Cyberbezpieczeństwo

1

Protokół HTTPS (czyli Hypertext Transfer Protocol Secure) to zabezpieczona wersja protokołu HTTP. Jego wdrożenie na stronie internetowej sprawia, że informacje przesyłane między serwerem a przeglądarką internetową nie dostaną się w niepowołane ręce. HTTPS szyfruje połączenie certyfikatem SSL lub TLS, gwarantując bezpieczeństwo danych użytkowników i właściciela witryny.

2

FileName | NWclients.txt | Hash| dd88482282785192d4a4ad4f8e32b3b6
FileName | SWclients.txt | Hash| c202036c9210959e7b587b08f080c378
FileName | NEclients.txt | Hash| 6c8fb699ac2ced0b5c9ea40aab9f8caf
FileName | SEclients.txt | Hash| 48d7eceee217e83cd685b537a3066b2f
FileName | Sclients.txt | Hash| abad7f7606e324f252bfebd6c09810e2
FileName | Nclients.txt | Hash| 65f586602d9476b7b561b5d98b2ea23b
FileName | income.txt | Hash| 1b319bc7ba0adc63f2af2cafdc59f5279d46dd33

Różni sie SEclients

```
SEclients.txt    d1c8f5b14685c1f3b748e9fa9b6860f0
```

3

Poprawny kod HMAC może stworzyć tylko osoba znająca tajny klucz *K*, co zapewnia autentyczność pochodzenia danych. Tylko osoba znająca klucz *K* może zweryfikować autentyczność danych zabezpieczonych kodem HMAC. Implementacje HMAC są oparte na standardowych kryptograficznych funkcjach skrótu takich jak SHA-2, SHA-1 czy MD5. Kody HMAC są stosowane w szeregu protokołów sieciowych np. w IPsec, gdzie klucze HMAC są niezależne od kluczy szyfrujących dane.

Tak jest zgodna z plikiem powyżej: 1b319bc7ba0adc63f2af2cafdc59f5279d46dd33

4. Wnioski

Jeśli chcemy dobrze zabezpieczyć nasze dane przed ich niechcianym przechwyceniem należy, szyfrować je na różnych poziomach i etapach oraz najlepiej żeby adressat mógł odczytać dane poprzez klucz do autoryzacji.