stateless auth tokens

елементарен трик

Васил Колев vasil@ludost.net

Проблемът

Често срещана практика

- нужен token за нещо
  - login
  - код за reset на парола
  - като цяло нещо, което да пратим и да удостовери, че че отсрещната страна го е получила
- генерира се random и се пише в таблица
- безсмислено действие
- подлежи на DoS

Решението

просто решение - подпис с криптографски hash/hash mac

- $userid.$timestamp.$somethingelse.$sign
- $sign = HMAC($userid.$timestamp.$somethingelse.$secret)
  - somethingelse може да се ползва за salt, за допълнителна сигурност
- проверява се се тривиално
- не изисква state
- не подлежи на DoS-ове

Инвалидация на token

- Автоматично от timestamp-а и изтичане на дадения живот на token-а
- За login - HMAC(*userid*.password.$secret)
  - смяната на паролата инвалидира token-а
- по-генерално решение - пазим кога е издаден последният валиден token
  - налага се да държим state, но е по-малко
- replay атаки?

Примери

VERP

- измислен от DJB
- https://en.wikipedia.org/wiki/Variable_envelope_return_path

TCP Syncookies

- също измислено от djb
- https://en.wikipedia.org/wiki/Syncookies

client-side session

- Всичко в сесията + подпис + timestamp
- на сървъра - само последен timestamp на промяна на сесията
- ползва се например в rails