Building Identity for an Open Perimeter

Tejas Dharamshi
Senior Security Software Engineer
Netflix, Inc.
@tejasdharamshi
Netflix Is Now Available Around the World

World’s Leading Internet TV Service Now Live in More than 190 Countries

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.
Application Landscape

Content & Studio

Device Partner

Over

700

apps

Engineering

Corporate

Media Partners
Location Independent Security Approach (LISA)

BeyondCorp

Google

Beyond the Edge

Intel

Zero Trust

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

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

Delegate AuthN & AuthZ
Signed and Verifiable Identity Information
Self-service
Pluggable
Zero Trust
Principle 2
Provisioning/De-provisioning
Zero Trust
Principle 3
Federation Hub (Layered Security)
Multi-factor Authentication

![Multi-factor Authentication example for Netflix]

- Approve
- Deny

- Netflix authenticator
  - Verification code: 536 618
  - Verification code: 531406

NETFLIX
Multi-factor Authentication
Federation Hub (Layered Security)
Are all access patterns the same?
Adaptive Authentication
Federation Hub (Layered Security)
Zero Trust
Principle 4
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 security settings on this device should be improved. Click the arrow next to each recommendation for instructions.

Netflix baseline policy

- **X** Your Firewall should be enabled
- ✔ System is up-to-date
- ✔ Disk Encryption is enabled
- ✔ Screen Lock is enabled
- ✔ Automatic Updates are enabled
- ✔ Remote Login is disabled

Last scan a few seconds ago by Stethoscope

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

Device security check passed

Continue to application
- Automatically launch next time

Last scan 5 hours ago by Stethoscope

rescan
view all devices
Federation Hub (Layered Security)
1. Unauthenticated Request
2. Redirect to IDP
3. Authenticate User
4. Authenticated Session
EZ Configuration

APACHE_MEECHUM = enabled
APACHE_MEECHUM_CLIENT = iatetester-java
APACHE_MEECHUM_SECRET = /run/metakern/decrypted/iatetester-java-secret
APACHE_MEECHUM_ADDITIONAL_SCOPES = allgooglegroups default iatetester-java

# Hostname for your application
APACHE_HTTPS_HOSTNAME = myapp.netflix.com

#==================================================================
# Locations
#==================================================================

# URLs requiring authentication. By DEFAULT, authenticate everything not
# explicitly whitelisted in APACHE_PLAINLOCATIONS. This expression must
# be in Apache LocationMatch compatible format. Note that if
# APACHE_LOCATIONS_FILE is set then APACHE_MEECHUM_LOCATIONS has no effect.
APACHE_MEECHUM_LOCATIONS = ^/

# URLs requiring oauth authentication. By DEFAULT, authenticate nothing.
Paved Road
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 (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
Zuul is a gateway service that provides dynamic routing, monitoring, resiliency, security, and more.
Zero Trust
Principle 5
Role Based Access Control (RBAC)

- Groups
- Organizations
- User attributes
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)
Choose Attributes of interest

The following attributes will be returned to your application from the GSOA endpoint.

You can also choose more user attributes as desired below.

- googleGroups
- orgHierarchy
- org.company
- org.department
- org.employeeType
- org.givenname
- org.jobProfile
- partnerGroups
- preferred_username

Filter the Google Groups

It is recommended that you specify which google groups your application is interested in. If no filters are specified, default behavior is to return all google groups.

You can specify the pattern of the desired google groups below. Once specified, google groups header returned from the Apache Module will only contain those groups if the user is part of those groups.

Pattern:

- Enter your google groups criteria

Add
Recap

Roles

Attributes

Orgs

Groups

Cleanup

Identity Silos

Authorization

Multi-factor Authentication

Password Policy

Lifecycle

Identity Silos

Recap
Identity as the Security Perimeter

Roles
Attributes
Orgs
Groups
Cleanup
Detection
Lifecycle
Identity Silos
Password Policy

NETFLIX

52

RSAC Conference 2019
Immediate Action Items

- Identify if your organization has privileged corporate network?
  - What access do users get as a result of this implied trust?

- Identify gaps in the provisioning and de-provisioning process in your organizations
  - Are you tapping into event sources?
  - What about de-provisioning?

- If you liked anything which is not open-sourced yet. Please email me @tdharamshi@netflix.com.
How to apply what we learnt today

- Adopt standards OpenId, OAuth 2.0, SAML and leverage IDP’s like PingFederate, Okta, Auth0 etc.
- See if apache module, alb authentication fits your organization needs.
- Adopt multi-factor authentication and adaptive authentication for stronger authentication
- How does your endpoint security strategy looks like?
  - Does your organization adopt BYOD?
  - Checkout Stethoscope app