Training: IBM

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

TRAINING GOALS:

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 lifecycle management; as well as 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. It explores in detail, the various technologies that are 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 by using RACF, SSL and the 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 scenarios 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.

- 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 co-processors work

- Explain how Kerberos authentication works
- Explain the LDAP terms of DN, objectclass, attribute, schema, back end, and directory
- Explain how to setup, customize, and operate z/OS PKI Services

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

CONSPECT:

Day 1

- Welcome
- Unit 1: Overview of z/OS security for on-demand business Unit 2: z/OS platform security: Part 1
- Unit 3: z/OS platform security: Part 2
- Unit 4: Introduction to digital certificates and PKI

Day 2

- Unit 5: The SSL protocol
- Unit 6: HTTP and Apache server, SSL client authentication and WebSphere Application Server security
- Unit 7: RACF and digital certificates
- Unit 8: Open Cryptographic Services Facility
- Exercise 1: Controlling access using the httpd.config file Exercise 2: SSL protocol

Day 3

- Exercise 2: SSL protocol (continued)
- Unit 9: Introduction to z/OS Communications Server security features Unit 10: System SSL overview
- Unit 11: TN3270 secure connection
- Unit 12: FTP server and client secure connection
- Unit 13: Cryptography overview: System z integrated cryptography

Day 4

- Exercise 3: SSL client authentication and RACF auto registration
- Unit 14: Network authentication services and Enterprise Identity Mapping Unit 15: LDAP Directory Services in z/OS and the Tivoli Director Server for z/OS
- Unit 16: An introduction to OpenSSH for z/OS
- Exercise 4: Securing FTP with SSL: FTPS, TLS, AT-TLS

REQUIREMENTS:

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

Difficulty level