Experimentálne porovnanie výkonu OpenVPN pri použití rôznych kryptografických algoritmov

Michal Petrucha, Ladislav Bačo

RNDr. Jaroslav Janáček, PhD.

Fakulta matematiky, fyziky a informatiky
Univerzita Komenského, Bratislava

26. mája 2014

Zadanie projektu

Úloha

Cieľom projektu je experimentálne zistiť vplyv použitého kryptografického algoritmu na maximálnu prenosovú rýchlosť dosiahnuteľnú medzi dvomi počítačmi pri nasadení OpenVPN, resp. vplyv na vyťaženia procesora v prípade, že dosiahnutá maximálna prenosová rýchlosť bude limitovaná inými faktormi. Na riešenie projektu je možné využiť sieťové laboratórium KI.

- statický kľúč vs. certifikáty, privátne a verejné kľuče
  - výhody: jednoduchšie nastavenie, žiadne PKI
- minimálna konfigurácia:

server

```
dev tun
ifconfig $SERVER_VPN_IP $CLIENT_VPN_IP
secret $STATIC_KEY
```

client

```
dev tun
remote $SERVER_IP
ifconfig $CLIENT_VPN_IP $SERVER_VPN_IP
secret $STATIC_KEY
```

- ďalšie parametre:
  - HMAC autentifikácia paketov: `auth SHA512`
  - šifrovací algoritmus: `cipher AES-256-CBC`
  - veľkosť kľúča: `keysize n`
  - kompresia: `comp-lzo yes|no`

- `nc, pv`
- gigabit ethernet, bez OpenVPN
  - `/dev/zero` $\approx$ 112 MBps
  - `/dev/urandom` $\approx$ 5 MBps ??
  - `video.mp4` $\approx$ 80 MBps
  - bottleneck: HDD $\rightarrow$ ramdisk
- s OpenVPN:
  - 40 šifrovacích algoritmov
  - 25 hašovacích funkcií
  - kompresia
  - aspoň dva druhy súborov (nulový, náhodný)
  - obojsmerné posielanie
  - $40 \cdot 25 \cdot 2 \cdot 2 \cdot 2 = 8000$ testov!!
- to určite nechceme robiť ručne. . .

Testovací skript
Inicializácia

- ramdisk, adresáre pre test
- náhodný súbor z `dev/urandom`, odoslanie klientovi nulový súbor z `/dev/zero`
- generovanie kľúča, odoslanie klientovi
- vytvorenie, sychnronizácia a spoločná podmnožina použiteľných šifier a hašov

```
openvpn --show-ciphers, openvpn --show-digests
sort $TEST_DIR/ciphers.* | uniq -d | awk '{print $1}'
> $CIPHERS
```

- Testovacie prostredie:
  - Debian GNU/Linux 7.4, Intel Pentium 4@2.80GHz, 1GB RAM
  - OpenVPN 2.2.1
  - OpenSSL 1.0.1e-2+deb7u6
- `for COMP in no yes; do`
  `for DIGEST in $(cat $DIGESTS); do`
  `for CIPHER in $(cat $CIPHERS); do`
- vygenerovanie konfiguračných súborov, štart OpenVPN
- posielanie súborov z klienta na server a zo servera na klienta

```
BEFORE=$(get_time)
nc $(get_peer_ip) $NC_PORT < $1
AFTER=$(get_time)
echo "$AFTER - $BEFORE" | bc -l
```

  - fungujú iba CBC šifry!
  - neukončovanie `nc` listenera → sleep

Výsledky

- 16 šifier
- 25 hašov
- 3200 testov
- 1000 GB
- 30 hodín
- spracovanie meraní pomocou Pythonu a SQLite

súbor	avg	stdev	median	min	max
random	1.0027	0.002	1.0027	0.9796	1.0075
zero	0.6614	0.0943	0.6627	0.5164	0.84

Tabuľka: Vplyv kompresie na čas prenosu; čas prenosu bez kompresie: 1

Výsledky

šifra	avg	stdev	median	min	max
BF-CBC	1.0	0.0	1.0	1.0	1.0
CAMELLIA-128-CBC	1.0148	0.0036	1.014	1.0096	1.0236
CAMELLIA-256-CBC	1.0573	0.0044	1.0583	1.0456	1.0655
CAMELLIA-192-CBC	1.058	0.0046	1.0599	1.0467	1.0663
CAST5-CBC	1.0781	0.0078	1.0799	1.0603	1.0894
DES-CBC	1.1026	0.0119	1.1034	1.0776	1.1402
SEED-CBC	1.1045	0.0068	1.1058	1.0852	1.1147
DESX-CBC	1.1134	0.0109	1.1159	1.0887	1.1321
AES-128-CBC	1.2823	0.0221	1.2867	1.2235	1.3078
AES-192-CBC	1.3687	0.0293	1.376	1.2925	1.4016
RC2-64-CBC	1.4211	0.0364	1.4294	1.3309	1.4679
RC2-40-CBC	1.4213	0.0368	1.4306	1.3314	1.4694
RC2-CBC	1.4213	0.0365	1.4315	1.3318	1.4687
AES-256-CBC	1.4553	0.0376	1.4671	1.3593	1.498
DES-EDE-CBC	1.5821	0.0508	1.5934	1.4585	1.6539
DES-EDE3-CBC	1.5824	0.0504	1.592	1.4599	1.6551

Tabuľka: Vplyv šifrovacieho algoritmu na čas prenosu; čas prenosu pri použití BF-CBC: 1

Výsledky

haš	avg	stdev	median	min	max
MD4	1.0	0.0	1.0	1.0	1.0
RSA-MD4	1.0027	0.0066	1.0013	0.9985	1.0272
MD5	1.0082	0.0019	1.0084	1.0039	1.0111
RSA-MD5	1.0092	0.002	1.0092	1.005	1.0114
ecdsa-with-SHA1	1.0494	0.0098	1.0509	1.0312	1.0643
DSA-SHA1-old	1.0498	0.0094	1.0512	1.0328	1.0631
SHA1	1.0502	0.0094	1.0507	1.032	1.0627
DSA-SHA	1.0505	0.0099	1.0523	1.0328	1.0649
RSA-SHA1-2	1.0505	0.0095	1.0525	1.033	1.0656
RSA-SHA1	1.0506	0.0097	1.0524	1.0324	1.065
DSA-SHA1	1.0507	0.0102	1.051	1.0327	1.0654
DSA	1.0509	0.0095	1.052	1.0336	1.0644
RIPEMD160	1.0741	0.014	1.0746	1.0492	1.0936
RSA-RIPEMD160	1.0746	0.0147	1.0761	1.0503	1.0949
RSA-SHA	1.0846	0.0161	1.0873	1.0574	1.1073
SHA	1.0857	0.0165	1.0863	1.0582	1.1101
RSA-SHA224	1.133	0.0246	1.1346	1.0907	1.1695
SHA224	1.1331	0.0241	1.1346	1.0911	1.1687
SHA256	1.1367	0.0254	1.1369	1.0942	1.1735
RSA-SHA256	1.1369	0.0253	1.1369	1.0944	1.174
RSA-SHA512	1.2056	0.0383	1.2098	1.1504	1.2561
SHA512	1.206	0.0379	1.2113	1.1506	1.2593
SHA384	1.2106	0.0397	1.2164	1.1521	1.2651
RSA-SHA384	1.2108	0.0396	1.2163	1.1525	1.2635
whirlpool	1.327	0.0589	1.3344	1.2401	1.4065

Tabuľka: Vplyv hašovacej funkcie na čas prenosu; čas prenosu pri použití MD4: 1

Záver

- kompresia zero vs. random
- najrýchlejšia šifra: BF-CBC (AES, 3DES o 30-60% pomalšie)
- najrýchlejší haš: MD4, MD5 (ale bezpečnosť...)
- vhodný kompromis: SHA1 (5% pomalšie ako MD4)
- OpenVPN default: BF-CBC, SHA1 :-)

	šifra	haš	čas
1	BF-CBC	MD4	1.0
2	BF-CBC	RSA-MD4	1.0027
3	BF-CBC	MD5	1.0102
4	BF-CBC	RSA-MD5	1.0114
...	...	...	...
11	BF-CBC	SHA1	1.0612

	šifra	haš	čas
...	...	...	...
396	DES-EDE3-CBC	SHA384	1.9069
397	DES-EDE3-CBC	RSA-SHA384	1.9082
398	AES-256-CBC	whirlpool	1.9115
399	DES-EDE-CBC	whirlpool	2.051
400	DES-EDE3-CBC	whirlpool	2.053

Odkazy:

- https://github.com/laciKE/openvpn_test/
- https://openvpn.net/index.php/open-source/documentation/miscellaneous/78-static-key-mini-howto.html