Ročníkový projekt (LS)

1 Práca počas LS

Tento semester zahŕňal:

- doladenie a testovanie gramatiky z predchádzajúceho semestra,
- návrh architektúry aplikácie (ďalej len "editor"),
- zoznámenie sa s integráciou gramatiky do editora,
- vytvorenie editora spolu s boilerplate kódom,
- implementácia zvýrazňovania syntaxe,
- tvorba viacerých farebných schém pre editor,
- integrácia s oficiálnym YARA kompilátorom a validácia pravidiel,
- testovanie a ladenie.

2 Architektúra a komponenty editora

2.1 Komponent editora

Editor je vlastne React komponent ktorý používa CodeMirror ako základný textový editor. Využíva Tree-sitter parser na zvýraznenie syntaxe. Pri upravovaní pravidla sa volá parser a oficiálny YARA kompilátor, ktorý kontroluje platnosť pravidla a poskytuje spätnú väzbu v podobe chybových hlásení v riadkoch editora.

2.2 Tree-sitter parser

Parser je vygenerovaný z gramatiky pomocou Tree-sitter. Je zabalený do WebAssembly modulu, ktorý je volaný z editora.

2.3 Tree-sitter queries

Tree-sitter queries sú definované pre každú sekciu YARA pravidla. Queries umožňujú identifikovať syntaktické konštrukcie a poskytujú informácie o ich pozícii v zdrojovom kóde. Tieto informácie sú využité na zvýraznenie syntaxe.

2.4 YARA kompilátor

Samotná knižnica Libyara z oficiálneho repozitára je zabalená do WebAssembly modulu pomocou Emscripten. Editor volá kompilátor pri každej zmene pravidla (po malom voliteľnom časovom oneskoreni) a ukazuje hlásenia od kompilátora priamo v editore.

3 Uživateľské rozhranie

Uživateľské rozhranie je minimalistické. Pozostáva z editora, ktorý zaberá väčšinu plochy a z hornej lišty, ktorá obsahuje tlačidlo pre výber farebnej schémy a kontrolky nesprávnosti pravidla a počtu kompilačných upozornení.

4 Výsledok

Výsledkom je funkčný editor YARA pravidiel, ktorý umožňuje:

- zvýrazňovanie syntaxe,
- kontrolu sémantiky a platnosti pravidla,
- zobrazenie chýb a upozornení priamo v editore,
- výber farebnej schémy,
- zobrazenie počtu kompilačných upozornení.

Editor nedokáže správne kontrolovať použitie všetkých možných modulov. Podpora modulov je obmedzená na tie, ktoré sú implementované v oficiálnom YARA kompilátore. V prípade, že sa v pravidle použije nepodporovaný modul, editor ho pravdepodobne označí ako chybu. Toto však používateľovi nebráni v písaní pravidla, pokiaľ vie pravidlo napásať správne aj bez podpory editora.

5 Ďalšie kroky

Pre ďalší vývoj je možné realizovať:

- podporu viacerých YARA modulov,
- automatické formátovanie kódu.