API Security

PHP|Tek 2012

Rob Richards
rrichards@mashery.com

Who am I?

Rob Richards

Mashery

Email: rrichards@mashery.com

Twitter: @mashery

Slides: www.cdatazone.org

MASHERY

www

MASHERY

Danger! Danger!

MASHERY

Traditional Web Site

- Browser based
- Tightly controlled ecosystem
  - UI
  - Data
  - Interaction

MASHERY

APIs

- Accessed by any number of apps, devices, browsers
- Increased threat exposure
  - Direct attack on API
  - End-user deception attack
  - Inadvertent attack

MASHERY

Apps Gone Wild!

MASHERY

I'm Under Attack!

(A True Story)

- Customer becoming flooded

MASHERY

I'm Under Attack!

(A True Story)

- Customer becoming flooded
- Looks like a DDoS

MASHERY

I'm Under Attack!

(A True Story)

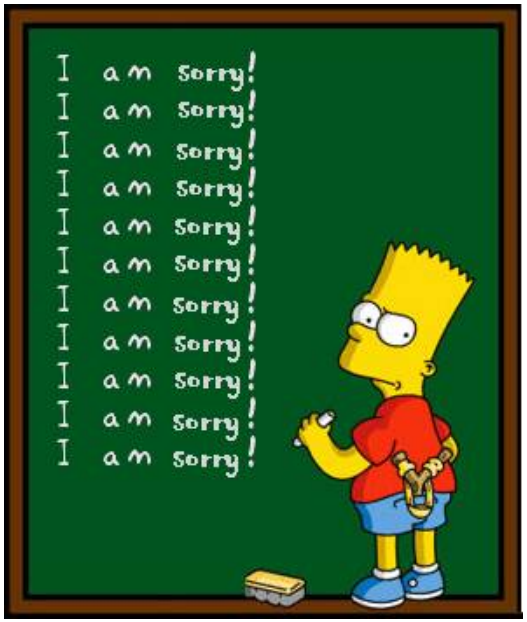
- Customer becoming flooded
- Looks like a DDoS
- Identify Attacker

MASHERY

I'm Under Attack!

(A True Story)

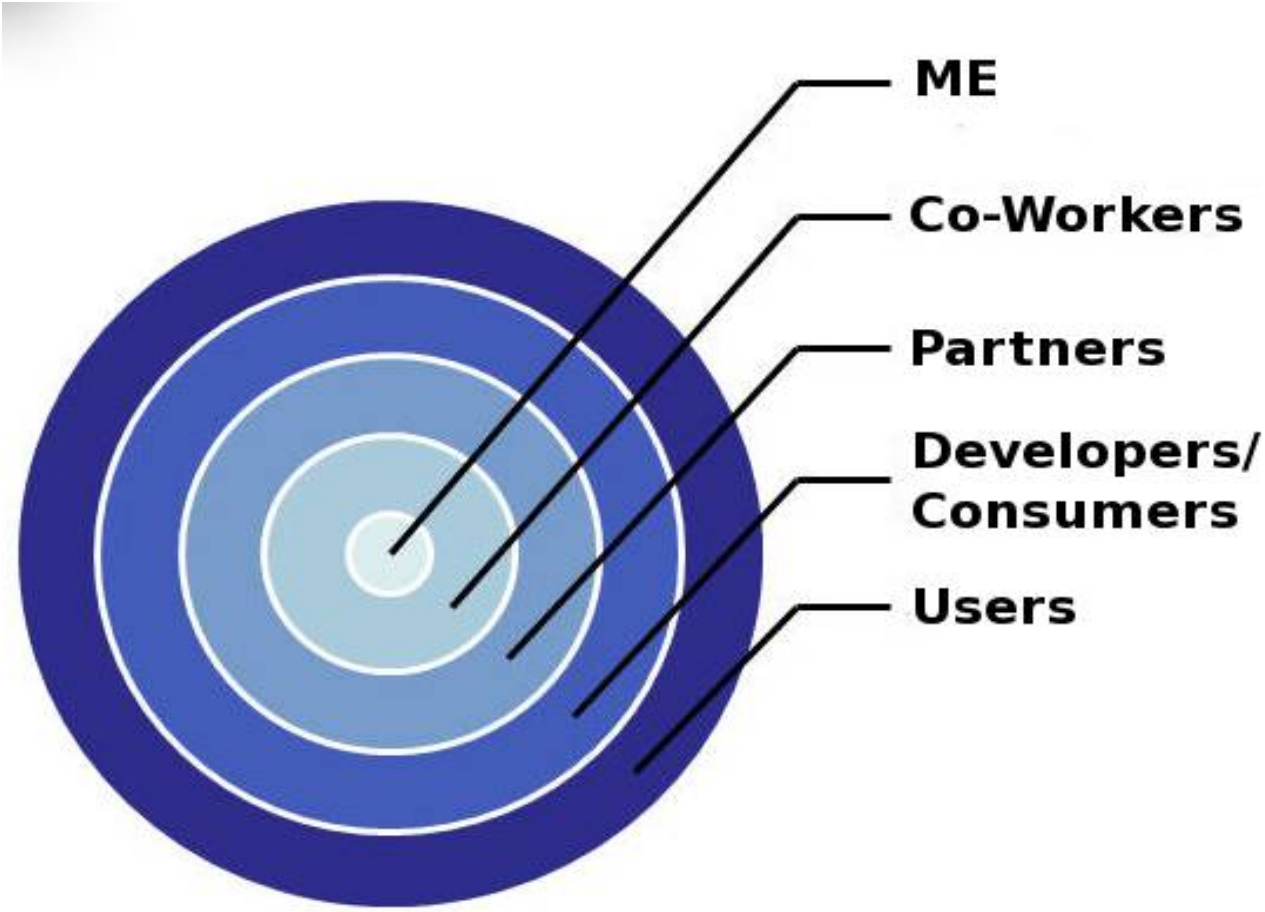
- Customer becoming flooded
- Looks like a DDoS
- Identify Attacker
- Poorly coded app
  - distributed to tens of thousands of devices



MASHERY

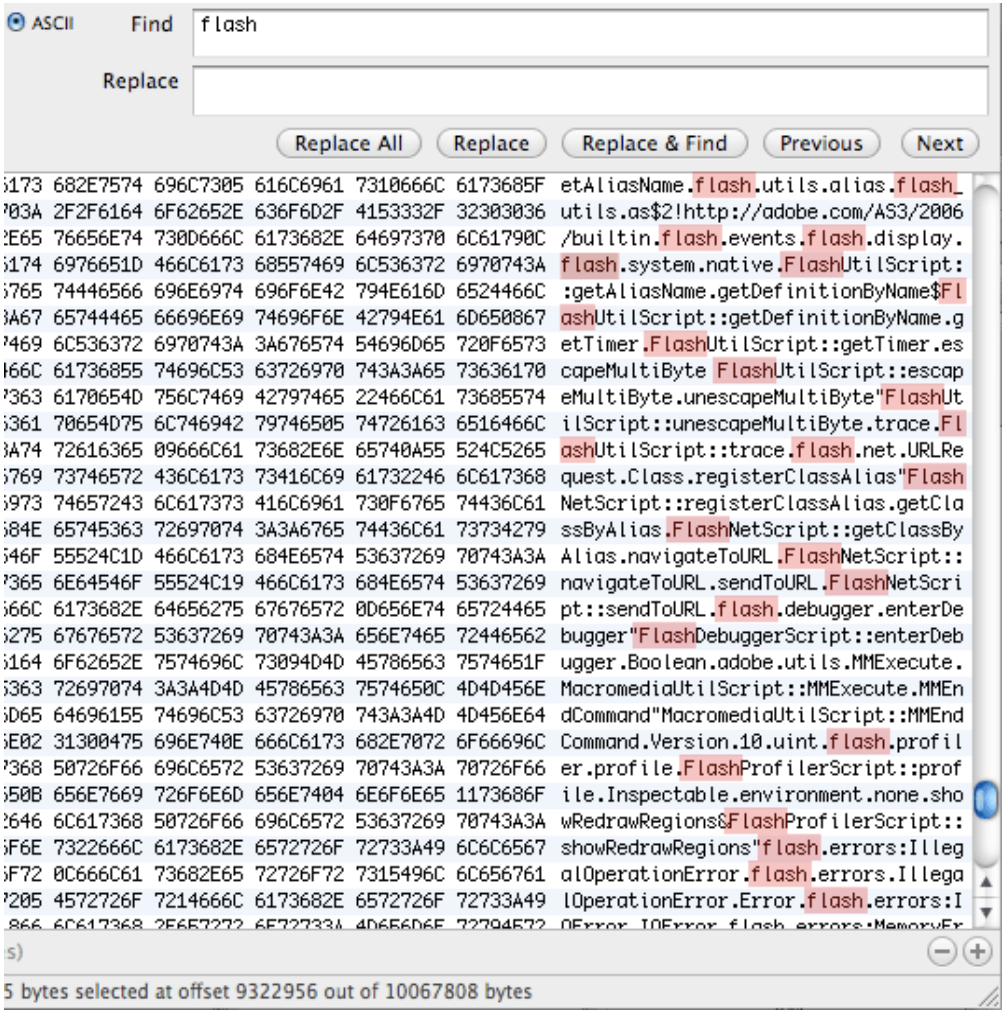

TRUST NO ONE

Threat Zones



MASHERY

iPhone App



MASHERY

Charles Proxy

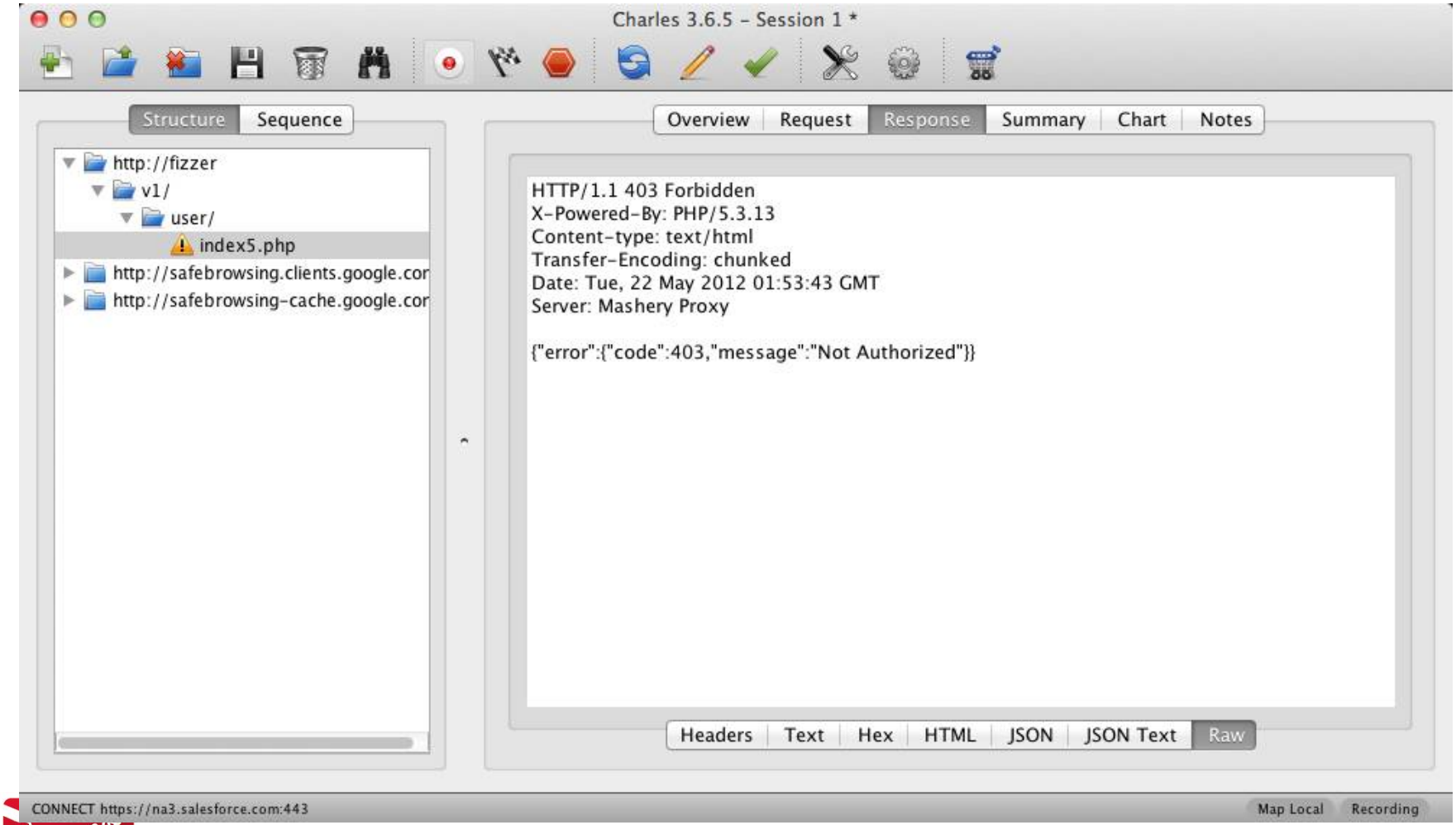
Your Friendly Neighborhood Application Spy Tool!

http://www.charlesproxy.com/

Charles CA Root Certificate:
http://www.charlesproxy.com/ssl.zip

MASHERY

Charles Proxy



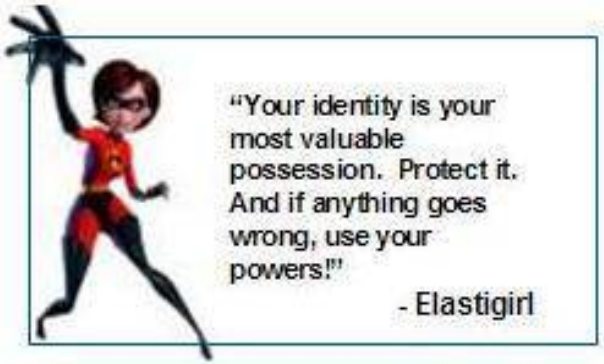
MASHERY

SSL

MASHERY

Digital Identity

"a set of claims made by one digital subject about itself or another digital subject"



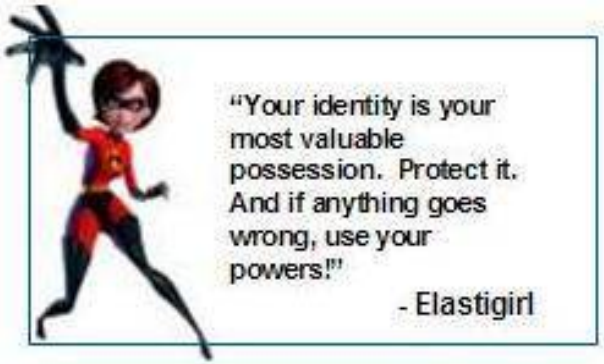
MASHERY

Laws of Identity, Kim Cameron - http://www.identityblog.com/?p=352

Application Identity

apikey=2745529bacf89590115d3657ac9d0442

Use Strong Keys



MASHERY

Laws of Identity, Kim Cameron - http://www.identityblog.com/?p=352

Authentication (AuthN)

"Authentication is the process of confirming a claimed identity."

MASHERY

Christopher Logan - http://web.mit.edu/ist/isnews/v20/n02/200206.html

Authentication (AuthN)

- Username/password
- TLS
- HMAC (Hash-based Message Authentication Code)
- WS-Security
- External to API

MASHERY

Authorization (AuthZ)

"Authorization is the act of granting permission for someone or something to conduct an act. Even when identity and authentication have indicated who someone is, authorization may be needed to establish what he or she is allowed to do."

MASHERY

Christopher Logan - http://web.mit.edu/ist/isnews/v20/n02/200206.html

Authorization (AuthZ)

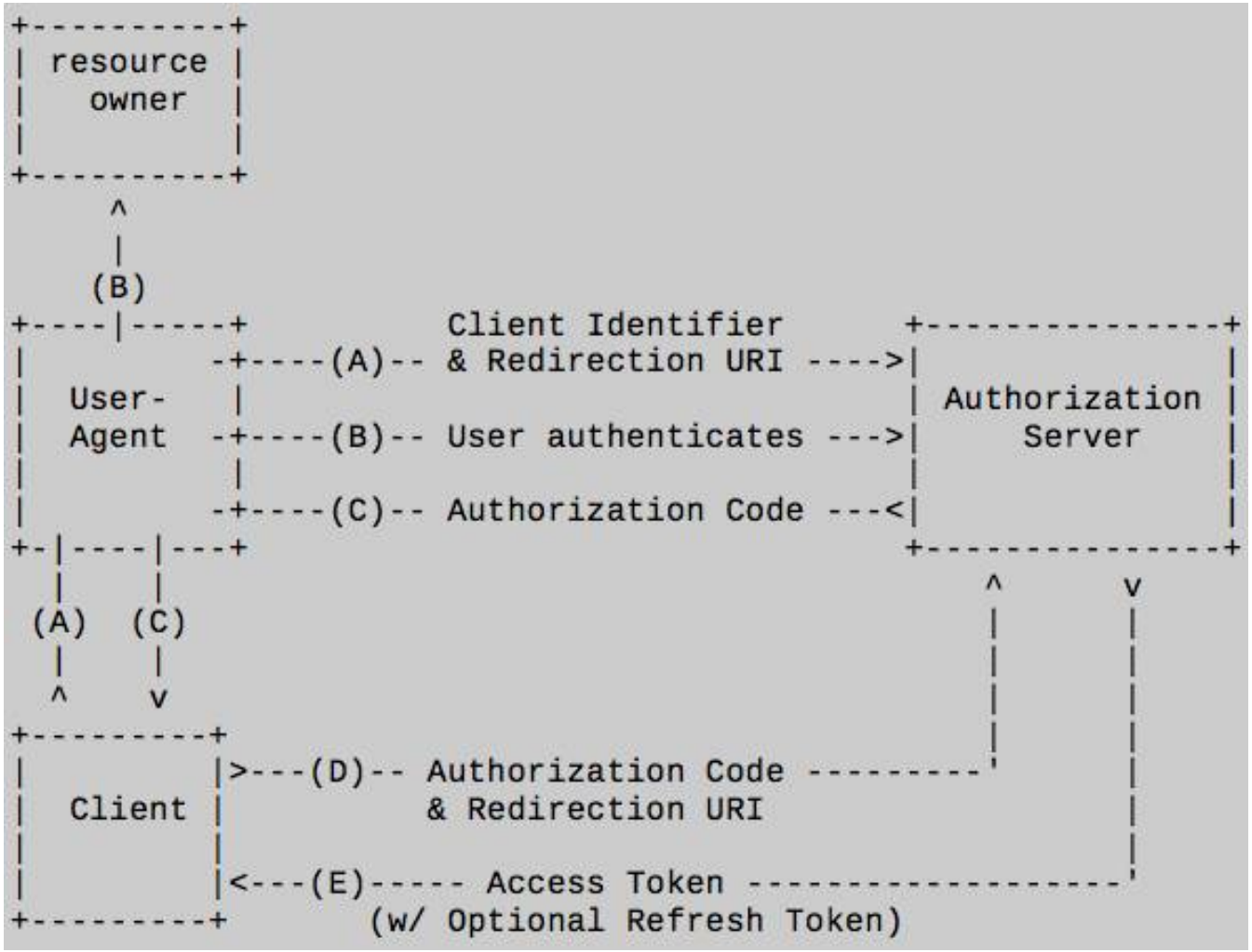
- OAuth
- Security Assertion Markup Language (SAML)

MASHERY

OAuth

MASHERY

Oauth
Authorization Code Flow



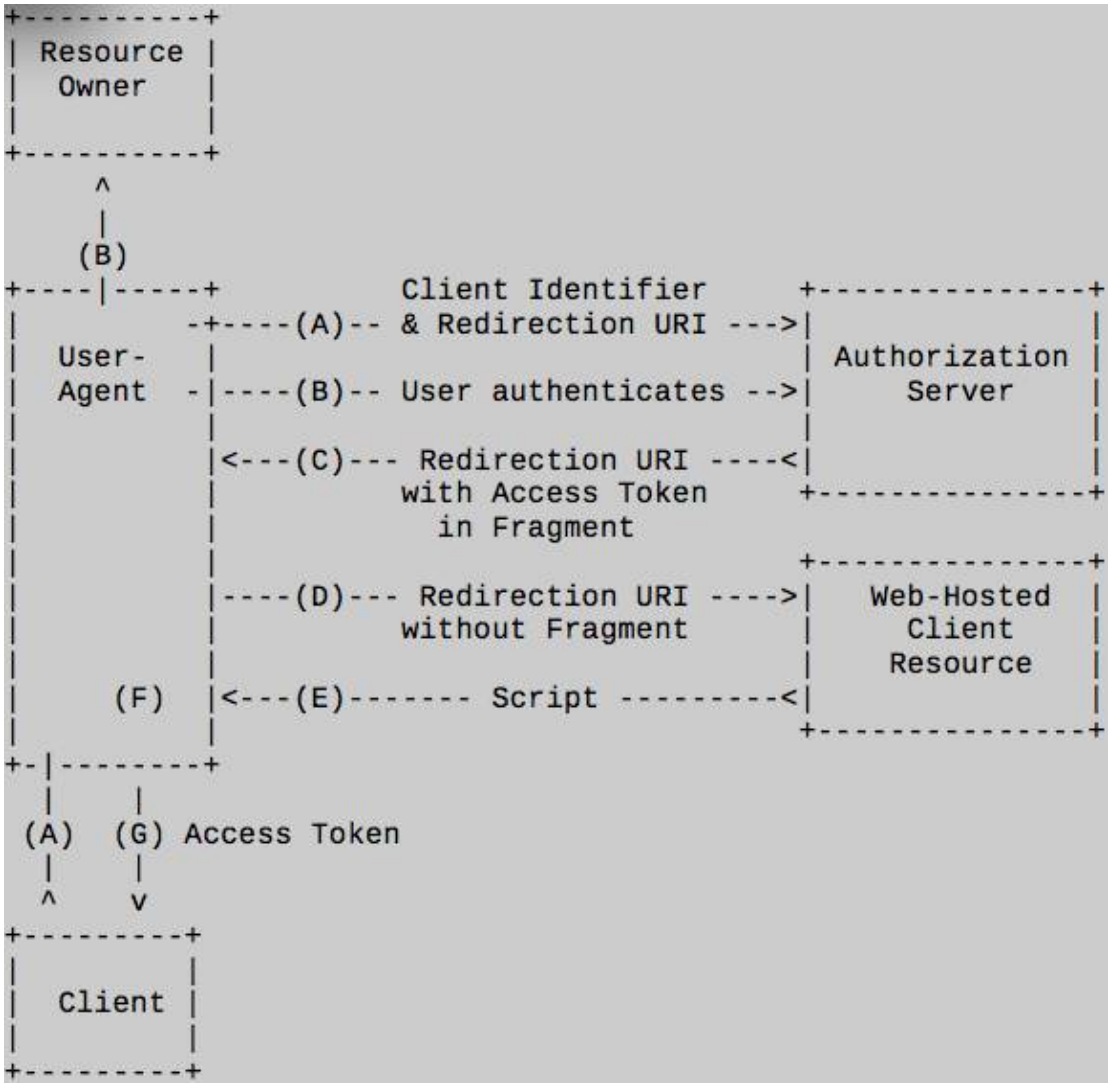
MASHERY

Oauth
iPhone Custom Schemes

Key	Type	Value
Localization native development region	String	en
Bundle display name	String	${PRODUCT_NAME}
Executable file	String	${EXECUTABLE_NAME}
Icon file	String	
Bundle identifier	String	com.tutsplus.mobile.${PRODUCT_NAM
InfoDictionary version	String	6.0
Bundle name	String	${PRODUCT_NAME}
Bundle OS Type code	String	APPL
Bundle versions string, short	String	1.0
Bundle creator OS Type code	String	????
▼ URL types	Array	(1 item)
▼ Item 0	Diction…	(2 items)
URL identifier	String	com.tutsplus.mobile.Receiver
▼ URL Schemes	Array	(1 item)
Item 0	String	readtext
Bundle version	String	1.0
Application requires iPhone environmer	Boolean	YES
Main nib file base name	String	MainWindow
▶ Supported interface orientations	Array	(3 items)

MASHERY

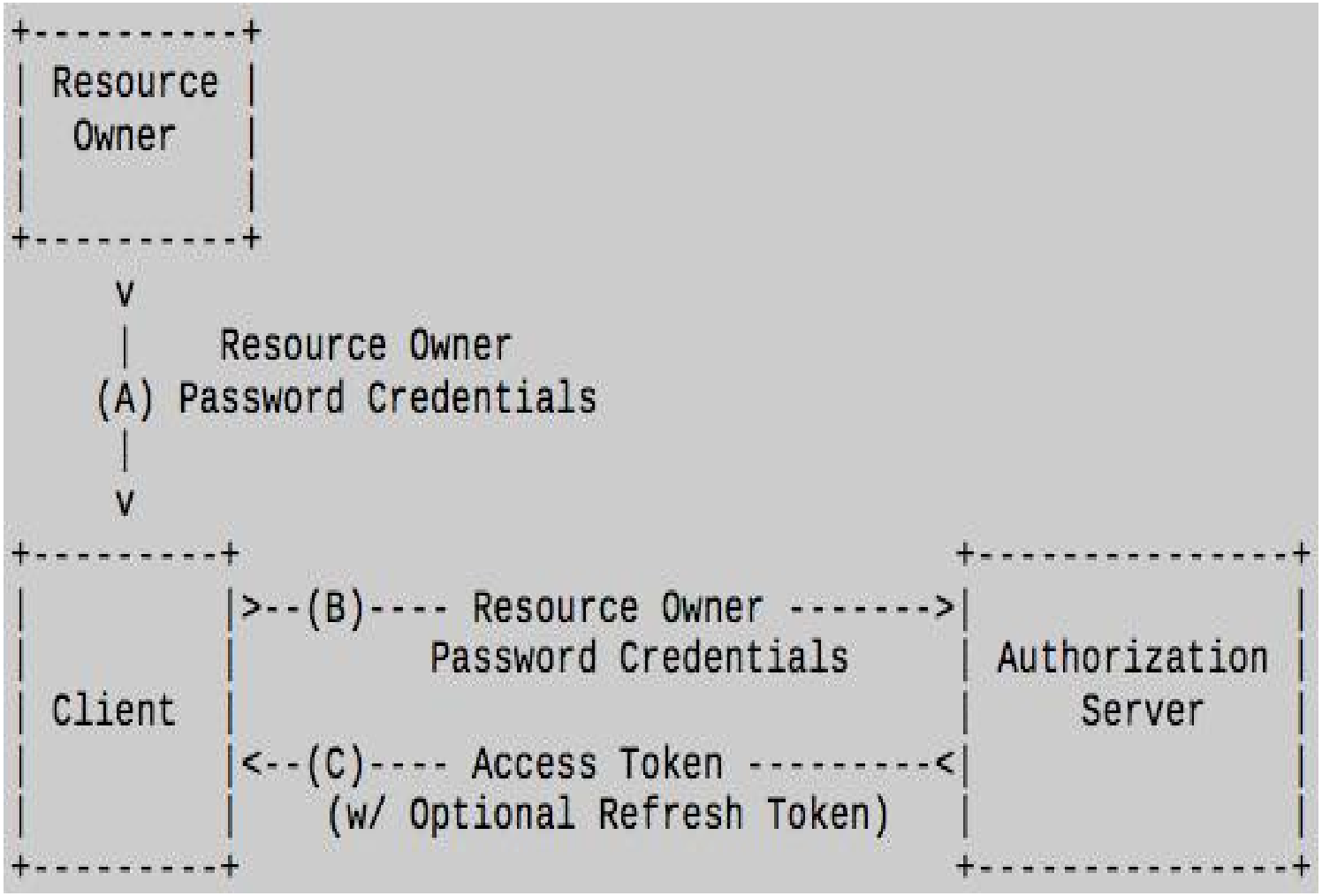
Oauth
Implicit Grant Flow



MASHERY

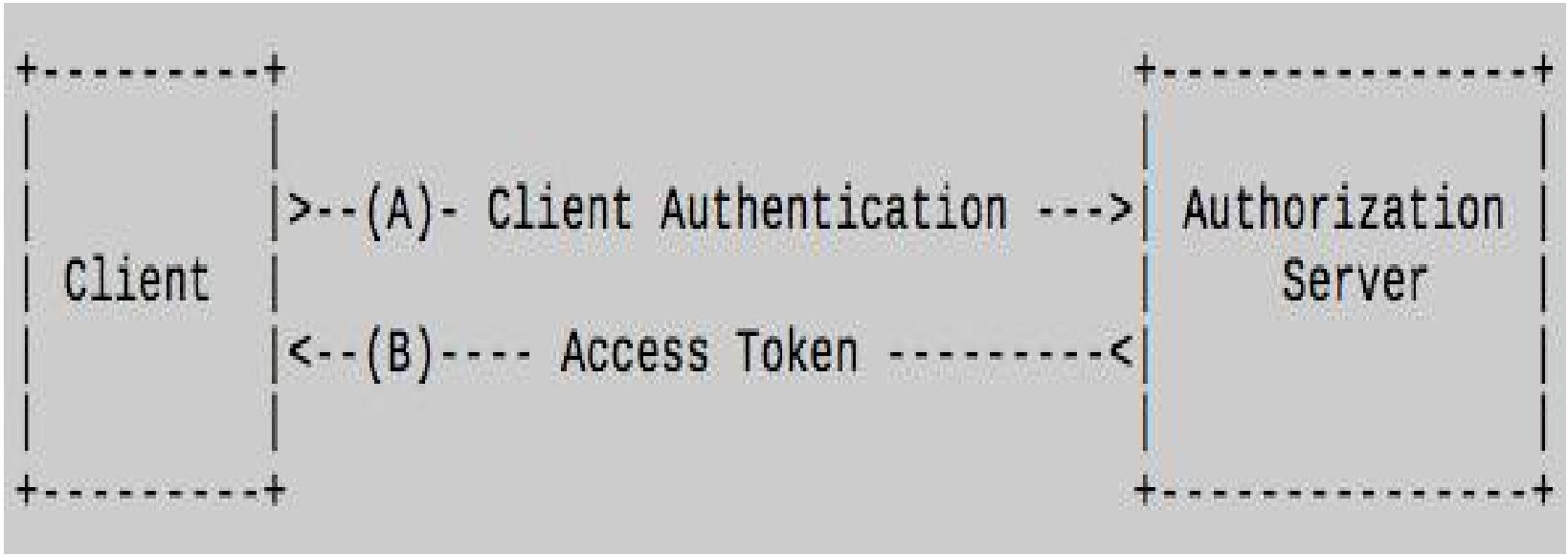
Oauth

Resource Owner Password Credentials Grant



MASHERY

Oauth
Client Credentials Grant



MASHERY

Oauth
Extensions

http://tools.ietf.org/html/draft-ietf-oauth-v2-bearer-19

http://tools.ietf.org/html/draft-ietf-oauth-v2-http-mac-01

http://tools.ietf.org/html/draft-ietf-oauth-saml2-bearer-12

MASHERY

Cryptography

- Digital Signatures
  - Authenticate
  - Message Integrity
  - Non-repudiation
- Data Encryption

MASHERY

XML Encryption

```
<?xml version='1.0'?>
<PaymentInfo xmlns='http://example.org/paymentv2'>
  <Name>John Smith</Name>
  <EncryptedData
Type='http://www.w3.org/2001/04/xmlenc#Element'
   xmlns='http://www.w3.org/2001/04/xmlenc#'>
    <CipherData>
      <CipherValue>A23B45C56</CipherValue>
    </CipherData>
  </EncryptedData>
</PaymentInfo>
```

MASHERY

XML Digital Signature

```
<Signature Id="MyFirstSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
  <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
  <Reference URI="">
    <Transforms>
      <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <DigestValue>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK.../DigestValue>
  </Reference>
</SignedInfo>
 <SignatureValue>...</SignatureValue>
 <KeyInfo>
  <X509Data>
    <X509Certificate>MIIB9zCCAWCgAwIBAgIERZwdkzANBgkqhk….</X509Certificate>
  </X509Data>
 </KeyInfo>
</Signature>
```

MASHERY

Crypto with JSON

Upcoming standards for using signatures and encryption with JSON data structures.

http://self-issued.info/docs/draft-jones-json-web-signature-json-serialization-01.html
http://tools.ietf.org/html/draft-ietf-jose-json-web-signature-02
http://tools.ietf.org/html/draft-ietf-jose-json-web-encryption-02

MASHERY

JSON Web Signature (JWS)

Payload

```
{
   "iss":"joe",
   "exp":1300819380,
   "http://example.com/is_root":true
}
```

```
eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQ
ogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ
```

JSON header describing structure and algorithm to use:

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

```
eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9
```

MASHERY

JSON Web Signature
(JWS)

JWS Secured Input:

eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ

Base64 encoded HMAC SHA-256 JWS Secured Input:

dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk

MASHERY

JSON Web Signature (JWS)

JSON Web Signature JSON Serialization (JWS-JS):

```
{
 "headers":
["eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9"],
 "payload":
"eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsD
QogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnV
lfQ",
 "signatures": ["dBjftJeZ4CVP-
mB92K27uhbUJU1p1r_wW1gFWFOEjXk"]
}
```

MASHERY

JSON Web Encryption (JWE)

Payload:

{"iss":"joe",
"exp":1300819380,
"http://example.com/is_root":true}

eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogIm
h0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ

Header:

{"alg":"RSA1_5",
"enc":"A256GCM",
"iv":"__79_Pv6-fj39vX0",
"x5t":"7noOPq-hJ1_hCnvWh6IeYI2w9Q0"}

eyJhbGciOiJSU0ExXzUiLA0KICJlbmMiOiJBMjU2R0NNIiwN
CiAiaXYiOiJfXzc5X1B2Ni1mZyIsDQogIng1dCI6Ijdub09Q
cS1oSjFfaENudldoNkllWUkydzlRMCJ9

MASHERY

JSON Web Encryption
(JWE)

```
{
  "headers":
["eyJhbGciOiJSU0ExXzUiLA0KICJlbmMiOiJBMjU2R
0NNIiwNCiAiaXYiOiJfXzc5X1B2Ni1mZyIsDQogIng1
dCI6Ijdub09QcS1oSjFfaENudldoNkllWUkydzlRMCJ
9"],
  "encrypted_keys":[
    "TBD_key_1_value_TBD",
    "TBD_key_2_value_TBD"],
  "ciphertext":"TBD_ciphertext_value_TBD"
}
```

MASHERY

Questions?

We're Hiring!

MASHERY