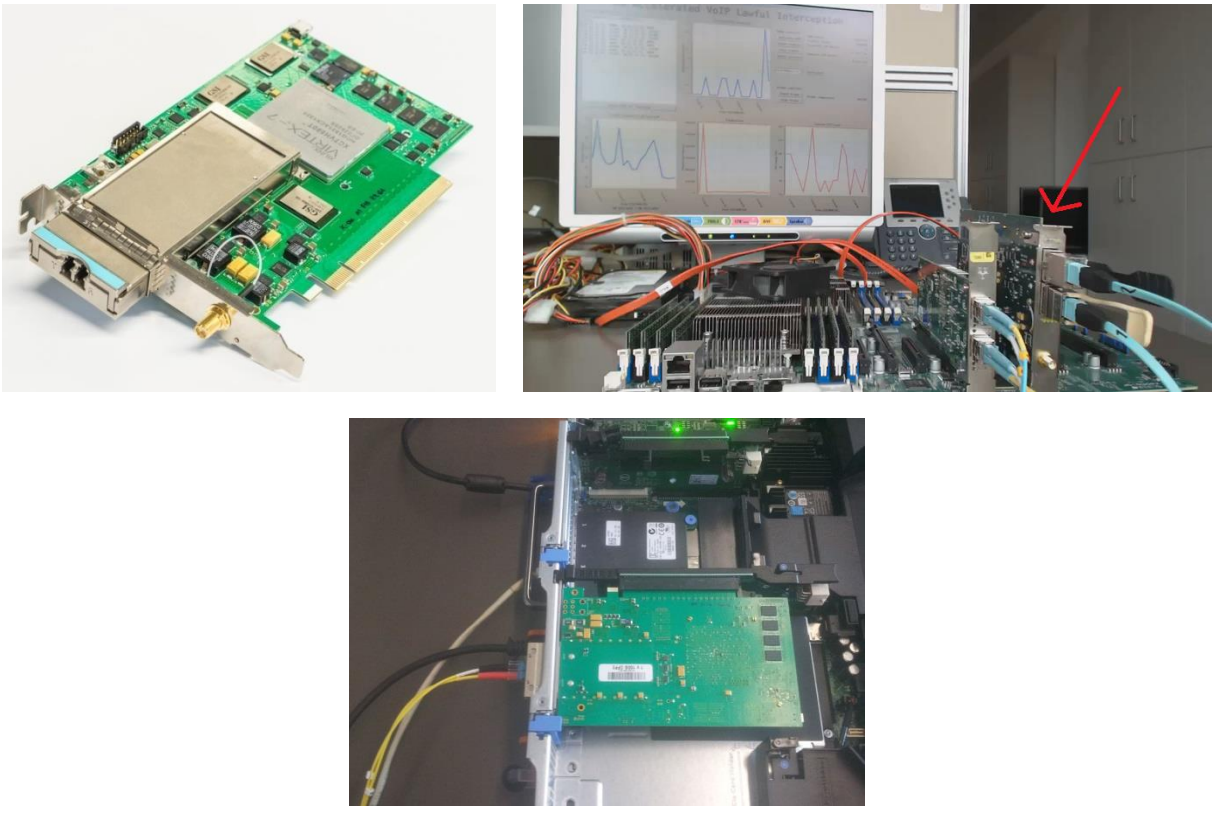
Prototyp vysokorychlostní sondy pro monitorování IPv6 provozu

Autoři

- Kekely Lukáš, Ing.
- Žádník Martin, Ing. Ph.D
- Vrána Roman, Bc.
- Matoušek Jiří, Ing.
- Kořenek Jan, Ing. Ph.D.

Popis výsledku

Prototyp vysokorychlostní sondy je rekonfigurovatelnou platformou pro monitorování a bezpečnost 100Gb sítí s využitím akcelerační karty na bázi FPGA. Výsledek je primárně zaměřený na oblast zákonných odposlechů. Prototyp se sestává ze serveru, síťové karty Combo 100G, firmware pro kartu Combo 100G a programového vybavení (software) pro server. Karta Combo 100G umožňuje hardwarově akcelerovat zpracování síťového provozu tak, aby bylo možné zaznamenávat veškerou komunikaci odposlouchávaných entit, případně řešit další bezpečnostní aplikace založené na analýze aplikačních protokolů. Díky technologii FPGA je možné provést změnu konfigurace karty a přizpůsobit funkci cílovému prostředí a aplikaci. Karta je zapojena v hostitelském PC do PCI-Express x16 generace 3. Po restartu serveru je do FPGA vložena konfigurace (firmware), který implementuje část funkcionality legálních odposlechů (legal interception – LI). Firmware komunikuje se softwarem běžícím v hostitelském serveru. Pro komunikaci a přenos dat je využita knihovna NetCOPE a systém SDM [1].



Obr. 1: Akcelerační karta Combo 100G s FGPA Virtex-7, testovací prostředí a prototyp

Firmware nahraný do karty Combo 100G realizuje následující funkce:

- přiřazení časové značky každému příchozímu paketu,
- parsování IP adres, čísel transportních portů a protokolu ze záhlaví paketu,
- filtrace a označení paketu na základě vyparsovaných polí (SDM),
- zahození nezájmových paketů na základě pravidel vkládaných ze software a přeposlání nezahozených paketů do software.

Software běžící v hostitelském serveru realizuje následující funkce:

- nahrání a konfigurace firmware, konfigurace a spuštění LI programů,
- připojení se na LI systém (k mediační funkci),
- konfigurace odposlechů přes rozhraní CCCI,
- parsování aplikačních protokolů za účelem získání Intercept Related Information (IRI),
- odesílání IRI na LI systém přes rozhraní INI2,
- záchyt zájmových paketů,
- odesílání odposlechnutých paketů přes rozhraní INI3,
- řízení Softwarově Definovaného Monitoringu (SDM).

Po startu sondy se sonda automaticky připojí k předem nakonfigurovanému LI systému. Ovládání sondy z LI systému probíhá pomocí CCCI (CC Configuration Interface) rozhraní, pomocí INI2 jsou odesílány na LI systém IRI zprávy a pomocí INI3 rozhraní je odposlouchávaný provoz odesílán na LI systém. Sonda je kompatibilní s LI systémem SLIS.

Využitý hardware, firmware a software

Realizovaný výstup vznikl v rámci projektu SEC6NET. K realizaci výsledku byla využita karta Combo 100G od firmy INVEA-TECH. Výkonné jádro SDM a systém NetCOPE byly implementovány v rámci smluvního výzkumu a spolupráce se sdružením CESNET.

Reference

- [1] Kekely, L.; Kucera, J.; Pus, V.; Korenek, J.; Vasilakos, A.V., "Software Defined Monitoring of Application Protocols," in Computers, IEEE Transactions on , vol.PP, no.99, pp.1-1

  doi: 10.1109/TC.2015.2423668

  URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7087363&isnumber=4358213