Review of Master's Thesis

Student: Zuzelka Jozef, Bc.
Title: Control of External Devices on macOS to Prevent Data Leaks (id 22637)
Reviewer: Veselý Vladimír, Ing., Ph.D., DIFS FIT BUT

1. Assignment complexity — **considerably demanding assignment**

Zadání je propojeno s potřebami firmy Safetica, ve které student působí. Cílem bylo analyzovat stávající způsoby řízení přisupu k souborům a USB připojeným médiím v intencích operačního systému macOS. Vzhledem ke komplexnosti použitých technologií (tj. macOS kernel, jeho drivery a rozhraní/kity pro user-space aplikace) a jejich proprietárního charakteru se jedná o značně obtížné zadání.

2. Completeness of assignment requirements — **assignment fulfilled**

Zadání bylo splněno.

3. Length of technical report — **exceeds requirements**

Práce má 73 stran textu v husté LaTeXové šablonce, 96 stran i s pomocnými provozy. V rámci na fakultě vzniklého počítadla http://standardpages.herokuapp.com/standardpages/ má 121.65 stran, 99% textu a 1% obrázků.
Dle výše uvedeného tedy přesahuje obvyklé rozmezí pro diplomové práce.

4. Presentation level of technical report — **60 p. (D)**

Práce je logicky strukturovaná a její (pod)kapitoly odrážejí body zadání. Nicméně obsahově je značně nevyvážená - majoritu práce tvoří související teorie, minoritu pak popis implementace a testování. Po vyčerpávající teorii by znalý čtenář očekával neméně detailně a kvalitně zpracovanou praktickou část; toto očekávání však není naplněno.

5. Formal aspects of technical report — **70 p. (C)**

Práce je psaná v angličtině bez význačnějších prohřešků vůči gramatice (sem tam interpunkční znaménko) či typografii (osobně bych výskyty *chapter* či *section* psal vždy s velkým prvním písmenkem; taktéž se v práci vyskytuje československý a nikoli anglický způsob zápisu čísel - bez oddělovače řádů a desetinná čárka místo tečky). Student zvolil zajímavé formátování poznámek pod čarou, kde některé hyperetextové odkazy jsou bezproporčním (jen čistá URL) a jiné zase proporčním písmem (ty odkazující na internetový archiv), který však na tištěném papíře postrádá smysl.

6. Literature usage — **55 p. (E)**

Práce obsahuje excesivní množství bibliografických pramenů. Tyto s tématem souvisí, nicméně některé z nich by se daly konvertovat jen na poznámky pod čarou (obzvláště ty poukazující na GitHubové repozitáře nějaké technologie) a jiné zase sloučit dohromady (např. vybrané zdroje z http://developer.apple.com). Ovšem při čtení teoretické části jsem narazil na několik pasáží, které byly jen převyprávěním obsahu hesla Wikipedie (sekce 2.2: https://en.wikipedia.org/wiki/Classic_Mac_OS v bibliografii není) a nebo převzaté z konferenční prezentace (druhý odstavec čtvrté kapitoly: https://asciiwwdc.com/2019/sessions/702 v bibliografii sice je, ale na jiném místě) bez toho, aniž by byly na patřičném místě odcitovány. Při následné diskuzi student připustil, že i Wikipedie byla jedním z mnoha zdrojů, ze kterých čerpal, a litoval, že při práci s všemi těmi citovanými zdroji nebyl pečlivější a důslednější. Osobně jsem měl při čtení teorie několikráte pocit, že čtu myšlenky a teze od několika různých osob, což může naznačovat překotnou integraci ze zdrojů bez dostatečného a dostačujícího přefrázování.

7. Implementation results — **90 p. (A)**

Realizační výstup představuje několik jednotek souborů psaných v jazycích C++ a Objective-C, které využívají DiskArbitration a Endpoint Security frameworky. Zdrojové kódy jsou čitelné a jsou v nich použity vhodné návrhové vzory.

8. Utilizability of results

Prototypová implementace data-loss prevention řešení pro platformu macOS je funkční a naplňuje vytyčené use-case použití, které omezují přístup k souborům na USB disky a cloudové sdílecí služby. Vzhledem k studentově aktuálnímu pracovnímu působení se dá očekávat, že firma jeho know-how nabyté v rámci diplomové práce zúročí při budoucím rozšiřování funkcionality svého produktového portfolia.

9. Questions for defence

- Vysvětlete aktuální dopad potenciálního využití symlinků k obcházení Vaší současné implementace; diskutujte potenciální řešení tohoto problému.
- V příloze B je zmíněna operace "Exchange data", která však není vyhodnocena. Okomentujte to, prosím.

10. Total assessment

69 p. satisfactory (D)

Aktuální práci hodnotím na pomezí stupně C a D. Jedná se skutečně o těžké zadání, kde už samotné nastudování problematiky je nelehký úkol vzhledem k dostupnosti a aktuálnosti zdrojů k proprietárnímu operačnímu systému. Záběr teoretické části je enormní, kazí jej však špatná práce s literaturou a prezentační úroveň. Implementační prototyp ukazuje možnosti, kterými se mohou vydat DLP řešení pro platformu macOS. Na jedné straně se studentovi nedá upřít množství úsilí, které do řešení diplomové práce vložil (včetně implementace); na druhé však i přes toto nasazení vykazuje diplomka zbytečné vady, kterým by se měla jakákoli kvalifikační práce vyvarovat (jako např. neadekvátní popis implemntace a testování).

In Brno 29 June 2020

Veselý Vladimír, Ing., Ph.D.
reviewer