OPONENTNÍ POSUDEK DOKTORSKÉ DISERTAČNÍ PRÁCE

Téma disertační práce:	Bezpečnostní chyby na mobilní platformě, jejich zneužívání a návrh proaktivního opatření s využitím umělé inteligence
Vypracováno na pracovišti:	Ústav informatiky a umělé inteligence, FAI UTB
Studijní obor:	Informační technologie
Autor práce:	Ing. Milan Oulehla
Školitel:	doc. Ing. Zuzana Komínková Oplatková, Ph.D.
Odborný konzultant:	Ing. David Malaník, Ph.D.
Oponent:	prof. Ing. Petr Dostál, CSc.

Aktuálnost tématu disertační práce

Předložená disertační práce je věnována významné oblasti informační bezpečnosti. Zdůvodnění se věnuje autor v kapitolách 1.1 Úvod do problematiky a 2.1 Aktuální stav v oblasti bezpečnosti mobilních aplikací. Obzvláště názorně je významnost a aktuálnost tématu doložena na obr. 1.1, Podíl mobilních zařízení na webovém provozu na obr. 2.1 a obr. 2.2, který představuje nárůst počtu mobilních aplikací a publikovaných zranitelností v klíčových databázích. Téma práce je aktuální i z pohledu způsobu jejího řešení a to za použití metod etického hackingu, reverzního inženýrství a pokročilých metod strojového učení (umělé inteligence) v úzké spolupráce s aplikovanou praxí představovanou firmou AVG Technologies. Téma dizertační práce hodnotím jako velmi aktuální.

Splnění stanovených výzkumných cílů v disertační práci

Cíle disertační práce jsou stanoveny a velmi podrobně rozpracovány v kapitolách 3.1 - 3.3. Jde o tyto cíle: Popis závažných bezpečnostních chyb současných mobilních aplikací, Popis útočných mechanismů mobilního malwaru, Navržení mechanismu detekce mobilního malwaru pomocí umělé inteligence, především neuronových sítí. Cílem disertační práce ovšem nemůže být "Popis", uvedený termín je v tomto případě velmi zavádějící. Přes tento uvedený nedostatek v názvu konstatuji splnění cílů v jejich deklarovaném analytickém rozsahu. Klíčovým momentem v řešení je vnímání mechanismů z pohledu útočníka. Uvedený postup reverzní analýzy je unikátní a je rozpracován v kapitole 4. Zejména významnou hodnotím kapitolu 4.3 Ruční dynamická analýza, 4.4 Ruční statická analýza a 4.5 Automatizované metody vyšetřování. Dále kapitola 4.6 pojednává o nalezených zranitelnostech v rámci výzkumu. Detailní analýza architektury mobilního malware je popsána v kapitole 5. Detekce mobilního malaware pomocí umělé inteligence je zpracována v kapitole 6. Tato kapitola dle mého názoru představuje hlavní cíl celé práce. Otázkou je, zda detekce pomocí neuronových sítí, tak jak je v práci představena, je optimální způsob využití strojového učení a umělé inteligence. Uvedené by mohlo být cílem dalšího výzkumu.

Metody použité při vypracování disertační práce

Metody použité v práci jsou primárně analyticko-syntetického charakteru. Jako celek působí použitá vědecko-výzkumná metoda doplněná reverzním inženýrstvím jako dostatečná a v úzkém kontaktu na praxi. Postup řešení a zvolená metoda je vhodná a velmi dobře použitelná pro tento typ práce.

Postup řešení problému, výsledky disertační práce a konkrétní přínos práce doktoranda
Komplexní bezpečnostní výzkum popsaný v dizertační práci byl zaměřen na nalezení závažných bezpečnostních chyb současných mobilních aplikací, analýzu mobilního malwaru a návrh a experimentální ověření nového způsobu detekce mobilního malwaru pomocí umělé inteligence. V každé z těchto oblastí byly vytvořeny výstupy, které mohou pomoci nejen v navazujícím vědeckém bádání, ale mohou být přínosné pro technickou praxi. Nejvýznamnějšími přínosy pro vědu a praxi, kterých bylo v dizertační práci dosaženo je návrh a experimentální ověření mechanismu detekce mobilního malwaru pomocí metod umělé inteligence, především pomocí neuronových sítí. Detekce vzorků malwaru a legitimních aplikací měly přesnost při trénování - 99,5 % a přesnost při testování - 98,23 % (str. 320, kap. 7 Přínos pro vědu a praxi).

Význam pro praxi a pro rozvoj vědního oboru
Práce je zpracována formou, kdy výstupy jsou velmi dobře přenositelné do bezpečnostní praxe expertů penetračních laboratoří a analytiků antivirových společností. V uvedené oblasti je práce velkým přínosem a umožňuje provést transfer získaných poznatků do předmětů oborů řešících problematiku softwarového inženýrství, zejména pak pro specializace zaměřené na kybernetickou bezpečnost. Význam pro vědní obor je v navržení detekce mobilního malwaru pomocí neuronových sítí.

Formální úprava a jazyková úroveň disertační práce
Jazyková úroveň práce je na velmi dobré úrovni a i přes její velký rozsah je přehledná a srozumitelná. Po formální i stylistické stránce splňuje požadavky na doktorskou disertační práci.

Publikační a další vědecko-výzkumná činnost doktoranda
Publikační činnost doktoranda prokazuje jeho odbornost a je dostatečná. Unikátnost a originalitu jeho tvůrčí práce vedle recenzovaných zahraničních časopisů podtrhuje účast na podání celosvětové patentové přihlášky spojené s tématem bezpečnosti citlivých dat. Propojení vědecko-výzkumné práce s praxí prokazuje také jeho výzkumné působení v Laboratoři penetračních testů Ústavu informatiky a umělé inteligence. Jako velmi cenný výstup pro praxi hodnotím na str. 319 uvedený tutoriál v časopise "Hakin9 - IT security magazine" s názvem "Hidden APK" patřící mezi 20 nejlepších odborných tutoriálů tohoto odborného světového časopisu v letech 2016 -17.

Dotazy k obhajobě
Provádíte filtraci dat, abyste zvýšil detekční schopnosti neuronové sítě. Pokud se ve vzoru odfiltrovaná data vyskytnou, znamená to, že je nebude možné detekovat?
Používáte jednoduchou neuronovou síť. Proč jste nepoužil hlubokého strojového učení (deep learning) vzhledem ke složitosti řešeného problému?

Závěrečné vyjádření
Práci doporučuji k obhajobě a po jejím úspěšném obhájení udělit jmenovanému titul Ph.D. v příslušném oboru.

Ve Brně dne:

prof. Ing. Petr Dostál, CSc.

Kontaktní informace:
prof. Ing. Petr Dostál, CSc., https://www.vutbr.cz/lide/petr-dostal-27610

OPONENTNÍ POSUDEK DOKTORSKÉ DISERTAČNÍ PRÁCE

Téma disertační práce:	Bezpečnostní chyby na mobilní platformě, jejich zneužívání a návrh proaktivního opatření s využitím umělé inteligence
Vypracováno na pracovišti:	Ústav informatiky a umělé inteligence, FAI UTB
Studijní obor:	Informační technologie
Autor práce:	Ing. Milan Oulehla
Školitel:	doc. Ing. Zuzana Komínková Oplatková, Ph.D.
Odborný konzultant:	Ing. David Malaník, Ph.D.
Oponent:	prof. Ing. Jiří Dvořák, DrSc., profesor technické kybernetiky

Aktuálnost tématu disertační práce

Předložená disertační práce je věnována trvale významné oblasti informační bezpečnosti. Hledání a nalézání chyb vědecko výzkumnou metodou, pojmenování bezpečnostního rizika a pohled na problematiku z různých úhlů jen podtrhují unikátnost řešení výzkumného tématu. Na základě výše uvedeného práci hodnotím jako aktuální a velmi významnou.

Splnění stanovených výzkumných cílů v disertační práci

V práci byly definovány tři klíčové cíle - oblasti: nalezení bezpečnostních chyb aktuálních mobilních aplikací, analýza mobilního malwaru a detekce mobilního malwaru pomocí strojového učení a umělé inteligence. Všechny cíle byly v práci detailně a srozumitelně popsány a vhodnou formou vyřešeny. Vzhledem k současné úrovni poznání lze jednoznačně konstatovat, že cíle byly splněny.

Metody použité při vypracování disertační práce

Práce byla systémově řešena více vědecko výzkumnými metodami. Jako klíčová, byla dle mého názoru aplikována metoda analytická. Její aplikace při získávání vzorků mobilního malware, reverzní analýze aplikačního protokolu, experimenty s mobilními botnety prokázaly vhodnost použití této metody. Postupy použité v práci odpovídají tématu práce a jednoznačně prokazují vysokou odbornou úroveň doktoranda teoreticky vědecky pracovat a získané výsledky konfrontovat s požadavky praxe.

Kontaktní informace:
prof. Ing. Jiří Dvořák, DrSc., https://www.vutbr.cz/en/people/jiri-dvorak-497

Postup řešení problému, výsledky disertační práce a konkrétní přínos práce doktoranda

Postup řešení celé práce, vědecko výzkumného projektu, je analyticko syntetický. Svým obsahem, rozsahem (354 stran), jde o mimořádně velké a ucelené dílo, prokazující kompetenční potenciál autora, jeho odbornou erudici a aplikační schopnosti. Výsledky disertační práce jsou propojeny s výzkumnými požadavky praxe (doloženo sdílením testovacích a výzkumných databází s AVG Technologies CZ). Přínos práce doktoranda je nejen v komplexnosti analýzy, ale hlavně ve vlastním návrhu a experimentálním ověření mechanismu detekce mobilního malware pomocí metod umělé inteligence, neuronových sítí. V disertační práci jsou představeny a vysvětleny desítky původních, vlastních autorských schémat a obrázků. Rozsah a kvalita jejich prezentace jsou na velmi vysoké úrovni.

Význam pro praxi a pro rozvoj vědního oboru

Význam práce pro rozvoj vědního oboru a praxi je v oblasti komplexního a systémového přístupu k řešení tématu práce, zejména návrhu a aplikaci detekce škodlivého kódu pomocí strojového učení a neuronových sítí. Z pohledu významu pro praxi vysoce oceňuji použití metody ruční dynamické analýzy spojené s metodikou testování neošetřených výjimek aplikace. Přínosem je také návrh proaktivních opatření spojených s využitím algebry oprávnění. Vše výše uvedené také ukazuje, jakými směry by bylo možné v dalším výzkumu oblasti bezpečnosti mobilních aplikací pokračovat.

Formální úprava a jazyková úroveň disertační práce

Práce je psána spisovným českým jazykem a i přes velký rozsah je přehledná, srozumitelná, kapitoly na sebe logicky navazují, text je prostý chyb a formálně splňuje vysoké nároky na doktorskou disertační práci.

Publikační a další vědecko výzkumná činnost doktoranda

Publikační činnost doktoranda je dostatečně obsáhlá, původní a na vysoké odborné úrovni. Zdůrazňuji a vysoce oceňuji podání celosvětové patentové přihlášky spojené s operacemi nad citlivými daty. Jako velmi cenný a mnou vybraný zdůrazněný výstup pro dopady v praxi reverzního inženýrství hodnotím jeho tutoriál v profesionály kybernetické bezpečnosti uznávaném celosvětovém technologickém časopise "Hakin9" (práce Ing. Oulehly s názvem "Hidden APK" byla zveřejněna jako jedna z 20 nejlepších odborných tutoriálů v uvedené oblasti v roce 2018).

Dotazy k obhajobě

Práce je velmi komplexně a hluboce pojata, v plně systémových a technologicko kybernetických souvislostech. Kladu tyto otázky:

- Byla použitá profesionální datová sada AVG Technologies CZ jedinou dostupnou učící/testovací sadou? Pokud ano, nebyly by dosažené výsledky při použití více rozdílných datových sad při učení neuronové sítě úspěšnější?
- Budou výsledky vaší práce využity ve vašem dalším výzkumu a praxi na pracovišti PTLAB Fakulty aplikované informatiky UTB ve Zlíně?

Závěrečné vyjádření

Předkládanou práci doporučuji k obhajobě před příslušnou komisí a po jejím úspěšném obhájení udělit jmenovanému titul Ph.D. v doktorském studijním programu Informační technologie.

Vzhledem k vysoké odbornosti, unikátnosti celkového řešení a mimořádnému přínosu pro vědu i praxi doporučuji tuto práci nominovat na Cenu Siemens v roce 2020.

Ve Zlíně dne: .....

prof. Ing. Jiří Dvořák, DrSc.

Kontaktní informace:
prof. Ing. Jiří Dvořák, DrSc., https://www.vutbr.cz/en/people/jiri-dvorak-497

OPONENTNÍ POSUDEK DOKTORSKÉ DISERTAČNÍ PRÁCE

Téma disertační práce:	Bezpečnostní chyby na mobilní platformě, jejich zneužívání a návrh proaktivního opatření s využitím umělé inteligence
Vypracováno na pracovišti:	Ústav informatiky a umělé inteligence
Studijní obor:	Informační technologie
Autor práce:	Ing. Milan Oulehla
Školitel:	doc. Ing. Zuzana Komínková Oplatková, Ph.D.
Konzultant:	Ing. David Malaník, Ph.D.
Oponent:	doc. Ing. Petr Hrůza, Ph.D.

Aktuálnost tématu disertační práce

Předložená disertační práce se zabývá problematikou bezpečnosti mobilní platformy, která je v současné době z bezpečnostního hlediska značně specifická. Mobilní platforma, stejně jako otázky jejího zabezpečení, jsou v kontextu kybernetické bezpečnosti poměrně novým fenoménem, projevujícím se nižším stavem poznání než je tomu v jiných příbuzných oblastech, například jakou je problematika zabezpečení osobních počítačů, serverů či počítačových sítí. Z výše uvedeného vyplývá nutnost řešit návrhy adekvátních bezpečnostních mechanismů respektující specifika mobilní platformy, stejně jako nutnost jejich průmyslové standardizace. Tyto kroky není ovšem možné provést bez rozsáhlého vědeckého výzkumu. V kontextu výše uvedených skutečností hodnotím nejen téma, ale především rozsáhlost a systematické zpracování disertační práce jako **vysoce aktuální a přínosné** s potenciálem přispět k navržení nových bezpečnostních metodik, norem či standardů.

Splnění stanovených cílů v disertační práci

Výzkumné cíle jsou v disertační práci definovány v kapitole 3 a jsou rozděleny do tří hlavních témat: bezpečnostní chyby současných mobilních aplikací, útočné mechanismy mobilního malwaru a detekce mobilního malwaru pomocí umělé inteligence. Každý z výše uvedených cílů má dílčí podcíle, jejich struktura vyplývá z povahy daného cíle. Výzkumné cíle jsou velmi rozsáhlé a systematicky pokrývají celý rozsah dané problematiky (od bezpečnostních chyb mobilních aplikací, před mobilní malware, který je zneužívá, až po způsoby jeho detekce). Uvedená skutečnost má zásadní vliv na výslednou podobu disertační práce. Bezpečnost mobilní platformy je mladým oborem, což se mimo jiné projevuje nižší mírou dosud publikovaných poznatků. Proto oceňuji způsob, jakým autor disertační práce přistoupil k řešení daného problému. Neboť tento způsob vyžadoval provedení velkého množství zkoumání, analýz a experimentů. **V kontextu těchto skutečností shledávám všechny cíle, jakož i jejich dílčí podcíle splněné v plném rozsahu.** Předložená disertační práce má vysokou úroveň nových poznatků.

Metody použité při vypracování disertační práce

V disertační práci bylo použito větší množství výzkumných metod, což je dáno povahou a rozsáhlostí řešené problematiky. Velmi důležité a vhodné bylo použití metod dynamické a statické analýzy společně s metodami reverzního inženýrství neboť autorovi umožnily odhalení celé řady závažných bezpečnostních hrozeb ve zkoumaných mobilních aplikací. Uvedené metody rovněž pomohly odhalit útočné mechanismy současného mobilního malwaru. Pro oblast zkoumání vlastností mobilního malwaru byly rovněž významné experimenty, které autor při psaní práce provedl. V části disertační práce zabývající se detekcí mobilního malwaru byly použity metody datové analýzy a klasifikační metody založené na umělé inteligenci, především pak na neuronových sítích. Použití všech výše uvedených výzkumných metod shledávám jako adekvátní a vhodné pro bádání v dané oblasti. **Celkově mohu konstatovat, že použité metody jak svým rozsahem, tak i jejich vhodným použitím v disertační práci dávají výsledkům vysokou relevanci.**

Postup řešení problému, výsledky disertační práce a konkrétní přínos práce doktoranda

Popsaný postup řešení daného problému je v disertační práci unikátní hned z několika důvodů, z nichž nejdůležitější jsou: rozsah a kvalita provedených výzkumů, systematické uchopení problematiky a rozsah publikovaných výsledků. Z výše uvedeného je patrné, že autor ve své disertační práci shrnuje mnohaletý výzkum, který vyžadoval nejen velkou časovou dotaci, ale především vysokou odbornou erudici. Z výsledků je rovněž zřejmé, že autor disertační práce často čelil problémům, pro které nenašel oporu v odborných pramenech. To vyžadovalo kromě velkého množství provedených experimentů a testů i schopnost analytického pohledu a tvůrčího uchopení problematiky. Z kontextu soudobé odborné literatury se jako důležitý jeví oddíl 5.1.2 Vyšetřovací metody získaných vzorků mobilního malwaru, ve kterém autor provádí rozsáhlou analýzu vzorku malwaru a používá techniku restaurování zdrojových kódů poškozených dekompilačním procesem. Dekomplikační procesy jsou obecně problematické a není možné se na takto získané zdrojové kódy stoprocentně spolehnout. Proto hodnotím navržené techniky restaurování zdrojových kódů jako velmi přínosné. Dále pozitivně hodnotím skutečnost, že se disertační práce neomezuje pouze na analyticky vedený výzkum, ale přichází s vlastním proaktivním opatřením, kterým je návrh a experimentální ověření nového způsobu detekce mobilního malwaru pomocí umělé inteligence a to především pomocí neuronových sítí. Kvalita a relevance publikovaných detekční výsledků je rovněž kladně ovlivněna rozsáhlou profesionální datovou sadou společnosti AVG Technologies CZ, se kterou (jak autor ve své práci uvádí) měl možnost pracovat.

Význam pro praxi a pro rozvoj vědního oboru

Význam práce pro rozvoj vědního oboru a praxi je v oblasti **systémového přístupu** k řešení tématu práce.

Výsledky publikované v předložené disertační práci jsou přínosné zejména pro:

- odborníky z řad akademické obce,
- experty a společnosti zabývající se informační bezpečností, zejména pak bezpečností mobilní platformy,
- forenzní a penetrační laboratoře,
- a v neposlední řadě i pro softwarové společnosti vyvíjející mobilní aplikace.

Pro odborníky z řad akademické obce bude nejzajímavější problematika detekce mobilního malwaru pomocí umělé inteligence. Jako nejvýznamnější považuji dosaženou detekční přesnost, které dosáhla naučená neuronová síť na neznámých vzorcích malwaru (tedy na testovací množině). Pro tento směr výzkumu je klíčové již samotné ověření detekčních schopností neuronových sítí nad rozsáhlou datovou sadou garantované kvality. Nicméně práce přináší i další zajímavé výsledky, jako například experimenty s počty neuronů ve skryté vrstvě a kombinování různých přenosových funkcí ve skryté a výstupní vrstvě. Přínosné jsou také experimenty, které umožnily srovnání přesnosti detekčních výsledků neuronových sítí s dalšími metodami umělé inteligence.

Pro bezpečnostní experty a společnosti zabývající se informační bezpečností, zejména pak bezpečností mobilní platformy, shledávám stěžejní význam v oddílu 5.2 Charakteristiky mobilního malwaru. Zde autor odhalil celou řadu vzorců chování. Z nichž za nejdůležitější považuji analýzu malwaru typu Hidden APK, která ukazuje dosud nepublikované pokročilé maskovací techniky soudobého mobilního malwaru. Dále to jsou experimenty s mobilními botnety, v nichž se autorovi podařilo potvrdit hypotézu o nedostatečné statické analýze Google Play.

Pro forenzní a penetrační laboratoře, ale i pro softwarové společnosti vyvíjející mobilní aplikace, je nejpřínosnější oddíl 4.6 Zranitelnosti ve vyšetřovaných mobilních aplikacích. Zde autor práce popisuje celou řadu dosud nepublikovaných závažných bezpečnostních hrozeb. Forenzní a penetrační laboratoře mohou tyto výsledky zahrnout do svých testovacích metodik. Společnosti zabývající se vývojem mobilních aplikací mohou získané poznatky využít pro revizi či tvorbu svých metodických pokynů týkajících se otázek zabezpečení.

Rovněž oceňuji skutečnosti, že obsah práce není pouze teoretický, ale přináší celou řadu konkrétních postupů či vylepšení. Jako příklad lze zmínit doporučení pro vytváření dynamických testů popsané v oddíle 4.3 Ruční dynamická analýza.

Formální úprava a jazyková úroveň disertační práce

Práce je psána v českém jazyce, který má spisovnou formu a zároveň splňuje nároky kladené na vědecké publikace. Navzdory skutečnosti, že je práce rozsáhlá, její členění je přehledné a struktura má celistvý charakter. Řazení jednotlivých kapitol je koncepční, kdy poznatky předchozí kapitoly podporují kapitolu následující. Celkově lze říci, že předložený text splňuje všechny formální a jazykové nároky kladené na doktorskou disertační práci.

Publikační a další vědecko výzkumná činnost doktoranda

Předložená publikační činnost autora odpovídá požadavkům kladených na studenty doktorských studijních programů, dokonce tyto požadavky převyšuje. Autor publikoval své výsledky ve dvou časopisech a na devíti konferencích. Obzvláště oceňuji podání mezinárodní patentové přihlášky „Identity and License Verification System for Working with Highly Sensitive Data" a stejně také článek Hidden APK.

Dotazy k obhajobě

Závěrem mohu konstatovat, že předložená disertační práce splňuje po faktické i formální stránce požadavky kladené na disertační práci, obsahuje nové, zajímavé a prakticky využitelné výsledky, které autor publikoval v časopisech a na konferencích. Především oceňuji, že výsledky disertační práce přispěly k podání mezinárodní patentové přihlášky.

Při obhajobě disertační práce požaduji reakci studenta na následující problémy:

1. V práci popisujete útoky založené na modifikaci nízko úrovňového jazyka Smali. Uvedený jazyk je určen pro stroje, nikoliv pro programátory. To znamená, že jeho analýza a vytváření kódů jsou velmi náročné a zdlouhavé. Můžete říci, jak jste se zrovna s touto problematikou při řešení disertační práce vypořádal a zda ve své práci přinášíte postupy či vylepšení, které jsou použitelné v analytické a penetrační praxi?

2. V oddíle 5.2.5 Mobilní botnety – experimenty ukazujete, jak vytvořit malware rezistentní vůči bezpečnostním mechanismům Google Play. Na konci tohoto oddílu je pak pouze krátké upozornění, že bylo útočeno pouze mobilním zařízením, které patřilo Univerzitě Tomáše Bati ve Zlíně. Můžete detailněji popsat opatření, pomocí kterých jste zajistil, že se Vaše útoky vyhnou mobilním zařízením běžných uživatelů, na nichž byl prostřednictvím Google Play nainstalován bót?

3. Ve vaší disertační práci jsou metody umělé inteligence použity k detekci mobilního malwaru. Nicméně umělá inteligence může být atraktivní i pro útočníky a tvůrce mobilního malwaru. Setkal jsem se při svém výzkumu se škodlivým softwarem, který využívá metody umělé inteligence?

Závěrečné vyjádření

Ve smyslu ustanovení § 47 zákona č. 111/1998 Sb. o vysokých školách doporučuji disertační práci Ing. Milana Oulehly k obhajobě před příslušnou komisí a na základě úspěšné obhajoby navrhuji udělit titul philosophiae doctor (Ph.D.) v doktorském studijním programu Informační technologie.

V Brně dne

podplukovník
doc. Ing. Petr HRŮZA, Ph.D.
Proděkan pro studijní
a pedagogickou činnost FVL

Kontaktní informace: