Google Cloud

Edge Security

Fundamentals of Authentication and Authorization

Securing your API

Identity Tracking

Is concerned with tracking usage by an application and/or user

“do you have a ticket?”

Authentication

Involves validating application and/or user credentials

"who are you?"

Authorization

Involves determining what the application and/or user can do

"what can you do?"

Identity tracking

Concerned with tracking usage by an application and/or user

Not concerned with authorizing access, just who/which app is using service

Applications generally tracked using API keys

Users tracked via credentials

Other identity tracking can be done via IP address and Host header

Authentication

Act of confirming whether someone or something is, in fact, who or what it is declared to be

Credentials provided are compared to those on file in a database of authorized users' information

If the credentials match, the process is completed and the user is considered to be authenticated

Standards: AD/LDAP, OpenID Connect

Authorization

The process of

an administrator granting rights or

checking user account permissions for access to resources

Authentication precedes authorization

"*to authorize*" is to define an access policy

Standards: OAuth v2.0, SAML 2.0

Common patterns

APIKey

```
…/target?apikey=45c78ece5b77647854a84dfb4ba96dc8
```

Access Token

```
…/target?access_token=4WCAchNNtVyK8JsACl1HP7ml
```

```
Authorization: Bearer 4WCAchNNtVyK8JsACl1HP7ml
```

```
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
```

THANK YOU