Semestrální práce:

Kontrolní součty (MD5 a jiné) a jejich použití

Předmět: KAS - Kybernetická bezpečnost a šifrování
Datum: 29. 11. 2023
Autor: Jaroslav Körner

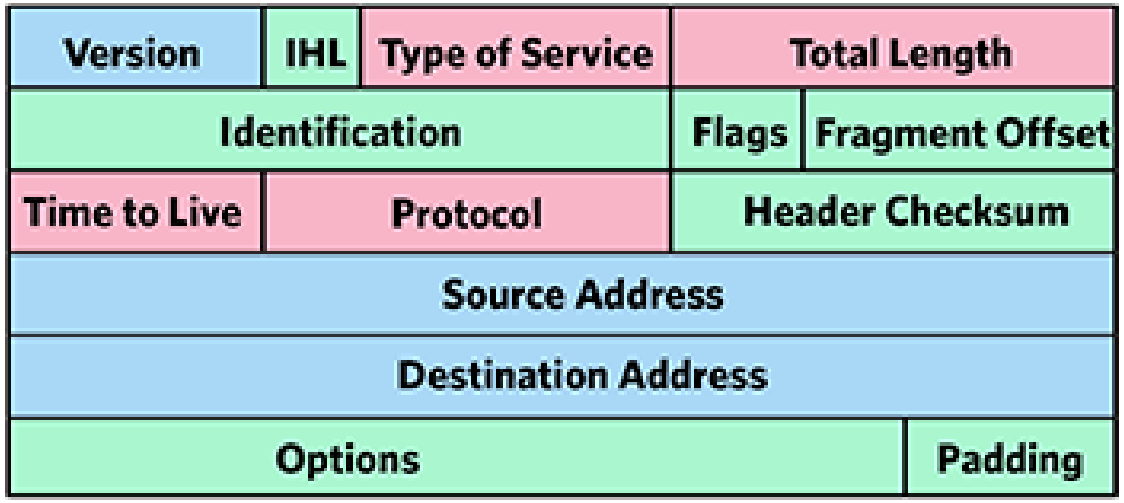
Kontrolní součty

32-Sum

1. Rozdělí zprávu na $n * 32b$.
2. Inicializujeme akumulátor na "0".
3. Aplikuje se "$sum()$" a "$mod(32)$".
4. Opakujeme krok 2 dokud nezpracujeme celou zprávu.
5. Určíme **dvojkový doplněk** (inverzní prvek pro sčítání).
6. Příjemce po přičtení všech přijatých slov získá 0.

Aplikace kontrolních součtů

- **Btrfs**, **Ext4**,
- **Ethernet** (IEEE 802.3), **SCTP**, **SATA**, **iSCSI**
- **ISBN-10**, **EAN-13**, **Bzip2**, **Zip**, **Gzip**, **PNG**, **MPEG-2**



Hash

- Královnina zpráva:

1. "Jsem těhotná asi s kočím z Mostu. Královna"
2. "Jsem těhotná, asi skočím z mostu. Královna"

- MD5 otisky:

1. `3c723007c372b83ea3e28161f174dbd`
2. `04005f28f6f6bed78a8a316df66a07f`

MD5

1. Inicializace akumulátorů.
2. Funkcemi využívajících operace `XOR`.
3. Netriviální proházení bitů.
4. Hodnoty se přičtou do akumulátorů.
5. Zpět na krok 2. dokud se vše nezpracuje.
6. Akumulatory se zřetězí na výstup (128b otisk).

```
word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98
word D: 76 54 32 10
```

```
F(X,Y,Z) = XY v not(X) Z
G(X,Y,Z) = XZ v Y not(Z)
H(X,Y,Z) = X xor Y xor Z
I(X,Y,Z) = Y xor (X v not(Z))
```

Použití:

- autenticita souborů při internetové komunikaci
- ochrana proti chybě přenosu:
  - nespolehlivým médiem (kontrolní součet)
  - úmyslné záměně souborů (otisk hashovací funkce)
- ukládání hesel (kryptografické hashovací funkce)
- asociativní vyhledávání v datech

Zdroje:

- Miroslav Němeček - Kontrolní součty a jejich výpočty v C
- Lukas Hron - kontrolni soucet checksum
- Computerphile: Hashing Algorithms and Security
- googlesource: crc32
- EAN13Barcode
- rfc: Rivest-MD5
- rfc: ISBN
- rfc: Computing the Internet Checksum

Otázky

- DALL-E
- IPv4

Děkuji za pozornost