Supervisor assessment of Master's Thesis

Student: Surovič Marek, Bc.
Title: Static Behavioral Malware Detection over LLVM IR (id 18603)
Supervisor: Vojnar Tomáš, prof. Ing., Ph.D., UITS FIT VUT

1. **Assignment comments**
   Zadání práce vyšlo z vlastní iniciativy studenta. Práce nenavazovala na předchozí projekty, ale student na ní pracoval dva roky (po prvním roce práci nestihl dokončit). Zadání práce je podle mého názoru velmi obtížné, neboť vyžadovalo nastudování a aplikaci poznatků z několika náročných oblastí, včetně problematiky fungování a detekce pokročilého malware, teorie stromových automatů a jejich použití pro detekci malware (popsané v náročných výzkumných článcích) či systém LLVM. Ne ve všech oblastech jsem přitom byl studentovi schopen detailně radit. Studenta jsem na náročnost tohoto zadání upozornil, a to i opakovaně na začátku druhého roku řešení. Student se rozhodl v práci pokračovat. S ohledem na náročnost zadání, ale také ne zcela vyrovnanou aktivitu a nakonec i jistým osobním problémům, student práci dokončil jen s obtížemi. Nicméně zadání práce byť s výhradami a v minimálním rozsahu podle mého názoru splnil.
2. **Literature usage**
   Student byl schopen si sám dohledat potřebné zdroje informací a použít je.
3. **Assignment activity, consultation, communication**
   Studentova aktivita byla poněkud nevyrovnaná. Byla zde období, kdy práce pokračovala rychle vpřed, student zvládal samostatné studium a aplikaci velmi netriviálních poznatků, o čemž mě sám od sebe systematicky, nadšeně a do hloubky informoval. Student se dokázal vyrovnat i s různými slepými cestami, na které při řešení své náročné práce narazil. Pak se ale vyskytovala také období, kdy práce nepokračovala (zřejmě) vůbec.
4. **Assignment finalisation**
   Některé části práce jsem viděl v dostatečném předstihu. V samotném závěru ale nastalo krizové období, kdy se zdálo, že práce ani nemusí být dokončena. Nakonec ale student práci dokončil, byť některé její části nejsou rozpracovány tak, jak by ideálně být měly.
5. **Publications, awards**
   Výsledek práce nebyl prezentován formou publikací. Zadání práce má sice potenciál vést i k výsledkům výzkumného charakteru, ale obtížnost dosažení takových výsledků je vysoce nad rámec diplomové práce.
6. **Total assessment** **satisfactory (D)**
   S ohledem na výše uvedené hodnotím aktivitu studenta při řešení jeho diplomové práce stupněm D. Je pravda, že jeho aktivita nebyla zcela vyrovnaná, že některé části nebyly dokončeny tak, jak by dokončeny mohly být, ale tyto skutečnosti v mých očích vyvažuje vysoká náročnost práce a značné úsilí, odvaha a iniciativa, které student do práce investoval.

In Brno 7. June 2016

.....
signature