Securing CA-OPS/MVS

Course Summary

Description

This course is designed to help installations implement best practices in securing access to the CA-OPS/MVS product. From the OPS/MVS side, this course views both the OPS/MVS facilities that require secure access and the exits and security rules provided to secure them. From the security product side, specific security resource definitions are discussed, using mainstream MVS security products CA-ACF2, IBM's RACF, and CA-Top Secret. Quizzes and hands-on labs are used to reinforce presented topics.

Objectives
At the end of this course, students will be able to:

- Write and debug OPS/MVS SEC rules
- Control access to the different points of entry into OPS/MVS
- Control OPS/MVS access entirely through an MVS security product.
- Code and test CA-ACF2 definitions for OPS/MVS
- Code and test RACF resource definitions for OPS/MVS
- Code and test CA-Top Secret rules for OPS/MVS
- Define OPS/MVS access in UNIX System Services
- Know guidelines for writing secure automation applications

Topics

- Intro to CA-OPS/MVS Security
- Introduction to MVS Security interfaces
- Writing and debugging OPS/MVS SEC rules
- Introduction to CA-ACF2 security definitions (Optional)
- Introduction to RACF resource definitions (optional)
- Introduction to CA-Top Secret rules (optional)
- Developing secure automation

Audience

This course is designed for Systems Programmers, Security Administrators, and Automation Analysts.

Prerequisites

Students should have experience with MVS high-level architecture, data center policies and procedures. Prior knowledge of your installation security package, CA-OPS/MVS, and REXX is helpful but not absolutely required.

Duration

One day

Note: Optionally, an instructor can be retained for additional day(s) to assist in the security implementation.

Securing CA-OPS/MVS

Course Outline

I.   Intro to CA-OPS/MVS Security
  A. Business requirements for OPS/MVS security
  B. Best practice OPS/MVS security administration.
  C. OPS/MVS points of entry
  D. The security access required by the OPS/MVS product itself.
  E. Securing UNIX System Services
  F. OPS/MVS Security case study
  G. Security migration planning, development, testing, and migration

II. Introduction to MVS Security interfaces

III. Writing and debugging OPS/MVS SEC rules

IV. Introduction to CA-ACF2 security definitions (Optional)

V.   Introduction to RACF resource definitions (optional)

VI. Introduction to CA-Top Secret rules (optional)

VII. Developing secure automation