Building identity for an open perimeter

Tejas Dharamshi
Senior Security Software Engineer
@tejasdharamshi
Las Vegas, January 6, 2016 -- Netflix launched its service globally, simultaneously bringing its Internet TV network to more than 130 new countries around the world. The company made the announcement -- and the service went live -- during a keynote by Co-founder and Chief Executive Reed Hastings at CES 2016.
#netflix everywhere
B2B
Over 700 apps

Device Partner

Content & Studio

Open Connect

Employee Landing Page

Big Data Portal

Lemur

Corporate

Engineering

Media Partners
Zero Trust
Principle 1
Zero Trust
Principle 1
Netflix Identity Platform
(aka Meechum)
Federation

SSO

Standards (OpenId Connect, OAuth 2.0, SAML)
Layered Security
Signed and Verifiable Identity Information
User Experience

Identity Provider

Delegate
Signed and Verifiable Identity Information
Self-service
Pluggable
Zero Trust
Principle 2
Provisioning/De-provisioning
Zero Trust

Principle 3
Federation Hub (Layered Security)
Are all access patterns the same?
Adaptive Authentication
This device is properly configured.

Netflix baseline policy

- System is up-to-date
- Your Firewall is enabled
- Disk Encryption is enabled
- Screen Lock is enabled
- Automatic Updates are enabled
- Remote Login is disabled

Last scan 5 hours ago by Stethoscope
Authenticate
CHECKING DEVICE SECURITY

The OS X device you are using is unidentified.

Run the Stethoscope app

Automatically launch next time

The Stethoscope app is a way to check your computer's security settings when accessing Netflix systems.

Learn more
Authenticate

CHECKING DEVICE SECURITY

The OS X device you are using does not match our recommended security settings.
Please follow the directions to make your device more secure.

Check again

CONTINUE
Authenticate

CHECKING DEVICE SECURITY

This device is properly configured.

Netflix baseline policy

- System is up-to-date
- Your Firewall is enabled
- Disk Encryption is enabled
- Screen Lock is enabled
- Automatic Updates are enabled
- Remote Login is disabled

Last scan 5 hours ago by Stethoscope

Device security check passed

Continue to application

Automatically launch next time

rescan

view all devices
Federation Hub (Layered Security)
1. Unauthenticated Request
2. Redirect to IDP
3. Authenticate User
4. Authenticated Session
**Allowed Grant Types**

- **Authorization Code (Recommended - Default option for ezconfig)**  
  Intended for traditional web apps as well as native and mobile apps. This flow offers optimal security, as tokens are not revealed to the browser and the client app can also be authenticated.

- **Implicit**  
  Intended for browser (JavaScript single-page-applications) based apps that don’t have a backend. The ID token is received directly with the redirection response from Meechum. Client_secret is not required and thus refresh tokens are not allowed with this flow.

- **Refresh Token**  
  This grant type enables refresh tokens to be included with access tokens. Once the original access token expires, the corresponding refresh token can be sent to Meechum to obtain a fresh access token without requiring the resource owner to re-authenticate.

- **Remote Access Token Validation**  
  This grant type enables an application to remotely validate Meechum access tokens with the introspection endpoint.

**Actions**

- Update Token Manager
- Configuration
- Regenerate Secret
- Delete

**Help**

- Help
- security-help
mod_auth_openidc

mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. It can also function as an OAuth 2.0 Resource Server, validating OAuth 2.0 bearer access tokens presented by OAuth 2.0 Clients.

Overview

This module enables an Apache 2.x web server to operate as an OpenID Connect Relying Party (RP) to an OpenID Connect Provider (OP). It authenticates users against an OpenID Connect Provider, receives user identity information from the OP in a so called ID Token and passes on the identity information (a.k.a. claims) in the ID Token to applications hosted and protected by the Apache web server.

It can also be configured as an OAuth 2.0 Resource Server (RS), consuming bearer access tokens and validating them against an OAuth 2.0 Authorization Server, authorizing Clients based on the validation results.

The protected content and/or applications can be served by the Apache server itself or it can be served from elsewhere when Apache is configured as a Reverse Proxy in front of the origin server(s).

By default the module sets the REMOTE_USER variable to the id_token sub claim, concatenated with the OP's Issuer identifier (sub@iss). Other id_token claims are passed in HTTP headers and/or environment variables together with those (optionally) obtained from the Userinfo endpoint.

It allows for authorization rules (based on standard Apache Require primitives) that can be matched against the set of claims provided in the id_token/userinfo claims.

mod_auth_openidc supports the following specifications:

- OpenID Connect Core 1.0 (Basic, Implicit, Hybrid and Refresh flows)
- OpenID Connect Discovery 1.0

https://github.com/zmartzone/mod_auth_openidc
Application Load Balancers
Access Control

Access Control provides a mechanism to constrain "User" to "App" access.

You can constrain access to your app to specific domains. Further, you can constrain access to groups and users in the selected domains.

Please select the domains you want to constrain access to:

- Netflix.com (employee's only)
- NetflixContractors.com (contractors and vendors only)
- NetflixCS.com (customer service only)
- Svc.netflix.net (service accounts only)
- Pandora Prod (Partner Directories)
- Pandora Test (Partner Directories)
- Moon.film (Prodicle production)

Groups

- Identity and Access Engineering
  - iaee@netflix.com

Users

- Antonia Ellis
  - antoniae@netflix.com

- iaee@
Identity as the Security Perimeter

Roles

Attributes

Orgs

Cleanup

Password Policy

Lifecycle

Groups

Detection

Identity Silos

OpenID

2FA

SAML

Apache

Spinnaker

NETFLIX
Thank you. Questions?

Tejas Dharamshi
Senior Security Software Engineer
@tejasdharamshi