

Hodnocení vedoucího bakalářské práce

Student: Lysoněk Milan
Téma: Existující útoky na SSL/TLS (id 20047)
Vedoucí: Fiedor Tomáš, Ing., UITŠ FIT VUT

1. Informace k zadání

Práce je realizována v rámci firmy RedHat ve spolupráci se Standou Žídkem a Hubertem Kariem (jejichž hodnocení studenta je promítnuto v tomto posudku). Práci považuji za mírně složitější, vzhledem k nutnosti důkladného nastudování protokolu SSL/TLS, principů útoků na komunikači zabezpečenou tímto protokolem a problematiku testování síťových protokolů.

2. Práce s literaturou

Student nastudoval poskytnutou literaturu. Zbytek zdrojů si byl schopen vyhledat a nastudovat sám (převážně se však jedná o specifikace CVE).

3. Aktivita během řešení, konzultace, komunikace

Student byl mimořádně aktivní. Student se s RedHat konzultanty pravidelně scházel každý týden již od loňského léta, kdy se seznamoval s problematikou bezpečnosti síťových protokolů a rozšiřováním funkcionality knihovny `tlslite-ng`, na které je rovněž postavena tato práce. Student byl aktivní i přes e-mailové konzultace, komunikoval i s vývojaři knihoven třetích stran, a byl vždy řádně připraven.

Student se se mnou, jakožto formálním vedoucím, sešel několikrát a dostatečně konzultoval psaný text. O postupování práce jsem byl průběžně informován z hromadné e-mailové konverzace mezi studentem a všemi konzultanty.

4. Aktivita při dokončování

Práce byla dokončena v dostatečném předstihu, bez žádných stresů a problémů. Její obsah a forma byla dostatečně konzultována. Text práce byl rovněž konzultován i s hlavním konzultantem z RedHatu (Standou Žídkem), který byl s formou spokojen. Implementační část práce prošla důkladným `code-review` udržovatele knihoven `tlsfuzzer` a `tlslite-ng` (Hubertem Kariem).

5. Publikační činnost, ocenění

Nejsem si vědom žádné publikace ani ocenění. Výstupy práce jsou však reálně používané v rámci knihoven `tlsfuzzer` a `tlslite-ng` vyvíjené v rámci firmy RedHat. Práce výrazně posunuje funkcionalitu těchto knihoven a použitelnost pro testování SSL/TLS. Na základě výsledků byla studentovi nabídnuta stáž v RedHatu a možnost budoucí spolupráce.

6. Souhrnné hodnocení

výborně (A)

Z pohledu formálního vedoucího, bera na vědomí hodnocení technických konzultantů z RedHatu, hodnotím práci Milana Lysoňka *výborně (A)*. Student se oblasti věnoval již během loňského léta, kdy se seznamoval s `open source` pracovním prostředím i oblastí síťových protokolů, práci pravidelně konzultoval se všemi konzultanty, a výsledky jeho práce jsou reálně využity pro testování různých implementací SSL/TLS protokolů.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto hodnocení v listinné i elektronické formě.

V Brně dne: 23. května 2017

.....
podpis