draft-ietf-oauth-security-topics

Access tokens phishing

John Bradley, Torsten Lodderstedt

IETF-99
July 18, Prague
What’s the setup?

- Client wants to access RS via Standard API (e.g. e-Mail, Banking, eSignature)
- Client is configured with RS URL at runtime
- Change to OAuth trust model!
What if ...
… RS X is a bad guy and impersonates the client?

- RFC 6749/50 & 6819 assume static trust relationship that is established upfront
What can we do?
What if the client would know upfront which places it is safe to send access tokens to?

```json
{
    ...
    "resource_servers": [
        "email.example.com",
        "storage.example.com",
        "video.example.com"
    ],
    ...
}
```

puts the burden of security checks to clients
Audience Restriction

AS

unknown RS

Obtain Access Token for https://rsx.evil.com*

Client

RS X
https://rsx.evil.com

https://rsx.evil.com

https://rsx.evil.com

RS 1
https://rs1.legit.com

https://rsx.evil.com

* RS URL and/or fingerprint of its TLS certificate

Audience does not match
Audience Restriction (Options)

1. **URL**
   - Must be exactly the URL the client will be using for RS requests
   - May be very fine grained - application level scoping
   - AS may generalize it (needs to tell client in the token response)

2. **TLS server certificate fingerprint**
   - Must be taken from the TLS handshake - may require preflight request to RS
   - Would allow to detect “certificate spoofing”
   - More coarse grain than URLs (since host-based)
Proof of Possession

AS

Obtain Access Token for Client (with key A)

Client

Signature (key A, ...)

RS X

https://rsx.evil.com

Client Key A, ...

Signature (key A, ...)

Key material

RS 1

https://rs1.legit.com

Client Key A, ...

Signature (key A, ...)

RS X is unable to create signature
Signature does not match
Proof of Possession (Existing Proposals)

● Transport
  ○ Token Binding - draft-ietf-oauth-token-binding
  ○ MTLS - draft-ietf-oauth-mtls

● Application
  ○ Signed Request - draft-ietf-oauth-signed-http-request
  ○ Jpop - draft-sakimura-oauth-jpop
What should the BCP recommend?

AS publishes legit RSs

Audience Restriction
- URL
- TLS server certificate fingerprint

Proof of Possession
- Transport
  - Token Binding
  - MTLS
- Application
  - Signed Request
  - Jpop

Something else?
Related Topics

- Access Token leakage at compromised RS
- Eavesdropping on the data center internal network