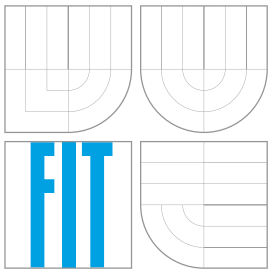
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

MANUÁL K APLIKACI BAKALÁŘSKÉ PRÁCE: TVORBA METADAT PŘI ODPOSLECHU KOMUNIKACE V REÁLNÉM ČASE

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

STANISLAV BÁRTA

BRNO 2012

Kapitola 1

Překlad a spuštění aplikace

Na přiloženém DVD je připraven image operačního systému, který obsahuje přeloženou aplikaci a všechny potřebné balíky jsou nainstalovány. Použití připraveného image je popsáno v kapitole 2. V následující sekci jsou uvedeny pokyny, které je nutno splnit pro překlad aplikace na jiném počítači.

1.1 Překlad aplikace

Pro překlad aplikace je potřeba mít nainstalované balíky libpcap a libpcap-dev. Mezi zdrojovými soubory je připraven soubor Makefile programu make, který překlad automaticky provede. Stačí zadat příkaz `make` v terminálu s nastavenou cestou adresáře obsahujícího zdrojové soubory.

1.2 Spuštění aplikace

Aby mohla aplikace správě fungovat, je třeba aby existovala Administration Function a Mediation Function, ke kterým je třeba se připojit. Pro účely testování aplikace provádějící odposlechy byly vytvořeny pomocné aplikace, které zajišťují částečnou funkčnost těchto bloků. Pro překlad pomocných aplikací jsou také připraveny soubory Makefile pro automatizovaný překlad. Aplikaci provádějící odposlechy je nutno spustit s administrátorskými právy, aby mohl být prováděn odposlech na zadaném rozhraní.

1.2.1 Mediation Function (MF)

Pomocná aplikace, která přijímá vytvořené zprávy IRI a pouze je přepisuje na standardní výstup. Aplikaci je nutné spustit s parametrem:

- `-p <port_pro_komunikaci_s_aplikaci_provadejici_odposlech>`

1.2.2 Administration Function (AF)

Pomocná aplikace, pomocí které je možno zadávat nebo rušit požadavky na odposlechy. Aplikaci je nutné spustit s parametrem:

- `-p <port_pro_komunikaci_s_aplikaci_provadejici_odposlech>`

1.2.3 Aplikace provádějící odposlech komunikace

Aplikaci je možné spustit teprve poté, co jsou spuštěny obě dříve uvedené pomocné aplikace a je ji nutno spustit s následujícími parametry, které je možno zadat v libovolném pořadí:

- `--af_ip <ip_adresa_administration_function>`
- `--af_port <port_pro_komunikaci_s_administration_function>`
- `--mf_ip <ip_adresa_mediation_function>`
- `--mf_port <port_pro_komunikaci_s_mediation_function>`
- `--interface <nazev_rozhrani_kde_provadet_odposlech>`

Je možno zadat volitelný parametr, který aplikaci řekne, aby zpracovávala komunikaci probíhající pouze na portech specifických pro sledované protokoly pro komunikaci v reálném čase. Tímto parametrem je:

- `--pouze_specificke_porty`

1.3 Ovládání aplikace

Aplikaci provádějící odposlechy nelze ovládat přímo a po jejím spuštění je její činnost řízena prostřednictvím pomocné aplikace AF. Požadavky na zadání nebo zrušení odposlechu se zapisují na standardní vstup v podobě: *Akce;Protokol;Typ;Identifikátor*, kde jednotlivé položky nabívají hodnot z následujícího seznamu.

Akce jedna z možností `PRIDAT` nebo `ODEBRAT`

Protokol jedna z možností `XMPP`, `IRC` nebo `OSCAR`

Typ `IPv4`, `IPv4-ROZSAH` nebo `ID`

Identifikátor podle zadaného typu `<IP adresa>`, `<IP adresa>/počet_bitů_sítě` nebo `<identifikátor uživatele daného protokolu>`

Pokud nejsou zadány všechny uvedené položky, aplikace takový požadavek ignoruje.

Kapitola 2

Testování

Pro testování aplikace je na přiloženém DVD vytvořen obraz operačního systému Debian s přeloženými aplikacemi. Dále jsou zde nachystány klientské aplikace protokolů XMPP, IRC a OSCAR s připravenými účty pro testování.

V operačním systému je vytvořen účet s uživatelským jménem `user` a heslem `user`. Heslo pro příkaz sudo je také `user`. Účet uživatele root není vytvořen a pro spouštění aplikací s administrátorskými právy je třeba využít příkazu sudo.

Binární aplikace jsou umístěny na ploše v adresáři `bakalářská práce` a zdrojové kódy jsou umístěny v podadresáři `zdroje` a jsou rozděleny do adresářů podle příslušné aplikace.

2.1 Klientská aplikace protokolu XMPP

Pro testování odposlechů protokolu XMPP je nainstalována aplikace Psi, ve které je vytvořen uživatelský účet. Přihlašovací údaje jsou v tabulce 2.1 a v aplikaci jsou uloženy.

Uživatelské jméno	**Heslo**
testovani_bp@jabbim.cz	user

Tabulka 2.1: Přihlašovací údaje pro klientsou aplikaci protokolu XMPP

2.2 Klientská aplikace protokolu IRC

Pro testování odposlechů protokolu IRC je nainstalována aplikace XChat IRC s nastaveným uživatelským jménem `testovani_bp`. Pokud by toto uživatelské jméno bylo již využíváno, použije se uživatelské jméno `testovani_bp_` případně `testovani_bp__`.

2.3 Klientská aplikace protokolu OSCAR

Pro testování odposlechů protokolu OSCAR je nainstalována aplikace Pidgin, ve které je vytvořen uživatelský účet. Přihlašovací údaje jsou v tabulce 2.2 a v aplikaci jsou uloženy.

Uživatelské jméno (UIN)	Heslo
624269901	a1b2c3

Tabulka 2.2: Přihlašovací údaje pro klientsou aplikaci protokolu OSCAR

2.4 Připravené soubory se zachycenou komunikací

Přiložené DVD obsahuje .cap soubory se zachycenou komunikací jednotlivých protokolů pro komunikaci v reálném čase. Stejné soubory jsou uloženy na ploše virtuálního operačního systému v adresáři `cap soubory`. Tyto soubory lze použít pro testování aplikace bez nutnosti spouštět klientské aplikace. Pomocí aplikace Tcpreplay, která je ve virtuálním operačním systému předinstalována, je možné zachycenou komunikaci přehrát na požadovaném rozhraní.