# Hodnocení vedoucího bakalářské práce

**Student:** Ambrušová Eva, Bc.
**Téma:** Detekce škodlivých domén pomocí analýzy DNS provozu (id 17699)
**Vedoucí:** Kováčik Michal, Ing., UPSY FIT VUT

1. **Informace k zadání**
   Cílem bakalářské práce byla detekce škodlivých doménových jmen pomocí pasivní analýzy DNS provozu. Nejprve bylo nutné vykonat analýzu charakteristik škodlivých doménových jmen a identifikovat možnosti detekce vůči doménám legálním. Navržený algoritmus detekuje škodlivé domény pomocí skladby doménového jména a využívá na to entropii a frekvenční analýzu pomocí n-gramů. Algoritmus byl testován na datech z reálného provozu.
2. **Práce s literaturou**
   Studentka si nastudovala vícero vědeckých článků věnujících se problematice. Zdroje si aktivně a samostatně dohledávala.
3. **Aktivita během řešení, konzultace, komunikace**
   Studentka byla během řešení aktivní. Konzultace často iniciovala a probíhali pravidelně. Na konzultace chodila připravená a průběžně postupovala v zlepšování řešení. Sama také navrhla některé součásti detekce.
4. **Aktivita při dokončování**
   Aktivita studentky byla v průběhu řešení rovnoměrná. Práce byla dokončena v dostatečném předstihu a obsah práce byl konzultován. V období před odevzdáním se studentka věnovala testování a dolaďování technické správy. Studentka pracovala v mnoha aspektech samostatně.
5. **Publikační činnost, ocenění**

6. **Souhrnné hodnocení** **výborně (A)**
   Studentka se práci věnoval dostatečně dlouho. Byla vykonaná analýza škodlivých a legitimních domén, na základě které byla navržena klasifikace. Výslední implementace je dobře odladěná a testována na reálném provozu. Součástí odevzdaného řešení jsou taky skripty pro generování grafů v nástroji gnuplot. Výsledek práce je prakticky použitelný pro detekci škodlivých domén. Proto navrhuji nadprůměrné hodnocení stupněm A (výborně).

V Brně dne: 4. června 2015

.....
podpis