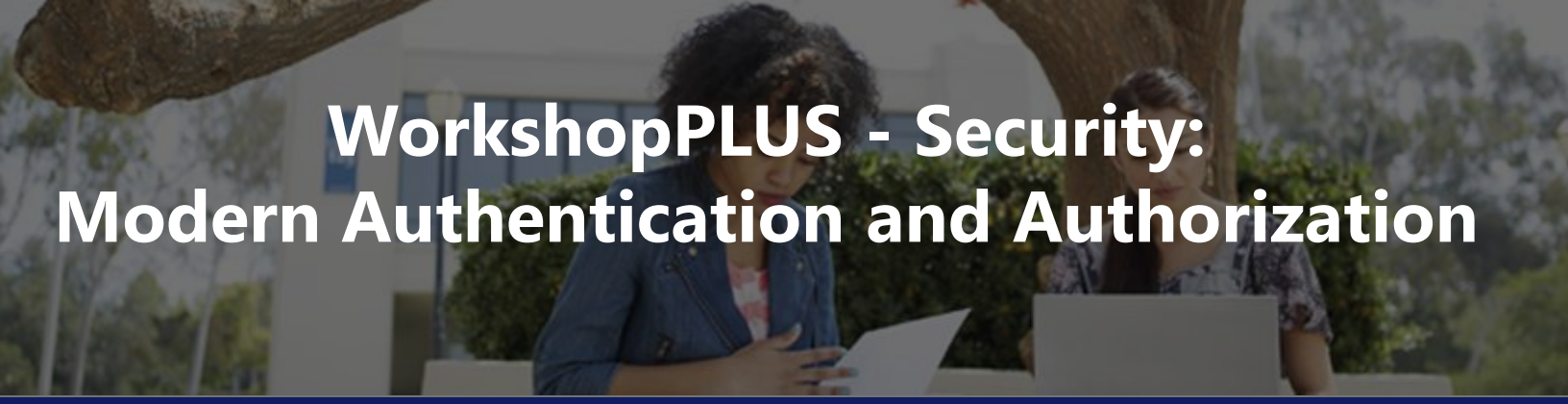


WorkshopPLUS - Security: Modern Authentication and Authorization

WorkshopPLUS
Focus Area: Security and Compliance

Duration: 3 Days

Level: 300

Overview

Building applications operating in the internet environment requires understanding of options available for performing authentication and authorization. These options include, both a variety of protocols such as OAuth2 and WS-Federation, as well as tools and toolkits such as Azure AD, ASP.NET identity handling and MSAL.

The purpose of this three-day WorkshopPLUS is to train application architects and developers, to develop applications requiring cloud-appropriate authentication and authorization technology.

The WorkshopPLUS covers both common architectural patterns, industry standard protocols and tools used to implement these. The tools and infrastructure aspects of the course are focused on Microsoft technology.

This WorkshopPLUS presents level 300 content targeting technical roles involved in building software such as architects and developers to help them understand the new approach based on standard protocols such as OAuth2, OpenID Connect, JWT and SAML.

Objectives

- Understand how access control, authentication and authorization changes when applications and/or users use the internet.
- Learn how to use Microsoft infrastructure, Azure AD (corporate or B2C), and development tools to secure your applications using industry protocols such as OAuth2 or SAML.

Agenda

Day 1

Architecture: architectural patterns, practices and protocols used for handling authentication and authorization in zero-trust environments.

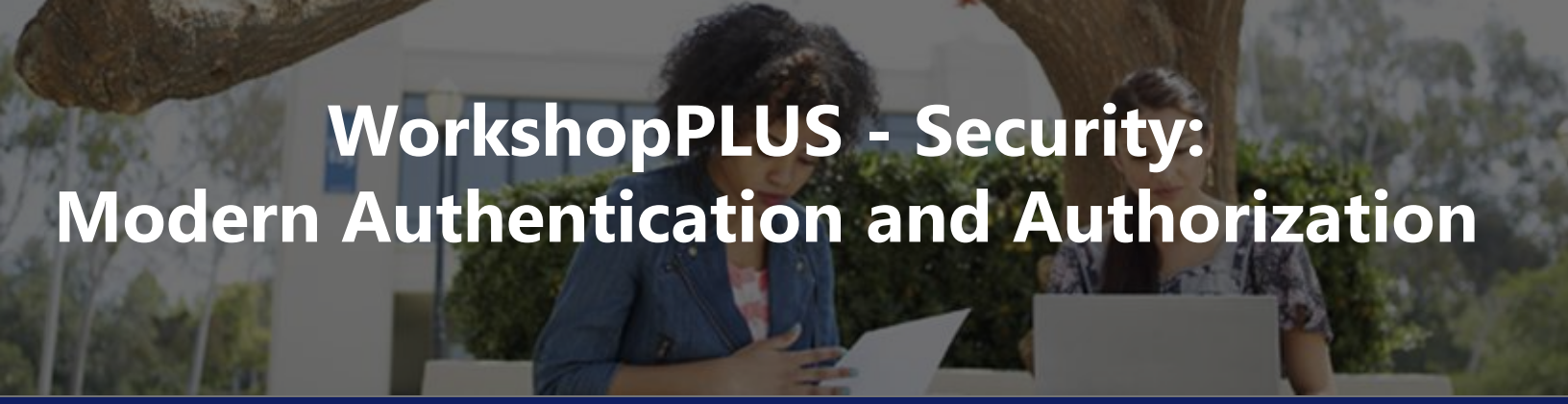
Day 2

Infrastructure: using Azure AD and Azure B2C as token issuers Using Azure App Services PaaS environment to secure web applications.

Day 3

Coding: developing applications using modern authentication protocols, using toolkits like MSAL and Microsoft.Identity.Web package.

Microsoft



WorkshopPLUS - Security: Modern Authentication and Authorization

WorkshopPLUS
Focus Area: Security and Compliance

Duration: 3 Days

Level: 300

Syllabus

Day1

Architecture:

- An overview of authentication and authorization issues in internet-based applications and the purpose of various protocols (e.g. OpenID Connect, OAuth2, SAML)

OAuth2 and OpenID Connect:

- This modules delves into the details of these two protocols. It reviews the various flows defined by OAuth2 and how they apply to common application topologies. It also describes their security threat models.

Day2

Azure AD:

- Purpose and features of the Azure AD, with focus on application authentication and authorization support: types of identities handled by AAD, application registration details and process and their effect on available access controls.

Microsoft Graph and Azure AD PowerShell:

- Introduction to programmatic access to Azure AD and other MS cloud services.

Azure AD B2C:

- Introduces the Azure AD tenant type specifically designed for consumer and citizen identities, including support for social and custom identities.

Web App Service 'Easy Auth'

- Feature of the Azure Web App service for providing authentication support for.

Day3

Developing Applications:

- This module focuses on hands-on use of knowledge acquired in the previous modules to implement a set of related applications using OAuth2 protocols, Microsoft Graph APII and various other features of Azure AD (e.g. application roles).

ASP.NET identity handling:

- Review of toolkits used to initiate passive protocols in web applications and handle (validate/augment) received security tokens.

MSAL toolkits:

- Review of APIs used to obtain OAuth2 and OIDC tokens from Azure AD, ADFS and/or federated providers (Gmail, FB, etc.).

Prerequisites

- Experience with Visual Studio
- Basic knowledge of C# to understand the source code shown on demos and to complete the labs

For more information

Contact your Microsoft Account Representative for further details.

Hardware Requirements

The workshop provides a lab environment accessible through a browser. It also includes a free Azure subscription. Attendees may choose to use own workstations with:

- Windows 8.1 or later
- Visual Studio 2019 (Free Community edition or higher)
- Fiddler with https decryption enabled
- .NET Core 5.x SDK
- Internet access with at least 1 Mbps bandwidth per student

Microsoft