Uživatelský manuál pro ovládání hardwarově akcelerované sondy pro legální odposlechy

FIT VUT Technický report

Martin Žádník, Lukáš Kekely, Roman Vrána, Martin Holkovič, Barbora Franková

Fakulta informačních technologií, Vysoké učení technické v Brně

Poslední změna: 24. září 2015

Uživatelský manuál pro ovládání hardwarově akcelerované sondy pro legální odposlechy

Martin Žádník, Lukáš Kekely, Roman Vrána, Martin Holkovič, Barbora Franková

Fakulta informačních technologií
Vysoké učení technické v Brně
Božetěchova 1/2, 612 66 Brno
{xkekel00, izadnik}@fit.vutbr.cz, {xvrana20, xholko00, xfrank08}@stud.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

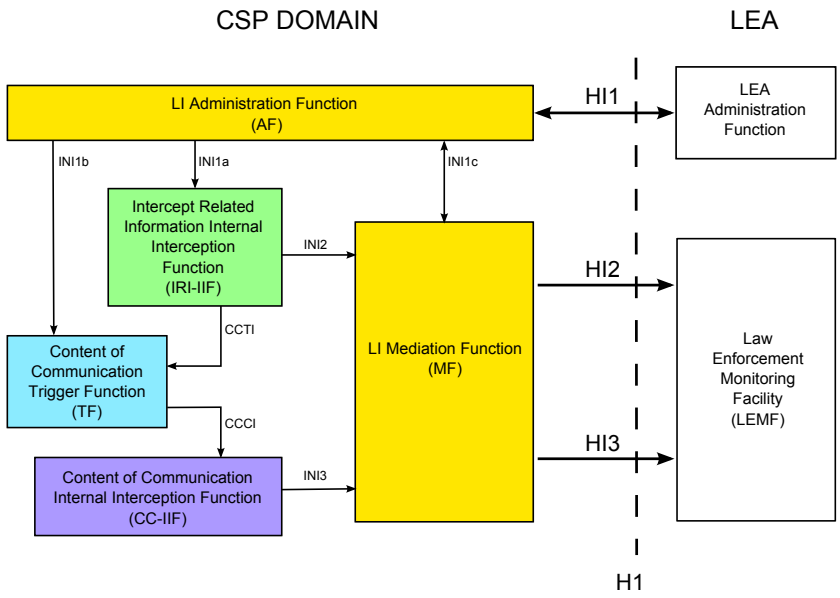
Vysokorychlostní sonda je postavena na síťových kartách (ComboV3) umožňující hardwarovou akceleraci zpracování síťového provozu tak, aby bylo možné zaznamenávat veškerou komunikaci odposlouchávaných cílů. Tato karta je zapojena v hostitelském PC do PCI-Express sběrnice.

Karta ComboV3 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 ComboV3 realizuje následující funkce:

- přiřazení časové značky každému příchozímu paketu,
- výpočet hashe z identifikátorů paketu a přidělení k softwarovému vláknu zpracovávající aplikace



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

– zahození/přeposlání paketu na základě softwarové analýzy provozu.

Software LI běžící v hostitelském počítači realizuje následující funkce:

– nahrání a konfigurace firmware, konfigurace a spuštění LI programů,
– konfigurace odposlechů přes rozhraní CCCI,
– softwarovou analýzu provozu pro vyhodnocení zájmových dat a konfiguraci firmware karty
– zpracování dat aplikačních protokolů pro sledování dynamické identity pomocí funkce IRI-IIF dle 1
– odesílání odposlechnutých paketů přes rozhraní INI3.

2 Postup zprovoznění sondy

2.1 Zprovoznění serveru

Vysokorychlostní sonda může být zprovozněna na jakémkoli serveru složeném z běžně dostupného hardware. Jedinou proprietární součástí je karta Combo V3 a její ovladače. Příkladem takového serveru může být server SuperMicro X9DRG-QF. Kartu je vhodné zapojit do PCI-Express slotu, jehož sběrnice je připojena k CPU, který má u sebe připojené paměťové moduly. Toto je nutné dodržet u víceprocesorového serveru, aby nebyla snížena výkonnost nutnou komunikací mezi CPU. Po připojení serveru do elektericke a datové sítě je nutné nainstalovat operační systém (dop. Centos 6, RHEL 6 nebo podobný) s linuxovým jádrem verze

2.6.32. Konkrétní verze se může lišit podle dostupnosti ovladačů k ostatnímu HW.

Zkontrolujte, zda má server konektivitu do Internetu, tj. "0.0% packet loss":

```
ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=5.13 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=4.55 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=56 time=4.54 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=56 time=4.59 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0.0% packet loss, time 3004ms
rtt min/avg/max/mdev = 4.542/4.706/5.133/0.251 ms

ping www.seznam.cz
PING www.seznam.cz (77.75.76.3) 56(84) bytes of data.
64 bytes from www.seznam.cz (77.75.76.3): icmp_seq=1 ttl=247 time=4.66 ms
64 bytes from www.seznam.cz (77.75.76.3): icmp_seq=2 ttl=247 time=4.64 ms
64 bytes from www.seznam.cz (77.75.76.3): icmp_seq=3 ttl=247 time=4.67 ms
64 bytes from www.seznam.cz (77.75.76.3): icmp_seq=4 ttl=247 time=4.44 ms

--- www.seznam.cz ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 4.441/4.606/4.674/0.117 ms
```

2.2 Zprovoznění LI funkcionality na serveru

- Stažení balíku hw_li_probe.tar.gz z Internetu.

  ```
  wget http://www.fit.vutbr.cz/research/prod/index.php?
  file=/product/438/hw_li_probe.tar.gz&id=438&notitle=1
  ```

- Rozbalení balíčku.

  ```
  tar -xvf hw_li_probe.tar.gz
  ```

- Instalace ovladačů a software pro kartu ComboV3 Před instalací vlastního LI software je nutné zpraovznit kartu ComboV3 pro zachytávání dat. K tomuto slouží přiložené balíčky

  combo-drivers Ovladače a moduly jádra ke kartě ComboV3.
  libcommlbr Knihovna obsahující funkce společné pro ostatní uvedené balíčky.
  libcombo Knihovna pro karty Combo.
  libsze2 Knihovna pro datové rozhraní karty ComboV3 (závisí na libpcap)
  libnetconf Knihovna pro konfiguraci zařízení pomocí protoklolu NETCONF (vyžadována některými SW nástroji).

swtools Balíček softwarových nástrojů pro testování rozhraní SZE, práci s firmware a čtení hardwarových statistik.

sdm Balíček se software pro ovládání Software Defined Monitoring a příslušný firmware.

libtrap Knihovna pro komunikaci modulů LI software.

Pořadí insatlace těchto balíčků by mělo být přibližně následující:

1. libcommlbr
2. libcombo
3. combo-drivers
4. libsze2
5. libnetconf
6. swtools
7. libtrap
8. sdm

Instalaci těchto balíčků je možné provést ze zdrojových kódů postupem standardním pro linuxové autotools (`./configure`, `make`, `make install`). Případné odchylky jsou pak uvedeny v readme souborech těchto balíčků. Zdrojové kódy jsou posledních verzí jsou přiloženy v přídavném balíčku. Pokud máte přístup k repozitáři s těmito balíčky, pak je možné provést instalaci touto cestou. Odkazy na repoztiáře jsou uvedeny níže. Stačí je zkopírovat do souboru `liberouter.repo` do složky `/etc/yum.repos.d/`. Odkazy jsou:

```
[liberouter-INTERNAL]
name=Liberouter RPM repository
baseurl=https://liberouter:chibei0Yie@homeproj.cesnet.cz/
rpm/liberouter/internal/$basearch
enabled=1
gpgcheck=1
gpgkey=http://homeproj.cesnet.cz/rpm/liberouter/
RPM-GPG-KEY-liberouter

[Liberouter-devel]
name=Liberouter Devel - Tools for Monitoring and Configuration
baseurl=http://homeproj.cesnet.cz/rpm/liberouter/devel/$basearch
enabled=1
gpgcheck=1
gpgkey=http://homeproj.cesnet.cz/rpm/liberouter/
RPM-GPG-KEY-liberouter
```

– Kontrola serveru před instalací HWLI balíčku. Pokud kontrola skončí chybou, pak pravděpodobně chybí některé knihovny pro správnou funkci software sondy. Pro vyřešení problémů kontaktujte Ing. Martina Žádníka, Ph. D. <izadnik@fit.vutbr.cz>.

```
cd hw_li_probe/scripts
./li_check_deps.sh
```

– Správný výstup `li_check_deps.sh` musí odpovídat následujícímu výpisu (verze interpretu Python případně typ instalované ComboV3 karty se mohou lišit):

```
[root@ant-3 scripts]# ./li_check_deps.sh
Checking installed ComboV3 card ...
COMBO-100G1/COMBO-10G10                 [ INSTALLED ]

Checking installed drivers ...
szedata2                                [ INSTALLED ]
szedata2-cv3                            [ INSTALLED ]
combo6core                              [ INSTALLED ]
combov3                                 [ INSTALLED ]

All drivers are installed in system.

Checking presence of drivers in kernel ...
szedata2                                [ LOADED ]
szedata2-cv3                            [ LOADED ]
combo6core                              [ LOADED ]
combov3                                 [ LOADED ]

All drivers are loaded.



Checking libraries ...
libtrap                                 [ INSTALLED+DEVEL ]
libsdm                                  [ INSTALLED+DEVEL ]
libsze2                                 [ INSTALLED+DEVEL ]
libcombo                                [ INSTALLED+DEVEL ]
libcommlbr                              [ INSTALLED+DEVEL ]
libnetconf                              [ INSTALLED+DEVEL ]

Checking SW tools ...
combod                                  [ INSTALLED ]
crctest                                 [ INSTALLED ]
csboot                                  [ INSTALLED ]
csbus                                   [ INSTALLED ]
csbus-i2cms                             [ INSTALLED ]
cscard-ident                            [ INSTALLED ]
csid                                    [ INSTALLED ]
c10g4ctl                                [ INSTALLED ]
dmactl                                  [ INSTALLED ]
ethctl                                  [ INSTALLED ]
```

```
hfexctl                                 [ INSTALLED ]
hgenctl                                 [ INSTALLED ]
ibufctl                                 [ INSTALLED ]
i2cctl                                  [ INSTALLED ]
obufctl                                 [ INSTALLED ]
sze2counter                             [ INSTALLED ]
sze2fastwrite                           [ INSTALLED ]
sze2loopback                            [ INSTALLED ]
sze2machinegun                          [ INSTALLED ]
sze2multiread                           [ INSTALLED ]
sze2pcap                                [ INSTALLED ]
sze2read                                [ INSTALLED ]
sze2tap                                 [ INSTALLED ]
sze2test                                [ INSTALLED ]
sze2write                               [ INSTALLED ]
tsuctl                                  [ INSTALLED ]

Checking firmware availability ...
COMBO10G10                              [ AVAILABLE ]
COMBO100G1                              [ AVAILABLE ]




Checking python version ...
Python 2.X                              [ INSTALLED ] 2.6.6
Python 3.X                              [ INSTALLED ] 3.3.2

Python interpreter installed in correct versions.
Configuration interface will be available.
```

– Instalace balíčku hw_li_probe.tar.gz. Instalace softwarových komponent li sondy probíhá standardně do složky `/usr/local/`. Dodatečný software je pak instalován do složky `/opt/liprobe/`. Instalační cesty lze změnit v souboru Makefile v proměnných `INSTALL_PATH` a `ADD_SW_INSTALL_PATH`. Pro instalaci stačí tedy provést příkazy.

```
make
make install
```

  Součástí balíčků je i demonstrační verze SDM firmware uložená ve složce fw. Tu je možné nahrát pomocí skriptu přiloženého ve stejné složce.
– Pokud selže jeden z kroků při instalaci, pak server není pravděpodobně správně nainstalován. Pokud výstup skriptu odpovídá výše uvedenému výstupu. Pak se obraťte na ...

3 Instalace sondy do sítě

Zachycení dat na sondě je realizováno 100Gb portem na kartě ComboV3. Dle typu transceiveru CFP 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. Z tapu vedou dva monitorovací porty, které se zapojí pomocí optických kabelů do monitorovacích portů Combo V3. Připojte sondu k Internetu pomocí management portu a zkontrolujte konektivitu. Před začátkem odesílání dat je nutné, aby byly spuštěny všechny funkce SLIS.

4 Konfigurace a ovládání sondy

Výchozí konfigurace sondy je uložena v souboru `probe_default.ini`. Ten je vytvořen při instalaci sondy ve složce `/etc/liprobe/defaults`. Tuto konfiguraci je možné hned používat. V případě potřeby je možné konfiguraci upravit pomocí programu `probe_control` Dále tento program slouží k ovládání sondy. Může pracovat jak dávkově, tak i interaktivně. Činnost programu je ilustrována v následujících příkladech:

- Spuštění v interaktivním režimu:

```
probe_control -i
Welcome to LI probe supervisor
Command: _
```

- Výpis stavu softwarových komponent sondy a stavu hardware při vypnutém SW:

```
#interaktivně
Welcome to LI probe supervisor
Command: report all

CCCID               OFFLINE
Filterd             OFFLINE
INI3D               OFFLINE

Interface:          0
Link speed:         10 Gb/s
Total packets:      0
Received:           0
Discarded:          0

Interface:          1
Link speed:         10 Gb/s
Total packets:      0
```

```
Received:           0
Discarded:          0

#dávkově
probe_control report all
CCCID               OFFLINE
Filterd             OFFLINE
INI3D               OFFLINE

Interface:          0
Link speed:         10 Gb/s
Total packets:      0
Received:           0
Discarded:          0

Interface:          1
Link speed:         10 Gb/s
Total packets:      0
Received:           0
Discarded:          0
```

Výpis stavu software obsahuje informaci o stavu jednotlivých komponent. V případě, že dojde k nějaké události je ve výpisu uvedena závažnost a je vypsán poslední záznam z logu patřičné komponenty. Stav hardware pak udává rychlost přípojené linky a čítače celkového množství paketů, přijatých paketů a paketů zahozených již na vstupu z důvodu nedostatku kapacity nebo chyby.

– Výpis konfigurace software podle aktuálního souboru:

```
Command: config show
General probe settings
Intercepted Interface:              sze


Path to executable files:           /usr/local/bin/
Paths to log files:                 /var/log/liprobe/modules/


Communication map
SLIS <---> Probe:                   localhost
                                    21105 (CCCI)
                                    21103 (INI3)

Internal CCCI <---> filterd:        localhost
                                    65200
```

```
                                    UNIX Socket

Internal INI3 <---> filterd:        localhost
                                    65300
                                    UNIX Socket
```

– Nastavení komunikační mapy sondy. Novou konfiguraci sondy je nutné uložit a Sw musí být restartován, aby se projevily změny.

```
Command: config set communication
New SLIS hostname/ip address: localhost
New CCCI system hostname/ip address: localhost
New INI3 system hostname/ip address: localhost
Interface for internal communication
between CCCI and filterd [tcp/unix]: tcp
Interface for internal communication
between INI3d and filterd [tcp/unix]: tcp
Port to SLIS for CCCI [0 - 65535]: 21005
Internal port for CCCI and filterd [0 - 65535]: 32000
Internal port for INI3D and filterd [0 - 65535]: 32001
Port to SLIS for INI3D [0 - 65535] :21003
Command: config show
General probe settings
Intercepted Interface:              sze


Path to executable files:           /usr/local/bin/
Paths to log files:                 /var/log/liprobe/modules/


Communication map
SLIS <---> Probe:                   localhost
                                    21005 (CCCI)
                                    21103 (INI3)

Internal CCCI <---> filterd:        localhost
                                    32000
                                    TCP Socket

Internal INI3 <---> filterd:        localhost
                                    32001
                                    TCP Socket
```

Při průběhu nastavení je možné ponechat volbu prázdnou. Hodnota bude automaticky doplněna podle poslední známé konfigurace. Změna nastavení sondy je možná pouze při interaktivním režimu.

Tabulka 1. Význam proměnných obsažených v konfiguračních souborech sondy

Proměnná	**Sekce**	**Akce**
probe_ifc	GENERAL	Rozhraní použité pro záchyt provozu
exe-path	Paths	Cesta ke spustitelným souborům sw sondy
log-path	Paths	Cesta k souborům s hlášeními sondy
slis-host	Communication	IP adresa/hostname serveru s LI systémem
ccci-host	Communication	IP adresa/hostname PC obsluhujícím zprávy CCCI
ini3-host	Communication	IP adresa/hostname PC odesílající zachycená data na INI3
slis-ccci-port	Communication	port pro komunikaci mezi LI serverem a sondou pro CCCI rozhraní
ccci-filterd-port	Communication	port pro komunikaci mezi sw komponentami pro CCCI a filtrem
ini3-filterd-port	Communication	port pro komunikaci mezi sw komponentami pro INI3 a filtrem
slis-ini3-port	Communication	port pro komunikaci mezi LI serverem a sondou pro INI3 rozhraní
ccci-filterd-ifc	Communication	typ rozhraní mezi sw komponentami pro CCCI a filtrem (UNIX nebo TCP socket)
ini3-filterd-ifc	Communication	typ rozhraní mezi sw komponentami pro INI3 a filtrem (UNIX nebo TCP socket)

5 Spuštění a ovládání sondy

Po nastavení konfigurace je možné ovládat sondu programem `probe_control`, který může být spouštěn dávkově nebo interaktivně. V dávkovém režimu probíhá ovládání pomocí `probe_control <příkaz>`. Interaktivní režim je pak spouštěn příkazem `probe_control -i`. Význam příkazů je popsán v tabulce 2.

Tabulka 2. Příkazy ovládající sondu a jejich význam

Příkaz	**Akce**
start	Provede spuštění softwarových částí sondy.
restart	Ukončí běžící softwarové části a provede jejich znovuspuštění.
stop	ukončí běžící LI programy, spustí programy LI programy.
report	Vypíše stav softwarových částí a čítače obsažené ve firmware.
config	(pouze v interaktivním režimu) Umožňuje změnit konfiguraci softwarových částí.
exit	(pouze v interaktivním režimu) Ukončí interaktivní režim programu probe_control.
watch	(pouze v interaktivním režimu) Nastaví periodickou kontrolu stavu sondy.
help	(pouze v interaktivním režimu) Vypíše nápovědu k příkazům interaktivního režimu.
logging	(pouze v interaktivním režimu) Vypíše úroveň závažnosti pro oznámení stavu. Pokud je k příkazu uvedena hodnota, pak ji nastaví. Urovně závažnosti jsou shodné se systémem syslog.

6 Kapacita pravidel

Počet pravidel, které je možné skrze SLIS nakonfigurovat na sondě je omezen. Provoz lze zachýtávat podle síťového toku identifikovaného pěticí zdrojová a cílová IP adresa, zdorjový a cílový port a protokol L4 vrstvy. Dále je možné zachytávat všechen provoz na dané IP adrese a portu nebo provoz odpovídající pouze IP adrese případně síťové masce/prefixu. Kapacita pravidel se pohybuje maximálně cca 30 000 pravidel pro síťové toky a 30 000 pro pravidla typu IP adresa + port (efektivně 30 000 * plný rozsah portů na obou protokolech). Maximánlní počet pravidel pro IP adresy/masky je "omezen"dostupnou pamětí serveru, avšak vzhledem k efektivitě předchozích pravidel by měla tato pravidla být využívána co nejméně.

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 100Gbps portu. Typ transceiverů a kabelu musí být buď SM nebo MM.
3. Zkontrolujte, že máte správný konfigurační soubor (`probe_config.ini` příp. `probe_default.ini`).
4. Zkontrolujte, že je dostupné připojení k SLIS

```
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

   ```
   probe_control stop
   ```

7. Zkontrolujte obsah složky /var/run/liprobe/. Pokud obsahuje jiné soubory než probe_monitor.pid, tak je smažte.
8. Následně proveďte restart LI programů příkazem:

   ```
   probe_control start
   ```

9. Pokud se všechny komponenty ohlásí stavem OK a přesto sonda nefunguje správně. Zkontrolujte logy ve složce /var/log/liprobe/modules/.
10. Zašlete na adresu izadnik@fit.vutbr.cz email s popisem chyby a přiložte soubory ze složky: /var/log/ liprobe/

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.