Advanced z/OS Security: Crypto, Network RACF, and Your Enterprise

ES66G

Delivery Type: Classroom
Duration: 4 days

Overview

System z continues to extend the value of the mainframe by leveraging robust security solutions to help meet the needs of today's on demand, service-oriented infrastructures. System z servers have implemented leading-edge technologies, such as high-performance cryptography, multi-level security, large-scale digital certificate authority and life cycle management, improved Secure Sockets Layer (SSL) performance, advanced Resource Access Control Facility (RACF) function, and z/OS Intrusion Detection Services. This advanced z/OS security course presents the evolution of the current z/OS security architecture and explores in detail the various technologies involved in z/OS Cryptographic Services, z/OS Resource Access Control Facility (RACF), and z/OS Integrated Security Services.

In the hands-on exercises, you begin with your own z/OS HTTP Server in a TCP/IP environment. Throughout the exercises, you make changes to the configuration to implement authentication via RACF, SSL, and use of digital certificates. Use is made of facilities such as RACDCERT to manage digital certificates, PKI Services, and RACF auto registration. You will also implement different scenario to implement ssl security for a typical tcpip application, FTP: SSL, TLS, server authentication, client certificates, and AT-TLS. These exercises reinforce the concepts and technologies being covered in the lectures.

Pre-Requisites

You should have:

- ✓ General z/OS knowledge, including basic
- ✓ UNIX System Services skills
- ✓ Experience configuring any of the Web servers on z/OS Basic knowledge of TCP/IP and RACF

Objectives

- ✓ Describe the components of network security, platform security and transaction security on z/OS
- ✓ Describe how RACF supports UNIX users and groups
- ✓ Describe Web server security flow on z/OS

- Explain the contents and use of a digital certificate
- Explain the difference between asymmetric and symmetric cryptographic techniques
- Explain SSL V3 client authentication
- Explain the basics of WebSphere Application Server and Web services security
- Utilize the RACDCERT command
- Discuss the OCSF service providers
- Explain VPN (IPSec), SSL/TSL, and AT-TLS and the differences between them
- Discuss the z/OS Communication Server policy agent, IDS, and IP filtering
- Describe and utilize System SSL
- Explain how TN3270 and FTP SSL support works
- Explain how IBM secure hardware cryptographic coprocessors work
- Explain how Kerberos authentication works
- Explain the LDAP terms of DN, objectclass, attribute, schema, back end, and directory
- Explain how to set up, customize, and operate z/OS PKI Services

Target Audience

This class is intended for z/OS system programers and security specialists in charge of designing and implementing z/OS security for Web-enabled applications.