OAuth 2.0 : Etude des vulnérabilités d'implémentation de ce protocole

Institut Mines-Télécom

Auteurs

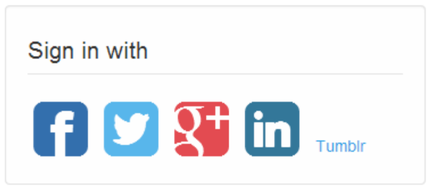
Sleh Choura

Laurent Raynaud

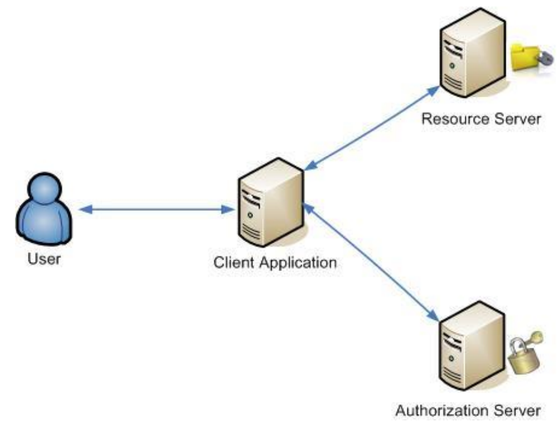
Partenaires

Un protocole de délégation d'autorisation

Le mécanisme:



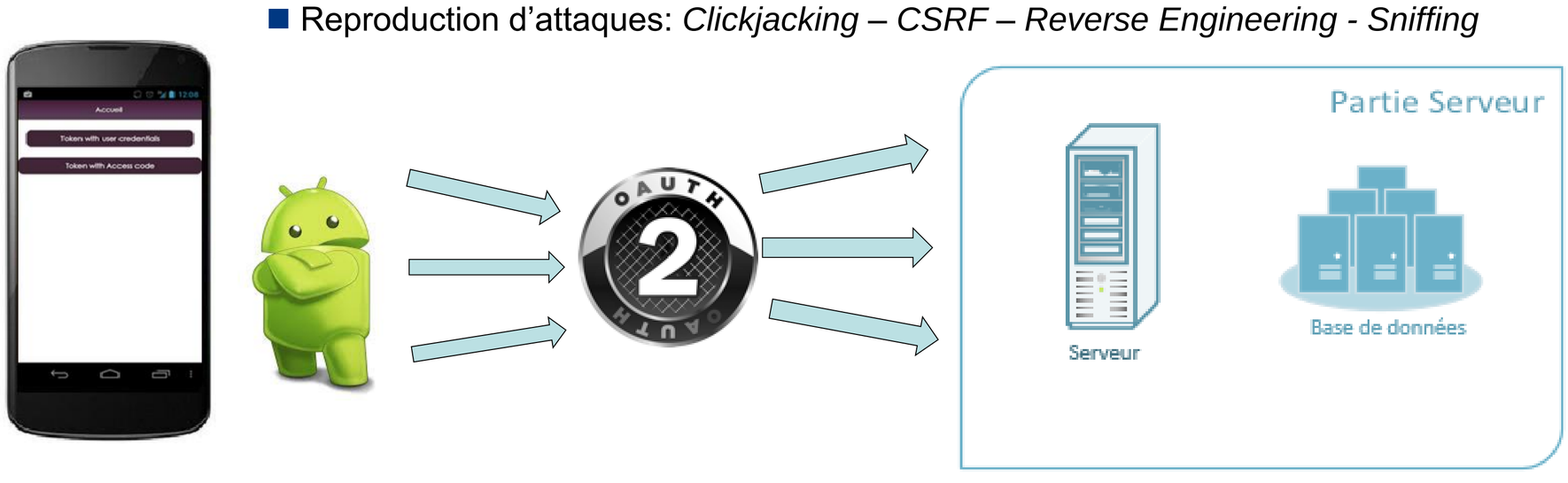
- Centralisation des données
- Nécessite **4 entités** : un utilisateur , une application cliente (mobile ou web), un serveur d'autorisation et un serveur de données
- **3** types de **clients**: Applications web, mobile et basé sur un user-agent.
- Négociation d'un **jeton d'accès** selon **4 modèles différents** : Par un code d'autorisation, de manière implicite, avec les identifiants de l'utilisateur et enfin avec les identifiants de l'application.



Notre Implémentation

Description:

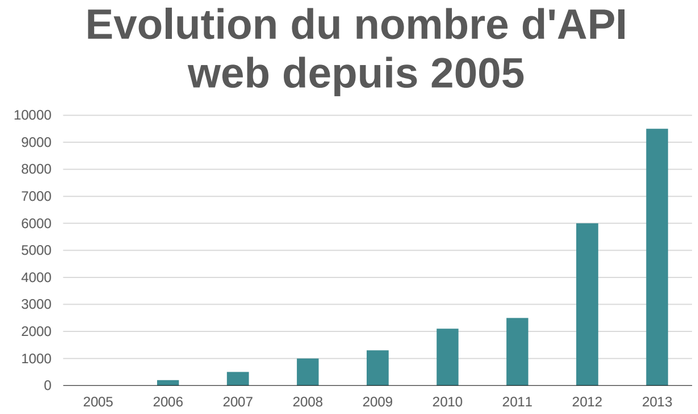
- Application cliente Android
- 2 types d'autorisation implémentés : par code d'autorisation et
- Un serveur d'autorisation et de ressource confondu
- Reproduction d'attaques: *Clickjacking – CSRF – Reverse Engineering - Sniffing*



Enjeux de sécurité

Comment réussir une bonne implémentation?

- Communication en HTTPS
- Enregistrement des clients sur la partie serveur
- Paramètre « state » implémenté sur le client
- Limiter les « scope » permis



Un réel besoin de sécuriser ces APIs web de plus en plu nombreuses qui repose aujourd'hui entre les mains de c protocole.

Janvier 2015

Contact laurent.raynaud@telecom-sudparis.eu **Site web** www.tsp-oauth.zz.mu