Oponentský posudek dizertační práce na téma:

Distribuovaný systém klasifikace útoků pro VoIP infrastrukturu využívající protokol SIP

Dizertační práci vypracoval: Ing. Jakub Šafařík
Vedoucí dizertační práce: doc. Ing. Miroslav Vozňák, Ph.D.

Oponent: prof. Ing. Ivan Zelinka, Ph.D.
Fakulta elektrotechniky a informatiky
VŠB – Technická univerzita Ostrava

Předložená dizertační práce se zabývá metodami strojového učení za účelem klasifikace SIP útoků ve VoIP sítích. Téma dizertace je vysoce aktuální a zapadá do konceptu výzkumu v oblasti kybernetické bezpečnosti v rámci nově akreditovaného studijního oboru Fakulty elektrotechniky a informatiky v Ostravě.

Cíle dizertace vychází z kvalitně provedené rešerše současného stavu poznání a jsou uvedeny v kapitole páté, kde se jedná o:

- návrh nového přístupu automatické klasifikace používající k detekci prvků umělé inteligence a statistických metod s minimálně třemi druhy klasifikací,
- a experimentální ověření funkcionality na referenčních datech reálných SIP útoků a porovnání s existujícími metodami.

Konstatuji, že doktorand **splnil výše uvedené úkoly,** naplnil cíle dizertace a výsledky považuji za přínosné v oblasti autonomní detekce útoků v SIP komunikaci.

Doktorand v práci poukázal na slabiny VoIP infrastruktury a popsal stávající postupy detekce hrozeb. Aby se mohl zabývat vývojem klasifikátorů pro rozpoznání

útoků s využitím umělé inteligence, musel se nejdříve vypořádat s otázkou, jak získat kvalitní sadu, na které by vybrané metody aplikoval. Zdrojová data o útocích jsou získávána na honeypotech a student implementoval sofistikovaný distribuovaný systém honeypotových sond, čímž získal kvalitní a hodnotou datovou sadu, navíc s možností prakticky permanentní aktualizace.

Ve své práci navrhl klasifikátory umožňující univerzální detekce hrozeb a experimentálně ověřil možnosti jejich využití v autonomním režimu. Implementované algoritmy nakonec porovnal s dalšími dostupnými klasifikačními metodami. Ve své práci navrhl dvě verze neuronové sítě v prostředí JAVA, které označuje ANNv1 a ANNV2, dále využil aplikaci WEKA obsahující nástroje strojového učení a nakonec i prostředí MATLAB. Použité metody a přístupy považuji za vhodné.

Přínosy práce shrnul přehledně v deváté kapitole, kde bych především zmínil i praktický přínos ve formě návrhu a implementace informačního systému Beekeeper pro autonomní analýzu VoIP útoků, především pak jeho návaznost na další expertní systém MENTAT a WARDEN, které jsou provozovány v síti národního výzkumu a vzdělávání CESNET.

Dizertační práce přinesla nový návrh systému autonomní klasifikace útoků pomocí neuronových sítí a vybraných algoritmů strojového učení, což je jádro dizertace. Vlastní návrhy byly implementovány, experimentálně ověřeny a byla potvrzena aplikovatelnost nově navržených řešení.

Přínosy pro praxi potvrzuje fakt, že výsledků dosáhl při řešení projektu TA ČR DELTA, který je orientován na aplikovaný výzkum v mezinárodní spolupráci a vyvinuté nástroje s novými přístupy k detekci VoIP útoků jsou součástí komplexního systému, který by měl býti uveden na trh.

Po formální stránce k práci nemám připomínky, je sepsána přehledně a svědomitě.

Z pohledu evaluace publikačních výstupů uvádím, že jsem nalezl 25 indexovaných výsledků ve SCOPUS, z toho 15 příspěvků z konferencí a 10 článků v časopisech, většina z nich souvisí s tématem dizertace a lze konstatovat, že jádro dizertace bylo adekvátně opublikováno. Uchazeč prokázal schopnosti systematické vědecké práce a výsledky svého výzkumu publikoval.

Předložená **dizertační práce přináší původní poznatky,** jedná se o vědeckou práci a její přínosy jsou přehledně podány v závěru jak z teoretického tak i praktického pohledu.

K předložené práci pokládám následující připomínky do diskuze:

1. V kap. 8.1 popisujete optimální parametry pro ANNv2, zároveň v kap. 9. je uvedeno, že experimentální část se zaměřuje na nalezení optimalizovaného algoritmu řešícího problém klasifikace, přičemž z experimentů nejlépe vychází ANNv2. Jak jste postupoval při řešení optimalizačního problému, jaké konkrétní kroky jste realizoval k nalezení optima?
2. Jak bude reagovat navržený klasifikátor ANNv2 na zcela novou neznámou signaturu? Ideálně by mělo v autonomním režimu dojít k rozpoznání nového typu útoků, a pakliže je tento typ významný, tak by mělo dojít k automatickému vytvoření nového druhu detekovaného útoku, což by pomocí Vámi popisovaného clusteringu bylo možné, ale z práce nemůžu poznat, zda klasifikátor pracuje v tomto režimu. Objasněte tuto otázku a vysvětlete, jak se Vámi navržený ANNv2 klasifikátor chová.

Dizertace **splňuje** podmínky samostatné tvůrčí vědecké práce, obsahuje původní a autorem dizertační práce publikované výsledky vědecké práce, a proto

doporučuji

předloženou dizertační práci k obhajobě v souladu s § 47 zákona č. 111/1998 Sb.

.....

prof. Ing. Ivan Zelinka, Ph.D.

V Ostravě, 1.2.2017