FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Vít Souček
Vedoucí: práce:	Ing. Filip Štěpánek
Název práce:	Využití zranitelnosti Janus na operačním systému Android
Obor:	Počítačová bezpečnost

Datum vytvoření: 7. 6. 2020

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:
Zadání ZP bylo splněno. Výstupem je funkční implementace útoku pro mobilní zařízení s OS Android.

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

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:
Textová část ZP splňuje obsahově a velikostně náležitosti magisterské ZP. Text rozebírá aktuální dopad zranitelnosti Janus na zařízení s OS Android, zmiňuje útoky, které byly provedeny v minulosti a postup, jak zranitelnost využít a vzdáleně odposlouchávat oběť a jaké možnosti má útočník v rámci distribuce útoku a následného příjmu spojení se zvukovým obsahem. Součástí je i diskuze nad možnostmi obrany.
V rámci analytické části student rozebírá jednotlivé mechanismy OS Android, které ať už svojí zranitelností či robustností ovlivňují plánování útoku (například podpisové schéma OS Android). Návrh útoku řeší možnosti útočníka -- distribuci škodlivého kódu, vytvoření škodlivého instalačního balíčku (APK) a možnosti útočníka v rámci přijímání spojení a jejich správu. V rámci sekce "Volba cíle útoku" a dalších navazujicích částí mi přišla zajímavá diskuze nad tím, jak jednotliví výrobci mobilních telefonů spravují procesy na pozadí oproti oficiálním specifikacím OS Android a jak tato činnost ovlivňuje chování útočníka a jeho útok. Realizace se zabývá konkrétní implementací útoku a jeho jednotlivých částí a modulů. Zmíněny jsou Open Source aplikace, které byly využity při realizaci útoku a nutné úpravy za použití jazyka Smali (asembler pro Dalvik bytekod). Kapitola testování přímočaře popisuje výsledky testů -- zde bych zmínil i zajímavou část o tom, jak si s detekcí škodlivé aplikace poradí moderní antivirové programy.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*100 (A)*

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:
Vzhledem k stávající situaci jsem výsledky práce kontroloval vzdáleně -- od studenta jsem si nechal připravit sadu videí, na kterých byl útok demonstrován na fyzických zařízeních. Útok je možné aplikovat na reálná zařízení s minimálními změnami (IP adresa útočníka či jeho proxy serveru pro příjem spojení). S výsledky práce jsem plně spokojen.

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

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:

Výstupem je funkční a otestovaný prototyp útoku využívající zranitelnosti Janus (CVE-2017-13156). Samotný útok se skládá z více modulů/aplikací:
1.) Aplikace pro server útočníka, na kterém se v režimu příkazové řádky monitorují a spravují příchozí spojení ze zařízení potenciálních obětí. Spojení je možné poslouchat, přepínat a ukládat
2.) Aplikace pro mobilní telefon, která má za cíl odposlouchávat. Tato aplikace je jádrem škodlivého kódu, které se později vloží do legitimní aplikace a běží na pozadí v zařízení oběti
3.) Aplikace, která využije zranitelnosti a spojí škodlivou aplikaci z předchozího bodu s legitimní aplikací (v rámci ZP se jedná o dostupné Open Source aplikace). Výstupem pak je APK soubor, který cílí na potenciální oběť

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 pracoval zcela samostatně a pravidelně mě informoval o svém počínání. Průběžně prezentoval výsledky své práce, diskutoval problémy a možný další směr implementace.

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

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:

S výsledky textové i implementační části ZP jsem plně spokojen. Výstupem je funkční prototyp útoku cílící na vzdálené odposlouchávání jednoho či většího množstv mobilních telefonů s OS Android. Student pracoval během řešení ZP zcela samostatně a průběžně mě informoval o aktuálním stavu práce. Výsledný text může být pro nezasvěceného čtenáře složitější, ale i tak jsou vysvětleny všechny důležité pojmy a funkce OS Android, které je třeba vzít v úvahu k naplánování a implementování útoku využívajícího zranitelnost Janus (CVE-2017-13156). Součástí textu je diskuze nad možnostmi obrany, záplatování i popis mechanismů, které zabraňují zneužití na nejnovějších verzích operačního systému.

Práci hodnotím stupněm A a doporučuji k obhajobě.

Podpis vedoucího práce: