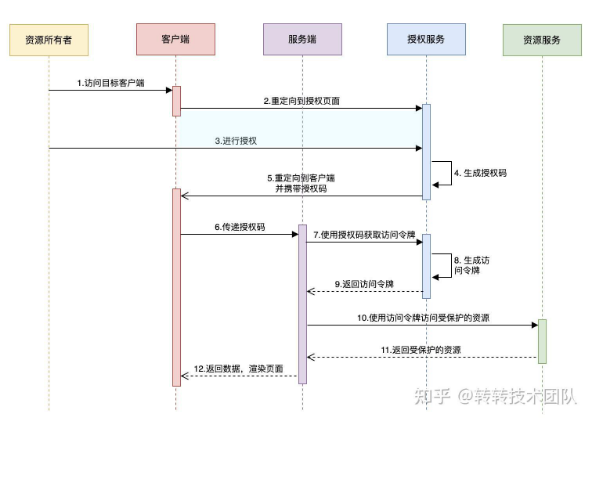
受众注入攻击



步骤 2 和 3\*\*：客户端（c）向授权服务器（as）的配置端点（知名路径）请求授权服务器（as）的配置文档（包含授权服务器支持的协议和扩展的端点列表、签发者标识符、用于验证签名的公钥等）

步骤 4\*\*：客户端注册其公钥（k\_c）并被分配一个客户端ID（cid\_c）

步骤 5\*\*：客户端断言（pk/Wt\_c）通过签名的方式验证客户端（c）的身份（向授权服务器（as））

6 授权服务器（as）收到 pk/WT，并验证：

- 使用客户端（c）注册的公钥（k\_c）验证签名

- iss 和 sub 声明包含客户端（c）的客户端ID（cid\_c）

- pk/WT 未过期

- 授权服务器（as）能在 aud 声明中的至少一个值里识别自身

\*\*目标\*\*: 恶意客户端冒充诚实客户端

\( c \) 以向诚实授权服务器 \( \alpha s \) (AS) 进行认证或授权

- \*\*阶段 1\*\*: 获取一个由诚实客户端 \( c \) 签名的有效客户端断言 (client assertion)，其受众 (aud) 值将被诚实授权服务器 \( AS \) (as) 接受。

- \*\*阶段 2\*\*: 使用一个或多个客户端断言来获取用户资源的访问权限，或以诚实用户的身份登录到某个客户端。

# 受众注入攻击 (第一阶段)

\*\*目标:\*\* 获取一个由诚实客户端 \( c \) 签名的有效客户端断言 (client\_assertion)，其受众 (aud) 值将被诚实授权服务器 (AS) \( as \) 接受。

\*\*假设:\*\* 诚实客户端 \( c \) 已向诚实授权服务器 \( as \) 注册，获分配客户端ID \( cid\_c \)，并使用 \( c \) 的密钥对 \( (k\_c, \hat{k}\_c) \) 进行身份验证。

1. 攻击者冒充客户端c的用户，尝试向一个由攻击者控制的授权服务器asatt进行身份验证。
2. 客户端c获取了身份认证服务器asₐtt的配置文档，该文档错误地列出了令牌端点tokenEPₐs（客户端c将在后续与asₐtt的所有交互中使用此tokenEPₐs作为令牌端点）。

3. 客户端c使用其与as通信时相同的公钥k\_c向asatt注册。按照常规流程，asatt会为c分配一个客户端ID——此时攻击者故意选择分配与as之前分配给c相同的客户端ID cid\_c。

4. 客户端c完成注册后，向授权服务器*asatt*​发送推送授权请求（PAR）。该请求中的客户端断言使用c的私钥*kc*​进行签名，包含表明客户端ID*cidc*​的iss和sub声明，以及值为*tokenEPas*​的aud声明。

第二阶段

攻击者使用在第一阶段获取的客户端断言（client\_assertion），向授权服务器 \(as\) 发送PAR请求，该请求包含：

- 客户端ID \(cid\_{c}\)

- 攻击者选择的权限范围（scope）

- 指向攻击者控制客户端的重定向URI（redirect\_URI）

攻击者诱导用户点击指向授权服务器(as)授权端点（重新授权）的链接。

用户出于对 ( as ) 和 ( c ) 的正当信任，点击了链接，完成身份验证，并被要求授权 \( c \) 的（看似合法的）请求。

攻击者利用客户端ac向授权服务器as发送令牌请求，该请求包含第一阶段的另一个客户端断言（即使用不同的jti随机数）。

结果：敌手客户端c冒充诚实客户端c来访问存储在授权服务器as中的资源。

| 扩展名称 | 攻击方式概述 |
| --- | --- |
| 令牌撤销 (Token Revocation) | 1. 攻击者可在配置文档中植入撤销端点 2. 攻击者通过注销诚实客户端c的操作获取客户端断言 |
| FAPI（金融级API） | 强制要求使用PAR扩展 |
| 令牌内省 (Token Introspection) | 1. 攻击者可在配置文档中植入内省端点 2. 客户端发送的内省请求将导致客户端断言泄露 |
| 设备授权许可 (Device Authorization Grant) | 恶意授权服务器as<sub>att</sub>在配置文档中发布认证端点，诱导消费设备与as<sub>att</sub>启动协议交互 |
| ****客户端凭证许可模式 (Client Credential Grant)**** | 攻击者利用已获取的有效客户端断言，在授权服务器(as)端冒用合法客户端(c)身份发起令牌请求，通过获取对c受保护资源的访问权限达成权限绕过 |
| ****解耦认证流程 (Decoupled Flow)**** | 攻击者向授权服务器(as)的后端通道认证端点发起伪造请求，通过冒用客户端(c)身份并指定任意用户ID实现身份欺诈 |

受众注入攻击的防御方案

第一阶段防御：防止攻击者诱骗城市开鹅湖段向攻击者控制的端点B发送包含攻击者选定受众声明值A的客户端断言

1. \*\*授权服务器(AS)端修复\*\*：要求特定的受众值（而不是接受多个不同的值）。

2. \*\*将实际端点作为受众值\*\*：强制要求客户端始终将受众(aud)声明的值设置为对应客户端断言将使用的确切端点（例如，攻击者AS的PAR端点 `parEP\_att`）。

3. \*\*将AS签发者标识符作为受众值\*\*：引入标识授权服务器(AS)的签发者(Issuer)标识符（本质上是AS的HTTPS域名，例如 https://attacker.com）作为受众值，以替代使用具体的端点URL（例如 `tokenEP\_as`）。

看断言的audiance参数是否是一个服务器或者是一个列表

如果是一个服务器，那么就无法使用该攻击，如果是个列表或者没啥限制就能攻击