TFTP w Coq-u lub s2n

26 marca 2019

1 Wstęp

Zadanie jest w dwóch wersjach: albo implementujemy TFTP w Coq-u, albo dodajemy kod do s2n. Skupimy się na razie na zadaniu w Coq-u, zaś o s2n powiemy w sekcji 5 poniżej.

2 Wstęp do TFTP w Coq-u

Zadanie polega na napisaniu docelowo w języku oprogramowania OCaml klienta protokołu TFTP [1], przy czym samo jądro klienta, obsługujące jego logikę ma zostać napisane w Coq-u i tamże zweryfikowane.

3 Etapy pracy

Praca nad zbudowaniem tego serwera będzie składała się z kilku etapów.

1. Zbudowanie w języku OCaml otoczki, która będzie odwoływała się do logiki, jaką napiszemy w Coq-u.
2. Napisanie w Coq-u implementacji logiki oraz specyfikacji tej logiki w postaci odpowiednich definicji oraz lematów.
3. Wykonanie dowodów, że podana implementacja zachowuje własności podane w lematach.

4 Wymagania dotyczące etapów

4.1 Otoczka w OCamlu

Klient TFTP musi wykonywać następujące operacje:

- Parsować parametry wywołania.
- Wchodzić w proces inicjacji i obsługi połączenia.

- W procesie tym czekać na odpowiedź serwera.
- Obsłużyć komunikację z serwerem.
- Zakończyć działanie po przesłaniu całej spodziewanej zawartości przez serwer lub zakończyć działanie po upłynięciu odpowiedniej ilości czasu.

Dodatkowo klient musi pozwalać na zapisywanie zawartości przesłanego pliku. Zależy nam, aby część programu napisana bezpośrednio w OCaml-u była funkcjonalna, ale nie zależy nam na tym, aby była ona rozbudowana.

4.2 Implementacja i specyfikacja w Coq-u

Sama implementacja w Coq-u powinna realizować funkcjonalność opisaną w sekcjach 2, 4, 6, 7 specyfikacji TFTP [1]. Siłą rzeczy wymagać to będzie zamodelowania pakietów opisanych w sekcji 5.

Zaimplementowane w Coq-u funkcje będą zależały od stanu wewnętrznego klienta. Stan ten obejmuje:

- stan protokołu (automat stanowy można odczytać z opisu w sekcjach 2, 4, 6, 7),
- opcjonalnie przysłany od serwera pakiet,
- informacje o pliku lokalnym, który jest zapisywany w wyniku komunikacji.

Funkcje będą produkowały nowy stan wewnętrzny oraz, opcjonalnie, pakiet, jaki ma zostać wysłany do serwera. Pakiety mają być reprezentowane jako wektory ośmiobitowych znaków.

4.3 Dowody

Chcielibyśmy, aby udowodnione zostały wszystkie oczekiwane własności napisanych programów.

5 s2n

W przypadku tej ścieżki zaliczenia należy uzgodnić z prowadzącym zakres prowadzonych prac oraz ich harmonogram. Docelowo ma powstać zweryfikowany fragment kodu, którego weryfikację można dołączyć do projektu s2n. Przykładowe sensowne projekty to dołożenie do istniejącej infrastruktury liczenie HMAC z nowymi algorytmami (np. sm3 lub SHA-3 w którejś wersji). Możliwy jest też projekt dwuosobowy, w którym prace polegałyby na dodaniu weryfikacji jakiegoś algorytmu szyfrowania.

Literatura

[1] K. Sollins. The TFTP protocol (revision 2). Technical report, Network Working Group, 1992. RFC1350.