Oponentní posudek doktorské disertační práce

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Obor:Inženýrská informatika

Školitel: doc. Mgr. Roman Jašek, Ph.D

Autor doktorské disertační práce: Ing. Tomáš Výmola

METODY DETEKCE ON-LINE HROZEB VE VIRTUÁLNÍM PROSTŘEDÍ

Aktuálnost tématu doktorské disertační práce

V předkládané disertační práci jsou řešeny velmi aktuální problémy dílčí systémově vymezené bezpečnosti počítačových systémů z pohledu vytvářeného specifického modelu online dynamiky hrozeb ve virtuálním prostředí dnes již moderního a aktuálního pojetí kybernetické války v informační společnosti.

Splnění cíle

Cílem disertační práce byl výběr vhodné identifikace aktuálních hrozeb předpokládaných cílených útoků na konkretní počítačové systémy, jejich možný popis jako modelu hrozeb a modelováním pak vyjádření možného zmenšování předpokládané množiny nebezpečí a také tomu odpovídající omezení vybraných rizik, které hrozí počítačovým systémům ve virtuálním prostředí.

Obsahem širšího zaměření výzkumu v této oblasti identifikace hrozeb je detekce online předpokládaných hrozeb s cílem tvorby modelu respektujícího vývojové tendence v předpokládaných strategiích jak dynamiky hrozeb na jedné straně, tak možných strategií dynamiky bezpečnostních rizik rozsáhlé podnikové sítě informačního a komunikačního prostředí na straně druhé.

Výsledkem uvedeného modelování tohoto dynamického procesu je jistý vymezený návrh modelu řešení metod detekce online hrozeb ve virtuálním prostředí systémově vyjádřené problematiky bezpečnosti počítačových systémů.

Autor správně vymezuje zadaný systém a dekomponuje jej na podsystémy vyjadřující integrovatelné skupiny problémů informační bezpečnosti s množinou detekce předpokladané množiny útoků a detekce možných hrozeb s uvažováním systémového okolí vnímaného kyberprostoru technického a sociálního prostředí. Vymezený prostor dává tak možnost pro jisté vyjádření postupů a výběru nástrojů v oblasti zabezpečení informačního systému a možnosti modelování dílčích úloh v laboratorních podmínkách.

Autor splnil uvedené cíle a popsal je v přehledné hierarchické struktuře této disertační práce. Těmito kapitolami autor naplnil také vhodnou modelovou představu vedoucí ke splnění zadaných cílů.

Postup řešení problému a výsledky disertační práce

Konstrukce autorem přínosného navrhovaného modelu je, že se správně zaměřuje na osvědčený směr známé obecné identifikace systémů (diagnostiky) s tím, že zde vychází z praktických a ověřených metodik a to s citlivým včleněním navrhovaného modelu do složitého hierarchického systému a s uvažováním omezených možností modelování dynamiky jádra řešeného problému detekce on-line hrozeb ve virtuálním prostředí. Uvedený postup řešení problému je náročný, ale také velmi zajímavý a to z pohledu nových možností dnes velmi zneužívaného kyberprostoru ve světě informačních a komunikačních systémů. Autor se zaměřil na využití systémů detekce k vyhledávání aktuálních hrozeb a na používání systémů detekce, které spolehlivě detekují pouze většinu incidentů, ale jsou bohužel neúčinné proti cíleným útokům na konkrétní počítačové systémy.

V úvodní části se autor zabývá možným rozdělením bezpečnostních řešení. Popisuje vybrané hlavní způsoby a přístupy k detekci hrozeb a jejich výhody a nevýhody. Dále se zde správně zabývá detekcí incidentů za využití systému honeypotů a také uznávanou metodikou incidentů. Zaměřuje se správně na Advanced Persistent Threat, rozebírá jednotlivé části incidentů a určuje slabá místa těchto typů útoků.

V praktické části disertace navrhuje autor, na základě uvedeného modelování, dílčí metodiku systému detekce pomocí honeypotů. Vychází se ze standartních vlastností honeypotů, rozšířených o nově navržené a vytvořené prvky, které zvyšují efektivnost detekce incidentů.

Velmi cennou je část praktické aplikace na modelování zadaného problému a to, že podle vytvořené metodiky a systémového návrhu byl vytvořen model pro novou laboratoř, která na aktuálních hrozbách porovnává účinnost jednotlivých způsobů detekce a to tak, že stanovené hypotézy jsou statisticky vyhodnocovány.

Význam pro praxi a pro rozvoj vědního oboru

Z hlediska konstrukce uvedeného prostředí autor velmi dobře využil svých teoretických znalostí a praktických zkušeností a dobře je popsal. Oceňuji systémové chápání problému a odborné směrování disertační práce zkušeným školitelem.

Význam předkládané práce pro rozvoj vědního oboru spatřuji především v systémovém vyjádření modelu a to v kontextu s uvedenými možnými požadavky oboru inženýrské informatiky. Předložená práce má své místo v oblasti řešených disertačních prací v uvedeném oboru.

Význam předložené práce pro praxi vidím především v systémovém uspořádání metodik a včlenění výsledků této práce do možného pohledu strategie řízení a odpovídajícího možného růstu podniku a modelování procesů v nových laboratorních podmínkách pracoviště s cílem dokazování hypotéz pro podnikové informační systémy.

Formální úprava disertační práce

Kriticky hodnotím některé citační nepřesnosti autora – např. neúplné citace u některých obrázků (obr. 4.1, 6.1, 6.2, 7.1 a dalších), neúplné popisy větvení algoritmu např. na obr. 9.10 (ano-ne), neúplné popisy os grafů (např. obr. 11.2 a dalších), nebo náhodně popisování titulkem graf nebo obrázek (obr. 11.2.), nebo uvedený matematický vztah např. 11.2 nepopisuje proměnné a jejich metriku. Kriticky se také dívám na seznam použitých zdrojů s neuvedením citací v textu vlastních publikací autora nebo citací řešeného výzkumného úkolu pracoviště.

Práce je jinak napsána přehledně, systémově velmi dobře a splňuje obsahově nároky na současné doktorské disertační práce ve vědním oboru.

Otázky do rozpravy:

1. Jak vytvoříte vhodnou kombinací detekčních metod s možným dalším cílem přenést uvedený koncept z teoretické roviny do praxe?
2. Uvádíte, že „velké množství technik detekce míří k rozmanitému testování různých systémů na detekci hrozeb, k novým návrhům na vylepšení těchto systémů a na optimalizaci bezpečnostních postupů" - jak budete v řešeném modelu a uvedené metodice eliminovat důsledky např. dnes již velmi dynamického profilu kyberterorismu na bezpečnost informačních systémů?

Závěr

Předkládanou práci doporučuji k obhajobě před příslušnou komisí a po úspěšném jejím obhájení udělit jmenovanému titul Ph.D. v uvedeném oboru.

V Brně 3. listopaadu 2013

prof. Ing. Jiří Dvořák, DrSc.
profesor technické kybernetiky, vědecký pracovník
Vysoké učení technické v Brně
Fakulta podnikatelská
Ústav informatiky

VŠB-TECHNICKÁ UNIVERZITA OSTRAVA

Fakulta
elektrotechniky a
informatiky

Posudek doktorské práce

Autor: Ing. Tomáš Výmola, UTB Zlín
Název práce: Metody detekce on-line hrozeb ve virtuálním prostředí.
V Ostravě 15.11.2013

Aktuálnost tématu, obsah a struktura práce

V práci je diskutována problematika metod detekce on-line hrozeb ve virtuálním prostředí na základě chování virtuálního postředí. Práce má formát samostatného díla, ne tedy ze samostatných publikovaných prací a doprovodných kapitol. Práce je alespoň pro mne napsána relativně mlhavě, na druhou stranu navržené postupy a metodiky jsou podloženy nejen uspokojivou publikační činností, ale i zřetelně dobrými zkušenostmi dokotranda.
Z hlediska aktuálnosti lze konstatovat, že práce představuje, alespoň podle mne, zajímavou, nicméně neúplnou kolekci metod detekce anomálií vevirtuálním prostředí. Dle mého názoru je téma vysoce aktuální a odráží potřebu nových netradičních informatických metod pro řešení ochrany dat. Práci lze v tomto směru považovat za úspěšný krok.

Úroveň zpracování

Na úroveň zpracování lze pohlížet ze dvou směrů a to z hlediska grafického a formálního zpracování. V obou ohledech nelze vytknout nic podstatného, tedy nenašl jsem žádné nedostatky, které zbytečně snižují kvalitu práce. Z grafického hlediska lze konstatovat kvalitní obrázky. Po formální stránce je práce na slušné úrovni. Kvalita je tedy akceptovatelná a splňuje všechny požadavky kladené na vědeckou práci.

Zvolené metody zpracování

V práci byly použity techniky detekce on-line hrozeb ve virtuálním prostředí. Všechny tyto metody mají výstupy rigorózně publikovány na konferencích, vědeckých časopisech což plně opravňuje jejich použití v práci.
Z těchto důvodů lze považovat použití zvolených metod za plně oprávněné a pro účely a cíle práce dostačující.

Kontaktní údaje:
Fakulta elektrotechniky a informatiky, VŠB-TU Ostrava
17.listopadu 15/2172, 708 33 Ostrava-Poruba
tel.: +420 596 919 353, fax: +420 596 919 597, e-mail: ivan.zelinka@vsb.cz

Výsledky práce a nové poznatky, které přináší

Vzhledem k faktu, že celá práce byla postavena jako souhrn aplikačních implementací, lze konstatovat pozitivní přínos práce jako takové. Nicméně z pohledu teoretického přístupu si nejsem jistý co nového v teorii tato práce přináší.

Připomínky a dotazy

V práci jsem se zaměřil na fakta a technickou stránku věci. V tomto směru mám následující připomínky a dotazy:

1. V práci jsem nedokázal jednoznačně rozlišit, co je z programového vybavení práce doktoranda a co je použitý program ze "třetí strany". Prosím osvětlete.Kolik a jaké programátorské práce jste udělal.
2. Co je teoretickým přínosem Vaší práce? Jak a v čem obohacuje Vaše práce současný stav?
3. Ve vaší práci používáte poměrně známé metody detekce anomálií, které mohou být samy o sobě, ale i v korelaci s ostatními událostmi (včetně jiných anomálií) poměrně složitými strukturami v dynamice sítě. Prosím, jaké další metody by jste použil? Nastiňte jakým způsobem by jste použil metody z oblasti umělé inteligence.

Závěr posudku

Doktorand Ing. Tomáš Výmola publikoval problematiku, související s doktorskou prací, spolu se svými kolegy v celé řadě více či méně významných publikací, plně dostačujících k podpoře výsledků a tvrzení obsažených v této práci.
Doktorand rovněž splňuje dle přiložených materiálů i další kritéria jako jsou pedagogické aktivity, apod.
Ve své doktorské práci prokázal Ing. Tomáš Výmola schopnost samostatné tvořivé vědecké práce. Předložená doktorská práce splňuje všechna potřebná ustanovení pro udělení titulu „doktor" dle zákona o vysokých školách a tudíž ji **doporučuji** k obhajobě.

prof. Ing. Ivan Zelinka, Ph.D.

Kontaktní údaje:
Fakulta elektrotechniky a informatiky, VŠB-TU Ostrava
17.listopadu 15/2172, 708 33 Ostrava-Poruba
tel.: +420 596 919 353, fax: +420 596 919 597, e-mail: ivan.zelinka@vsb.cz

Oponentní posudek disertační práce Ing. Tomáše Výmoly
„Metody detekce on-line hrozeb ve virtuálním prostředí"

Disertační práce Ing. Tomáše Výmoly navazuje na praktické zkušenosti doktoranda v oblasti, kdy jako správce informačních systémů a správce sítě řešil bezpečnostní incidenty.

Doktorand ukazuje, že vzhledem ke stále sofistikovanějším způsobům napadání počítačových systémů, které přináší přímé škody při ztrátě dat a jejich zneužití či nepřímé způsobené poškozením pověsti firem, jejíž systémy byly napadeny, je nutný komplexní způsob zabezpečení počítačových sítí, a to nejen antivirovými programy.

Zkoumaná problematika je aktuální a v souvislosti s nárůstem útoků na informační systémy, např. ve finančním sektoru, se její význam bude dále posilovat.

Z cílů práce, deklarovaných na str. 14, považuji za nejvýznamnější definovat postupy a způsoby detekce ke zvýšení bezpečnosti systémů, inovaci a rozšíření metod detekce na již realizovaných systémech a aplikaci systému a jeho vyhodnocení.

V kapitolách 4 a 5 doktorand charakterizuje hlavní detekční techniky – detekci anomálií a detekci vzorů, včetně zhodnocení jejich výhod a nevýhod.

Zajímavá je myšlenka honeypotů, nezabezpečených (ale bezcenných) systémů s lákavými názvy, které přitahují útoky a lze pak identifikovat jejich charakter a dokonce detekovat i šifrované útoky. Autor je rozebírá v kapitole 6, dělí podle interakce na low-interaction, medium-interaction a high-interaction a opět diskutuje jejich výhody a nevýhody.

Daleko nebezpečnější než „jednorázové" útoky, zaměřené na okamžitý efekt, jsou APT (Advanced Persistent Threat) útoky, které se snaží o trvalý přístup do napadeného systému. Disertant je blíže popisuje v kapitole 7 a rozebírá zde i speciální programy, jako např. exploit a backdoor.

V experimentální části (počínaje kapitolou 8) autor představuje návrh systému, který je založen na detekci on-line hrozeb s využitím honeypotů. Představuje architekturu systému, skládající se ze soustavy distribuovaných hoenypotů, agentního přístupu a subsystému administrace. Všechny části jsou podrobně popsány, slovní výklad je doplněn vývojovými diagramy, které jednoznačně definují posloupnost kroků detekčního algoritmu.

Pro analýzu možností aplikace a verifikaci navrženého systému autor navrhl experimentální laboratoř a vytvořil virtuální experimentální síť simulující reálnou instituci, která odpovídá firmě „střední" velikosti.

Experiment byl poměrně rozsáhlý a trval téměř 7 měsíců a lze tak konstatovat, že získané výsledky mají vypovídající schopnost a věrohodně dokládají, zda navržené řešení je schopné splnit požadované funkce.

Disertant ve zhodnocení výsledků ukázal, že systém hoenypotů mapovaných agentem je efektivnější než systém standardních honeypotů, což doložil i statistickými prostředky – pomocí testování hypotéz. Využití agentního přístupu také považuji za hlavní přínos v metodice detekce hrozeb ve virtuálním prostředí a prostředkem, který zvýší bezpečnost informačních systémů. Cenné je také to, jak autor naznačuje, že systém lze modifikovat i pro mobilní aplikace a cloudová řešení.

Navržený systém byl vyzkoušen nejen v laboratorních podmínkách, ale implementován i v praxi dvou organizací.

Práce má velmi dobrou jazykovou úroveň, takřka bez chyb a překlepů.

- Str. 12 uprostřed: „standartními“ – má být „standardními“, zde ale zřejmě nejde o překlep, protože autor slovo „standartní“ místo „standardní“ uvádí ve všech výskytech slova, např. na stranách 33., 41, 95.
- Str. 51: „Firewall s povolenými odchozenými spojení“, má být „spojeními“ a zřejmě i „odchozími“.
- Str. 95: „z grafu vyplívá“ – má být „vyplývá“.

Grafická úroveň práce je rovněž velmi dobrá a tabulky, diagramy, grafy dobře demonstrují probíraná témata a dosažené výsledky.

Formální připomínka:

- Vzhledem k velkému množství zkratek, které sice byly v práci průběžně vysvětlovány, by bylo vhodné pro lepší orientaci čtenáře vytvořit seznam zkratek, kde by bylo možné kteroukoliv z nich snadno najít.

Dotazy na disertanta:

1. Vysvětlete blíže funkci firewallu, k čemu je určen, na jakém principu pracuje a jak může spolupracovat se systémy detekce narušení?
2. Na str. 50 zmiňujete MySQL. Vysvětlete pojmy SQL injection a „escapování“. Jaké jsou možnosti zabránění SQL injection?

Závěr:

Lze konstatovat, že Ing. Tomáš Výmola. prokázal schopnost a připravenost k samostatné činnosti v oblasti výzkumu a vývoje, jeho disertační práce splňuje podmínky § 47 Zákona o vysokých školách č. 111/1998 Sb., lze sice mít výhradu, že z 9 článků jen jeden byl publikován na mezinárodním fóru, tím však nelze snižovat dosažené výsledky a jejich přijetí odbornou komunitou. Je nepochybné, že práce je přínosná po teoretické stránce a má významné praktické využití, proto ji

doporučuji k obhajobě

před komisí doktorského studijního oboru Inženýrská informatika

V Brně dne 19. listopadu 2013

Šeda

Prof. RNDr. Ing. Miloš Šeda, Ph.D.
Ústav automatizace a informatiky
Fakulta strojního inženýrství VUT v Brně