Session Management

Max McCarty

@maxRmccarty https://lockmedown.com

Overview

Protecting the Session ID

Time-limited Sessions

New Sessions on Authentication

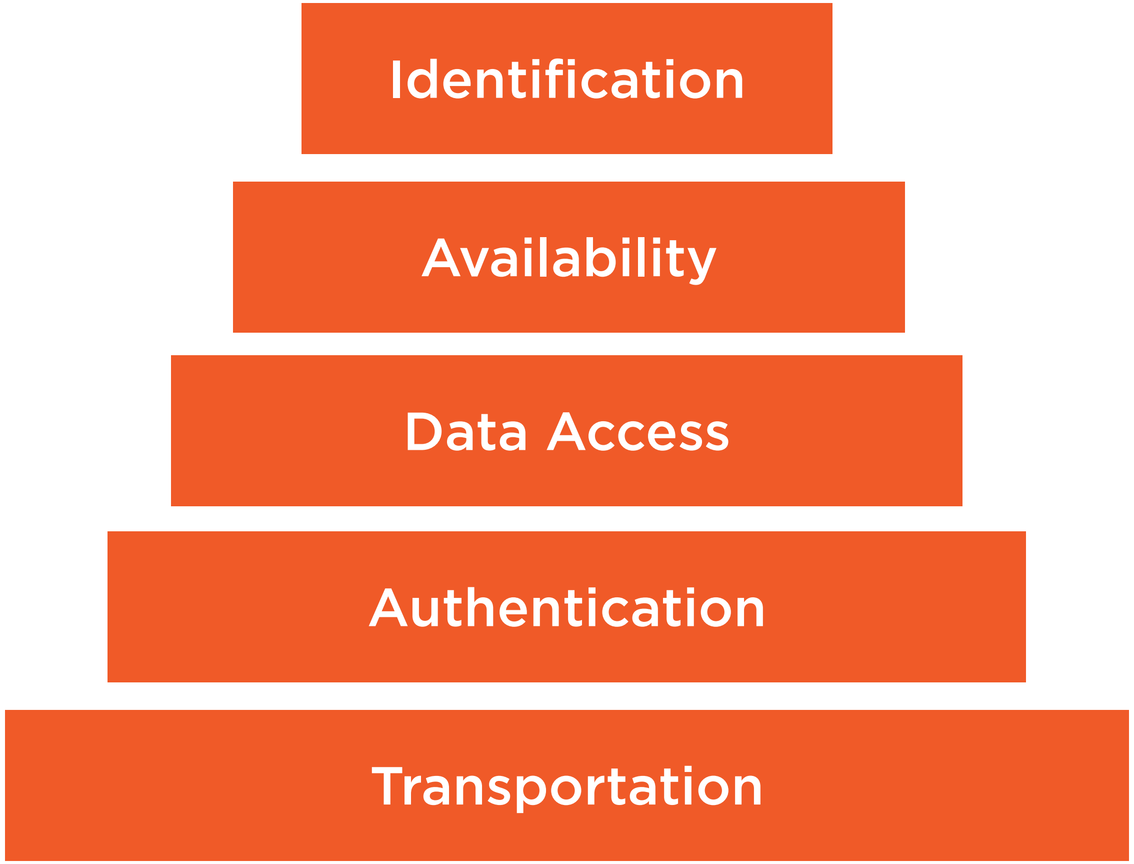
HTTPOnly Flagged Cookies

Transport Layer Security

Secure Flagged Cookies

Re-authentication On Key Access

Layered Security



Identification

Availability

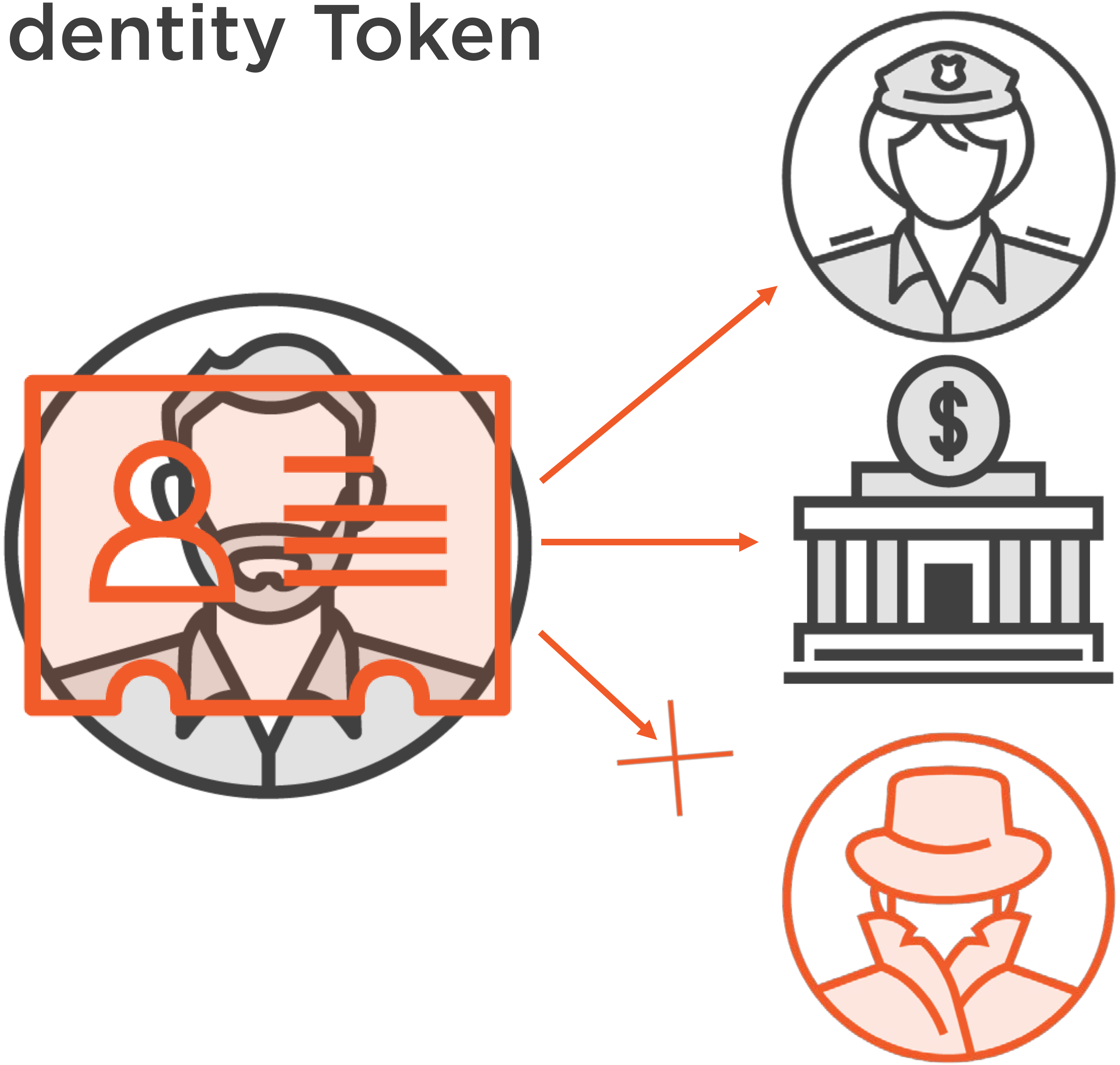
Data Access

Authentication

Transportation

Protecting the Session ID

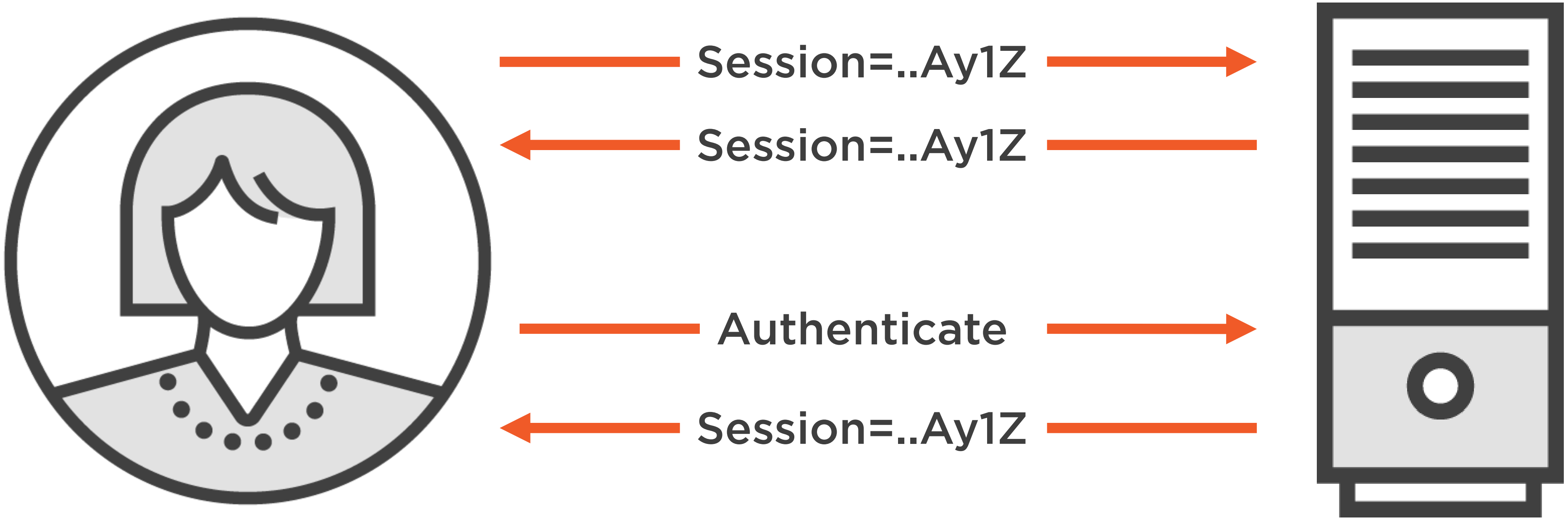
Identity Token



Time-limited Sessions

No Recycled Sessions

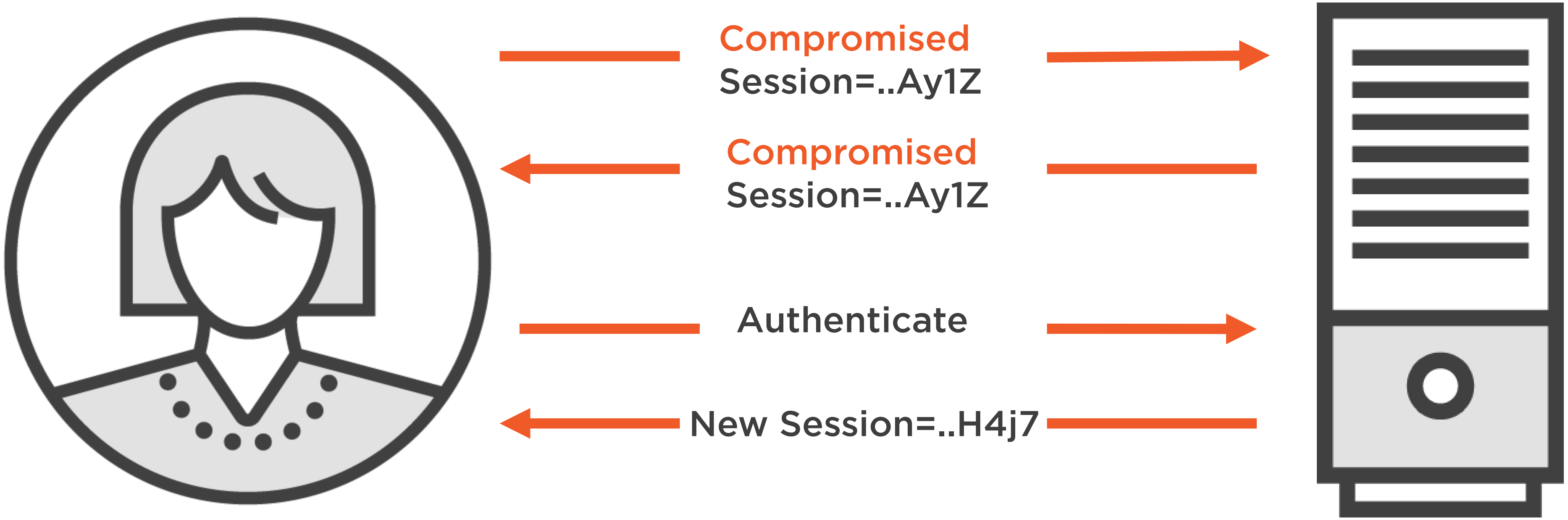
Recycled Sessions



Session Fixation Attacks

- Sessions that are fixated to a user through different authentication states
- Allows attackers to operate at elevated privileges after a user authenticates

Regenerated New Sessions



Compromised
Session=..Ay1Z

Compromised
Session=..Ay1Z

Authenticate

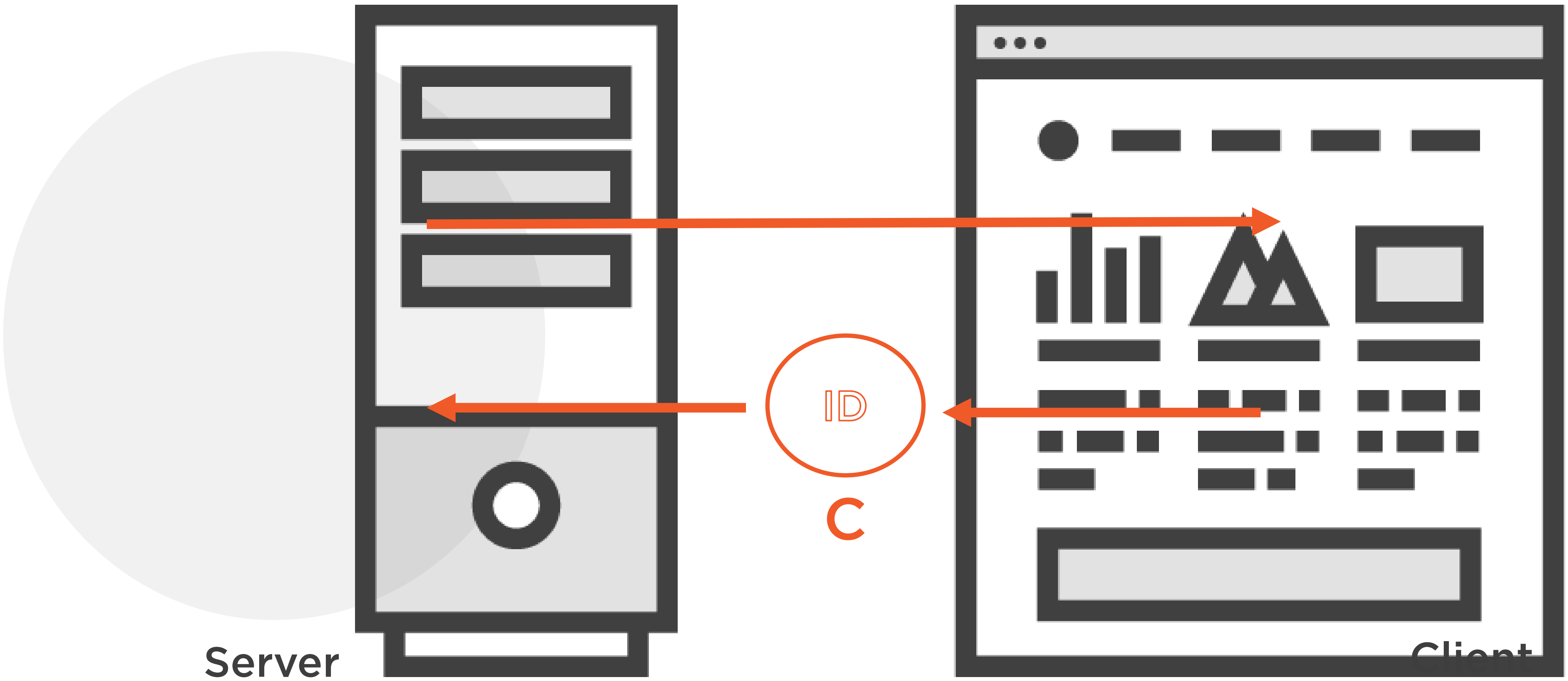
New Session=..H4j7

Protecting Cookies with *HTTPOnly* Flag

What is the use of Session Cookies?

Controlled

Uncontrolled



ID

C

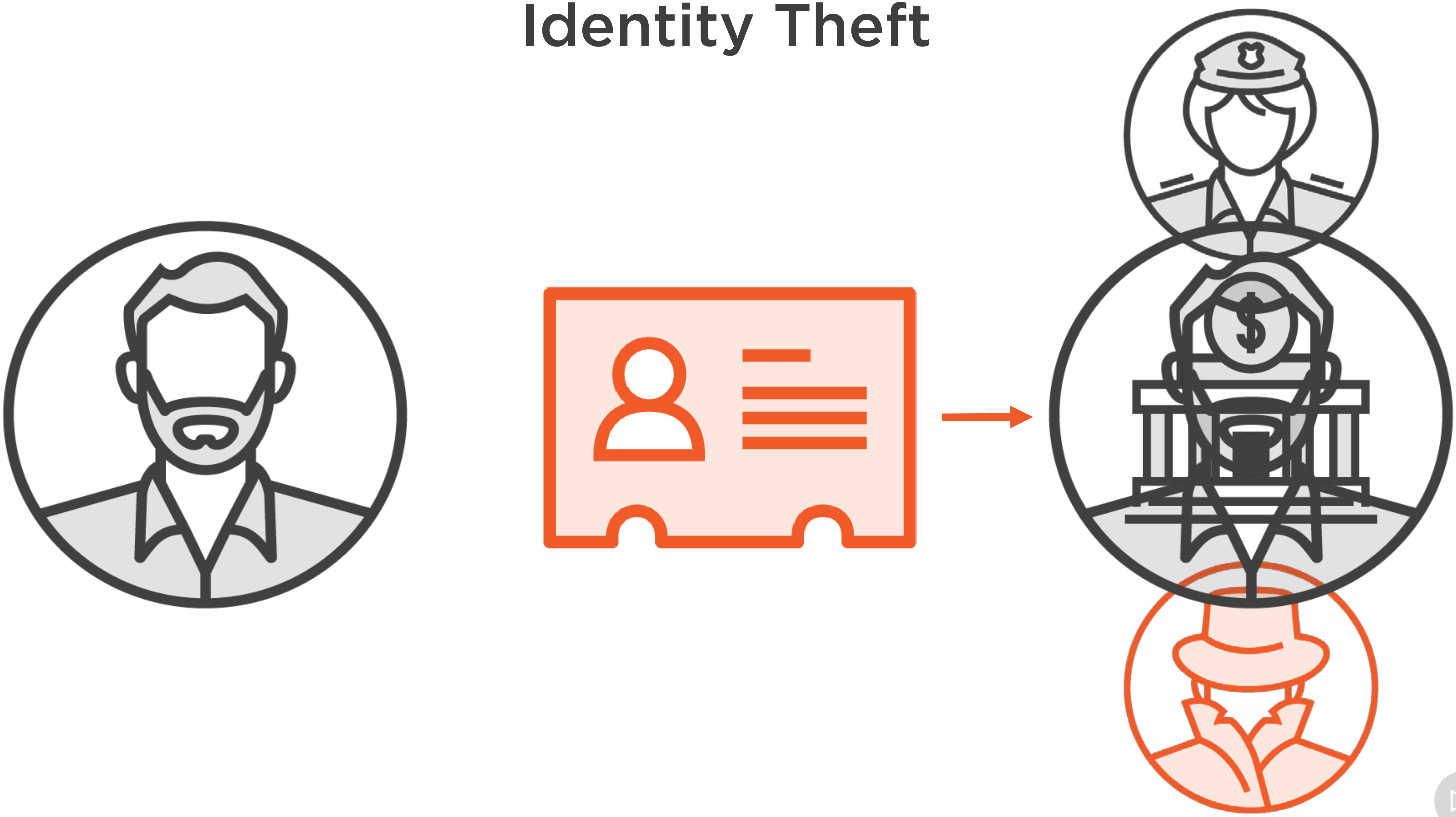
Server

Server

Client

Client

Identity Theft



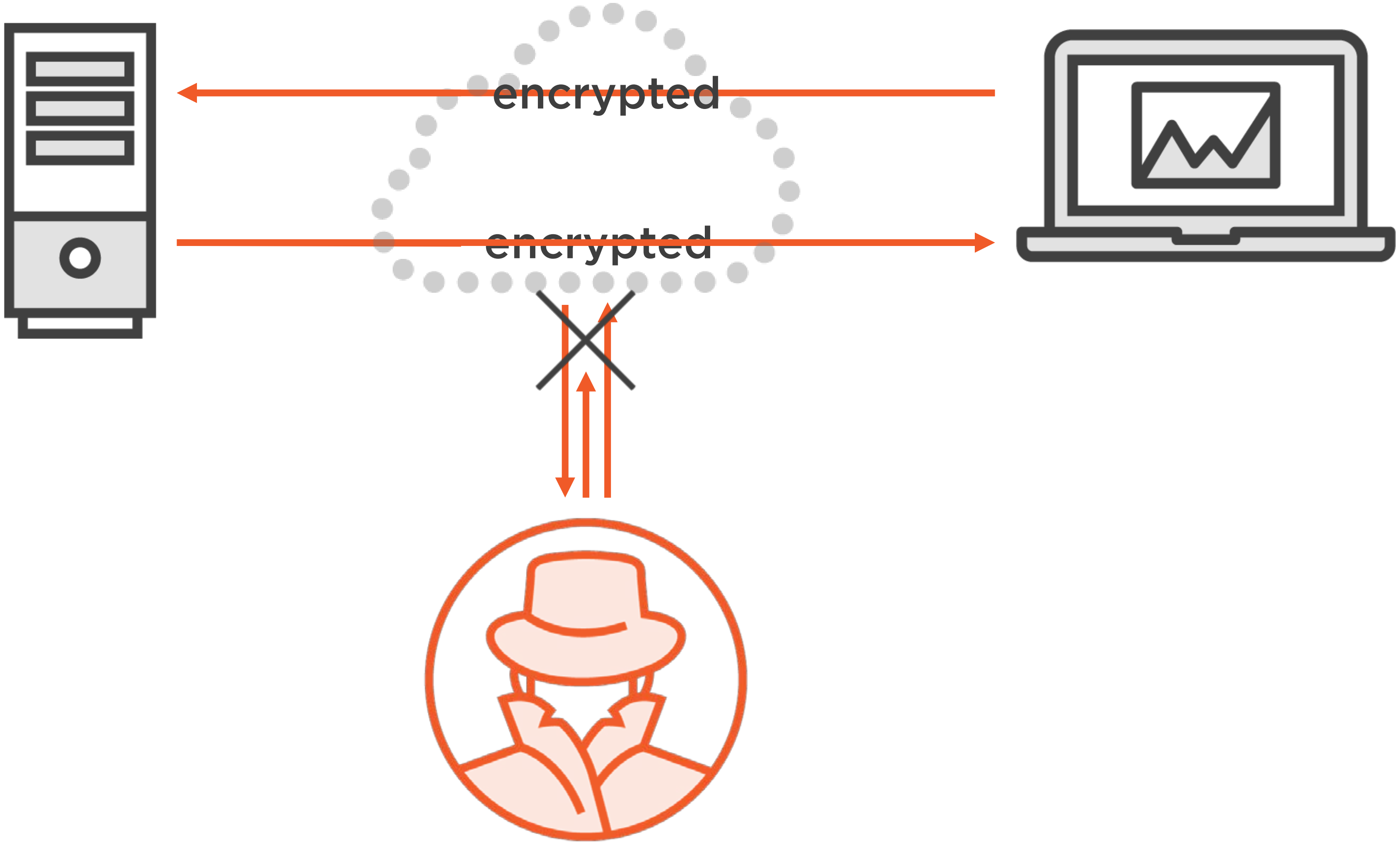
HTTPOnly

Set-cookie: mycookie=value; path=/; *HttpOnly*

A http response header informing the browser that the cookie cannot be accessed through client side scripts

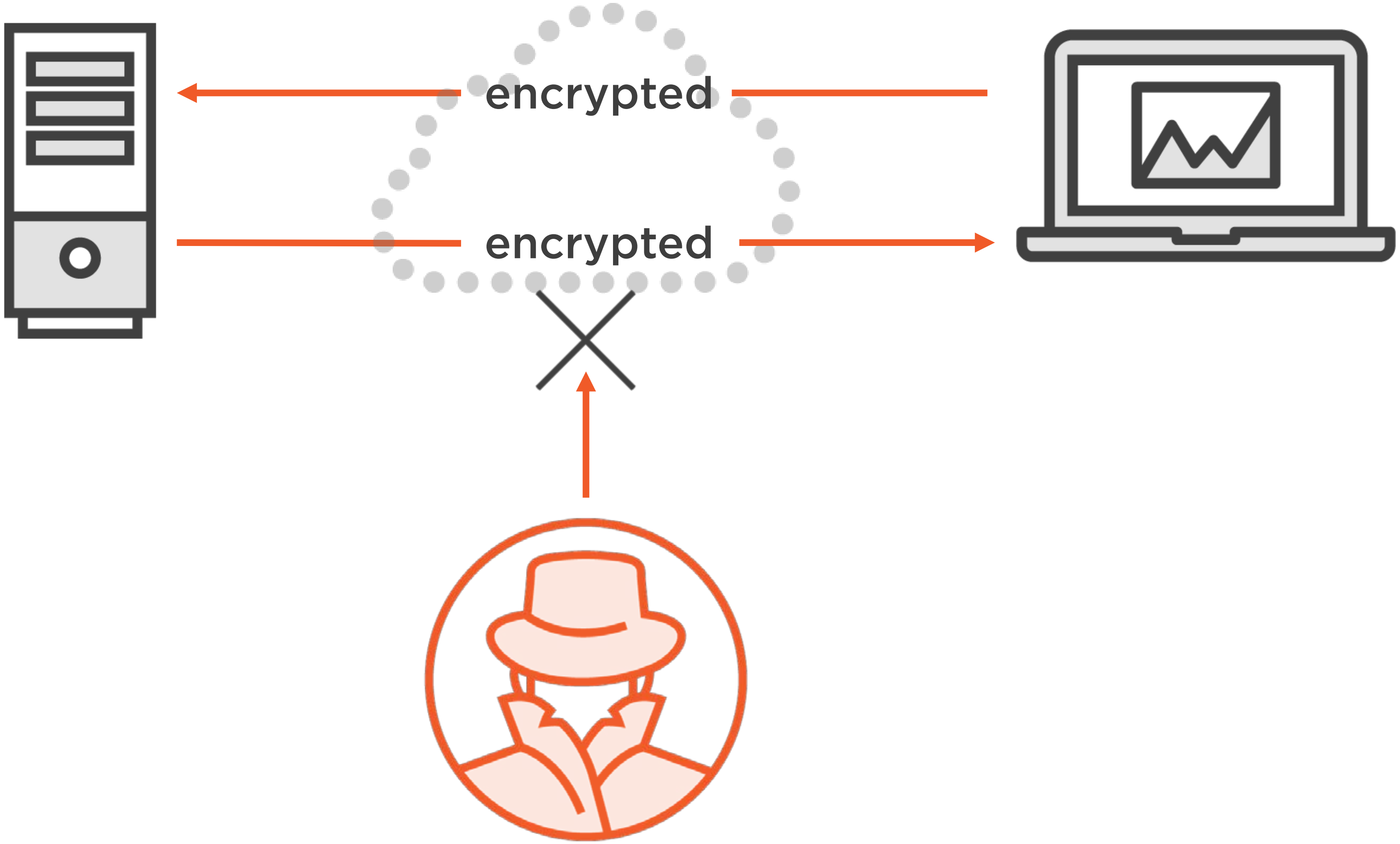
Transportation Layer Security

Man-in-the-Middle Attacks



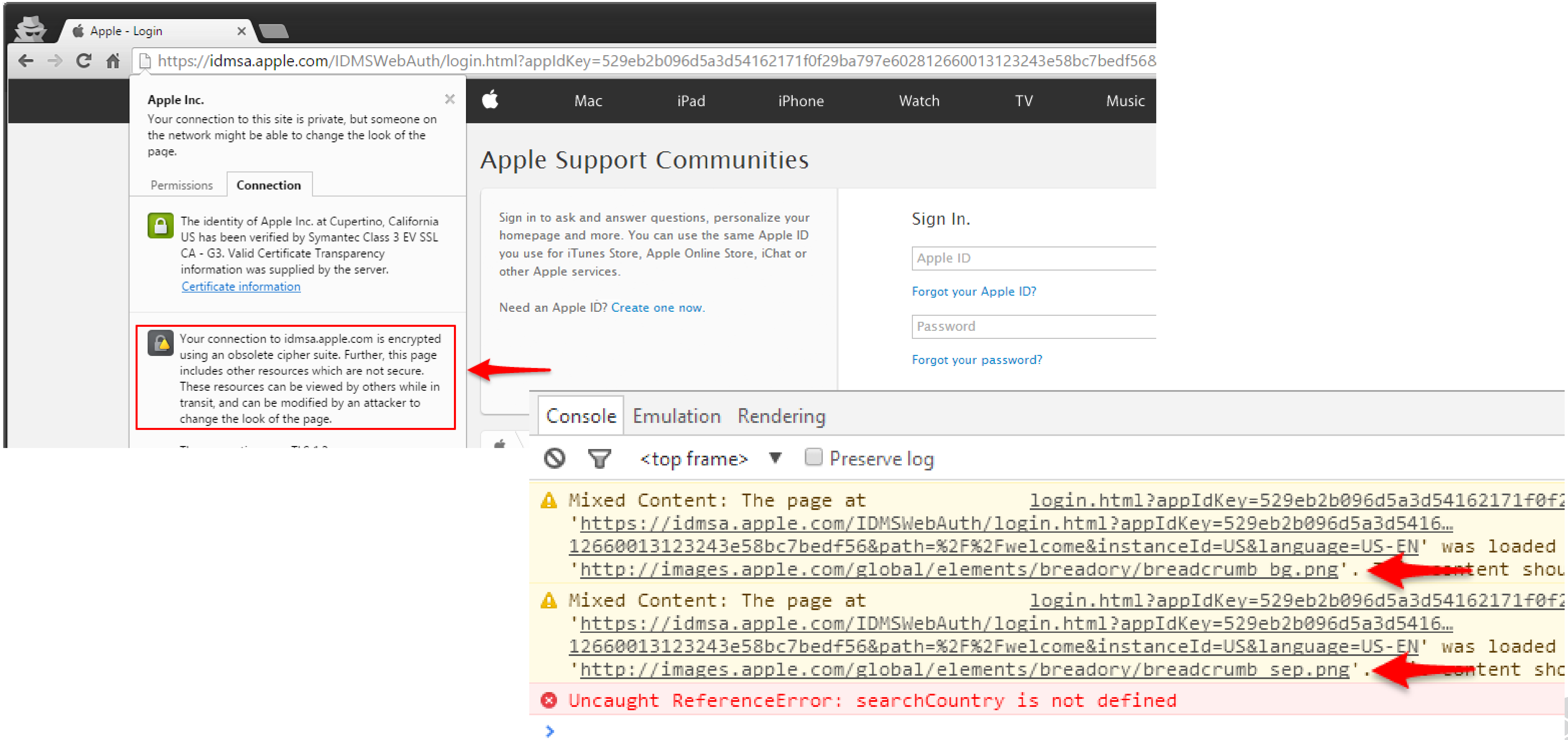
Secure Flagged Cookies

Man-in-the-Middle Attacks



On a secure page, what happens when a resource is loaded over HTTP?

Mixed Content



Apple Inc.

Your connection to this site is private, but someone on the network might be able to change the look of the page.

The identity of Apple Inc. at Cupertino, California US has been verified by Symantec Class 3 EV SSL CA - G3. Valid Certificate Transparency information was supplied by the server.

Your connection to idmsa.apple.com is encrypted using an obsolete cipher suite. Further, this page includes other resources which are not secure. These resources can be viewed by others while in transit, and can be modified by an attacker to change the look of the page.

Apple Support Communities

Sign in to ask and answer questions, personalize your homepage and more. You can use the same Apple ID you use for iTunes Store, Apple Online Store, iChat or other Apple services.

Need an Apple ID? Create one now.

Sign In.

Apple ID

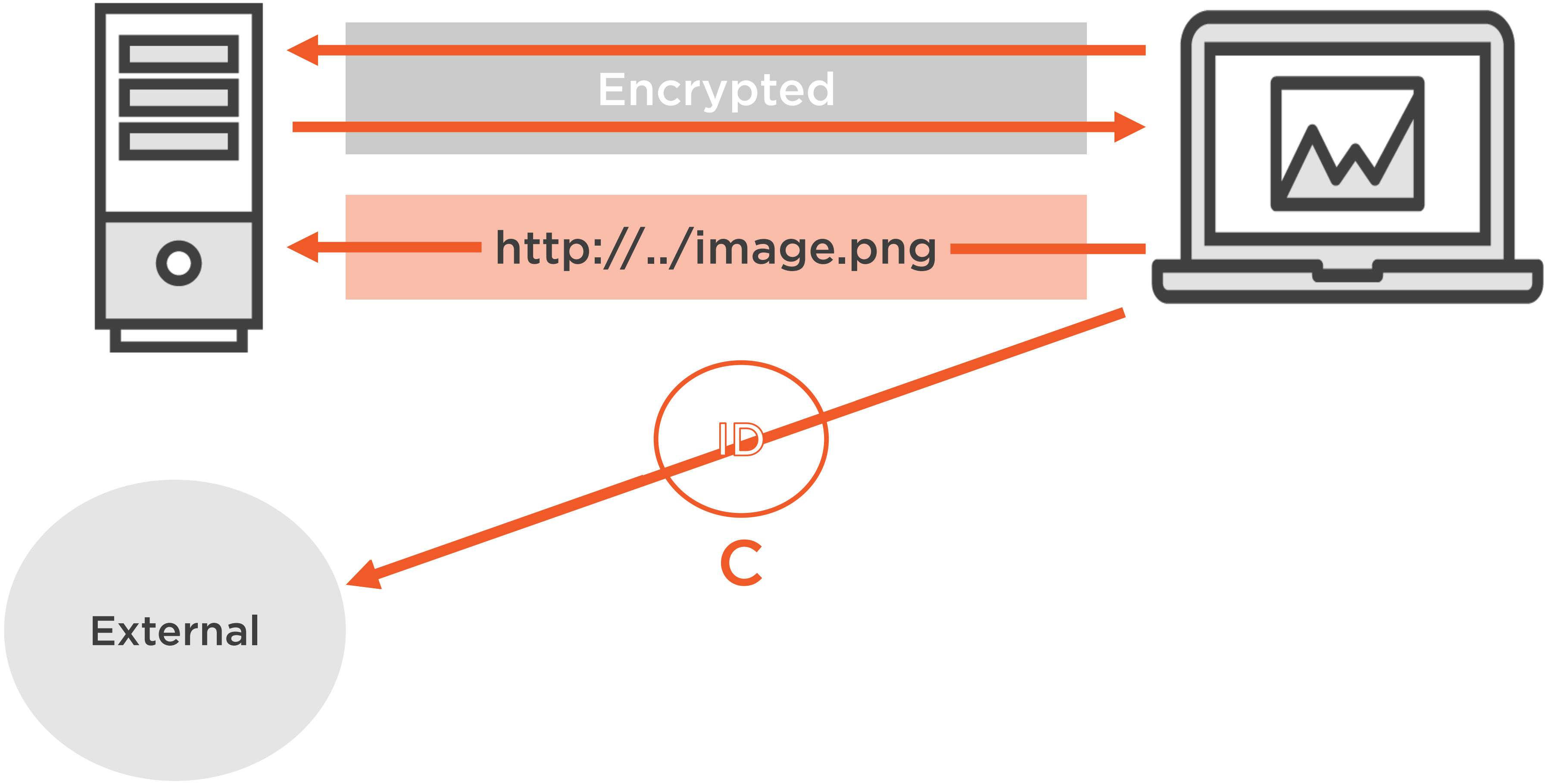
Forgot your Apple ID?

Password

Forgot your password?

```
⚠ Mixed Content: The page at        login.html?appIdKey=529eb2b096d5a3d54162171f0f2
  'https://idmsa.apple.com/IDMSWebAuth/login.html?appIdKey=529eb2b096d5a3d5416…
  12660013123243e58bc7bedf56&path=%2F%2Fwelcome&instanceId=US&language=US-EN' was loaded
  'http://images.apple.com/global/elements/breadory/breadcrumb_bg.png'.     ntent shou
⚠ Mixed Content: The page at        login.html?appIdKey=529eb2b096d5a3d54162171f0f2
  'https://idmsa.apple.com/IDMSWebAuth/login.html?appIdKey=529eb2b096d5a3d5416…
  12660013123243e58bc7bedf56&path=%2F%2Fwelcome&instanceId=US&language=US-EN' was loaded
  'http://images.apple.com/global/elements/breadory/breadcrumb_sep.png'.     ntent sho
⊗ Uncaught ReferenceError: searchCountry is not defined
>
```

Mixed Content Vulnerability



Secure

Set-cookie: mycookie=value; path=/; *secure*

A http response header informing the browser that the cookie should not be sent over an insecure request

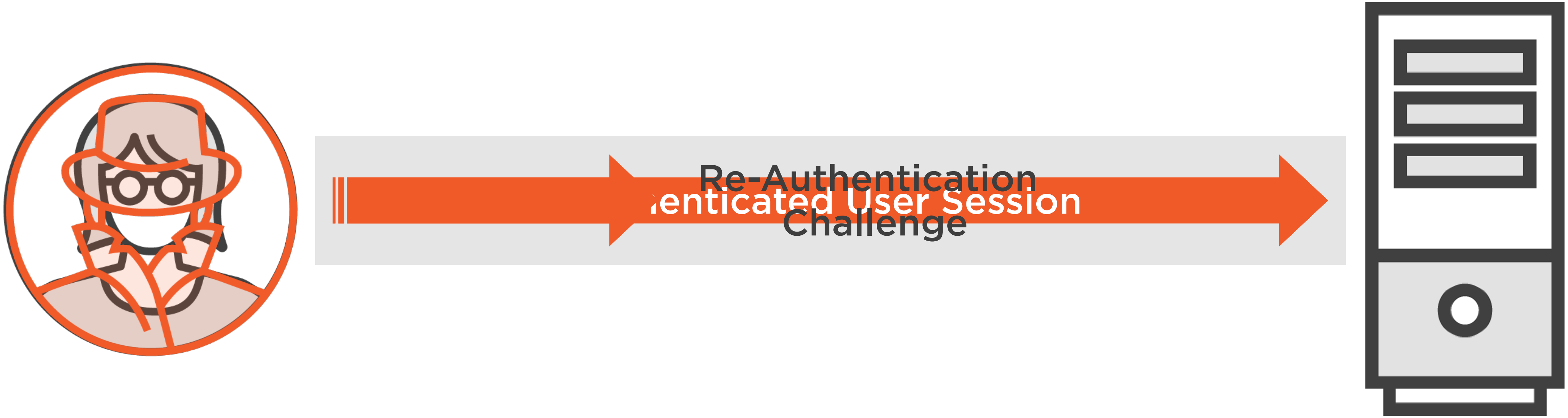
Re-authenticating on Key Access

ebay

amazon

GitHub

Minimizing the Damage of a Hijacked Session



Re-Authentication Challenge

ıenticated User Session

Summary

Protecting the Session ID

Time-limited Sessions

New Session on Authentication

HTTPOnly Flagged Cookies

Transport Layer Security

Secure Flagged Cookies

Re-authentication On Key Access