

Zadání bakalářské práce



145037

Ústav: Ústav informačních systémů (UIFS)
Student: **Dvořák Vojtěch**
Program: Informační technologie
Specializace: Informační technologie
Název: **Inkrementální statická analýza pro jazyk YARA**
Kategorie: Bezpečnost
Akademický rok: 2022/23

Zadání:

1. Nastudujte si teorii inkrementálních parserů a jejich použití pro analýzu zdrojových kódů v textových editorech a integrovaných vývojových prostředích (IDE).
2. Seznamte se s jazykem YARA (<https://yara.readthedocs.io/en/stable/>) a nástroji pro jeho statickou analýzu. Zaměřte se na projekt YLS (<https://github.com/avast/yls>), který poskytuje server protokolu LSP (Language Server Protocol).
3. Navrhněte knihovnu, která umožní statickou analýzu jazyka YARA pro účely použití ve vývojových prostředích za využití algoritmu pro inkrementální parsování.
4. Implementujte vámi navrženou knihovnu z předešlého bodu. Proveďte integraci s projektem YLS, kde dojde k nahrazení řešení statických analýz bez inkrementálního parsování za řešení s použitím vaší knihovny.
5. Vaše řešení otestujte vůči extenzivní sadě pravidel v jazyku YARA a porovnejte s řešeními bez inkrementálního parsování.

Literatura:

- Szor: The Art of Computer Virus Research and Defense, Addison-Wesley Professional (2005), ISBN 978-0321304544
- Recorded Future: The Threat Intelligence Handbook, CyberEdge Group (2018), ISBN 978-0999035467
- Tim A. Wagner and Susan L. Graham.: Efficient and flexible incremental parsing. (1998)
- Interní dokumentace společnosti Avast
- Dále dle doporučení vedoucího či konzultanta

Při obhajobě semestrální části projektu je požadováno:
První 3 body a začátek 4.

Podrobné závazné pokyny pro vypracování práce viz <https://www.fit.vut.cz/study/theses/>

Vedoucí práce: **Regéciová Dominika, Ing.**
Konzultant: Ing. Marek Milkovič
Vedoucí ústavu: Kolář Dušan, doc. Dr. Ing.
Datum zadání: 1.11.2022
Termín pro odevzdání: 10.5.2023
Datum schválení: 26.10.2022