálny prínos v prostredí podnikových informačných sietí obsahujúcich čoraz väčšie počty pripojených súkromných mobilných zariadení.

Predložená diplomová práca obsahuje po formálnej stránke všetky potrebné náležitosti, je písaná v zmysle pravidiel pravopisu až na občasný nesprávny slovosled, respektíve nesprávne skloňovanie. Pomerné rozdelenie práce medzi teoretický opis a praktickú časť je vyvážené, s dostatočným zameraním sa na vlastnú prácu diplomanta.

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Formulované otázky neznižujú celkovú úroveň práce diplomanta a dosiahnuté výsledky. Diplomant v predloženej práci dostatočne preukázal predpoklady pre samostatnú inžiniersku činnosť. Na základe uvedeného odporúčam diplomovú prácu k obhajobe.

K diplomovej práci mám nasledovné pripomienky, respektíve otázky:

- Útok na aplikáciu Signal bol vykonaný iba na virtuálnom zariadení v prostredí Android studio, alebo aj na reálnom fyzickom zariadení?
- Akým spôsobom bola inštalovaná upravená aplikácia popísaná v kapitole 12 do zariadenia? Bol potrebný priamy prenos na USB médiu, alebo bolo možné modifikovanú aplikáciu zaslať aj vzdialene?
- V kapitole 13.1.2. je spomínaná hĺbková podpora Samsung KNOX; existuje výrazný rozdiel v možnostiach zabezpečenia operačného systému Android od rôznych výrobcov?
- Niektoré obrázky v diplomovej práci obsahujúce iba logá považujem zbytočné.

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 10. 8. 2020

Podpis oponenta diplomové práce