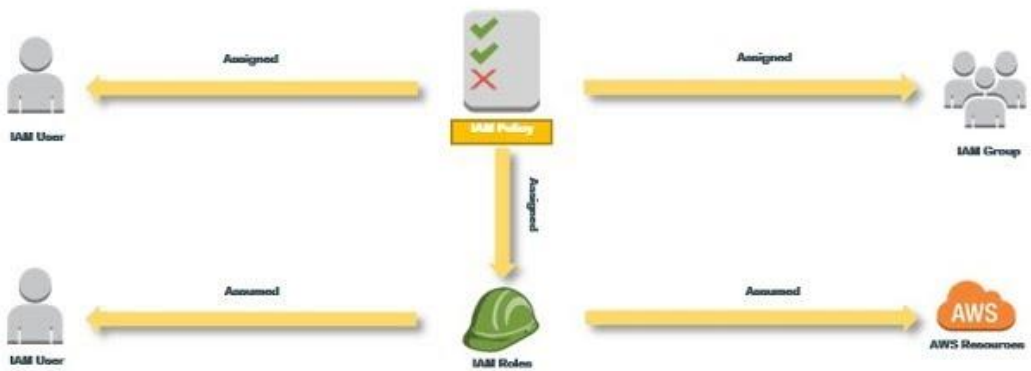
AWS Security:

Identity and Access Management

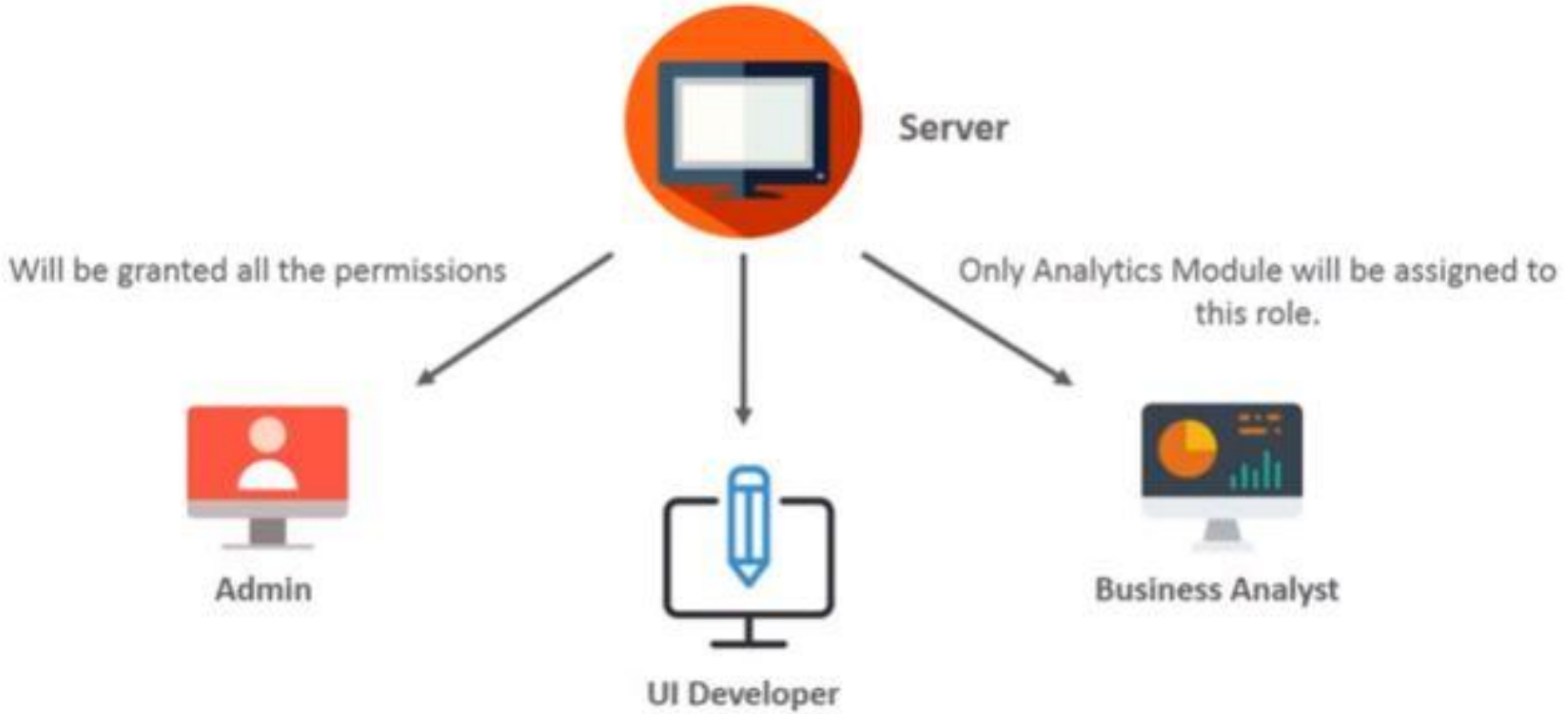
Users & Groups

Roles with permissions



Agenda

Why Do We Need Access Management?



Components

Users

Groups

Roles

Policies

Using **IAM**, you can create and manage AWS **users**, and use permissions to allow and deny their access to AWS resources.

Components

Users

Groups

Roles

Policies

The users created, can also be divided among **groups**, and then the **rules** and **policies** that apply on the **group**, apply on the user level as well.

Components

Users

Groups

Roles

Policies

An IAM **role** is an IAM entity that defines a set of permissions for making **AWS** service requests. IAM **roles** are not associated with a specific user or group. Instead, trusted entities assume **roles**, such as IAM users, applications, or **AWS** services such as EC2

Components

Users

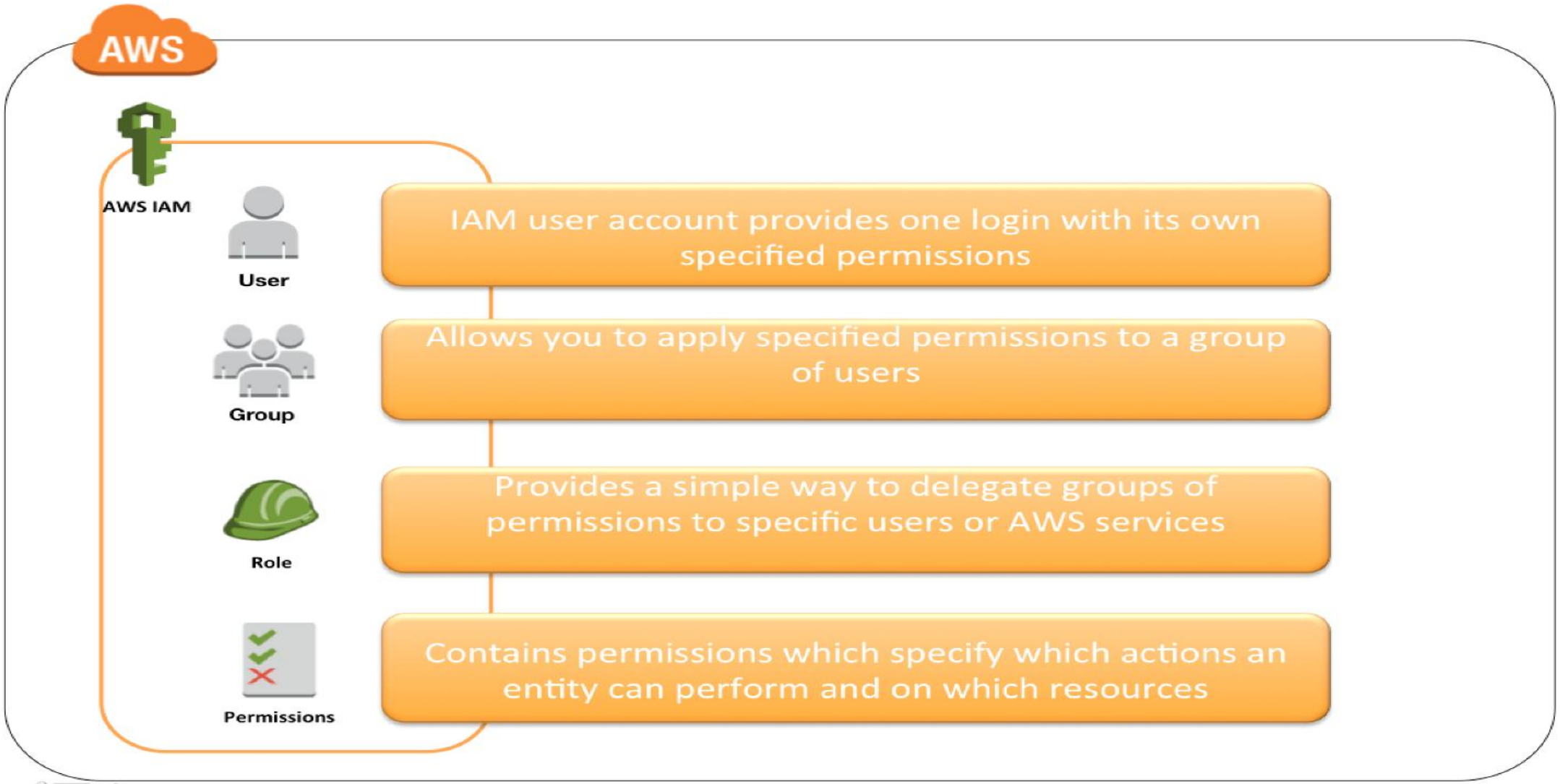
Groups

Roles

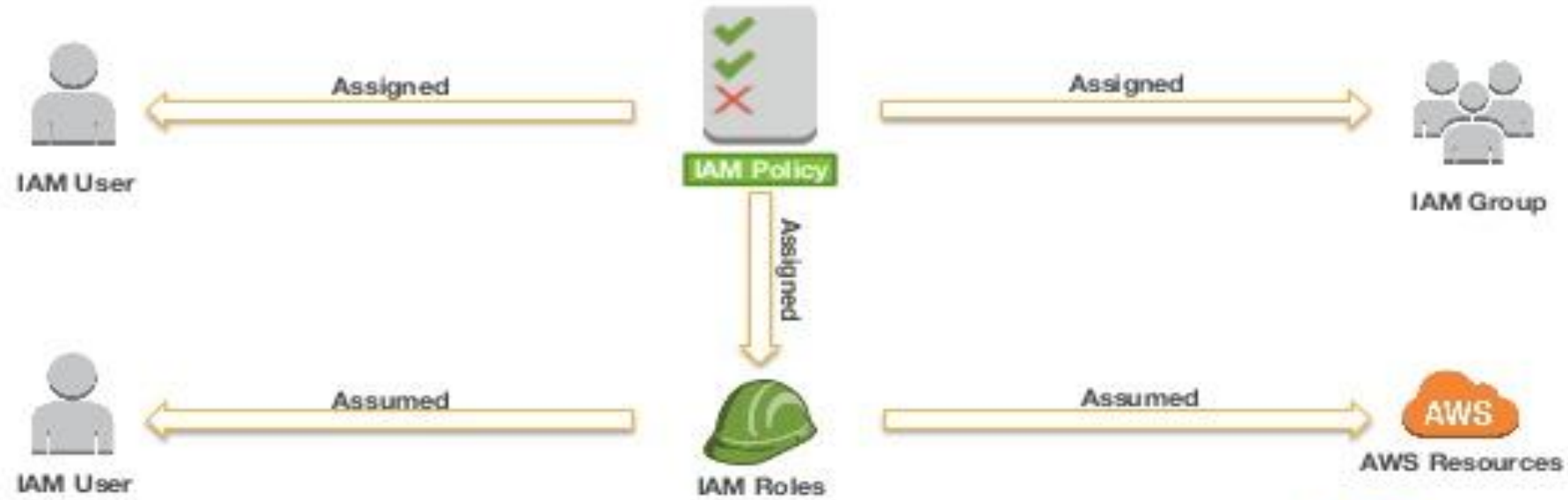
Policies

To assign **permissions** to a user, group, role, or resource, you create a ***policy***, which is a document that explicitly lists permissions.

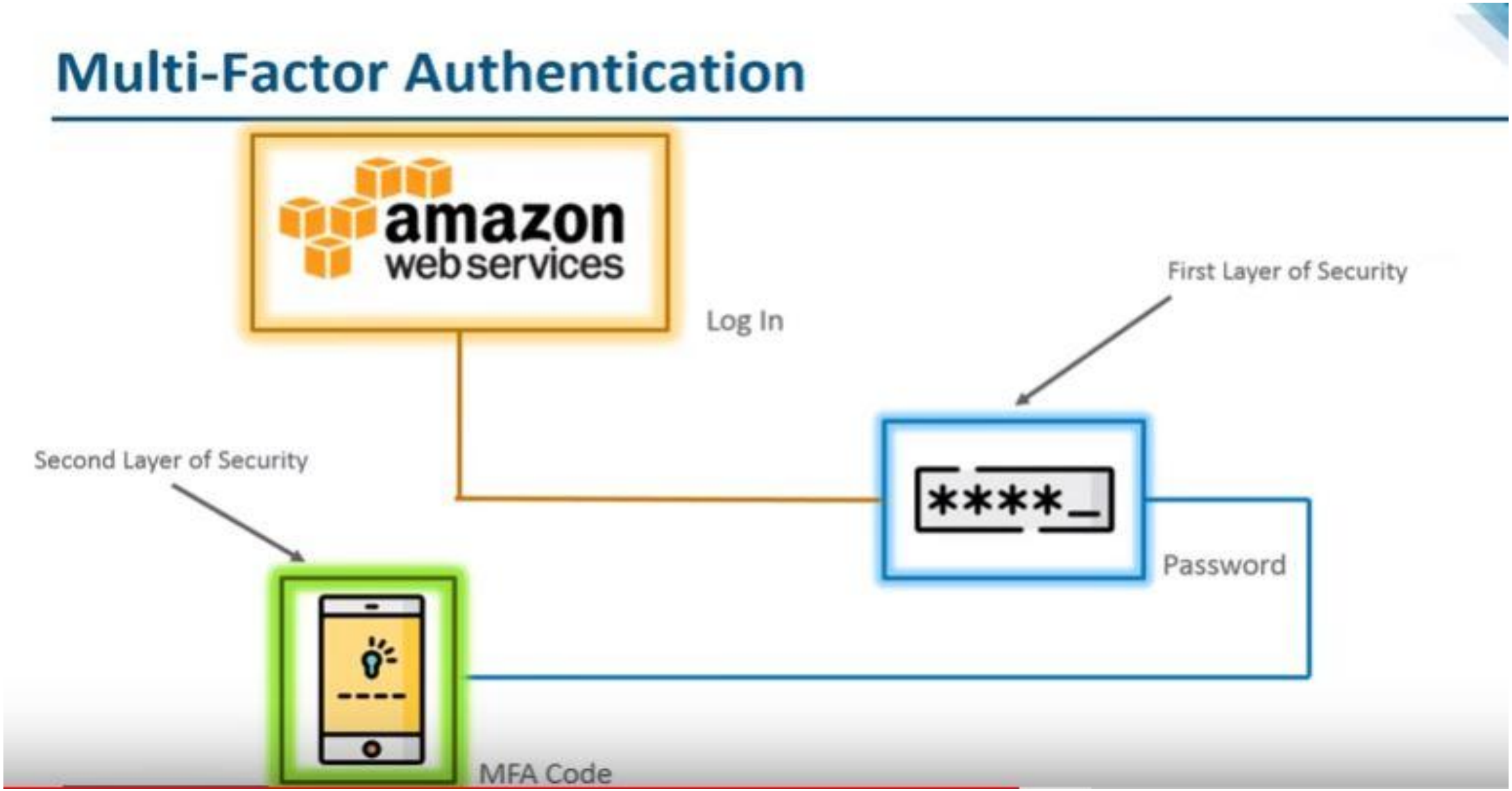
AWS IAM Identities



AWS IAM Policy Assignment



Multi-Factor Authentication



HANDS ON LABS