Securing Our Connection

Max McCarty

@maxRmccarty https://lockmedown.com

Overview

Acronym Soup: TLS, SSL and HTTPS

The Importance of TLS

Setting up a secure Server

Login Forms From the Top

Introducing the HSTS Header

Implementing HSTS

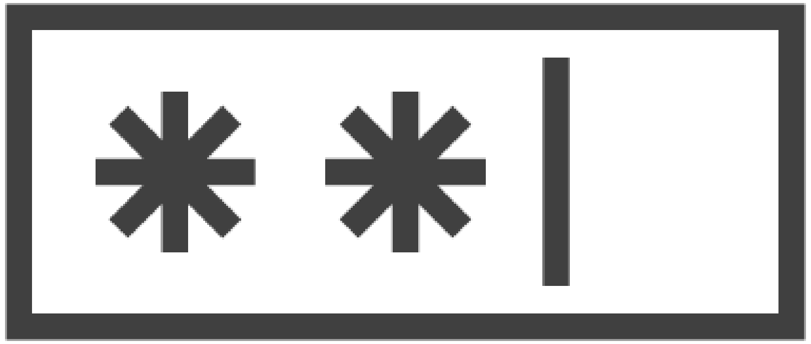
Introducing the CSP Header

Implementing CSP

Acronym Soup: TLS, SSL and HTTPS

Discussed Benefits of TLS

Transport User Credentials



Secure Session Cookie Content

TLS SSL HTTPS

SSL Becomes TLS

SSL

Originally Designed by Netscape

Receives patent in August, 1997

IETF takes over SSL maintenance 1999

TLS

IETF renames SSL to TLS to over Netscape Associations

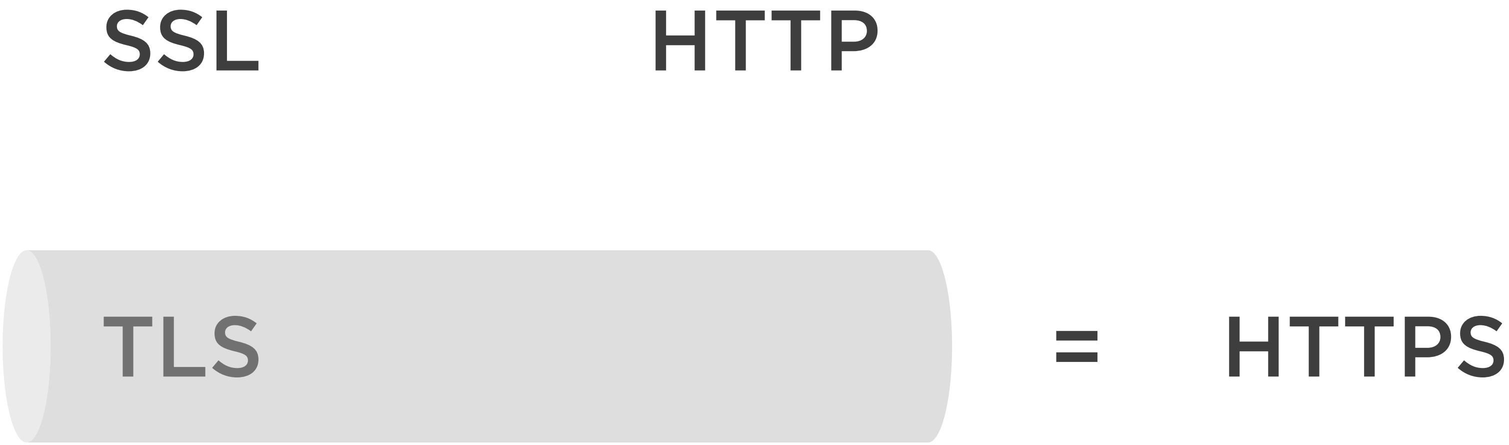
IETF releases TLS 1.0 RFC January, 1999

https://www.ietf.org/rfc/rfc2246.txt

HTTPS

Represents the use of the HTTP protocol over an established TLS tunnel.

**Is not a different protocol

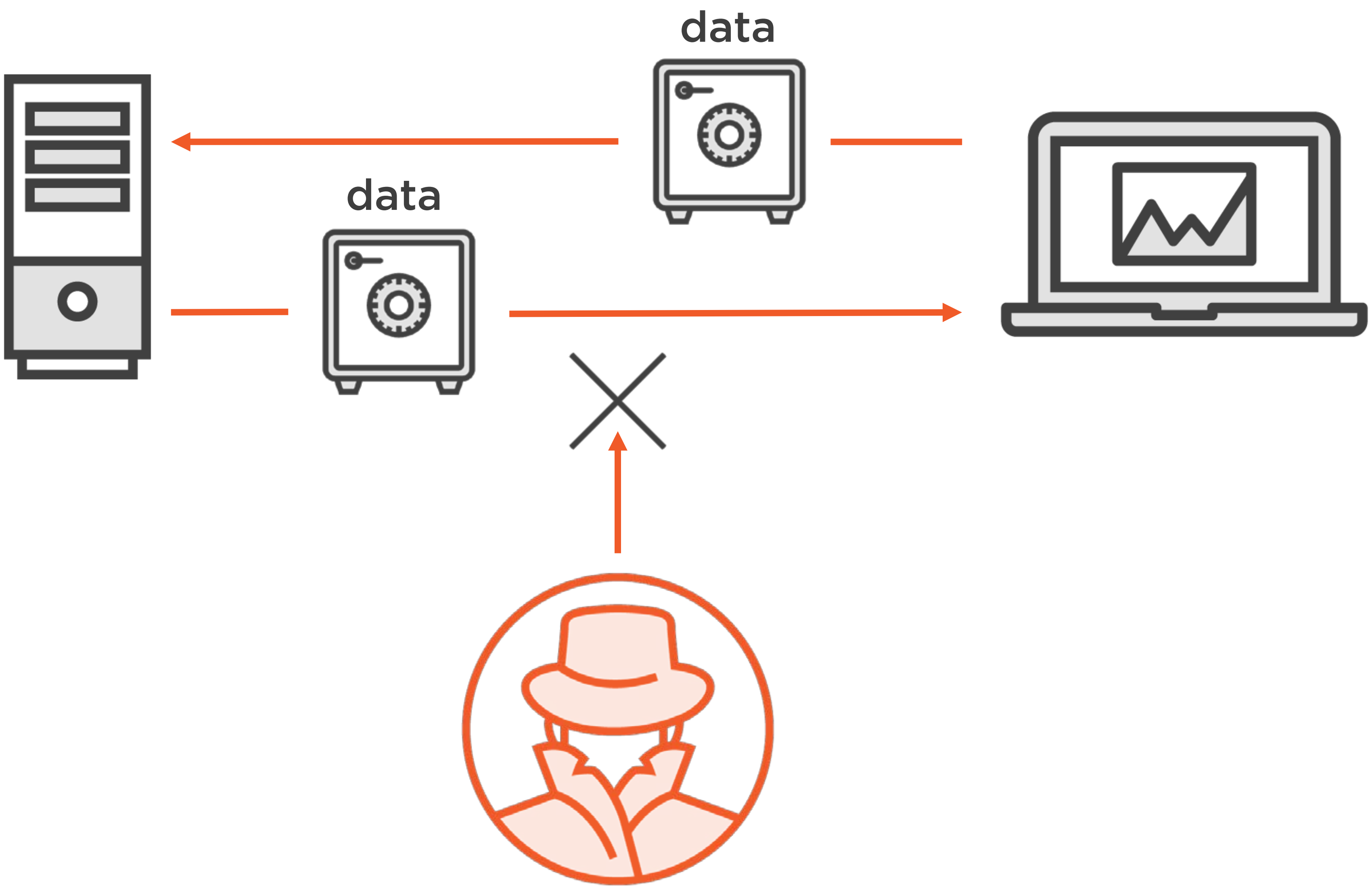


SSL HTTP

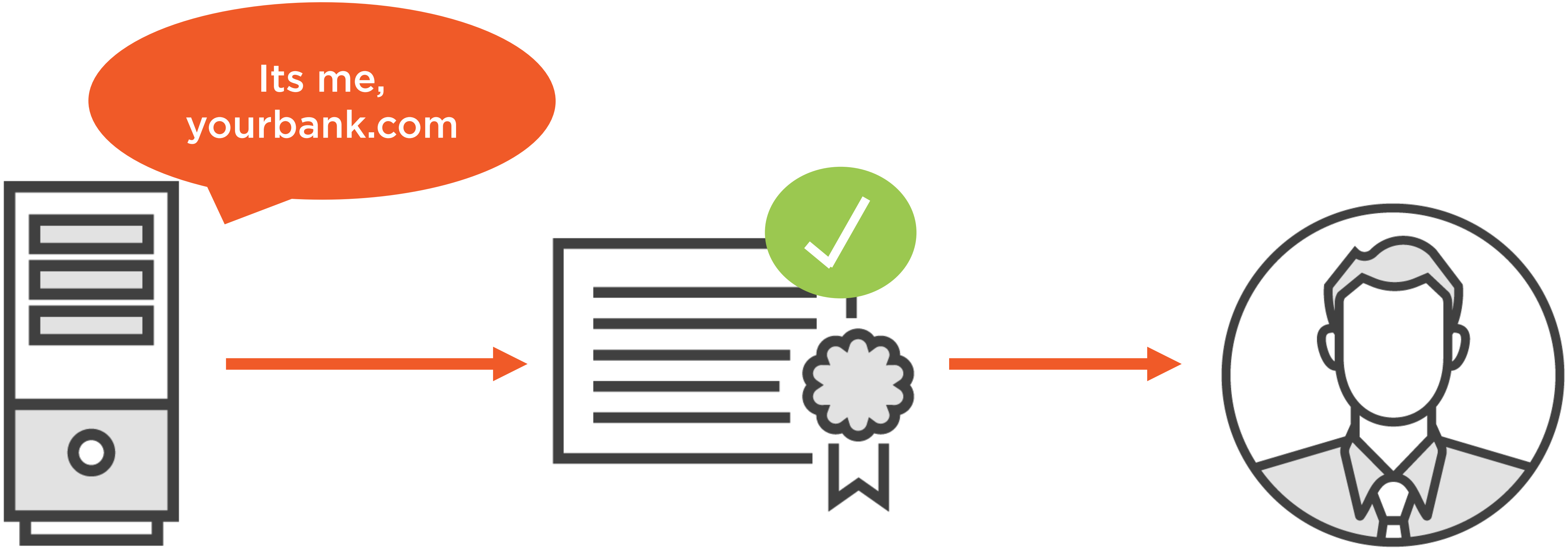
TLS = HTTPS

Importance of TLS

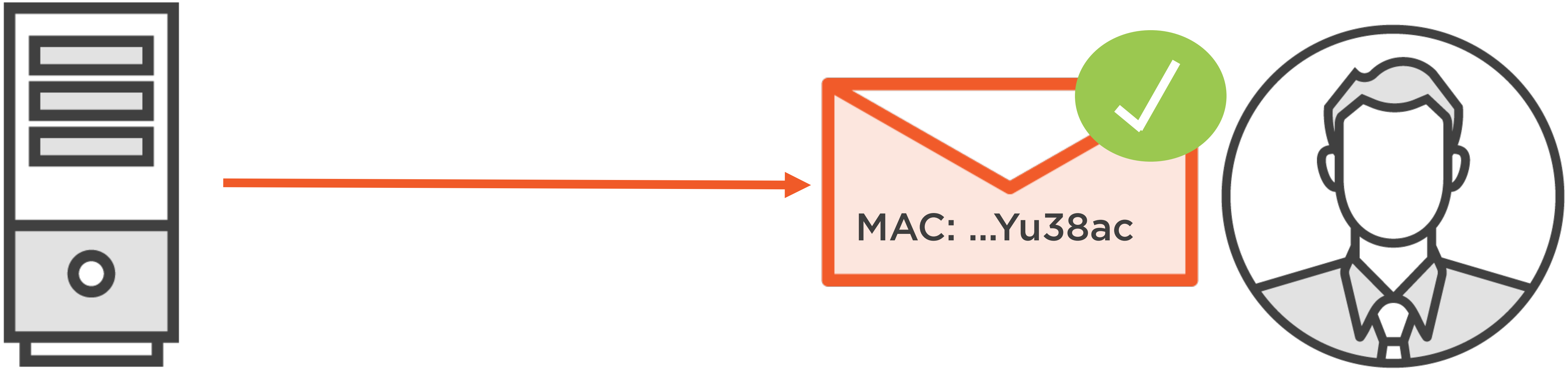
Confidential Data Exchange



Server Validity



Message Integrity



Setting Up a Secure Server

SSL Certificates

- Never use self-signed certificates in Production
- Consult OWASP’s TLS Protection Cheat Sheet
- Use only reputable Certificate Authorities to acquire Production SSL Certificates

Pro-Tip

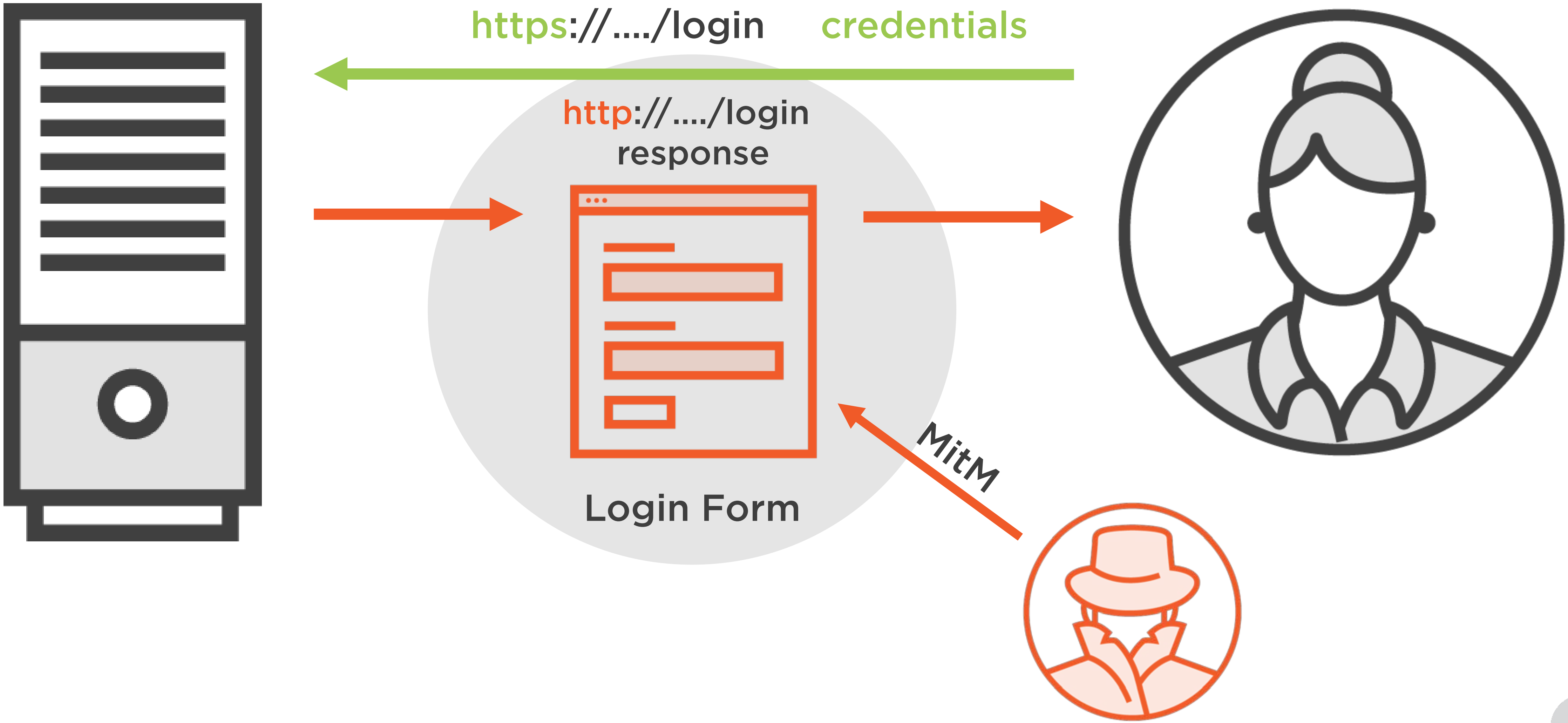
LetsEncrypt provides affordable (free) and hassle (free) certificates.

Pro-Tip

Use Nginx, Apache or suitable server to handle TLS connections to your application.

Login Forms From the Top

TLS Misconfiguration



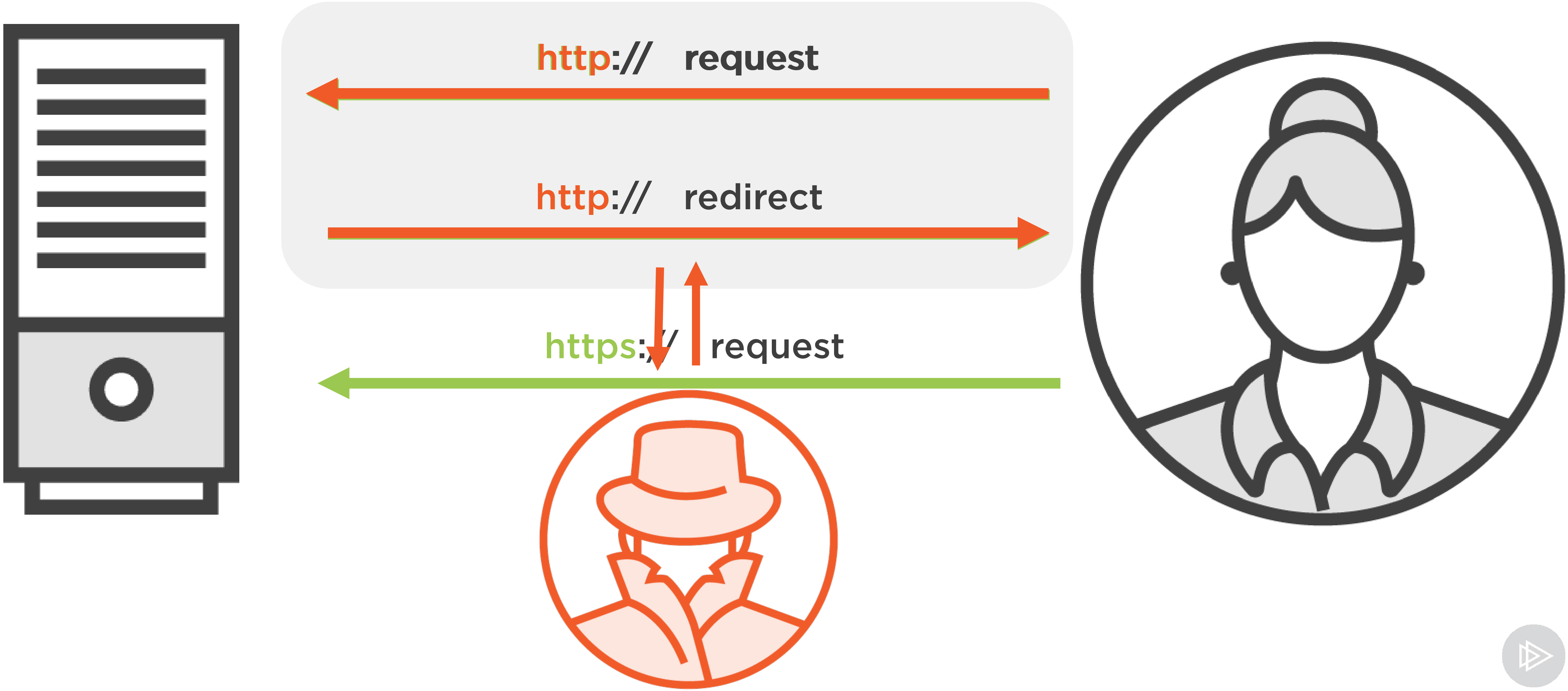
Key Points

Submitting sensitive data over HTTPS is not always enough

Server forms that handle sensitive data over HTTPS

Introduction to HTTP Strict Transport Security

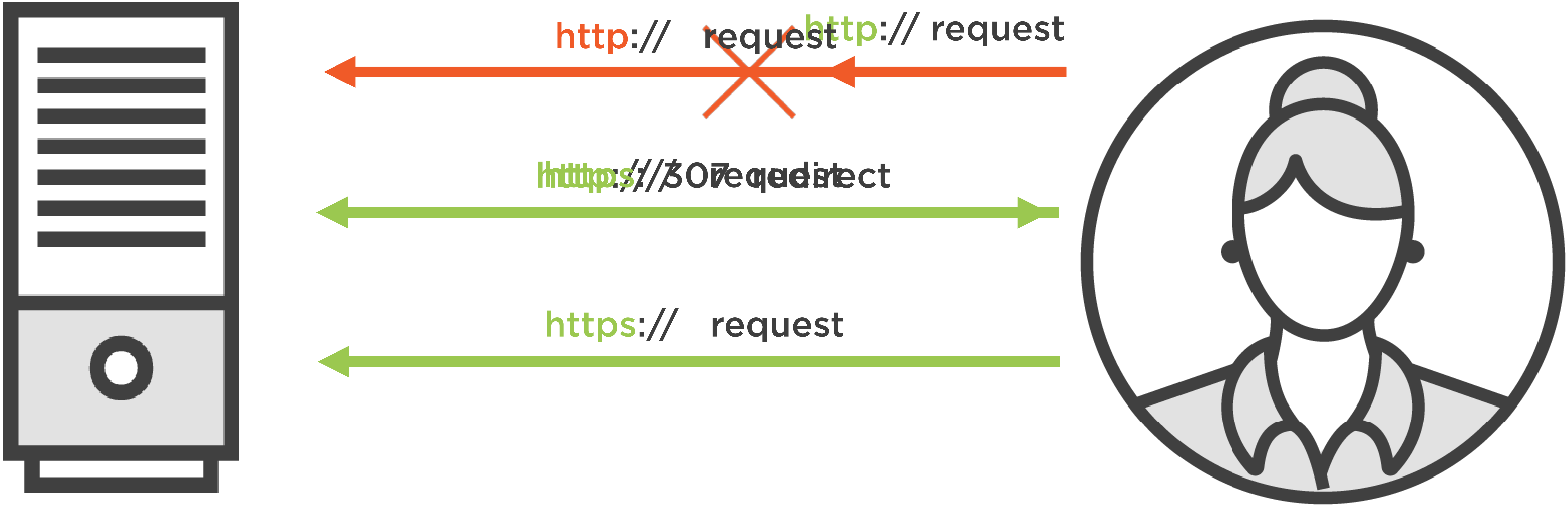
Initial Request and Response



HTTP Strict Transport Security

HTTP header to notify supporting browsers that future requests to this website should be made over HTTPS

Initial Request and Response



Configuring HSTS Properly

Do's

Only provide the HSTS over HTTPS

Issue 307 redirects to preserve request method

Always include the HSTS header

Do Nots

Never supply the HSTS header insecurely

Sporadically or only on specific resources provide the HSTS header

HTTP Strict Transport Security Attributes

IncludeSubdomains

Specifies that the HSTS policy also applies to any hosts whose domain names are subdomains of the Known HSTS Host's domain name

Preload

Correlated with Chromium, a preloaded list managed by Google for reducing the requirement of the initial HTTP request.

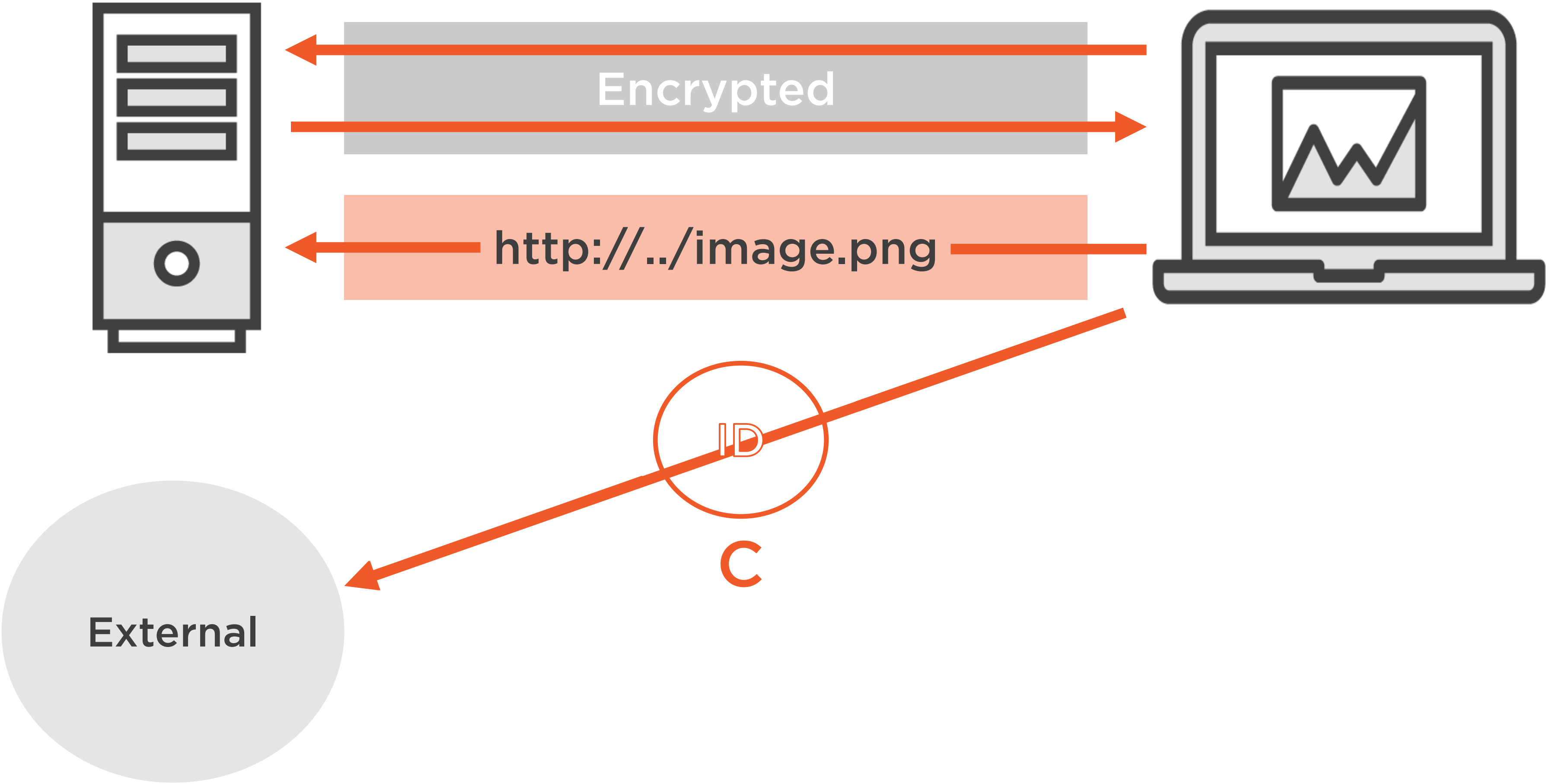
Introduction to Content Security Policy

Content Security Policy

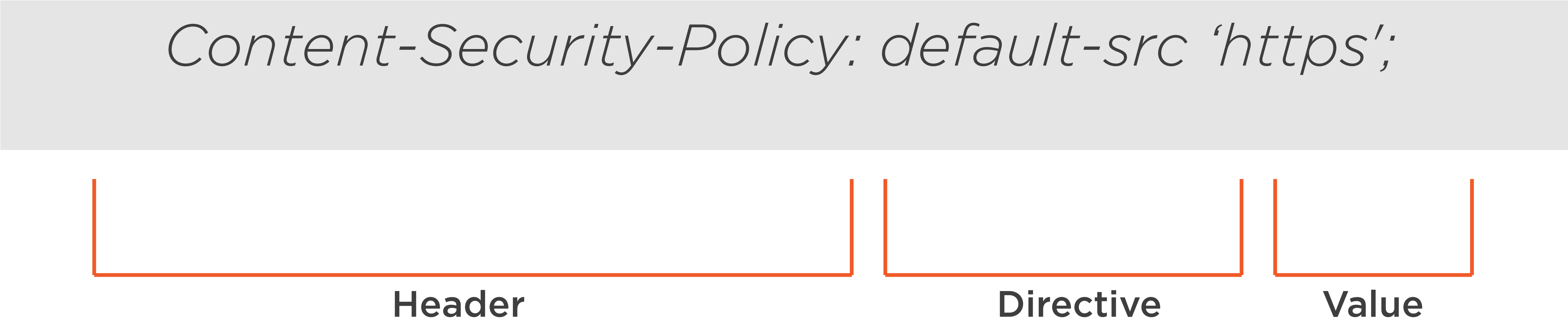
HTTP response header helps you reduce XSS risks on modern browsers by declaring what dynamic resources are allowed to load via a HTTP Header

https://content-security-policy.com/

Mixed Content Vulnerability



Content-Security-Policy Example



Content-Security-Policy: default-src ‘https’;

Header

Directive

Value

Content-Security-Policy Report Directive

```
Content-Security-Policy: default-src ’https′; report-uri http://..../cspviolations
```

Summary

Acronym Soup: TLS, SSL and HTTPS

The Importance of TLS

Setting up a secure Server

Login Forms From the Top

Introducing HSTS Header

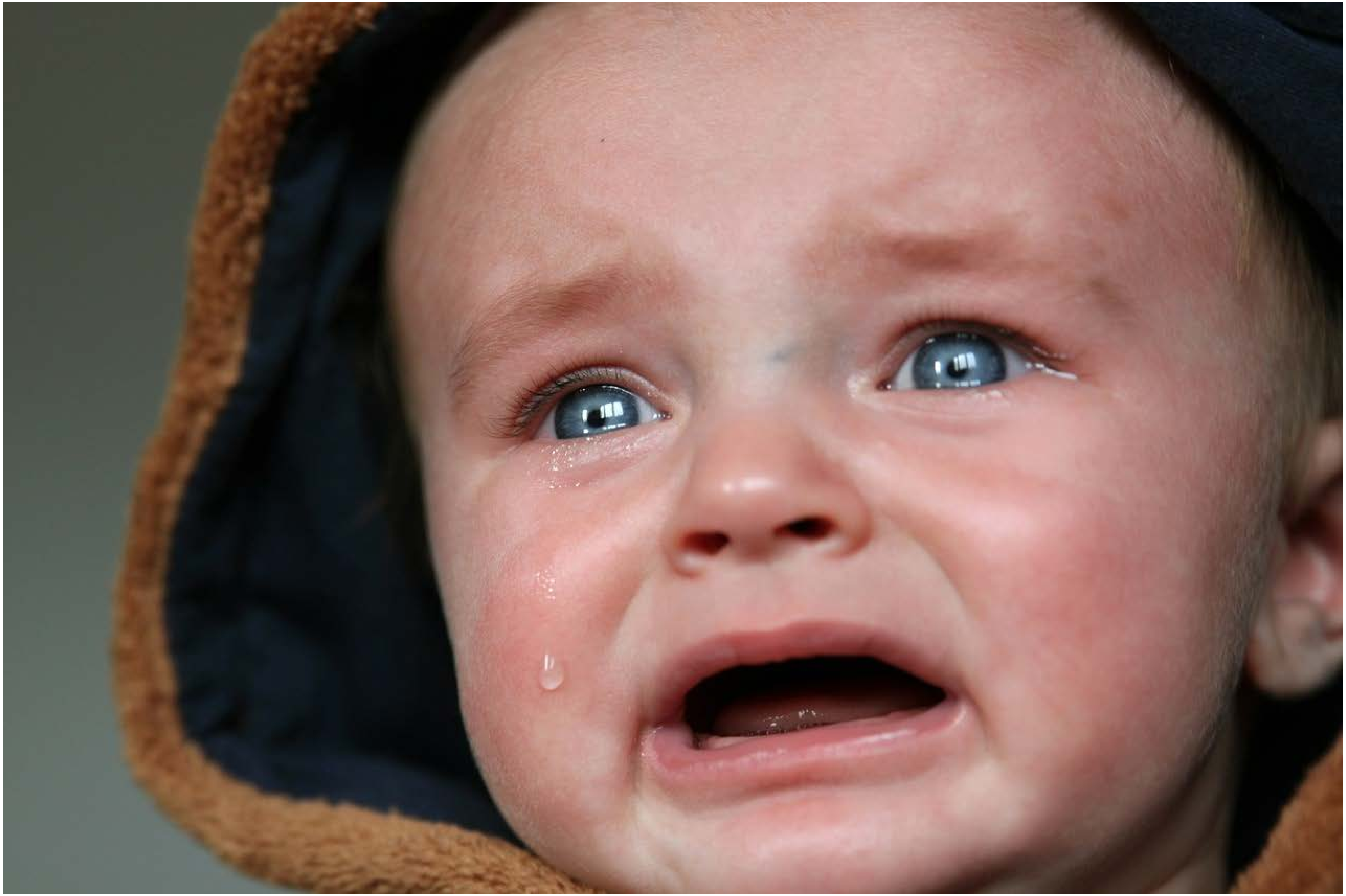
Implementing HSTS Header

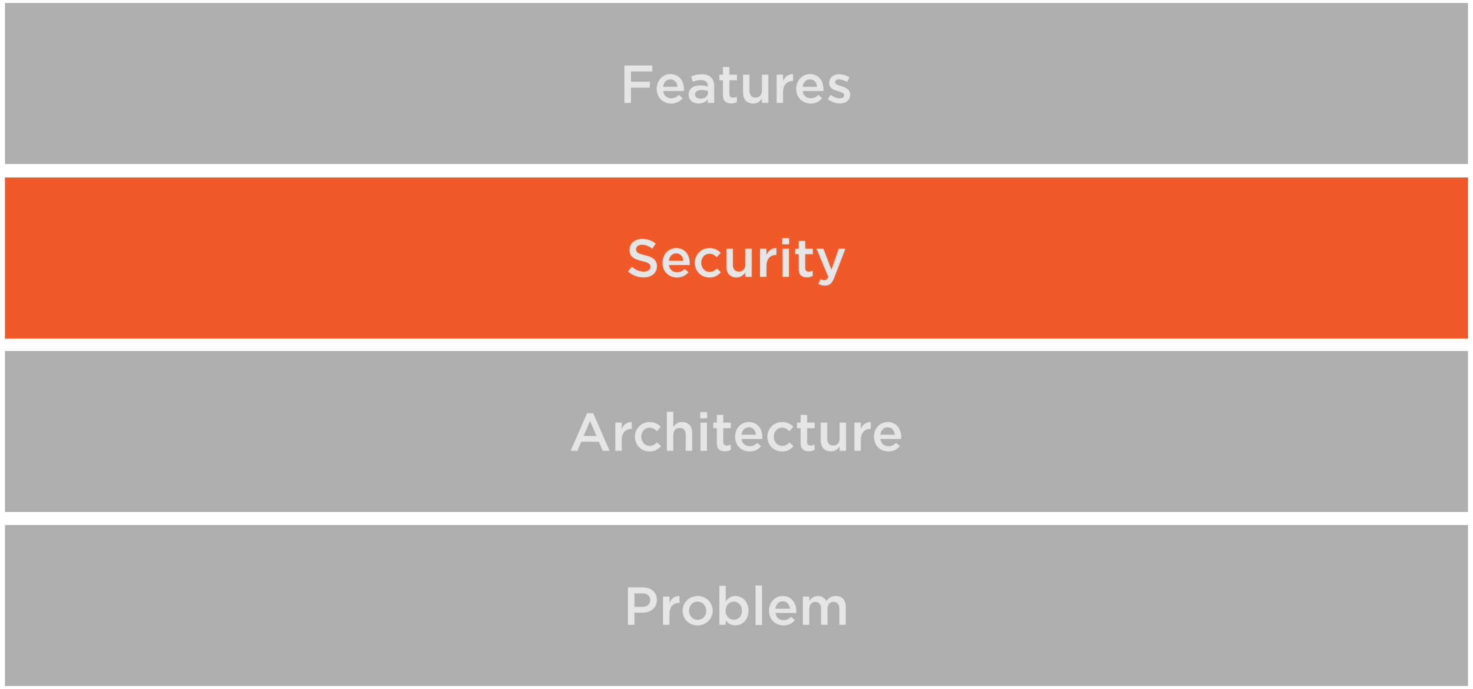
Introducing CSP Header

Implementing A CSP Header

“Failing to prepare, you are preparing to fail”

Benjamin Franklin





Features

Security

Architecture

Problem