Owen Joslin

CSEC.472.01 - Authentication and Security Models

L05 OAuth

1. Oauth 2.0
2. What is Oauth?
   1. Oauth: Open Authorization
   2. A framework or API that enables authorization and solves the access delegation problem across multiple applications.

A screenshot of a login page

Description automatically generated

1. What Are We Trying to Solve?
   1. Goal: Give the client access to the protected resource on behalf of the user.

A computer and a person with a computer

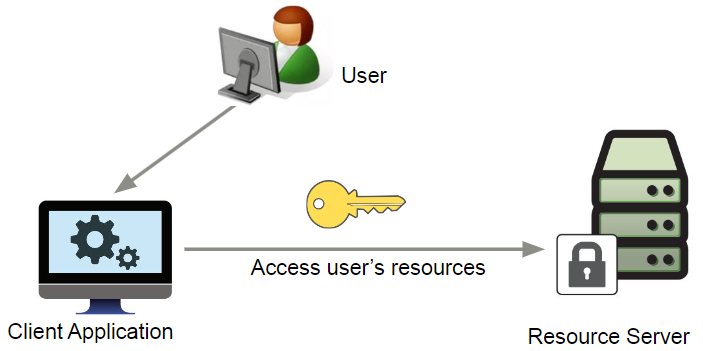
Description automatically generated with medium confidence

1. Naïve Solution
   1. Copy the user’s credentials and replay them to the protected resource.

A diagram of a computer network

Description automatically generated

1. Security Challenges
   1. The same key stored in the client and the resource server
   2. Users cannot control the authorization of the client
   3. The client knows user’s key, the more clients, the higher risk for key disclosure.
2. Try Again
   1. Service-specific credentials
      1. A special password (or token) that can be used to access just this protected resource
      2. E.g., only can read
      3. Good?



1. Introducing Authorization Server
   1. The Authorization Server gives us a mechanism to bridge the gap between the client and the protected resource
      1. Generates tokens for the client
      2. Authenticates resource owners (users)
      3. Authenticates clients
      4. Manages authorizations

A computer server with a logo

Description automatically generated with medium confidence

1. Oauth Roles
   1. Resource Owner
      1. Users
   2. Resource Server
      1. such as Facebook, Google app that holds information you own
   3. Client
      1. Your new apps/websites that need your information stored on google
   4. Authorization Server
      1. Google account server that checks user credentials
2. Oauth Process

A diagram of a facebook application

Description automatically generated

1. OAuth 2.0 Client Types
   1. Confidential clients—Clients that are capable of maintaining the confidentiality of their credentials.
   2. Public clients—Clients that are incapable of maintaining the confidentiality of their credentials.
2. OAuth 2.0 Client Profiles
   1. Web application—A web application is a confidential client running on a web server.
   2. User agent-based application—A public client that runs under the context of a web browser, such as JQuery or a Silverlight plug-in.
   3. Native application—A public client that is installed and executed on the client side on a device used by a resource owner such as desktops or mobile devices.
3. OAuth 2.0 Authorization Grant Types
   1. Authorization code
   2. Implicit
   3. Resource owner password
   4. Client credentials
4. Authorization Code Flow
   1. <https://www.youtube.com/watch?v=7D-OU4hZW70>

A screenshot of a computer

Description automatically generated

1. Implicit Flow
   1. <https://www.youtube.com/watch?v=KUruB156-h4>

A screenshot of a computer

Description automatically generated

1. Resource Owner Password Credentials Flow
   1. <https://www.youtube.com/watch?v=CGMiOHrOAYQ>

A screenshot of a computer screen

Description automatically generated

1. Client Credentials Flow
   1. <https://www.youtube.com/watch?v=XJuFcXI2v2k>

A screenshot of a computer

Description automatically generated

1. Refresh Token Flow
   1. <https://www.youtube.com/watch?v=jcKDsQfBgYY>

A screenshot of a computer

Description automatically generated

1. Attacks on Oauth
   1. Authorization Code Interception
   2. Token Leakage
   3. Client Impersonation (Client ID Spoofing)
   4. Authorization Code Replay
   5. Phishing
   6. Insufficient Token Validation
   7. Cross-Site Request Forgery (CSRF)
   8. Token Invalidation and Logout
   9. OAuth Token Scope Elevation
   10. Developer Misconfigurations
2. References
   1. <https://aaronparecki.com/oauth-2-simplified/#roles>
   2. [https://darutk.medium.com/diagrams-and-movies-of-all-the-oauth- 2-0-flows-194f3c3ade85](https://darutk.medium.com/diagrams-and-movies-of-all-the-oauth-%202-0-flows-194f3c3ade85)
   3. [https://datatracker.ietf.org/meeting/101/materials/slides-101-edu-s esse-introduction-to-oauth-20-01.pdf](https://datatracker.ietf.org/meeting/101/materials/slides-101-edu-s%20esse-introduction-to-oauth-20-01.pdf)
   4. Advanced API Security: OAuth 2.0 and Beyond, by Siriwardena, Prabath, Springer Electronic Books--Professional and Applied Computing., 2020, 2nd ed. 2020. (accessible via RIT Library)