The State of Authenticating RESTful APIs

@rob_winch


TOUCHING WIRES CAUSES
INSTANT DEATH
$200 FINE
Newcastle Tramway Authority

Authentication

Naïve approach…

https://api.example.com?
username=rob&password=secret

Naïve approach…

https://api.example.com?
username=rob&password=secret

Futurama

> Come on Bender. It's up to you to make your own decisions in life. That's what's separates people and robots from animals .. and animal robots!
>
> *Fry*

RFC-7231 Sensitive Information

“

Authors of services ought to avoid GET-based forms for the submission of sensitive data …

- RFC-7231: Section 9.4

Basic Authentication

```
HTTP/1.1 401 Access Denied
WWW-Authenticate: Basic realm="Rest"
Content-Length: 0
```

Basic Authentication

```
GET /messages/100 HTTP/1.1
Authorization: Basic cm9iOnNlY3JldA==
```

Digest Authentication

```
HA1 = MD5( "rob:rest@example.com:secret" )
    = 8ff99f404047cfbf7a5973437dd9453b

HA2 = MD5( "GET:/messages/" )
    = b3b2c648e81657249f8e940c9aa7a121

Response = MD5( "8ff99f404047cfbf7a5973437dd9453b:\
                 dcd98b7102dd2f0e8b11d0f600bfb0c093:\
                 00000001:0a4f113b:auth:\
                 b3b2c648e81657249f8e940c9aa7a121" )
         = 460b693843cc6d2c3b9bde8ec1eef505
```

Transport Layer Security (TLS)

- Confidentiality
- Integrity

goto fail;

Checking TLS

https://www.ssllabs.com/ssltest/

https://shaaaaaaaaaaaaaa.com/

BULLETPROOF SSL AND TLS

Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications

Ivan Ristić

Feisty Duck

Copyrighted Material

https://letsencrypt.org/

TLS Performance

- Computational overhead
- Latency overhead
- Cache

Adam Langley, Google

“On our production frontend machines, **SSL/TLS accounts for less than 1% of the CPU load**, less than 10 KB of memory per connection and less than 2% of network overhead.

https://goo.gl/IYJrqv

Doug Beaver, Facebook

"We have found that modern software-based TLS implementations running on **commodity CPUs are fast enough to handle heavy HTTPS traffic load** without needing to resort to dedicated cryptographic hardware.

https://goo.gl/pf8Xwh

Jacob Hoffman-Andrews, Twitter

> “HTTP keepalives and session resumption mean that most requests do not require a full handshake, so **handshake operations do not dominate our CPU usage**.

https://goo.gl/Re0ijb

TLS Optimize

- TLS Resumption
- Latency
- Online Certificate Status Protocol (OCSP)
- Cloudflare

Optimizing TLS

Is TLS Fast Yet.com

HTTP Basic over HTTPS?

oclHashcat

Hash Type	Speed
MD5	115.840 Bh/s
SHA1	37.336 Bh/s
SHA256	14.416 Bh/s
SHA512	4.976 Bh/s

Ubuntu 14.04, 64 bit
ForceWare 346.29
8x NVidia Titan X

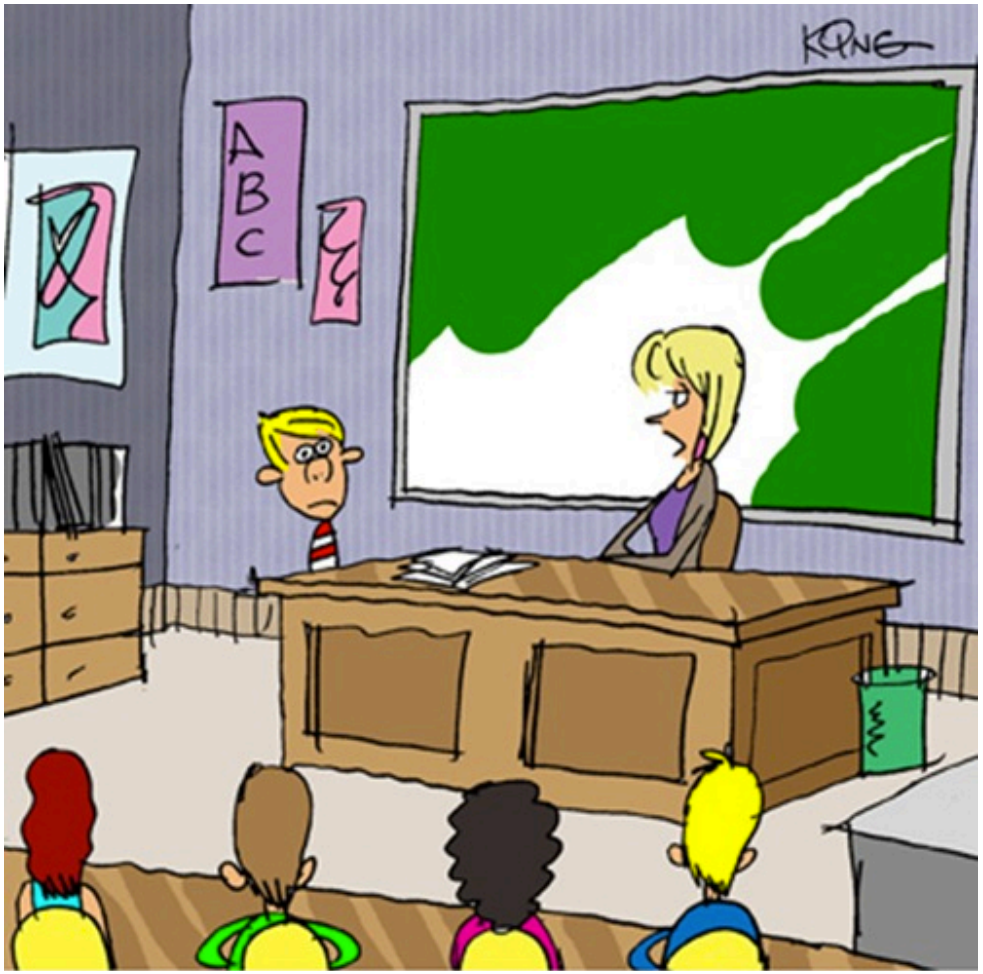
Introduce Session

```
username=winch&name=Rob+Winch
```

Encrypting the Session

```
Base64(IV,
       aes_cbc(k,IV,plainText))
```

- **k** – a secret key only known to server
- **aes_cbc** – encrypts the plainText using AES/CBC with the provided IV
- **plainText** – format of username=winch&name=Rob+Winch



Your handwriting is atrocious, not encrypted

Introduce Session

Can change properly encrypted value below:

```
username=winch&name=Rob+Winch
```

To have the following Plaintext

```
username=admin&name=Rob+Winch
```

https://goo.gl/2Uio0W

JWT Encoded

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.TJVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ

Header

```
{
  "alg": "HS256",
  "typ": "JWT”

}
```

Payload

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
```

JWT Signature

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  “secret”
)
```

Tony Arcieri
@bascule

Follow

JOSE/JWT considered harmful and dangerous (ask me why!)

2:03 PM - 27 Jul 2015

https://goo.gl/Hs383Z

Thomas H. Ptacek
@tqbf

Follow

Thinking about securing an API with JWT? First, punch yourself in the face. Then: just use a 256 bit random token, and a database.

10:54 AM - 28 May 2015

https://goo.gl/ZbP9Yp

JWT Encoded

eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.

Header

```
{
  "alg": "none",
  "typ": "JWT”

}
```

Payload

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
```

JWT Encoded

eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9. EkN-DOsnsuRjRO6BxXemmJDm3HbxrbRzXglbN2S…

Header

```
{
  "alg": "RS256",
  "typ": "JWT”

}
```

Payload

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
```

Creating RSASHA256

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  Private RSA Key
)
```

Verifying RSASHA256

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  provided signature,
  Public RSA Key
)
```

Header

```
{
  "alg": "HS256",
  "typ": "JWT”

}
```

JWT Signature

```
HMACSHA256(
   base64UrlEncode(header) + "." +
   base64UrlEncode(payload),
   RSA Public Key
)
```

HOW TO INSULT A DEVELOPER

Roy Fielding

“

… each request from client to server must contain all of the information necessary to understand the request, and **cannot take advantage of any stored context on the server**.

- Roy Fielding, Architectural Styles and the Design of Network-based Software Architectures

http://goo.gl/MzVy0V

Representational **STATE** transfer

“ **… session state can be transferred by the server to another service** such as a database to maintain a persistent state for a period and allow authentication

- Wikipedia

http://goo.gl/bd33t7


14

Summary

- Do NOT place sensitive information in URL
- Use HTTPS everywhere
- Use “cached” credentials
- Security prefers State

Presentation Available at
https://goo.gl/QTfCCW

@rob_winch