

# Posudek disertační práce

**Autor:** Ing. Maroš Barabas, VUT Brno

**Název práce:** : Bezpečnostní analýza síťového provozu pomocí behaviorálních signatur

## Aktuálnost tématu, obsah a struktura práce

V disertační práci je popisována a studována metoda bezpečnostních analýz síťového provozu pomocí behaviorálních signatur. Práce se skládá ze šesti kapitol a příloh. Obsahuje úvod do problematiky, popis použitých metod a jejich aplikace. Navržené postupy a metodiky jsou podloženy nejen uspokojujivou publikační činností, ale i dlouholetými zkušenostmi pracoviště doktoranda.

Z hlediska aktuálnosti lze konstatovat, že práce představuje implementaci existujících metod v kybernetické bezpečnosti. Dle mého názoru je téma aktuální a odráží potřebu nových netradičních metod v oblasti počítačové bezpečnosti. Práci lze v tomto směru považovat za úspěšný krok.

## Úroveň zpracování a splnění stanovených cílů

Na úroveň zpracování lze pohlížet ze dvou směrů a to z grafického a formálního zpracování. V obou ohledech nelze práci nic vážnějšího vytknout. Z grafického hlediska je práce na výborné úrovni (barevné i černobílé obrázky, laserový tisk,...).

Po formální stránce je práce dobrá a splňuje všechny požadavky kladené na vědeckou práci. Cíle jsou jasně a transparentně definovány. Z tohoto pohledu lze práci pokládat za formálně správnou.

## Zvolené metody zpracování

V práci byly použity metody patřící do solidní a rigorózní vědecké disciplíny. Výstupy práce dizertanta byly rovněž rigorózně publikovány na konferencích a workshopech.

Z těchto důvodů lze považovat použití zvolených metod za plně oprávněné a pro účely disertační práce dostačující, zvláště při aplikaci na reálná data.

## Výsledky disertační práce a nové poznatky, které přináší

Vzhledem k faktu, že celá práce je postavena hlavně na aplikaci již existujících metod a v oblasti teorie není přínos jednoznačný (včetně jasně definovaných cílů). V práci jsou sice shrnuty přínosy práce, ale tyto závěry jsou relativně vágní a povahy sumarizační.

## Připomínky a dotazy

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

- Prosím upřesněte více Váš přínos v rámci DP. Jak posouvá teorii?
- Jaké metody z oblasti umělé inteligence by jste mohl použít na behaviorální analýzu?
- Byly už použity Vaše přístupy v reálném provozu (firmy atp.)?

## Závěr posudku

Ing. Maroš Barabas vypracoval a ověřil známé metody v oblasti počítačové bezpečnosti. Problematiku související s disertační prací publikoval spolu se svým školitelem a kolegy v celé řadě více či méně významných publikací dostačujících k podpoře výsledků a tvrzení obsažených v této práci.

Ve své disertační práci prokázala Ing. Maroš Barabas schopnost samostatné práce.

I přes jisté nesrovnalosti a nepřesnosti v práci docházím k závěru **doporučit** tuto práci k obhajobě.



Prof. Ing. Ivan Zelinka, Ph.D.  
Katedra Informatiky  
Fakulta elektrotechniky a informatiky  
VŠB-TU Ostrava