# POSUDEK DIPLOMOVÉ PRÁCE

Autor: **Bc. Raman Samusevich**
Název: **Herně teoretická optimalizace detekce škodlivého chování**
Posudek vypracoval oponent práce: Ing. Martin Grill

Předložená diplomová práce se zabývá problémem detekce podvodného chovaní a narušení bezpečnosti v počítačových sítích racionálním útočníkem, který je schopen přizpůsobit se aktuálnímu nastavení detekčního systému a předejít detekci. Autor navrhuje využít herně-teoretický model k modelování interakce mezi detekčním systémem a útočníkem, který lze dále využít k lepšímu nastavení parametrů detekčního systému.

Práce obsahuje detailní přehled a klasifikaci možných útoků na detektory založené na technikách strojového učení. Nechybí ani vyčerpávající přehled literatury spolu s popisem základních konceptů teorie her nutných k pochopení navrhovaného řešení. Navržená užitková funkce dostatečně dobře reflektuje problém detekce podvodného chovaní uživatelů v počítačových sítích. Postup pro nalezení optimálního řešení navazuje na existující metody modelovaní interakce mezi útočníkem a obráncem, které dále rozšiřuje a upravuje. Navržený postup je detailně popsán včetně odvození algoritmů pro nalezení Nashovy a Stackelbergovy rovnováhy, které jsou navíc podpořené množstvím důkazů. Navrhovaná metoda je experimentálně ověřena na datech ze skutečného systému detekce podvodného chování a prezentované výsledky jsou velmi slibné. V porovnání s exitujícími algoritmy je výpočetní náročnost navržených algoritmů řádově nižší. V experimentech však chybí detailnější porovnání efektivity detekce s existujícími metodami pro případ racionálního útočníka.

Po formální stránce nemám práci co vytknout; je vypracována v LATEXu a obsahuje všechny náležitosti. Práce je napsaná v anglickém jazyce a po jazykové stránce není zcela perfektní, místy obsahuje chyby či překlepy, které v některých partiích snižují srozumitelnost textu. Příkladem může být sekce 6.2.2, kde se autor chybně odkazuje na tabulku 6.2.1, která navíc neobsahuje výsledky na validačních datech, odkazované z textu. Dále bych uvítal častější popisy jednotlivých členů vzorců a detailnější popisy u obrázků, které by výrazně usnadnily srozumitelnost textu.

Přes výše zmíněné výhrady je předložená diplomová práce nadstandartní svou kvalitou i rozsahem a je patrné, že autor dané problematice velice dobře rozumí, při řešení daného problému postupoval systematicky a dosáhl velice slibných výsledků. Proto hodnotím předloženou diplomovou práci známkou **A-výborně**.

V Praze, 6. 5. 2016

Ing. Martin Grill

Otázky:

1. Výsledné porovnání navrhované metody s existujícím řešením pro případ adaptivního útočníka je provedeno pouze pomocí finančních ztrát (obrázek 6.2.5). Do jaké míry navrhovaný model vylepšuje schopnost systému detekovat adaptivního útočníka? (Jaké jsou hodnoty TPR a FPR?)
2. Jak byla v experimentech nastavena konstanta $c_{FP}$ označující cenu analýzy jednoho falešného alarmu?
3. Jak by se změnil model, pokud bychom kromě $c_{FP}$ uvažovali i operační cenu za analýzu skutečně pozitivních alarmů (TP)? Tento přístup více odpovídá realitě, jelikož kapacita týmu bezpečnostních analytiků je omezená.