

# Návrh zadania diplomovej práce

*Predbežná verzia (vytváraná) <sup>1</sup>*

## Študent:

**Meno, priezvisko, tituly:** Tomáš Belluš, Bc.  
**Študijný program:** Informačná bezpečnosť  
**Kontakt:** tomas.bellus@gmail.com

## Výskumník:

**Meno, priezvisko, tituly:** Tibor Csóka, Ing. PhD.

## Projekt:

**Názov:** Sledovanie zlovoľných činiteľov nástržným systémom  
**Názov v angličtine:** Bait network based monitoring of malicious actors  
**Miesto vypracovania:** Ústav počítačového inžinierstva a aplikovanej informatiky, FIIT STU  
**Oblasť problematiky:** Mitigačné a detekčné nástroje v informačnej bezpečnosti

## Text návrhu zadania<sup>2</sup>

Pretože neexistuje spôsob, ako produkčné systémy exponované do verejných sietí úplne ochrániť proti zlovoľným činiteľom, zameriava sa výskum v oblasti informačnej bezpečnosti na detekciu a mitigáciu zlovoľnej aktivity za účelom zvyšovania bezpečnosti týchto systémov. Výskum pritom využíva nástroje (napr. honeynet, honeypot a sandbox) ako prostriedky pre oklamanie zlovoľného činiteľa s cieľom donútiť ho využiť ľubovoľné dostupné prostriedky pre realizáciu jeho agendy. Vysoká sofistikovanosť zlovoľných činiteľov kladie zvýšené nároky na nástroje používané pri výskume ich aktivity, v dôsledku čoho je potrebné na strane výskumníkov v informačnej bezpečnosti disponovať schopnosťou vytvárať vierohodné klamlivé ciele, ktoré motivujú činiteľov realizovať pokus o kompromitáciu nasaďeného systému. V súčasnosti je možné vďaka širokému spektru open-source technológií realizovať systémy pre pozorovanie zlovoľnej aktivity i na úrovni vytvorenia samostatnej a uzavretej infraštruktúry. Analyzujte možnosti nástrojov typu honeynet, honeypot a sandbox a popíšte ich možné využitie v skúmanej oblasti. Analyzujte možnosti realizácie systému honeynet tak, aby zbieral relevantnú telemetriu a dáta z pozorovanej aktivity zlovoľného činiteľa od vstupu do systému po jeho výstup zo systému, prípadne realizáciu kľúčového cieľa. Navrhnite honeynet s použitím vhodných metodík, algoritmov, postupov a open-source technológií vyplývajúcich z analýzy a to spôsobom, ktorý umožní pozorovania a telemetriu uchovávať a dodatočne analyzovať. Implementujte navrhnuté riešenie a overte použiteľnosť metodiky.

<sup>1</sup> Vytlačiť obojstranne na jeden list papiera

<sup>2</sup> 150-200 slov (1200-1700 znakov), ktoré opisujú výskumný problém v kontexte súčasného stavu vrátane motivácie a smerov riešenia

## Literatúra<sup>3</sup>

- Wenjun Fan, David Fernández, Zhihui Du, Adaptive and Flexible Virtual Honeynet, Tsinghua University, 2015
- Christian Abdelmassih, Container Orchestration in Security Demanding Environments at the Swedish Police Authority, Diplomová práca, 2018

V Bratislave dňa 10.12.2019

---

Podpis študenta

---

<sup>3</sup> 2 vedecké zdroje, každý v samostatnej rubrike a s údajmi zodpovedajúcimi bibliografickým odkazom podľa normy STN ISO 690, ktoré sa viažu k téme zadania a preukazujú výskumnú povahu problému a jeho aktuálnosť (uvedte všetky potrebné údaje na identifikáciu zdroja, pričom uprednostnite vedecké príspevky v časopisoch a medzinárodných konferenciách)