OpenSSH triky

Server

...

Klient

Visual Host Key - Grafický fingerprint klíče

 V SSH klientovi z balíku OpenSSH (Open BSD Secure Shell - což je mimochodem v UN*Xovém světě ten nejrozšířenější a asi i nejrozšířenější vůbec) se nedávno objevila nová funkce, která umožní kromě klasického textového MD5/SHA fingerprintu veřejného SSH klíče zobrazit navíc ještě grafický otisk (tvořený ASCII znaky). To má umožnit lépe si zapamatovat otisk a případně si všimnout jeho změny. To má smysl při přihlašování z místa, kde nemáte otisk uložený i z míst, kde je možné, že vám otisk někdo podstrčil, nebo podobně. <!–more–><br style="clear:left;" /> Funkci je možné povolit přidáním řádku

```
VisualHostKey yes
```

do konfiguračního souboru <tt>/etc/ssh/ssh_config</tt>.

Při každém přihlašování ke vzdálenému SSH serveru potom na svojí obrazovce uvidíte obrázek jako je níže (za ním bude následovat welcome banner serveru a většinou výzva pro zadání hesla). Tady můžete vidět grafický otisk serveru harvie.cz:

<pre>

```
0 ;) harvie@harvie-ntb ~ $ ssh harvie.cz
Host key fingerprint is 41:72:28:3d:f5:f5:d3:a2:0b:f6:e5:c7:a2:c4:b0:d3
+--[ RSA 2048]----+
|     ..o+   .    |
|    . ++ . . . . |
|     . .. .   + .|
|         .   . o |
|        S + . .  |
|         . B + . |
|          o E o o|
|           o . o |
|             .   |
+-----------------+
```

</pre> A na jiném serveru může grafický fingerprint vypadat třeba takhle: <pre>

```
130 ;( harvie@harvie-ntb ~ $ ssh 192.168.2.137
Host key fingerprint is 17:bb:27:2a:6b:e0:31:e1:5f:d7:fd:e1:27:76:b5:79
+--[ RSA 2048]----+
|                 |
|                 |
|          .      |
|    .      o     |
|   . .  S o. .   |
|    =   ..... ...|
|   . = . .o . ..=|
|    . +  . o  o+E|
|     ..o.    . oo|
+-----------------+
```

</pre>

Pokud by se taková funkce objevila třeba u grafického klienta Putty, jistě by zde byla zajímavá možnost vytvářet nějaké grafické koláže jako třeba: <tt>tyrkysový - lev - na měsíci - sleduje fialového - krokodýla - na obloze je nápis A1</tt> Což je nejen zvráceně ulítlé, ale také podle nauky o lidské paměti dobře zapamatovatelné (jako všechny jednoduché, ale zvráceně ulítlé motivy). Kromě poskládaného obrázku by klient mohl zobrazovat ještě podobnou textovou interpretaci pro kompatibilitu s čistě textovými klienty... Tím by se jistě zlepšila bezpečnost a zjednodušila by se nutnost nosit v hlavě fingerprinty. Samozřejmě na druhou stranu by bylo nutné udělat koláž dostatečně složitou, protože jinak by bylo snadné najít v podobném hashovacím algoritmu kolizi a tím vystavit server ještě většímu nebezpečí.

Tudíž pro začátek radím jenom

```
echo VisualHostKey yes >>/etc/ssh/ssh_config
```

(pokud jste tak ještě neučinili)