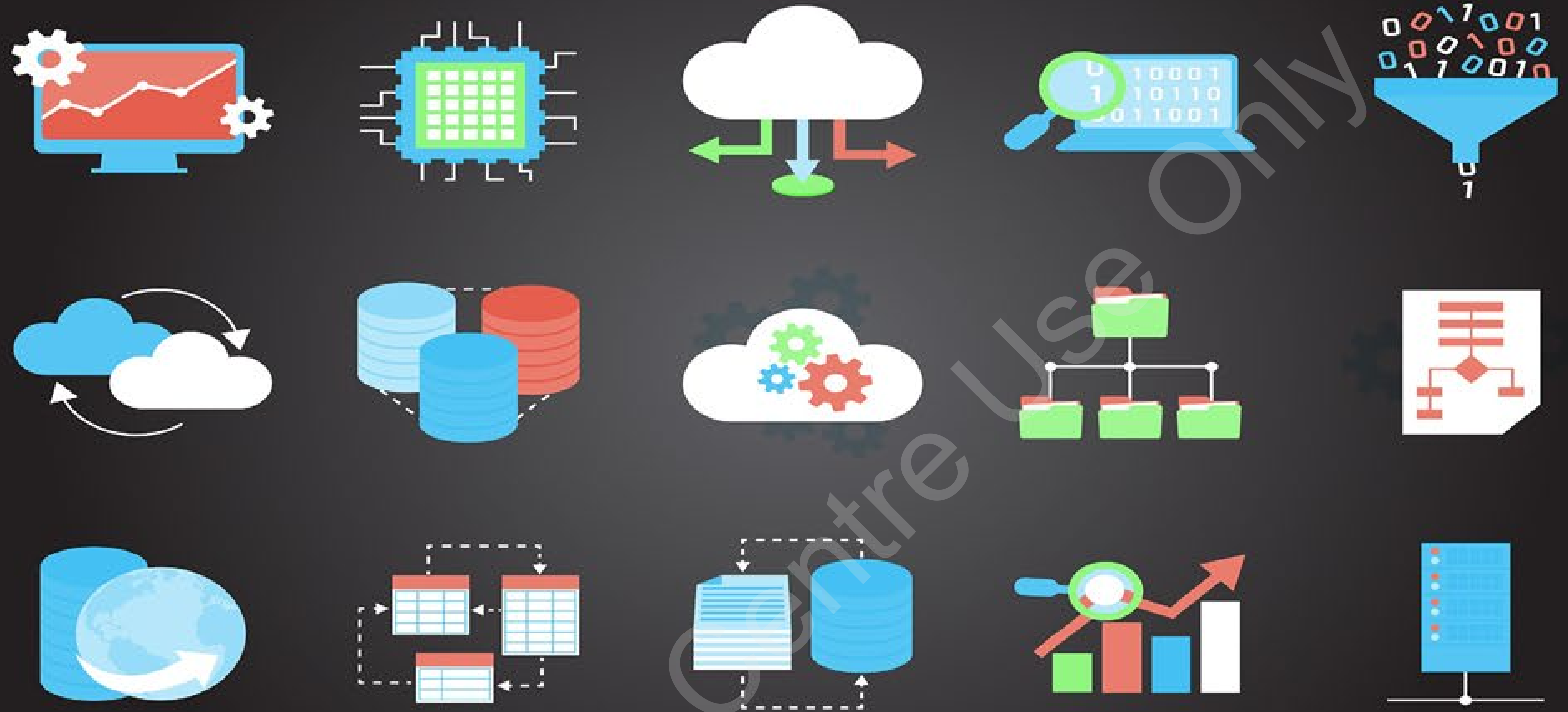


Session 08

Security in Web API

For Aptech Centre Use Only

Objectives

- Explain how to implement identity for authentication
- Describe how to use custom authorization
- Define CORS and XSRF
- Explain how to use authorization filters

For Aptech Centre Use Only

Implementing Identity for Authentication

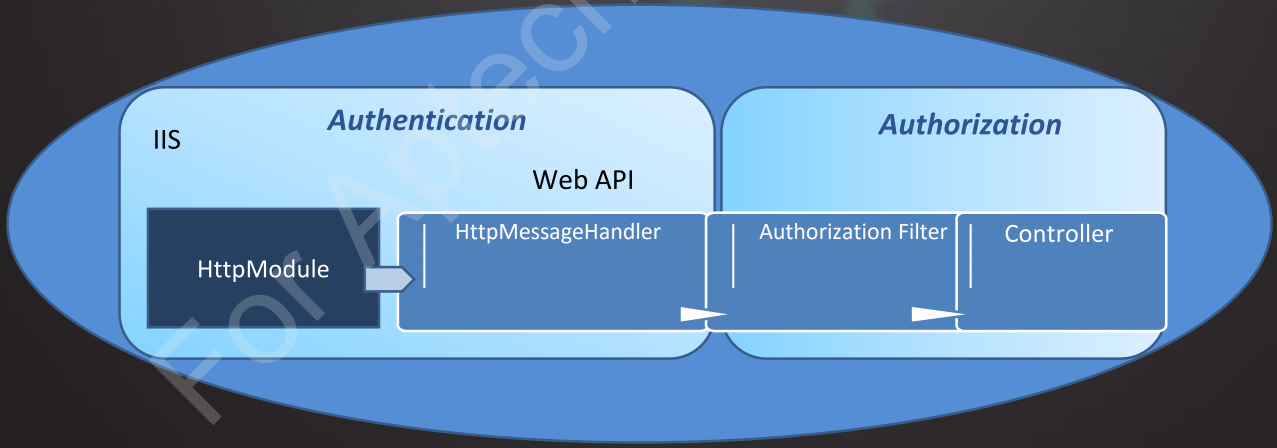
Two important phases of Web API security implementation:

Authentication

- This method is used to validate the identity of the user.

Authorization

- This method is used to determine if a given user is permitted to carry out a task.



For Aptech Centre Use Only

© Aptech Ltd.

Authentication

Key points to remember about authentication:

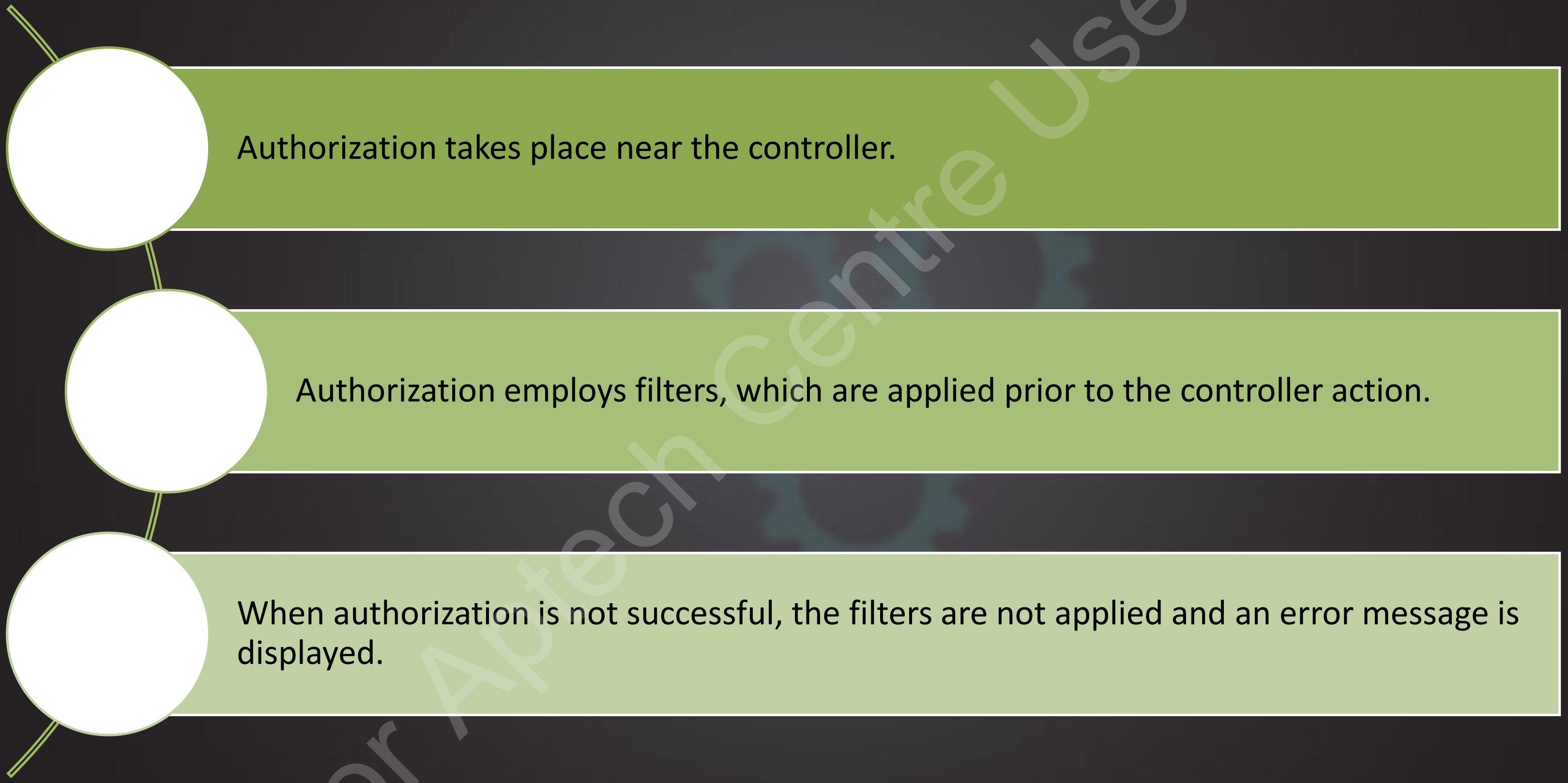
- In Web API, authentication is performed in the host.
- In order to authenticate users, Internet Information Server (IIS) employs HTTP modules.
- Users have the provision to select authentication modules, which are configured in IIS or ASP.NET for their projects.
- If custom authentication is required, they can create HTTP modules to suit their requirements.

For Aptech Centre Use Only

© Aptech Ltd.

Authorization [1-2]

Key points to remember about authorization:



Authorization takes place near the controller.

Authorization employs filters, which are applied prior to the controller action.

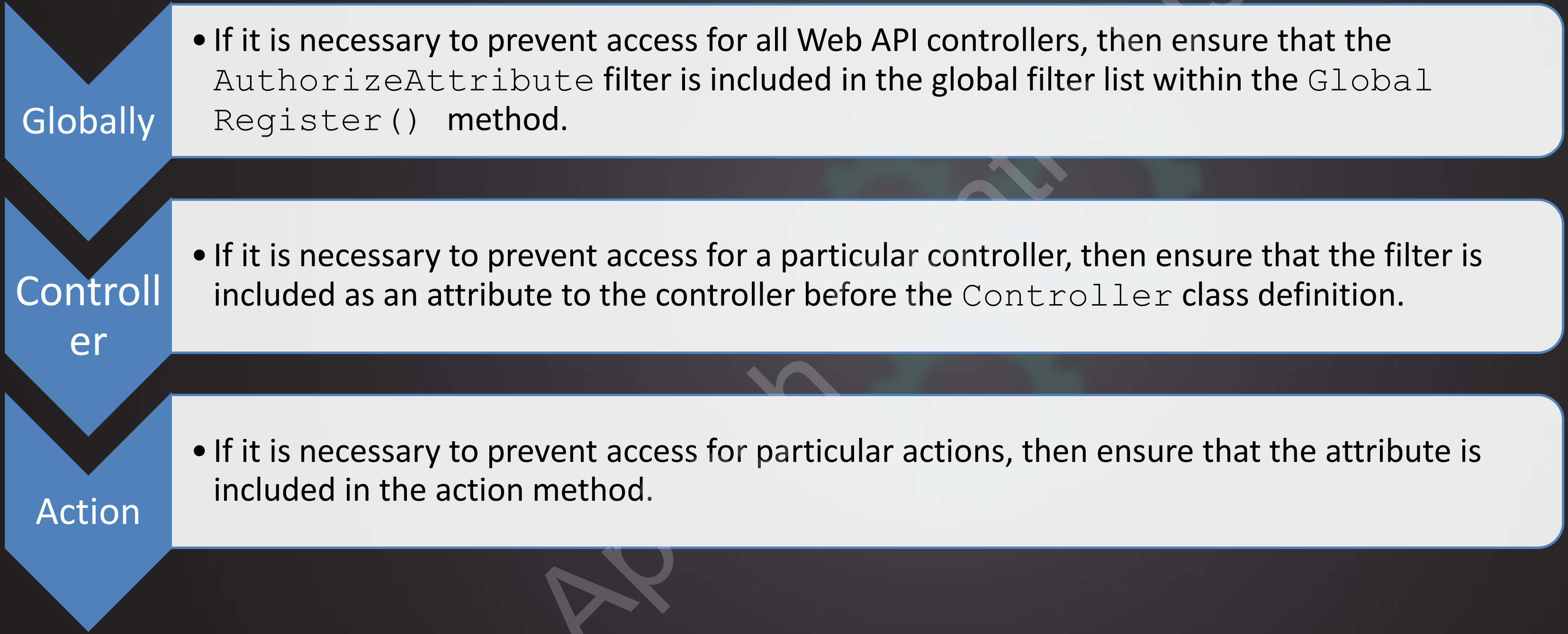
When authorization is not successful, the filters are not applied and an error message is displayed.

For Aptech Centre Use Only

© Aptech Ltd.

Authorization [2-2]

`AuthorizeAttribute` filter can be utilized globally or at an individual level as follows:



Globally

- If it is necessary to prevent access for all Web API controllers, then ensure that the `AuthorizeAttribute` filter is included in the global filter list within the `Global Register()` method.

Controller

- If it is necessary to prevent access for a particular controller, then ensure that the filter is included as an attribute to the controller before the `Controller` class definition.

Action

- If it is necessary to prevent access for particular actions, then ensure that the attribute is included in the action method.

For Aptech Centre Use Only

© Aptech Ltd.

Identity Authentication in Web API

Developers can provide security in two ways:

Basic authentication

- It is a process in which users are authenticated with the help of a service, such as RESTful service.

Token-based authentication

- It is also known as token-based authorization. After the authentication process is complete, a token is forwarded to the authenticated user through which he or she can get access to other resources.

For Aptech Centre Use Only

© Aptech Ltd.

Using Custom Authorization [1-2]

Sometimes, it is essential to set up the custom authorization filter, which is available in the `AuthorizeAttribute` class for implementing authorization.

Generally, authorization filters must be applied after the authentication filters, but prior to the controller action methods.

For Aptech Centre Use Only

Using Custom Authorization [2-2]

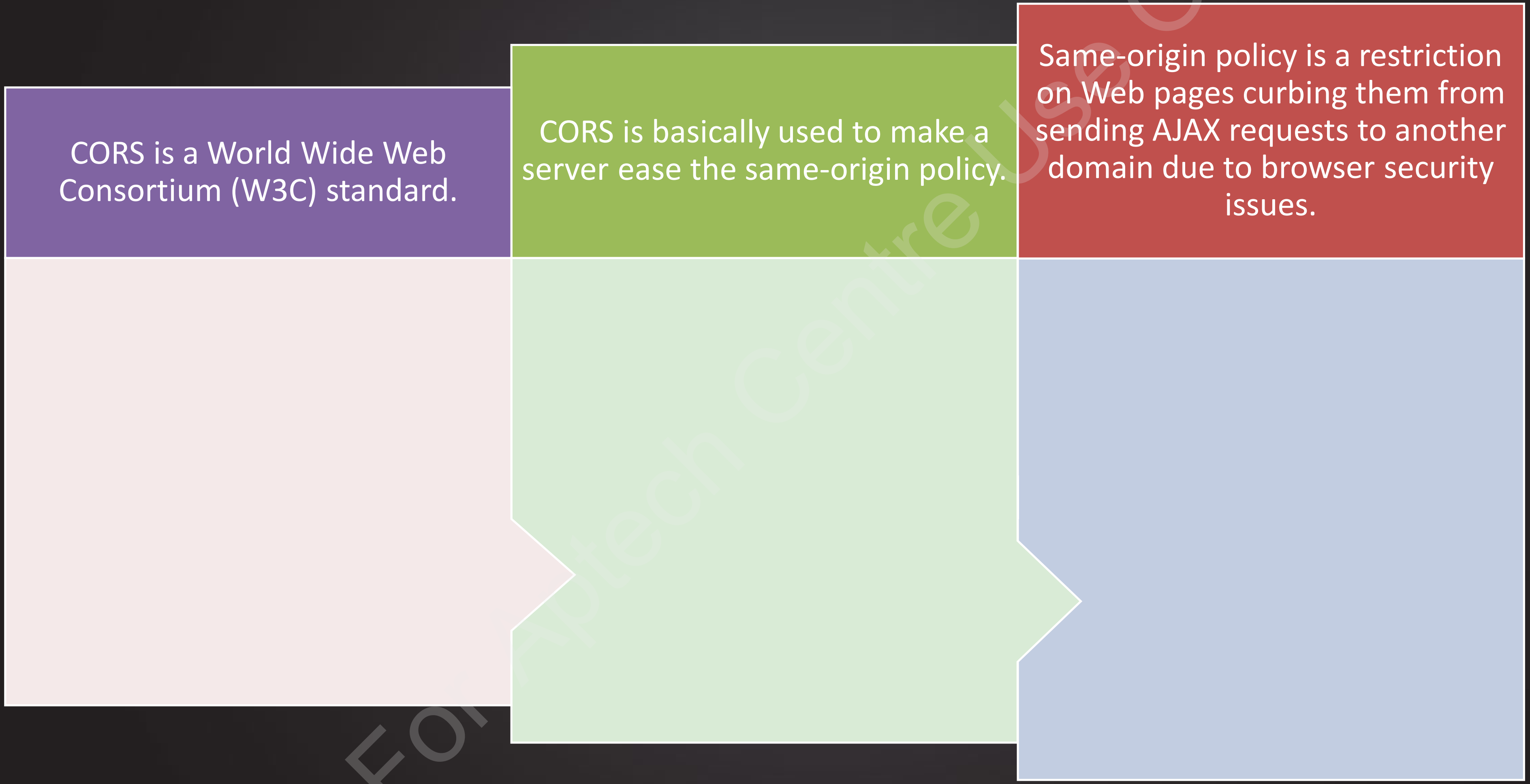
The `AllowAnonymous` attribute helps a user to go to the controller or its associated actions.

The `AuthorizeAttribute` offers the `HandleUnauthorizedRequest` method, which is virtual in nature and allows to perform custom logic when authorization fails.

For Aptech Centre Use Only

© Aptech Ltd.

Overview of CORS



CORS is a World Wide Web Consortium (W3C) standard.

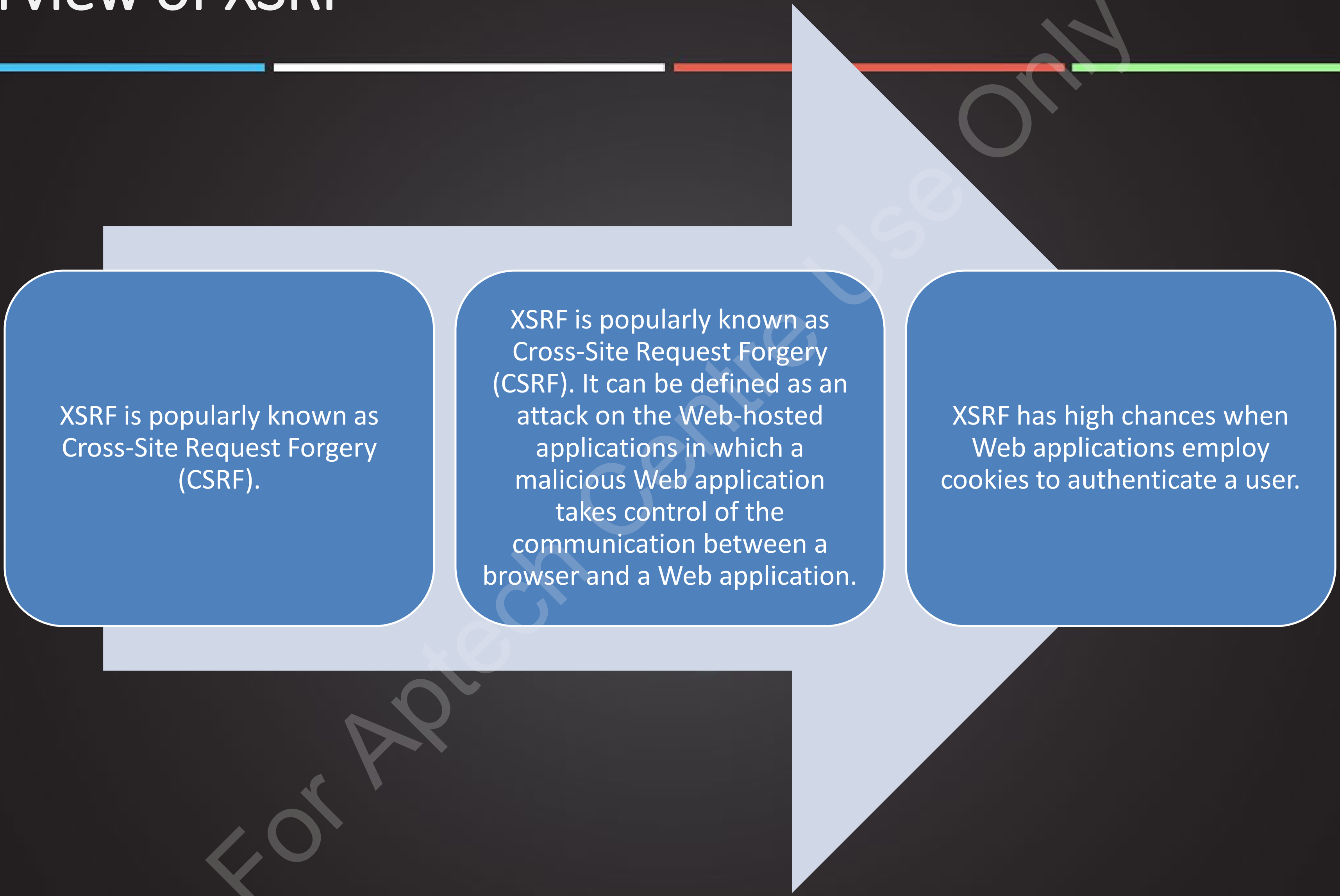
CORS is basically used to make a server ease the same-origin policy.

Same-origin policy is a restriction on Web pages curbing them from sending AJAX requests to another domain due to browser security issues.

For Aptech Centre Use Only

© Aptech Ltd.

Overview of XSRF



XSRF is popularly known as Cross-Site Request Forgery (CSRF).

XSRF is popularly known as Cross-Site Request Forgery (CSRF). It can be defined as an attack on the Web-hosted applications in which a malicious Web application takes control of the communication between a browser and a Web application.

XSRF has high chances when Web applications employ cookies to authenticate a user.

For Aptech Centre Use Only

© Aptech Ltd.

Summary

- Authentication and authorization are the two important phases of Web API security implementation.
- While authentication takes place in the host, authorization takes place closer to the controller.
- Authorize attribute filter can be utilized globally, or at the controller or at individual level.
- CORS stands for Cross Origin Resource Sharing and is a W3C standard. It is basically used to make a server ease the same-origin policy.
- XSRF is popularly known as cross-site request forgery. It is also called as CSRF.
- XSRF can be defined as an attack on Web-hosted apps in which a malicious Web application takes control of communication between a browser and a Web application.

For Aptech Centre Use Only

© Aptech Ltd.