Knihovna akceleračních modulů pro analýzu aplikačních protokolů v FPGA

Abstrakt

Softwarový balíček obsahuje knihovnu akceleračních modulů pro analýzu aplikačních protokolů v FPGA. Součástí knihovny je modul pro extrakci hlaviček protokolů a tři moduly pro vyhledávání řetězců popsaných regulárními výrazy v aplikačních datech. Součástí knihovny je i software pro generování výše uvedených modulů z konfigurace a pro jejich ovládání za běhu. Akcelerační moduly jsou široce konfigurovatelné a podporují široké spektrum požadované propustnosti od 1Gbit/s až po více než 10Gbit/s.

Modul pro extrakci hlaviček protokolů

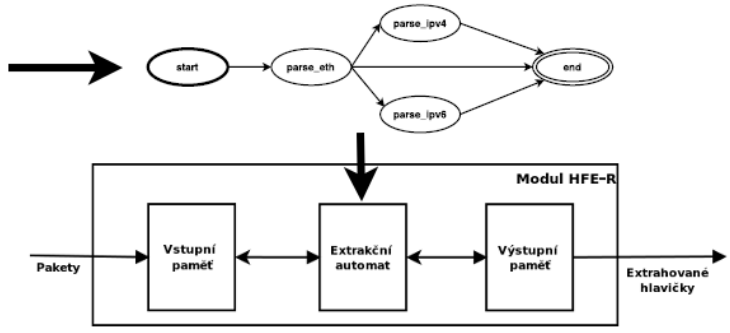
Modul pro extrakci hlaviček protokolů (HFE-R) je generovaný na základě popisu v jazyce P4. V jazyce P4 se popisuje struktura hlaviček jednotlivých protokolů, návaznost protokolů za sebou a specifikuje se, které položky z hlaviček mají být extrahovány. Modul je tudíž díky použití jazyka P4 velmi flexibilní a univerzální.

```
parser start {
    return parse_eth;
}

header ethernet_t eth;
parser parse_eth {
    extract(eth);
    return select(eth.etherType){
        0x0800 : parse_ipv4;
        0x86dd : parse_ipv6;
        default: end; }
}
```

```
header ipv4_t ipv4;
parser parse_ipv4 {
    extract(ipv4);
    return end;
}

header ipv6_t ipv6;
parser parse_ipv6 {
    extract(ipv6);
    return end;
}
```



Moduly pro vyhledávání řetězců popsaných regulárními výrazy v aplikačních datech

Moduly pro vyhledávání řetězců popsaných regulárními výrazy v aplikačních datech jsou v knihovně obsaženy tři. Podle jejich charakteru je můžeme rozdělit do dvou skupin. První skupina obsahuje moduly, jejichž zdrojový kód je generovány z množiny regulárních výrazů a tudíž není možné jejich konfiguraci měnit za běhu. Druhou skupinu tvoří moduly, které umožňují změnu množiny regulárních výrazů popisujících vyhledávané řetězce za běhu. Pro dosažení maximální možné propustnosti všechny moduly podporují zřetězené zpracování vstupních paketů.

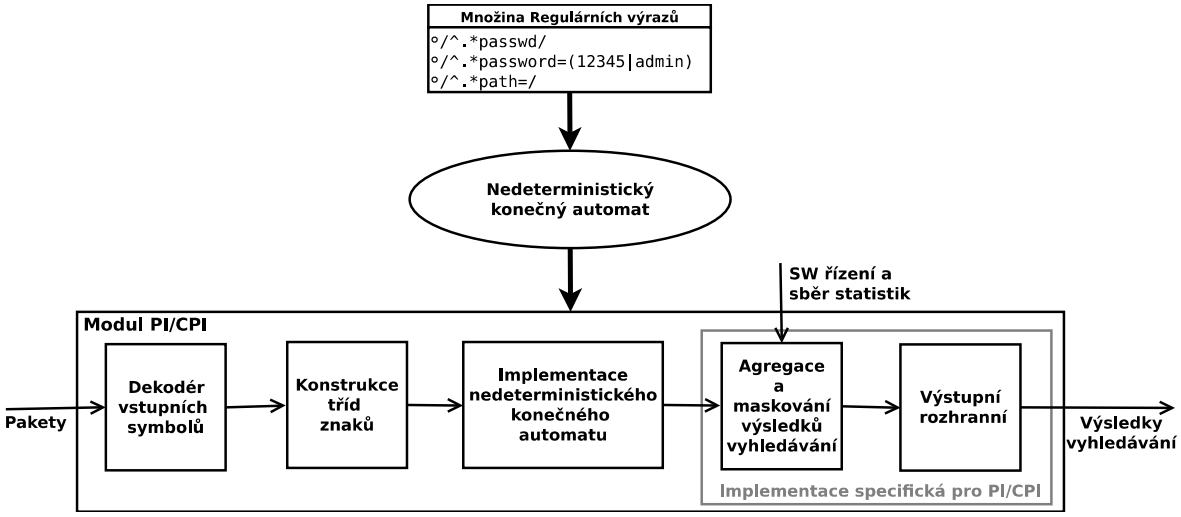
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Tato práce vznikla jako výsledek projektu VI20152019001 „Sondy pro analýzu a filtraci provozu na úrovni aplikačních protokolů“

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

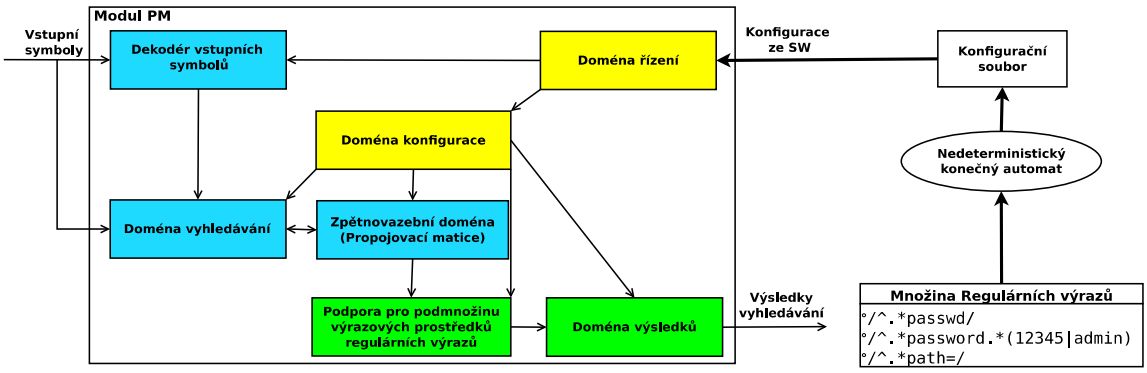
Moduly PROTOCOL_IDENTIFIER a CRYPTO_PROTOCOL_IDENTIFIER

Do první skupiny patří modul CRYPTO_PROTOCOL_IDENTIFIER (CPI) a modul PROTOCOL_IDENTIFIER (PI). Tyto dva moduly se liší účelem pro který byly navrženy, jádro provádějící vyhledávání mají oba společné. PROTOCOL_IDENTIFIER slouží pro identifikaci příslušnosti paketu k aplikačnímu protokolu. CRYPTO_PROTOCOL_IDENTIFIER slouží pro detekci protokolů používajících šifrování. Zdrojový kód těchto modulů je generován z dodané množiny regulárních výrazů ve formátu PCRE. Pro zvýšení flexibility je za běhu možné podporu pro jednotlivé regulární výrazy zapínat nebo vypínat. Výhodu těchto modulů je malá spotřeba zdrojů, nevýhodou je nemožnost měnit množinu regulárních výrazů popisujících vyhledávané řetězce za běhu.



Modul PATTERN_MATCH

Do druhé skupiny patří modul PATTERN_MATCH (PM). Tento modul umožňuje měnit, množinu regulárních výrazů popisujících vyhledávané řetězce za běhu. Modul je parametrizovatelný, umožňuje měnit maximální počet uložitelných regulárních výrazů a požadovanou propustnost modulu. Z důvodu snížení náročnosti modulu na zdroje FPGA podporuje modul pouze podmnožinu výrazových prostředků regulárních výrazů. Jednotka je konfigurovatelná za běhu konfiguračním souborem, který je vygenerován z množiny regulárních výrazů nástrojem pmgen. Konfigurace jednotky je přepínána atomicky v jednom taktu hodin, tudíž není propustnost jednotky omezena ani změnou konfigurace. Výhodou tohoto modulu je možnost měnit množinu regulárních výrazů popisujících vyhledávané řetězce za běhu, nevýhodou je větší spotřeba zdrojů a podpora části výrazových prostředků regulárních výrazů.



MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Tato práce vznikla jako výsledek projektu VI20152019001 „Sondy pro analýzu a filtraci provozu na úrovni aplikačních protokolů“

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA INFORMAČNÍCH TECHNOLOGIÍ