Sonda pro zákonné odposlechy na úrovni aplikačních protokolů pro sítě s rychlostí linek 10 Gbps

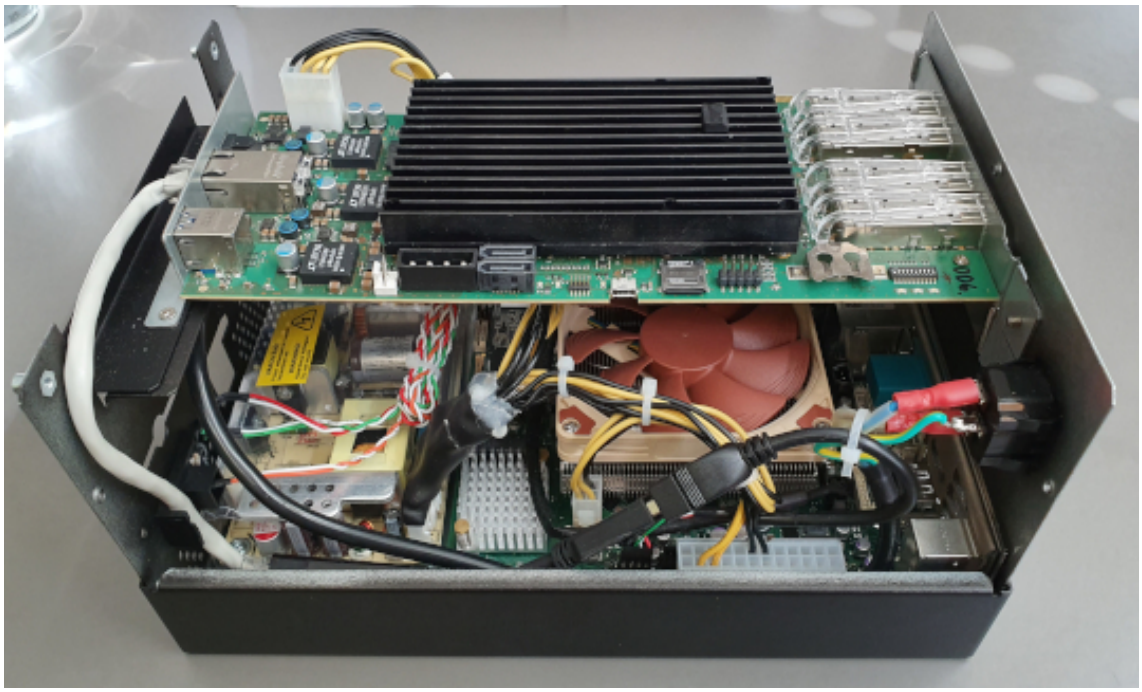
Vytvořený funkční vzorek umožňuje filtrovat komunikaci na síti s kapacitou linek 10 Gbps a následně vybrané pakety uložit na lokální úložiště. Filtraci komunikace a určování, které pakety mají být uloženy je možné specifikovat na základě IP adres (IPv4, IPv6), L7 identifikátorů (např. emailová adresa) nebo na základě jejich kombinací.

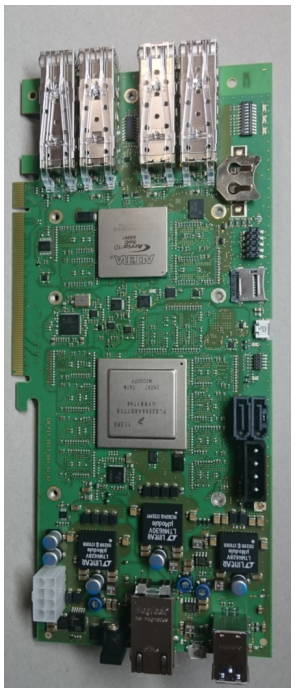
Sonda je cílena na nasazení do datových center a u poskytovatelů internetu s linkami do 10 Gbps. Také je připravena varianta pro nasazení do koncových sítí.

Pro usnadnění nasazení v neznámých sítích sonda umožňuje aktivovat alternativní režim, který zpřístupní statistické informace o provozu na připojené lince (seznam toků, struktura provozu, identifikace šifrovaných spojení). Mimo jiné tento režim uživatele informuje, zda síťové toky na připojené lince jsou kompletní a při aktivaci vybraného záchytu paketů nehrozí ztráta dat z důvodů nekvalitního připojení.

Základní parametry

- Využivá FPGA Intel Arria10 pro filtraci provozu na plné rychlosti 10 Gbps linky
- Hledání ID uživatelů a rozpoznání aplikačních protokolů přímo v hardware
- Správa cache potenciálně zajímavých síťových toků na úrovni hardware
- Vyrovnávací paměť na pakety potenciálně zajímavých síťových toků
- Hloubková analýza paketů až do úrovně aplikačních protokolů (SMTP, POP3, IMAP, FTP, SIP)
- Lokální uložení zachycených dat
- Kompletně samostatné zařízení





VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Tato práce vznikla jako výsledek projektu VI20152019001 podporovaného Ministerstvem vnitra České republiky.