# Uživatelský manuál pro ovládání hardwarově akcelerované sondy pro legální odposlechy

FIT VUT Technický report

*Lukáš Kekely, Martin Žádník*

Fakulta informačních technologií, Vysoké učení technické v Brně

Poslední změna: 5. dubna 2013

# Uživatelský manuál pro ovládání hardwarově akcelerované sondy pro legální odposlechy

Lukáš Kekely, Martin Žádník

Fakulta informačních technologií
Vysoké učení technické v Brně
Božetěchova 1/2, 612 66 Brno
{xkekel00, izadnik}@fit.vutbr.cz

**Abstrakt** Tento manuál se zabývá instalací, konfigurací a provozováním vysokorychlostní akcelerované sondy, která je určena pro zachycení a export síťového provozu pro účely zákonných odposlechů. Legální odposlechy slouží především pro pořizování důkazního materiálu při podezření na páchání trestné činnosti. Vysokorychlostní sonda je určena pro nasazení k velkým ISP a na páteřní linky, jejichž přenosová rychlost je velmi vysoká.

## 1 Popis vysokorychlostní sondy

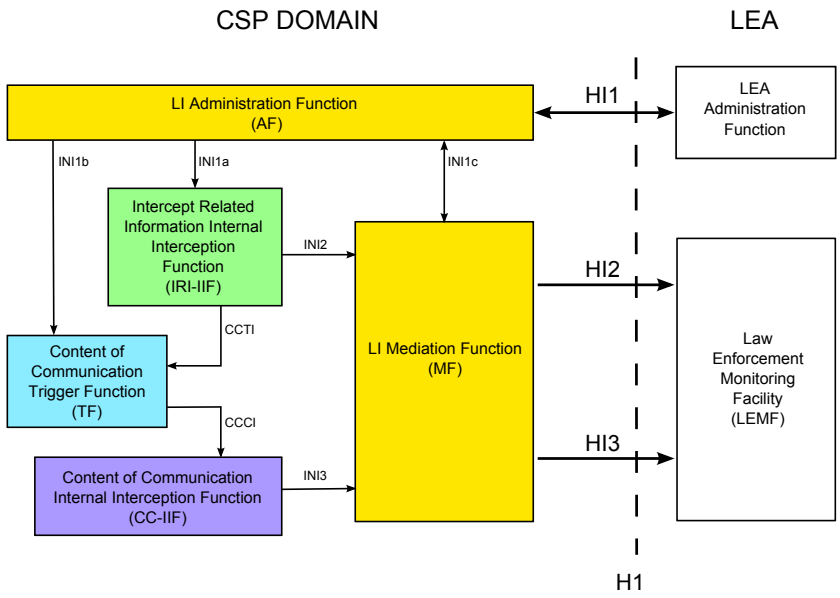
Vysokorychlostní sonda je postavena na síťových kartách (Combo v2) umožňující hardwarovou akceleraci zpracování síťového provozu tak, aby bylo možné zaznamenávat veškerou komunikaci odposlouchávaných cílů. Tato karta je zapojena v hostitelském PC do PCI-Express sběrnice. Pro detailnější informace o popisu této platformy konzultujte User manual NetCOPE platformy společnosti INVEA-TECH (doc/usersmanual.pdf).

Karta Combo v2 umožňuje nahrání firmware, který implementuje funkcionalitu legálních odposlechů (legal interception — LI). Ve smyslu ETSI standardů celá sonda realizuje Content of Communication Internal Interception Function dle obrázku 1. Ovládání sondy za běhu probíhá pomocí CCCI (CC Configuration Interface) rozhraní a pomocí INI3 rozhraní je odposlouchávaný provoz odeslán. CCCI i INI3 rozhraní slouží pro komunikaci s mediační funkcí (MF, Mediation Function). Mediační funkce zasílá příkazy k odposlechům na sondu přes CCCI rozhraní a získaná data přes INI3 rozhraní transformuje do HI3 rozhraní a přenáší do bezpečnostní agentury (LEA, Law Enforcement Agency). Sonda je kompatibilní se mediační funkcí SLIS.

V kartě je realizována časově kritická operace filtrace síťového provozu, zatímco software zajišťuje management filtru a komunikaci s mediační a administrační funkcí LI systému.

Firmware LI nahraný do karty Combo v2 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 vypársovaných polí,




**Obrázek 1.** Architektura systému pro zákonné odposlechy podle norem ETSI.

– zahození/přeposlání paketu (označeného číslem nalezeného pravidla) do hostitelského počítače.

Software LI běžící v hostitelském počítači realizuje následující funkce:

– nahrání a konfigurace firmware, konfigurace a spuštění LI programů,
– konfigurace odposlechů přes rozhraní CCCI,
– odesílání odposlechnutých paketů přes rozhraní INI3.

## 2 Postup zprovoznění sondy

### 2.1 Zprovoznění serveru

Nákup platformy (server s nainstalovaným OS a nainstalovaným NetCOPE prostředím) NetCOPE 05 0C. Zapojte server do elektrické sítě a připojte server k Internetu pomocí ethernetového kabelu přes management port serveru. Připojte klávesnici a obrazovku k serveru, spusťte server a přihlašte se údaji uvedenými v manuálu NetCOPE (netcopeusermanual.pdf). Heslo je vhodné změnit, aby nedošlo ke neoprávněnému přístupu na server. Zkontrolujte, zda má server konektivitu do Internetu:

```
ping www.seznam.cz
PING www.seznam.cz (77.75.72.3): 56 data bytes
64 bytes from 77.75.72.3: icmp_seq=0 ttl=249 time=15 ms
```

```
64 bytes from 77.75.72.3: icmp_seq=1 ttl=249 time=15 ms
64 bytes from 77.75.72.3: icmp_seq=2 ttl=249 time=0 ms

----www.seznam.cz PING Statistics----
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip (ms)  min/avg/max/med = 0/10/15/15
```

### 2.2 Zprovoznění LI funkcionality

Stažení balíku hwli-1.0 z Internetu:

```
wget www.stud.fit.vutbr.cz/~xzadni00/hwli-1.0.tar
```

Instalace balíčku hwli-1.0.

```
tar -xvf hwli-1.0.tar
cd hwli-1.0
make
make install
```

Pokud selže jeden z kroků při instalaci, není pravděpodobně správně nainstalován server s platformou NetCOPE a sonda nebude pracovat správně. Pro vyřešení problémů s NetCOPE kontaktujte support@invea-tech.com.

## 3 Instalace sondy do linky

Zachycení dat na sondě je realizováno dvěma 10 Gbps optickými síťovými porty na kartě Combo v2. Dle typu transceiveru SFP+ je možné zapojit SM (single mode) či MM (multimode). Samotný odposlech na lince se realizuje pomocí optického tapu, který je vložen do linky a rozděluje signál 70% linkový port, 30% monitorovací port. Z tapu vedou dva monitorovací porty, které se zapojí pomocí optických kabelů do monitorovacích portů Combo v2. Připojte sondu k Internetu pomocí management portu a zkontrolujte konektivitu. Před začátkem odesílání dat je nutné, aby byla spuštěna MF SLIS.

## 4 Konfigurace a ovládání sondy

Z pohledu uživatele je podstatný konfigurační soubor *li.conf*. Tento soubor umožňuje definovat veškeré uživatelské proměnné nutné pro nastavení odposlechů na sondě. Tabulka 1 obsahuje seznam těchto proměnných včetně vysvětlení jejich významu, případně doporučených nastavení.

Poté co jsou nastaveny proměnné pro LI, je možné využít skript *li* pro spuštění a ovládání sondy. Příkazy skriptu jsou následující:

- li start
- li restart

**Tabulka 1.** Uživatelské proměnné a jejich význam

| **Proměnná** | **Akce** |
|---|---|
| CCCISERVER | IP adresa serveru, na kterém běží MF SLIS obsluhující CCCI rozhraní. |
| CCCIPORT | Číslo TCP portu, na kterém MF SLIS naslouchá pro příchozí CCCI připojení. |
| INI3SERVER | IP adresa serveru, na kterém běží MF SLIS obsluhující INI3 rozhraní. |
| INI3PORT | Číslo TCP portu, na kterém MF SLIS naslouchá pro příchozí INI3 připojení. |
| ID | Unikátní číslo identifikující danou sondu. **Musí být pro každou sondu nastaveno unikátně.** |

- li reload
- li status
- li stop

Význam příkazů je popsán v tabulce 2.

**Tabulka 2.** Příkazy ovládající sondu a jejich význam

| **Příkaz** | **Akce** |
|---|---|
| start | Ukončí běžící LI programy, ukončí programy ovládající firmware, nahraje firmware do karty, nakonfiguruje firmware, spustí programy ovládající firmware, spustí LI programy přípojující se k mediační funkci |
| restart | Ukončí běžící LI programy, nahraje firmware do karty, nakonfiguruje firmware, spustí programy přípojující se k mediační funkci |
| reconnect | ukončí běžící LI programy, spustí programy LI programy |
| status | Vypíše stav firmware včetně čítačů (popis výpisu je uveden níže), vypíše stav běžících programů |
| stop | Ukončí běžící LI programy, ukončí programy ovládající firmware, ukončí příjem paketů na síťové rozhraní karty |

Popis výpisu stavu je uveden v tabulce 3.

## 5 Kapacita pravidel

Počet pravidel, které je možné skrze SLIS nakonfigurovat na sondě je omezen. Vzhledem k použitému algoritmu filtrování je možné definovat pouze maximálně dosažitelný počet pravidel za optimálních podmínek. Maximální počet pravidel každého typu filtru je 1526 pravidel. Za běžných podmínek je průměrně dosažitelné zaplnění 1000 pravidel.

**Tabulka 3.**

| Výpis | Popis |
|---|---|
| Counter | pokus |

## 6 Závěr

Tato sonda byla vyrobena v rámci projektu Sec6net na FIT VUT v Brně. Technické detaily sondy mohou být dohledány v technickém reportu [1].

## Reference

1. Lukas Kekely, M. Z.: Hardwarově akcelerovaná sonda pro legální odposlechy, FIT-TR-2012-005. 2012.