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: 30. května 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

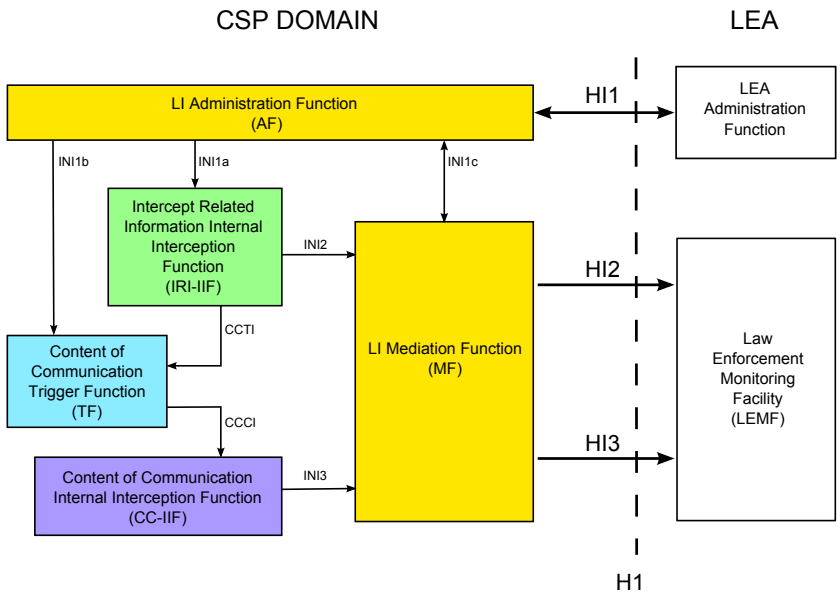
Vysokorychlostní sonda je postavena na síťových kartách (Combo v2) umožňující hardwarovou akceleraci zpracování síťového provozu tak, aby bylo možné zaznamenávat veškerou komunikaci odposlouchávaných cílů. Tato karta je zapojena v hostitelském PC do PCI-Express sběrnice. Pro detailnější informace o popisu 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. Tuto platformu prodává v současné době společnost INVEA-TECH. 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 přihlaste 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, tj. "0.0% packet loss":

```
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 na serveru

- Stažení balíku hwli-1.0 z Internetu.

  ```
  wget odkaz?/hwli-1.0.tar
  ```

- Rozbalení balíčku.

  ```
  tar -xvf hwli-1.0.tar
  ```

- Kontrola serveru před instalací HWLI balíčku. Pokud kontrola skončí chybou, pak není pravděpodobně správně nainstalován server s platformou NetCOPE a sonda nebude pracovat správně. Pro vyřešení problémů s NetCOPE kontaktujte support@invea-tech.com.

  ```
  cd hwli-1.0
  ./checkserver.sh
  ```

- Správný výstup checkserver.sh musí odpovídat následujícímu výpisu:

  ```
  [root@ant-3 scripts]# ./checkserver.sh
  Check PCI for INVEA-TECH COMBO card ....
  Card found:
  06:00.0 Ethernet controller: Cesnet, z.s.p.o. COMBO-LXT155 (rev f1)
  Check for NetCOPE packages....
  NetCOPE NetCOPE found:
  netcope-fw-combov2-10g2.x86_64        5.12.2-1  installed

  netcope-platform-combov2-10g2.x86_64  1.3.0-1   installed

  netcope-platform-common.x86_64        1.3.0-2   installed

  netcope-platform-handbook.noarch      1.3.0-2   installed

  netcope-sw-examples.noarch            1.3.0-2   installed

  netcope-tools-development.x86_64      1.3.0-1   installed

  Check for COMBO packages....
  Combo packages found:
  ```

```
combo-driver-udev-rules.noarch        0.7.3-2   installed

dkms-combo-driver.noarch              0.7.3-2   installed

libcombo.x86_64                       1.3.4-1   installed

libcombo-devel.x86_64                 1.3.4-1   installed

netcope-fw-combov2-10g2.x86_64        5.12.2-1  installed

netcope-platform-combov2-10g2.x86_64  1.3.0-1   installed

nic-fw-combov2-10g2.x86_64            5.12.2-1  installed

Check for SZE packages....
SZE packages found:
libsze2.x86_64                        1.1.0-1   installed

libsze2-devel.x86_64                  1.1.0-1   installed
```

– Instalace balíčku hwli-1.0. Instalace probíhá standardně probíhá do adresáře /usr/local. Instalace do jiného adresáře je možná změnou proměnné INSTALLDIR v Makefile.

```
make
make install
```

– Pokud selže jeden z kroků při instalaci, pak 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). Tomu musí odpovídat typ použitého kabelu. 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*. Pří standardní instalaci se tento soubor nachází v INSTALLDIR/etc/. 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.

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.**

5 Spuštění a ovládání sondy

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

- li start
- li restart
- li reload
- li status
- li stop

Význam příkazů je popsán v tabulce 2.

Výpis stavu níže odpovídá zadání příkazu *li status* na hwli-1.0 sondě. Výpis byl rozdělen do několika bloků a každý blok je komentován.

```
[netcope@sec6net-hwli ~]$ li status
```

- Informace o nahraném firmware v kartě.

```
Information on loaded firmware
Built at : 2010/08/25 10:17:23
Board    : combo
Subtype  : LXT155
S/N      : 9200066
Speedgr. : 2
Addon0   : 10G1
Chip0    : n/a
```

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

```
S/N0     : 9200087
Addon1   : 10G1
Chip1    : n/a
S/N1     : 9200087
Channels : 2/2 (RX/TX)
Firmware : ok
SW       : 0x41c1050c
HW       : 0x00070000
Text     : NIC_CV2_10G2
Caps     : 0x0000000f
ID ver.  : 0x0102
NetCope  : 0x0200
PCI brver: 6d05.01.0b (2013/01/22 15:15)

Driver [combov2] szedata2: active
  (0x41c10504-0x41c105ff) {}
  (0x41f10101-0x41f101ff) {}
  (0xf1010300-0xf10105ff) {}
  (0xa41c0101-0xa41c02ff) {}
  (0xc0330100-0xc03301ff) {}
```

– Následuje výpis stavu fyzického síťového rozhraní na kartě. Karta má celkem dvě rozhraní, každé je označeno hodnotou *Interface number*. Hodnota *IBUF* ENABLED značí povolený příjem paketů. Hodnota *IBUF* DISABLED značí zakázaný příjem paketů (čítače se nebudou inkrementovat). Hodnota *Packets*, *Received*, *Discarded*, postupně značí celkový počet paketů, přijaté pakety, které byly zpracovány, celkový počet zahozených paketů.

  Pakety mohou být zahozeny ze dvou důvodů:

  - Není dostatek místa v bufferech — *Buf overflow*,

- Paket neodpovídá pravidlům pro validní paket (chybné CRC, minimum frame length (minimální délka ethernetového rámce), MTU frame length (maximální délka ethernetového rámce)) — *Error packets*[1].

```
Number of received packets on physical network interfaces
-------------------------------------- IBUF Status ----
Interface number           : 0
IBUF                       : ENABLED
PACODAG overflow occurred  : False
DFIFO overflow occurred    : False
IBUF speed                 : 10 Gb/s
----------------------- IBUF Packets/Frames Stats ----
Packets                    : 9689669881
Received                   : 9689669881
Discarded                  : 0
Buf overflow               : 0
Error packets              : 0
---------------------------------- IBUF Settings ----
Frame error from GMII [1]  : enabled
CRC check             [2]  : enabled
Minimum frame length  [4]  : enabled
* length                   : 64 B
MTU frame length      [8]  : enabled
* length                   : 1526 B (max 16352 B)
MAC address check     [16] : enabled
* mode                     : [0x0] promiscuous

-------------------------------------- IBUF Status ----
Interface number           : 1
IBUF                       : ENABLED
PACODAG overflow occurred  : False
DFIFO overflow occurred    : False
IBUF speed                 : 10 Gb/s
----------------------- IBUF Packets/Frames Stats ----
Packets                    : 0
Received                   : 0
Discarded                  : 0
Buf overflow               : 0
Error packets              : 0
---------------------------------- IBUF Settings ----
Frame error from GMII [1]  : enabled
CRC check             [2]  : enabled
Minimum frame length  [4]  : enabled
```

[1] Pokud je nutné přijímat i nevalidní pakety, pak do příkazové řádky zadejte: ibufctl -A -m 0

```
* length                    : 64 B
MTU frame length      [8]  : enabled
* length                    : 1526 B (max 16352 B)
MAC address check     [16] : enabled
* mode                      : [0x0] promiscuous
```

– Komponenta filtru počítá kolik paketů bylo filtrem odmítnuto (Denied), kolik přeposláno do software (Allowed) a kolik paketů celkem filtr zpracoval (TOTAL).

```
Number of matched rules and received packets
 *** PACKET COUNTERS ***
Interface 0:
    Denied : 9689668401
    Allowed:          0
    TOTAL  : 9689668401
Interface 1:
    Denied :          0
    Allowed:          0
    TOTAL  :          0
```

Tato tabulka

```
Status of rule table
 *** FILTER STATUS ***
Status flag vectors:
    Disable: 00000000
    Ignore : 00000000
    Full   : 00000000
    Busy   : 00000000
Rule types:
    Type 0: READY
    Type 1: READY
    Type 2: READY
    Type 3: READY
```

– Výpis aktuálně uložených pravidel ve fitlru.

```
Rules stored in the hardware filter
 *** RULES INSIDE FILTER ***
```

– Na závěr jsou vypsány LI procesy.

```
Running LI processes
UID        PID  PPID  C    SZ   RSS PSR STIME TTY      TIME CMD
netcope  18573     1  0  4373   608   0 Apr06 ?
00:00:35 tsuctl -x /usr/local/mcs/hwli-1.0/design.xml
```

```
UID        PID  PPID  C    SZ   RSS PSR STIME TTY      TIME CMD
netcope  18577     1  0  4370  1004   5 Apr06 ?        00:00:00
/home/netcope/sonda/trunk/swtools/ccci/cccid -l DEBUG -d
/dev/combosix/0 -x /usr/local/mcs/hwli-1.0/design.xml -H 147.229.14.112
-P 21105 -i 123

UID        PID  PPID  C    SZ   RSS PSR STIME TTY      TIME CMD
netcope  18579     1  0 69228 262948  4 Apr06 ?        00:00:00
/home/netcope/sonda/trunk/swtools/sze2li1tcp/sze2litcp -s 147.229.14.112
-p 21103 -i 123
```

6 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.

7 Řešení poruchy

V případě poruchy sondy, počítač nevypínejte.

1. Zkontrolujte, že máte správně připojen management port do sítě.
2. Zkontrolujte, že máte připojeny optické kabely s odposlouchávaným provozem do 10Gbps portů. Typ transceiverů a kabelu musí být buď SM nebo MM.
3. Zkontrolujte, že máte správně nastavený konfigurační soubor *li.conf*.
4. Zkontrolujte, že je dostupný počítač s mediační funkcí SLIS (0% packet loss).

   ```
   ping <IP adresa MF SLIS>
   64 bytes from slis.policie.cz (147.229.176.14):
   icmp_seq=1 ttl=63 time=0.121 ms
   ^C
   --- slis.policie.cz ping statistics ---
   3 packets transmitted, 3 received, 0% packet loss,
   ```

5. Pokud vše proběhne bez varovného či chybového hlášení a sonda přesto nepracuje správně, postupujte dle následujících pokynů.
6. Spusťte příkaz

   ```
   li status > status_before_restart.log
   ```

7. Následně proveďte restart LI programů příkazem:

```
li restart
```

8. Spusťte příkaz

   ```
   li status > status_after_restart.log
   ```

9. Zašlete na adresu izadnik@fit.vutbr.cz email s popisem chyby a přiložte soubory: /var/log/messages, status_before_restart.log, status_after_restart.log.

8 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.