Test šifrovacích algoritmů v IPsec-tools verze 0.4 na linuxu: wifi 11Mbit/s

Vložil/a r4bbiT [1], 28 Únor, 2005 - 15:06

- Encryption [2]
- Networks & Protocols [3]
- Recenze [4]

Volba správného šifrovacího algoritmu je při ochraně dat pomocí šifrování na prvním místě, hned za ním je ekonomika šifrování. Tento článek by Vám měl pomoci vybrat si algoritmus, který Vám bude nejlépe vyhovovat.

Jak to probíhalo?

- Na obou sestavách, použit driver hostap 0.1.3
- Instalace Ipsec-tools verze 0.4
- Tvorba souboru pro přenos o velikosti **30036Kb**
- Přenos přes FTP protokol pomocí programu **wget**
- Generování klíčů příslušné délky
- IPSEC použit v módu **transport** bez autentizace
- Meření času nástrojem **time**
- Kopírování proběhlo 2x a do grafu byl zanesen průměr obou nameřených hodnot, které jsou pro přehled v tabulce
- Šifra která si vedla nejlépe tzn. nejmenší čas je vyznačena tučně

Sestava A:

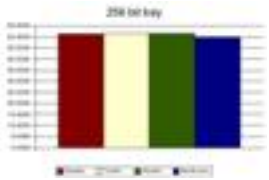
- **CPU:** Amd Duron 2000Mhz 64Kb
- **RAM:** 512MB
- **HDD:** 80GB 7200 rpm
- **Síťovka:** Z-com 626
- **Kernel:** 2.6.9

Sestava B:

- **CPU:** Intel Celeron M 1400 512Kb
- **RAM:** 256MB
- **HDD:** 40GB 4200 rpm
- **Síťovka:** Z-com 330
- **Kernel:** 2.6.9

256 bit key

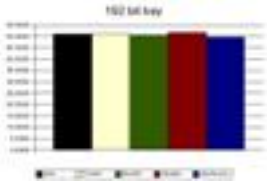
šifra	klí?	?as1	?as2	pr?m?r
Blowfish	256	51.5480	51.3500	51.4490
Rijndael	256	51.3440	51.3560	51.3500
Twofish	256	51.5010	51.7930	51.6470
Nešifrováno	###	49.6050	49.7030	46.6540



(kliknutím zobrazíte obrázek v původní velikosti) [5]

192 bit key

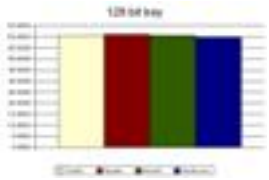
šifra	klí?	?as1	?as2	pr?m?r	
Blowfish	192	50.7840	50.4240		50.6040
Rijndael	192	51.2150	52.3400		51.7775
Twofish	192	51.3760	51.3000		51.3380
3DES	192	50.9250	50.9370	50.9310	
Nešifrováno	###	49.6050	49.7030		46.6540



(kliknutím zobrazíte obrázek v původní velikosti) [6]

128 bit key

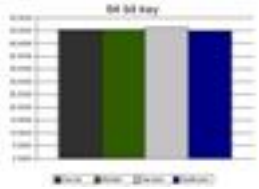
šifra	klí?	?as1	?as2	pr?m?r	
Blowfish	128	50.7280	50.7090		50.7185
Rijndael	128	50.9350	50.9810		50.9580
Twofish	128	50.9050	50.5310		50.7180
Nesifrovano	###	49.6050	49.7030		46.6540



(kliknutím zobrazíte obrázek v původní velikosti) [7]

64 bit key

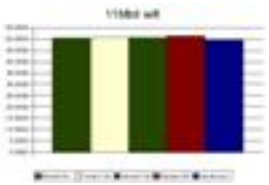
šifra	klí?	?as1	?as2	pr?m?r	
Blowfish	64	50.5300	50.2290		50.3795
DES-cbc	64	50.5110	50.3690		50.4400
DES-deriv	64	51.1400	51.0240		51.0820
Nešifrováno	###	49.6050	49.7030		46.6540



(kliknutím zobrazíte obrázek v původní velikosti) [8]

11Mbit/s wifi

šifra	klí?é	pr?m?r
Rijndael	256	51.3500
Blowfish	192	50.6040
Twofish	128	50.7180
Blowfish	64	50.3795
Nešifrováno	###	46.6540



[9]

Závěr

Jeden z důvodu, který mě vedl k provedení testu byl následek rozvoje technologií wifi, při kterém dochází k přenosu dat v nechráněném prostoru, kde je nutné data chránit. Použití WEPu se ukázalo jako nepříliš dostatečná ochrana. Rozhodl jsem se test provést pomocí IPSECu, protože splňoval vše co jsem potřeboval. Nechtěl jsem se starat o podporu šifrování přímo v aplikacích, tím pro mě byl IPSEC jasnou volbou jelikož jeho implementace zasahuje přímo do nejnižších vrstrev protokolu IP a tím chrání veškerý síťový provoz. Ve verzích protokolu ipv4 je nutné podporu zajistit "ručně", ve verzích ipv6 je implementován přímo do protokolu.

Test poukazuje na tři důležité body, jeden z nich je ten že šifrování na dostatečně silných (po hardwarowé stránece) počítačích je z ekonomického hlediska velice výhodne v porovanání s nešifrovaným přenosem. Druhým bodem je bezpečnost přenášených dat. Poslední co zbývá zmínit je volba správné šifry + klíče a to byl hlavní cíl který mě donutil k provedení testu, volba je patrná z grafu a tabulek.

URL článku:
https://www.security-portal.cz/clanky/test-%C5%A1ifrovac%C3%ADch-algoritm%C5%AF-v-ipsec-tools-verze-04-na-linuxu-wifi-11mbits

Odkazy:
[1] https://www.security-portal.cz/users/r4bbit
[2] https://www.security-portal.cz/category/tagy/encryption
[3] https://www.security-portal.cz/category/tagy/networks-protocols
[4] https://www.security-portal.cz/category/tagy/recenze
[5] https://www.security-portal.cz/img/clanky/44/256_11.jpg
[6] https://www.security-portal.cz/img/clanky/44/192_11.jpg
[7] https://www.security-portal.cz/img/clanky/44/128_11.jpg
[8] https://www.security-portal.cz/img/clanky/44/64_11.jpg
[9] https://www.security-portal.cz/img/clanky/44/11_wifi.jpg