Token Binding & OAuth: Status & Next Steps

Securing what were previously bearer tokens

Dr. Michael B. Jones
Identity Standards Architect at Microsoft

Brian Campbell
Distinguished Engineer at Ping Identity

July 13, 2017
The Problem With Bearer Tokens

One truth and a lie
Token Binding Solution

• Token Binding enables data structures to be cryptographically bound to a particular TLS channel
  – *Making them no longer bearer tokens*
  – Prevents them from being used in unintended ways
• Data structures that can be Token Bound include:
  – Browser cookies, ID Tokens, access tokens, refresh tokens, authorization codes
• Presentation will discuss:
  – Token Binding mechanisms
  – Kinds of threats they mitigate
  – Current deployment status
IETF Token Binding Specifications
Hello! Do you like my extension?

Figure 1. Message flow for a full handshake

* Indicates optional or situation-dependent messages that are not always sent.
Do you support Token Binding?

**TLS Handshake**

Client

```
ClientHello
...
  token_binding [24]
  token_binding_version [1,0]
  key_parameters_list [2,0]
```

Server

```
ServerHello
...
  token_binding [24]
  token_binding_version [1,0]
  key_parameters_list [2]
```

Key Parameters:
(0) rsa2048_pkcs1.5
(1) rsa2048_pss
(2) ecdsap256

Also need extensions:
Extended Master Secret
Renegotiation Indication
Token Binding over HTTPS

HTTP Request

GET /stuff HTTP/1.1
Host: example.com
Sec-Token-Binding: AIkAAgBBQLgtRpWFpN66kxhxGrtakerzcMtHw7Hv8
 yMk_-MdRXJXbDMYxZCwnCASRRmHHHL5wmpP3bhYt0ChRDbMapfh_QAQ
 N1He3Ftj4Wa_S_fzZVns4saLfj6aB0MSQW6rLs19IIvHze7LrGjKyCfPT
 KXjajebxp-TLPFZCc0JtqYT5_0MBAAAA

- Encoded Token Binding Message
  - (1 or more) Token Bindings
    - Type (provided / referred)
    - Token Binding ID (key type and public key)
    - Signature over type, key type, and EKM (TLS Exported Keying Material)
    - Extensions

- Proves possession of the private key on the TLS connection
- Keys are long-lived and span TLS connections
Browser cookies low hanging fruit

secure

HttpOnly
• Server associates Token Binding ID with cookie & checks on subsequent use
• Augments existing authentication and session mechanisms
• Transparent to users
• Deployment can be phased in
What about federation?

There’s an HTTP response header for that! Tells the browser that it should reveal the Token Binding ID used between itself and the RP (referred) in addition to the one used between itself and the IDP (provided).

HTTP/1.1 302 Found
Location: https://idp.example.com
Include-Referred-Token-Binding-ID: true

GET / HTTP/1.1
Host: idp.example.com
Sec-Token-Binding: ARIAAgBBQB-XOPf5eP1f7ikATiAFEG0S5031PmRfkyymzdWwHCx10njjxC3D0E_OVfBNqrIQxzIfkF7tWbyZfyAE6XpwTSAQBYqghFX78vMGdDX_Fd_b2d1HyH1MmkIz8iMVBY_reM980UaJFz5IB7PG9nZ11j58LoG5QhmQoI9NXYktKZRXxrYAAECAEFAdUFTnfQADkn1uDbQnvJEk6oQs38L92gv-KO-qlYadLoDIKe2h53hSiKwIP98iRj_unedkNkAMyg9e2mY4Gp7wwBAEU0waSNNz1e6gKohwN4SAZ5eNyx45Mh8VI4IWl1BipLoqrJR0K6dxFkgHRMuBROcLUGj5PiOoxybQH_Tom3gAA

Token bindings for both TLS connections conveyed
Token Binding for OpenID Connect

- Utilizes the Include-Referred-Token-Binding-ID header
- Binds the ID Token to the Token Binding ID the browser uses between itself and the Relying Party
- Uses token binding hash “tbh” member of the confirmation claim “cnf”
“Demo”

• Showing a bound:
  – ID Token SSO
  – Session Cookie

http://httpbin.org/

Relying Party (RP)
https://rp.example.io:3000

Identity Provider (IDP)
https://idp.example.com

Browser
Unauthenticated access request to RP is redirected for SSO
Authentication request to the IDP
ID Token delivered to RP

**Header: Algorithm & Token Type**

```json
{
"alg": "ES256",
"kid": "pSvDHj6T0f701sEHQ4isBm"
}
```

**Payload: Data**

```json
{
"sub": "4.1tc1ACC2cPc4rAC",
"name": "Brian Campbell",
"email": "brian@example.com",
"aud": "PA",
"jti": "58K18LFeZPS4pGFZvUrE",
"iss": "https://idp.example.com",
"iat": 1492444947,
"exp": 1492449557,
"p1.si": "NflguntFV7b0yrz3mRBl17ezi",
"nonce": "LyNCh162yFvnB3SkoPzKMeebhvQya1cFz62EcY2NA",
"auth_time": 1492444947,
"cnf": {
"thb": "suMuxh.I1RP-Zrj33luDQGR5rX359cmBe-wzdf3sBRUQ"
}
```
Authenticated access to RP
“Demo” Finished
OAuth Token Binding

- Access tokens with referred Token Binding ID
- Refresh tokens with provided Token Binding ID
- Authorization codes via PKCE
  - Native app clients
  - Web server clients
The Landscape

- Three IETF Token Binding specs soon to be RFCs
- Drafts supported in:
  - Edge, IE, and Chrome (but not on iOS)
  - On Google servers since January
  - .NET Framework 4.6 (for server side)
- Open Source
  - OpenSSL (https://github.com/google/token_bind)
  - Apache (https://github.com/zmartzone/mod_token_binding)
  - NGINX (https://github.com/google/ngx_token_binding)
  - Java (Brian Campbell has mods he plans to submit...)
- OpenID Connect Token Bound Authentication spec maturing
  - Online Token Binding demo available
- OAuth 2.0 Token Binding spec also maturing
Privacy Considerations

• Token Binding is not a *supercookie* or new tracking mechanism

• Client generates a unique key pair per effective top-level domain + 1 (eTLD+1)
  – E.g., example.com, www.example.com, and etc.example.com share binding but not example.org or example.co.uk

• Same scoping rules and privacy implications as cookies
Workshop Discussion Topics

• Detecting and preventing downgrade attacks
• Status of platform and library support for Token Binding
• Implementations and deployments to date and what we’ve learned from them
• Practical steps needed to deploy Token Binding for OAuth and OpenID Connect end-to-end
Where can I participate & learn more?

- Online Token Binding Demo
  - [https://www.ietf.org/mail-archive/web/unbearable/current/msg01385.html](https://www.ietf.org/mail-archive/web/unbearable/current/msg01385.html)
- IETF Token Binding mailing list
  - [https://www.ietf.org/mailman/listinfo/unbearable](https://www.ietf.org/mailman/listinfo/unbearable)
- IETF OAuth mailing list
  - [https://www.ietf.org/mailman/listinfo/oauth](https://www.ietf.org/mailman/listinfo/oauth)
- OpenID Enhanced Authentication Profile (EAP) mailing list
  - [http://lists.openid.net/mailman/listinfo/openid-specs-eap](http://lists.openid.net/mailman/listinfo/openid-specs-eap)
- My blog
- E-mail me
  - mbj@microsoft.com