Token Binding Standards and Applications:

Securing what were previously bearer tokens

Dr. Michael B. Jones
Identity Standards Architect at Microsoft

Brian Campbell
Distinguished Engineer at Ping Identity

May 10, 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?

Client

TLS Handshake

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

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

Server

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: AIkAAgBBQLgtRpWFPN66kxhxGrtaKrzcMtHzw7HV8yMk_-MdRXJXbDMYxZCwnCASRRrmHHHL5wmpP3bhYt0ChRDbMapfh_QAQN1He3Ftj4Wa_S_fzVns4salFj6aBoMSQW6rLs19IVvHze7LrGjKyCfPTKXjaebxp-TLPFZCc0JTqTY5_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
Binding Cookies

- 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: ARIAaBGQB-XOPf5eP1fcTAVrTAFEG05S03
lPmRfkyymzdWwHCx10njxC3D0E_OVfBNqrIQxzIIfkF7tWbyZGfya
E6XpwTSaQByq6FX7BwMgDX_Fd_b2d1HyH1mKiz8iMVBV_reM98O
uAJFz5IB7PG9nZ11j58LoG5QhmQoI9NXyKtKZRXxraYAAAECAEFAdU
FTnfQADkn1uDbQnvJEk6OQs38L92gv-KO-q1yAdLoDIKe2h53hSiK
wIP98iRj_unedkNkAYyg9e2mY4Gp7wBAEduwaSxNz1e6gKohwN4
SAZ5eNyxt45mH8VI4wo1BipLoqRJR0K6xFkWgHRMuBROcLGUj5Pi
OoxybQH_Tom3gAA

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

- Utilizes the `Include-Reflected-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

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

Identity Provider (IDP)
https://idp.example.com
Unauthenticated access request to RP is redirected for SSO
Authentication request to the IDP
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 (others?)
  – 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
• Brian working on spec for TLS terminating reverse proxies
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
Where can I participate & learn more?

• Online Token Binding Demo
• IETF Token Binding mailing list
  – https://www.ietf.org/mailman/listinfo/unbearable
• IETF OAuth mailing list
  – https://www.ietf.org/mailman/listinfo/oauth
• OpenID Enhanced Authentication Profile (EAP) mailing list
  – http://lists.openid.net/mailman/listinfo/openid-specs-eap
• My blog
  – http://self-issued.info/
• E-mail me
  – mbj@microsoft.com