DRUG

Piotr Niełacny

OAuth – Atak czasowy

9 listopada 2010

Plan wykładu

1. OAuth
   - Jak działa OAuth
   - Tworzenie klucza i podpisu
2. Atak czasowy
   - Definicja
   - Przykład

Plan wykładu

Podstawowe parametry

- `oauth_consumer_key` – przeważnie APP ID

Podstawowe parametry

- `oauth_consumer_key` – przeważnie APP ID
- `oauth_nonce` – losowy ciąg znaków unikalny dla zapytania

Podstawowe parametry

- `oauth_consumer_key` – przeważnie APP ID
- `oauth_nonce` – losowy ciąg znaków unikalny dla zapytania
- `oauth_signature_method` – nazwa używanej funkcji skrótu

Podstawowe parametry

- `oauth_consumer_key` – przeważnie APP ID
- `oauth_nonce` – losowy ciąg znaków unikalny dla zapytania
- `oauth_signature_method` – nazwa używanej funkcji skrótu
- `oauth_timestamp` – UNIX time

Plan wykładu

OAuth – tworzenie klucza

```
key = Secret&Token
```

OAuth – tworzenie sygnatury

```
oauth_sig = hmac(base_string, key)
```

Plan wykładu

Atak czasowy

W kryptografii atakiem czasowym nazywamy atak typu **side channel**, w którym atakujący próbuje skompromitować kryptosystem analizując czas odpowiedzi.

Plan wykładu

Atak czasowy

8.12800598144531 – całkiem różny
8.17031097412109 – różny od połowy
8.25114297866821 – prawidłowy

Pytania

Pytania?