# Knihovna softwarových modulů a firmware SDM pro filtraci sítového provozu na úrovni aplikačních protokolů pomocí FPGA SoC

Fakulta informačních technologií Vysokého učení technického v Brně
Božetěchova 2, 612 66 Brno

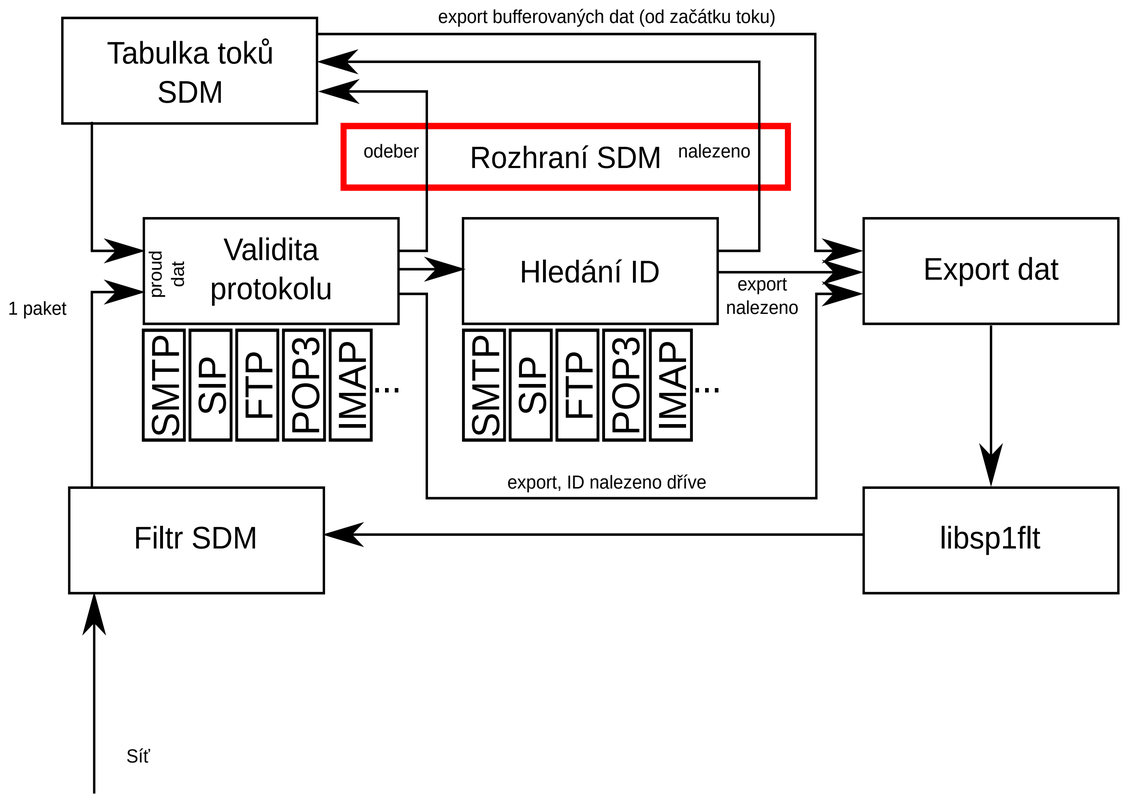
## Analýza aplikačních protokolů

Tento softwarový balíček obsahuje knihovnu softwarových modulů určených pro rychlé rozpoznání aplikačního protokolu a komunikujících uživatelů - podporovány jsou protokoly SMTP, SIP, FTP, POP3 a IMAP. Knihovna má definované rozhraní umožňující snadné přidání dalších protokolů.

## Softwarově definovaný monitoring

Knihovnu softwarových modulů využívá software pro softwarově definované monitorování (SDM) toků přenášených počítačovými sítěmi. Software umožňuje ovládání filtru v FPGA pomocí knihovny libsp1flt, která je součástí balíčku.

## Vzájemná spolupráce



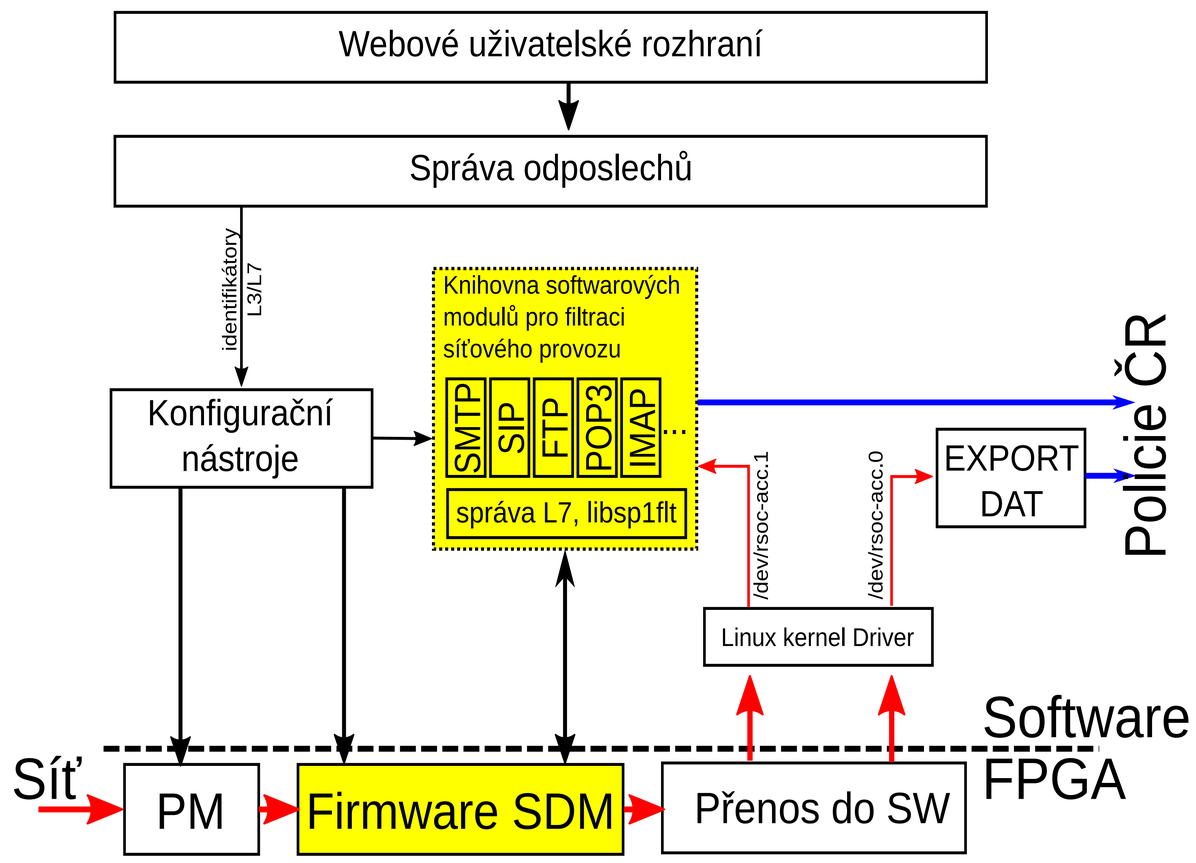

- Nutná koordinace mezi FPGA a software
- Řešením je portování SDM do projektu SProbe
- Nutno řešit portabilitu mezi sondami vyvářenými v rámci projektu SProbe

## Zákonné odposlechy

- Založeno na standardech ETSI
- Konfigurace pomocí unikátního identifikátoru odposlouchávaného v rámci podporovaného protokolu

## Nasazení nástroje

- Knihovna softwarových modulů detekuje hledané identifikátory v rámci toků TCP/UDP
- Akcelerovaná identifikace toků pomocí SDM
- Data určená k odposlechu předávaná Policii ČR




- Nasazení nástrojů na sondě vytvářené projektem SProbe


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