Package ezipupdate

Claas Hilbrecht *email: babel@fli4l.de* Das fli4l-Team

24. Oktober 2003

Inhaltsverzeichnis

1 Dokumentation des Paketes dropbear

1.1 DROPBEAR – Ein SSH2 Server für kleine Systeme

Dropbear ist ein SSH2 Server der speziell für kleine Systeme wie fli4l entwickelt wird. Dadurch ist es möglich einen SSH2 Server mit nur ca. 125 KB Größe zu erstellen. Verglichen mit dem SSH1 Server der bei fli4l mitgeliefert wird ergibt sich eine Platzersparnis von ca. 50 KB wenn man die opt.tgz Datei vergleicht.

Eine Secure-Shell bietet die Möglichkeit, eine verschlüsselte Verbindung mit dem fli4l-Router aufzunehmen. Außerdem können mit dem Secure-Copy-Befehl Dateien verschlüsselt übertragen werden. Wenn Public Key Anmeldung benutzt (siehe unten) verwendet wird, können Befehle auf dem fli4l-router und Dateiübertragungen auch scriptgesteuert ausgeführt werden. Es sollte auf jeden Fall ein Password mit der PASSWORD-Variablen in der config/base.txt gesetzt werden!

1.2 Konfiguration

In der Datei config/dropbear.txt sind einige Variablen wie fli4l üblich zu setzen, nämlich:

OPT_DROPBEAR Wird diese Variable auf 'yes' gesetzt, wird der Dropbear SSH2 Server aktiviert. Mit dem Wert 'no' wird die Verwendung des kompletten OPT–Paketes abgeschaltet.

DROPBEAR_SCP Kopiert das scp Programm vom original SSH Paket von fli4l mit auf dem Router. Das ist praktisch, wenn man Dateien per scp auf den Router kopieren will.

DROPBEAR_KEYPROG Kann auf 'yes' oder 'no' eingestellt werden. Nur um ein neues Hostkeypaar zu erzeugen ist es sinnvoll die Einstellung auf 'yes' setzen. Im „normalem“ Betrieb ist das Programm dropbearkey nicht notwendig.

Ein SSH Server benötigt ein sogenanntes Hostkeypaar das weltweit einmalig sein sollte und einen Rechner eindeutig identifiziert. Zwar wird ein Hostkeypaar im Dropbear opt mitgeliefert, aber das sollte nur für die ersten Tests benutzt werden. Soll der Dropbear permanent auf dem fli4l Router installiert werden sollte in jedem Fall jeder fli4l Router sein eigenes, individuelles Hostkeypaar bekommen. Würde jeder fli4l Router mit dem Hostkeypaar aus dem fli4l Paket arbeiten wäre es nicht möglich eine so genannte Man-in-the-Middle-Attacken zu erkennen. Wenn ein Haker es schaffen würde die IP-Adresse Ihres fli4l Routers zu übernehmen würde

Ihr SSH Client nicht erkennen dass Sie keine Verbindung mit Ihrem fli4l Router aufnehmen, sondern mit dem des Hakers. Genau vor diesem Szenario schützt das erstellen eines eigenen, nur Ihnen bekannten Hostkeypaares.

Die Hostkeys für Dropbear können mit dem Programm dropbearkey erstellt werden. Setzen Sie dazu den Wert DROPBEARKEY auf 'yes' und erstellen Sie eine neue fli4l Diskette und booten von dieser Diskette. Melden Sie sich dann auf dem fli4l Router an und erzeugen das neue Hostkeypaar mit folgenden Befehlen.

```
fli4l 2.1.4 # cd /tmp
fli4l 2.1.4 # dropbearkey -t rsa -f dropbear_rsa_host_key
Will output 1024 bit rsa secret key to 'dropbear_rsa_host_key'
Generating key, this may take a while...
Done.
fli4l 2.1.4 # dropbearkey -t dss -f dropbear_dss_host_key
Will output 1024 bit dss secret key to 'dropbear_dss_host_key'
Generating key, this may take a while...
Done.
fli4l 2.1.4 # cp dropbear*key /boot
```

Kopieren Sie jetzt die beiden auf der Diskette befindlichen Dropbear Hostkeydateien dropbear_dss_host_key und dropbear_rsa_host_key anstelle der originalen Hostkeydateien in das Verzeichnis etc/dropbear Ihrer aktuellen fli4l Installation. Setzen Sie danach den Wert DROPBEARKEY wieder auf 'no' um Platz auf der fli4l Diskette zu sparen.

DROPBEAR_PORT Ein SSH Server horcht standardmäßig auf Port 22. Bei Bedarf kann der SSH Server Dropbear auch auf einem anderen Port auf SSH Client verbinden horchen. Tragen Sie hier einfach die von Ihnen gewünschte Portnummer ein.

DROPBEAR_PUBLIC_KEYS_N Dropbear unterstützt die Möglichkeit der Anmeldung mit Public Keys. Sie können hier angeben, wieviele Public Keys Sie verwalten wollen.

Eine leicht verständliche Einführung in die Public Key Anmeldung können Sie im Internet auf den Seiten des Windowsclient Putty finden. Sie können dort direkt in das Kapitel „Using public keys for SSH authentication“ (siehe http://the.earth.li/ sgtatham/putty/0.53b/htmldoc/Chapter8.html#8).

DROPBEAR_PUBLIC_KEY_x Tragen Sie hier den Public Key ein. Am einfachsten geht das per Cut-and-Paste aus einem Terminalfenster.

Das Schlüsselpaar erzeugt man mit Hilfe von ssh-keygen (oder puttygen, wenn putty unter Windows als ssh Client eingesetzt wird). Wird beim Schlüsselerzeugen eine Passphrase vergeben (also ein Password, das man braucht, wenn man den Schlüssel benutzen will), sollte man über den Einsatz eines Schlüsselagenten nachdenken (siehe ssh-agent oder pageant).

Hinweis: Die privaten Teile der Schlüsselpaare (Datei 'identity'), deren öffentliche Teile in die Konfigurationsdatei übernommen werden, sind so sorgfältig zu behandeln wie Passworte, da sie die gleiche Funktion erfüllen. Zum ssh/scp-Zugriff sind immer beide Dateien beim Client erforderlich, mit dem öffentlichen Schlüssel allein (identity.pub) ist kein ssh-Zu- griff ohne Passworteingabe möglich.

1.3 Beispiel check/dropbear.txt Datei

Ein Beispiel für eine komplette config/dropbear.txt Konfigurationsdatei sieht so aus:

```
OPT_DROPBEAR='yes'

DROPBEAR_PORT='22'
DROPBEARKEY='no'

DROPBEAR_PUBLIC_KEYS_N='1'
DROPBEAR_PUBLIC_KEY_1='1024 35 <viele Zahlen> root@fli4l'
```

1.4 Literatur

Original Dropbear SSH2 Site: http://matt.ucc.asn.au/dropbear/dropbear.html

Claas Hilbrecht <babel@fli4l.de>, im Oktober 2003

A Anhang zum Paket dropbear