JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Federated Identity Systems

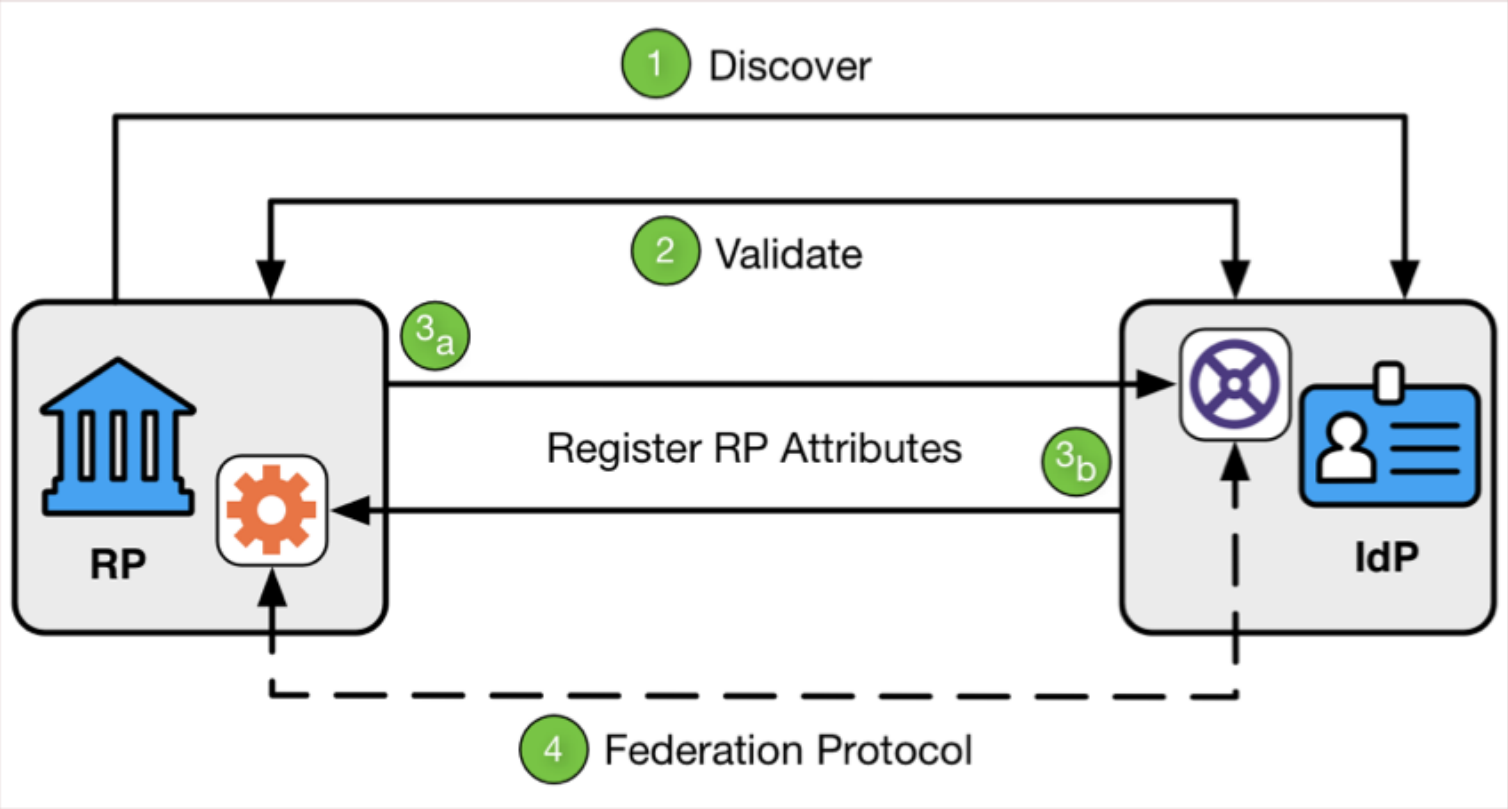
Security Architecture & Tool Sets

Federated Identity Systems

- Moves the trust boundary outside your organization to Google, Facebook, LinkedIn, or other identity providers

- Identity Provider (IDP)
  - Provides identities & release data to relying parties
- Relying Party (RP) or Service Provider (SP)
  - Members of the federation that provides services to the user when identified by identity provider
- Consumer or User
  - Asked to make decision on who to share their identity with by IDP in order to get services from RP/SP

Federated Identity Systems



Choosing a Federated Identity System

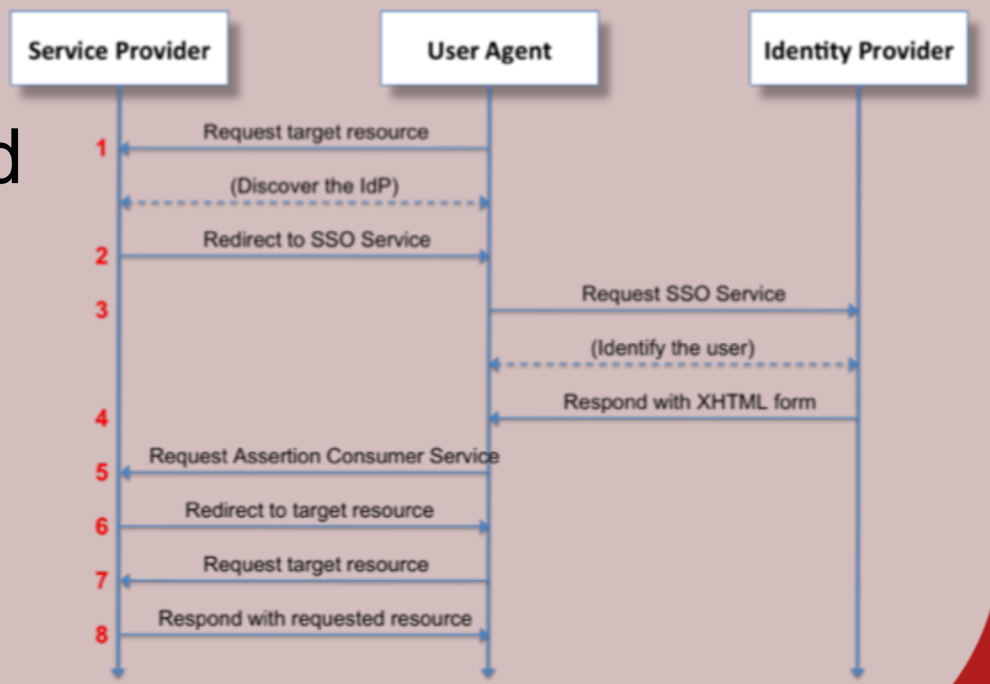
- Do you care that the user says who they are?
  - If not, use Google, Facebook, etc.
  - Otherwise, find identity provider that vets its users
- When users signup for your site using federated ID, you immediately provision a user account on your system mapped to the attributes released by IDP

Federated Identity Systems Technologies

- Security Assertion Markup Language (SAML)
- OAuth and OAuth 2.0
- Active Directory Federation Services (ADFS)
- OpenID Connect

Security Assertion Markup Language (SAML)

- XML-based language to send authentication and authorization data between IDP and RP
- Used to enable SSO for web apps & services
- Allows attribute, authentication, and authorization decisions to be exchanged



Service Provider | User Agent | Identity Provider

1. Request target resource
   (Discover the IdP)
2. Redirect to SSO Service
3. Request SSO Service
   (Identify the user)
   Respond with XHTML form
4. Request Assertion Consumer Service
5. Redirect to target resource
6. Request target resource
7. Respond with requested resource
8.

OAuth and OAuth 2.0

- Developed by the Internet Engineering Task Force (IETF) to provide an authorization framework to allow service provider applications to access HTTP-based services

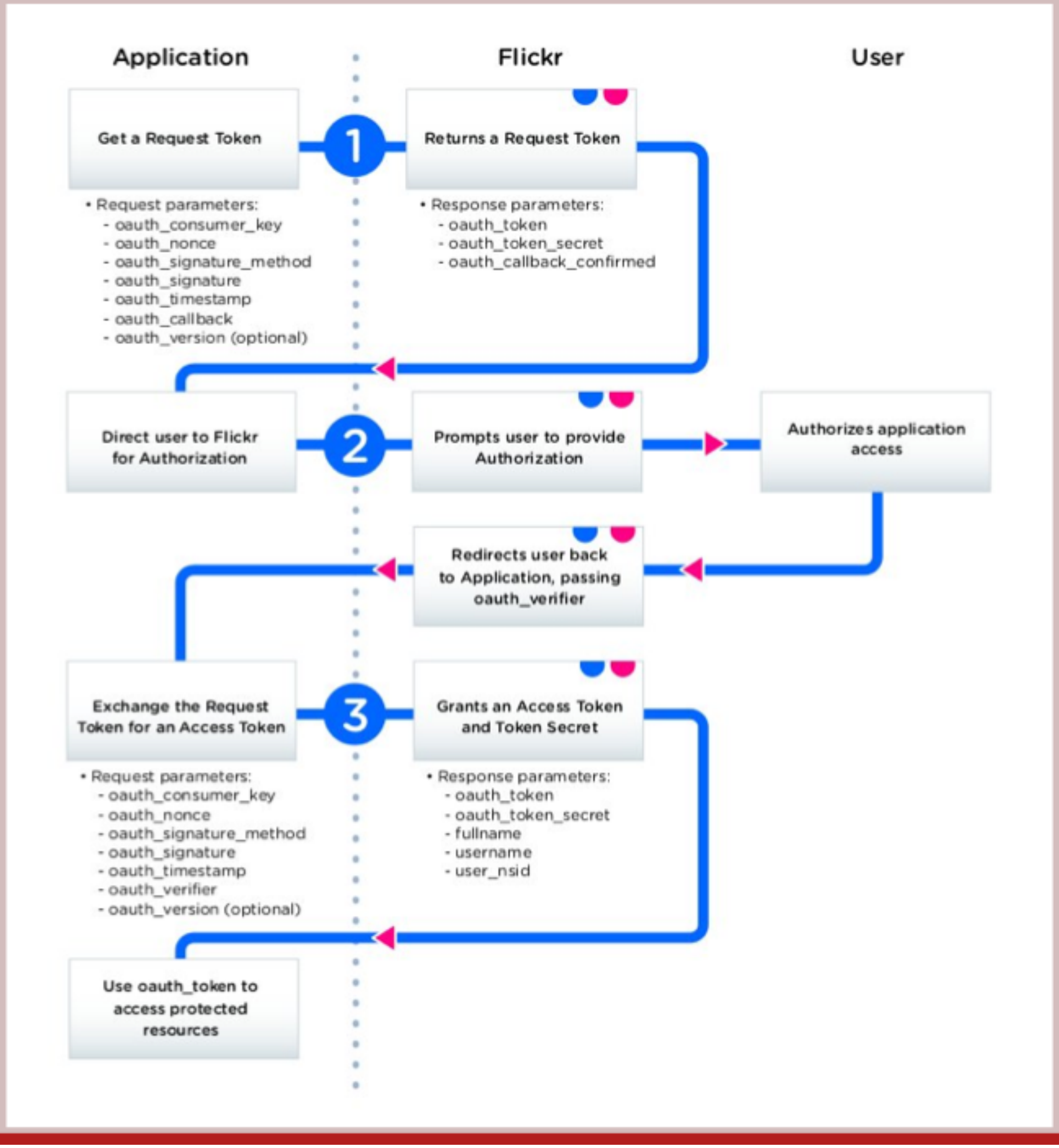
- Provides access delegation to allow service providers to provide actions on behalf of user

- Supports web clients, desktops, mobile devices, and other embedded device types

OAuth and OAuth 2.0

- OAuth has types of four parties served:
  - Clients
    - Applications that the user wants to access/use
  - Resource Owners
    - End user being serviced
  - Resource Servers
    - Servers provided by a service the user wants to access
  - Authorization Servers
    - Servers owned by the identity provider (IDP)

Flickr Federated Example (OAuth Authentication Process)



Application

Flickr

User

1

Get a Request Token

- Request parameters:
  - oauth_consumer_key
  - oauth_nonce
  - oauth_signature_method
  - oauth_signature
  - oauth_timestamp
  - oauth_callback
  - oauth_version (optional)

Returns a Request Token

- Response parameters:
  - oauth_token
  - oauth_token_secret
  - oauth_callback_confirmed

2

Direct user to Flickr for Authorization

Prompts user to provide Authorization

Authorizes application access

Redirects user back to Application, passing oauth_verifier

3

Exchange the Request Token for an Access Token

- Request parameters:
  - oauth_consumer_key
  - oauth_nonce
  - oauth_signature_method
  - oauth_signature
  - oauth_timestamp
  - oauth_verifier
  - oauth_version (optional)

Grants an Access Token and Token Secret

- Response parameters:
  - oauth_token
  - oauth_token_secret
  - fullname
  - username
  - user_nsid

Use oauth_token to access protected resources

Active Directory Federation Services (ADFS)

- Microsoft’s answer to federated identities
- Provides authentication and identify data as claims to service providers
- Partner sites use trust policies to match claims to claims supported by their services to make their own authorization decisions
- Works similar to the OAuth authentication process

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Incident Response for Federated Identity Systems

- Check your contract (if you have one)
- IDP usually responsible for notifying account owners (users) and RP/SP of a breach and required response (like password resets)
- RP/SP must determine their response if IDP was compromised (what response, if any)
- If your users' accounts are compromised, how will you provide them access?
  - Think about if a Facebook login got stolen…