FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student: Jaroslav Kříž
Vedoucí: práce: Ing. Josef Kokeš
Název práce: Bezpečnostní analýza Linux Unified Key Setup (LUKS)
Obor: Bezpečnost a informační technologie

Datum vytvoření: 27. 5. 2019

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	*1=zadání splněno,* *2=zadání splněno s menšími výhradami,* ***3=zadání splněno s většími výhradami,*** *4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Komentář:

Předmětem práce je bezpečnostní analýza nástroje LUKS. Ta sice proběhla, v rozporu se zadáním však byla zaměřena poněkud odlišným směrem. V důsledku toho chybí řešení bodů 3 (analýza UI programu za účelem nalezení kandidátů pro bližší analýzu zdrojového kódu) a 4 (analýza vybraných částí zdrojového kódu); bod 3 zde chybí úplně, bod 4 je zastoupen stručnými odkazy na dřívější cizí analýzy. Z mého pohledu přitom právě tyto body tvoří jádro toho, co by bakalářská práce měla demonstrovat, ostatní úkoly jsou výrazně jednodušší.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*70 (C)*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Komentář:

Odhlédneme-li od výhrady z předchozího bodu, je textová část práce vcelku v pořádku. Postupuje systematicky a probírá jednotlivé dílčí komponenty programu. Vítám důkladné vysvětlení antiforenzních stripů jakožto unikátního přínosu programu LUKS. Naopak nejsem příliš spokojen s kapitolou 1, která je poměrně povrchní a nesourodá (např. kapitola 1.1 nedává na daném místě moc smysl, kapitola 1.4.2 by měla být detailnější).

Z faktického hlediska mám výhrady k některým tvrzením: Není pravda, že kaskáda šifrovacích algoritmů je tak silná jako nejsilnější zúčastněný algoritmus (str. 25) - v optimálním případě je kaskáda silná jako složení algoritmů. Doporučení, že bychom měli pravidelně přešifrovávat svazek (str. 42, 43), přinejlepším není podloženo, pokud je vůbec správné (na str. 3 ostatně student tvrdí opak). Chybí mi vysvětlení, co je to iterace master klíče a jak se od ní liší iterace key slotu (str. 23-24, 39-41). U útoků hrubou hrubou silou i pomocí slovníku chybí metodika, jak byl útok proveden, tedy jaké heslo bylo zvoleno, jak byl konstruován slovník, jaký šifrovací algoritmus, hashovací funkce a operační mód byly použity, byl test spouštěn opakovaně pro různé kombinace těchto parametrů? Tabulka rychlosti výpočtu nezdůrazňuje dobře fakt, že zobrazuje prolomení hesla právě dané délky, ne hesla do dané délky včetně, což by bylo pro uživatele užitečnější, a že čísla jsou občas zaokrouhlena až příliš nepřesně (heslo tvořené malými písmeny a číslicemi o délce 5 znaků má uvedenou dobu prolomení 6 dní, ve skutečnosti je to za daných předpokladů 6,9984 dní).

Pozitivem je velmi malý výskyt jazykových chyb a překlepů. Narazil jsem asi na 4 chybné čárky a jedno nebo dvě chybná skloňování, jinak je text v pořádku.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*

3. Nepísemná část, přílohy *65 (D)*

Popis kritéria:
Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce
– opakovatelnost experimentů

Komentář:
Přiložené kódy jsou problematické, z různých hledisek.

Útok hrubou silou používá pro ověření správnosti hesla libcryptsetup. Z hlediska jednoduchosti implementace to chápu, z pohledu ověření bezpečnosti programu už méně - měla by být použita vlastní optimalizovaná implementace, která by lépe simulovala možnosti útočníka, který pochopitelně vyloučí všechny části kódu, které nutně nepotřebuje. V důsledku použití knihovní funkce je uživatel ukolébáván do falešného pocitu bezpečí, že je jeho heslo dostatečně silné, přitom pro krátká hesla může být rozdíl mezi optimalizovanou a neoptimalizovanou variantou až řádový (např. v důsledku opakované inicializace parametrů, které stačilo inicializovat jednou). Tato neefektivita je ostatně vidět i u generování hesla. Kromě toho by aplikace měla být psána s ohledem na bezpečné programování, např. k přetečení bufferu u pole table[] nedochází jen proto, že se toho uživatel díky vysoké hodnotě konstanty MAX_LENGTH nedožije. Kromě toho nevidím, jak může program fungovat pro větší délky hesla než 8 znaků (nebo 4 znaky, pokud byl program zkompilován v 32bitovém módu), protože sizeof(pass) má jinou hodnotu, než si student myslí.

Slovníkový útok využívá aplikaci John the Ripper pro vygenerování slovníku a aplikaci cryptsetup pro ověření hesla, což je v zásadě v pořádku, ale důsledkem je opět velmi pomalý chod. Bylo by lepší naimplementovat generování i ověřování hesel přímo v kódu s vynecháním zbytečných operací (práce s diskem apod.).

Reimplementace šifrovacího kódu se zdá být výrazně lépe napsaná než předchozí části, trpí však velmi slabou dokumentací, takže bez detailního zkoumání není zřejmé, co vlastně dělá. Každopádně mě zarazilo, že je sice podporován argument "--dump-master-key", ale jeho implementace je celá zakomentovaná.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*60 (D)*

Popis kritéria:
Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Komentář:
Výsledkem práce je konstatování, že LUKS dodržuje svoje specifikace, což bylo potvrzeno reimplementací jeho kryptografických funkcí pomocí alternativní šifrovací knihovny. Dále byly srozumitelně popsány některé zajímavé aspekty LUKSu (antiforenzní stripy) a provedeny základní testy odolnosti kontejnerů vůči útoku hrubou silou a slovníkovým útokem. Bohužel absence detailnějšího popisu metodiky snižuje užitečnost těchto informací. Velmi chybí analýza kódu aplikace jako takové.

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: *1=výborná aktivita,* *2=velmi dobrá aktivita,* *3=průměrná aktivita,* ***4=slabší, ale ještě dostatečná aktivita,*** *5=nedostatečná aktivita* 5b: *1=výborná samostatnost,* *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* ***4=slabší, ale ještě dostatečná samostatnost,*** *5=nedostatečná samostatnost*

Popis kritéria:
V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:
Student měl velkou tendenci závěrečnou práci odkládat, jak ve fázi projektu (kdy důsledkem bylo zadání obsahující body, které se následně ukázaly jako nad studentovy časové možnosti), tak ve fázi vlastního zpracování. Zároveň se ukazuje, že by potřeboval mnohem striktnější vedení a směrování, jinak příliš rychle opouští oblasti, které by měl zkoumat důkladněji, a zaměřuje se na oblasti méně podstatné.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*59 (E)*

Popis kritéria:
Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

Text hodnocení:
Práce se na pohled zdá být v pořádku, ale bohužel dílčí chyby jak v textové části, tak v implementaci, vzbuzují pochybnosti o důvěryhodnosti dosažených závěrů. Velmi mi také chybí provedení analýzy kódu programu ze zadání. Práce je i přesto obhajitelná, protože student vyvinul netriviální úsilí a řadu požadavků splnil, čímž přes všechny výhrady dokázal schopnost samostatné práce, přesto se nemohu ubránit jistému zklamání, že potenciál jak zadání, tak studenta zůstal nenaplněn. Hodnotím známkou E-dostatečně.

Podpis vedoucího práce: