Posudek školitele diplomové práce

Identifikace operačních systémů na základě chování

Autor diplomové práce: Bc. Benjamín Páterek

Diplomová práce se zabývá problematikou určení typu operačního systému běžícího na zařízení (např. osobním počítači) připojeném do počítačové sítě. Cílem práce je navrhnout takové metody, které umožní určení operačního systému na základě pasivního pozorování síťové komunikace každého zařízení, navíc i v situaci, kdy vlastní komunikace může být šifrována a nelze se tedy spolehnout na analýzu jejího obsahu. Jak i sám autor práce správně uvádí, tato problematika je velmi důležitá pro automatizovanou detekci struktury větších počítačových sítí a typů zařízení v nich, které lze následně využít pro zpřesnění detekce bezpečnostních hrozeb, popř. i k automatizaci správy sítě.
Práce začíná analýzou problematiky a vyhodnocením aktuálně existujících přístupů. Hlavní část práce pak sestává z kapitol, ve kterých autor postupně buduje metody pro vlastní identifikaci operačních systémů, v závěrečných kapitolách pak jednotlivé metody experimentálně porovnává a diskutuje jejich vlastnosti.
Návrh základní metody vychází z dostupných dat a jejich vlastností, kdy se jedná o klasifikaci operačního systému pomocí slovníku indikativních internetových domén a frekvencí jejich návštěv každým zařízením. Tato metoda je pak dále rozvíjena tvorbou lepších reprezentací jednotlivých zařízení pomocí kontrastního učení a konečně i návrhem techniky pro zlepšení slovníku domén. Návrhy metod jsou velmi dobře popsány včetně motivace a důvodů pro jednotlivá rozhodnutí učiněných během jejich tvorby. Experimentální část je zpracována rovněž velmi pečlivě s bohatou diskuzí nad výsledky a dává dobrý obraz o použitelnosti jednotlivých metod.

Celkově je předkládaná diplomová práce zpracována na velmi vysoké úrovni, dobře strukturovaná, experimenty byly pečlivě provedeny. Navržené metody lze aplikovat v praxi ve skutečných systémech pro monitorování počítačových sítí. Spolupráci s autorem hodnotím také velmi vysoko.

Diplomovou práci Bc. Benjamína Páterka na základě výše uvedeného navrhuji ohodnotit známkou **A (výborně)**.

V Praze dne 18. 5. 2021

Mgr. Jan Kohout, Ph.D.
Cisco Systems