Suggested Changes to OAuth Security BCP (Typos)

Jan 28, 2025

We suggest the following changes based on the latest RFC-to-be 9700 version (https://www.rfc-editor.org/authors/rfc9700.html). The text diff are highlighted **in bold**.

(1) Section 2.1.2. Implicit Grant

OLD:

> It also allows the authorization server to sender-constrain the issued tokens (see Section 2.2.

NEW:

> It also allows the authorization server to sender-constrain the issued tokens **(see Section 2.2)**.

Rationale:

Typo: missing right parenthesis.

(2) Section 4.4.1. Attack Description

OLD:

> Preconditions: For this variant of the attack to work, it is assumed that
>
> ...
>
> - the client stores the authorization server chosen by the user in a session bound to the user's browser and uses the same redirection endpoint URI for each authorization server.

NEW:

> Preconditions: For this variant of the attack to work, it is assumed that
>
> ...
>
> - the client stores the authorization server chosen by the user in a session bound to the user's browser and uses the same **redirection URI** for each authorization server.

Rationale:

Use the common term “redirection URI” (45 instances) instead of “redirection endpoint URI” (appeared only here). Besides, “redirect URI” also appears 9 times throughout the BCP document. Shall we use a unified term (*e.g.*, “redirection URI”)?

(3) Section 4.4.1. Attack Description

OLD:

Variants:

...

- Implicit Grant: In the implicit grant, the attacker receives an access token instead of the code in Step 4. The attacker's authorization server receives the access token when the client makes either a request to the A-AS userinfo endpoint or a request to the attacker's resource server (since the client believes it has completed the flow with A-AS).

NEW:

Variants:

...

- Implicit Grant: In the implicit grant, the attacker receives an access token instead of the code in Step 4. The attacker's authorization server receives the access token when the client makes either a request to the A-AS userinfo endpoint **(defined in [OpenID.Core])** or a request to the attacker's resource server (since the client believes it has completed the flow with A-AS).

Rationale:

The “userinfo endpoint” is not defined in standard OAuth and not mentioned elsewhere in the Security BCP. A reference to the OpenID Core specification is added.

(4) Section 4.4.1. Attack Description

OLD:

Variants:

...

- Per-AS Redirect URIs: If clients use different redirection URIs for different authorization servers, clients do not store the selected authorization server in the user's session, and authorization servers do not check the redirection URIs properly,

attackers can mount an attack called "Cross-Social Network Request Forgery". These attacks have been observed in practice. Refer to [research.jcs_14] for details.

NEW:

Variants:

...

- Per-AS Redirect URIs: If clients use different redirection URIs for different authorization servers, clients do not store the selected authorization server in the user's session, and authorization servers do not check the redirection URIs properly, attackers can mount an attack called "**Cross Social-Network** Request Forgery". These attacks have been observed in practice. Refer to [research.jcs_14] for details.

Rationale:

According to the original paper of [research.jcs_14], they call the attack “Cross Social-Network Request Forgery” instead of “Cross-Social Network Request Forgery”.