Securing and Encrypting Network Traffic with z/OS Communications Server and Policy Agent

Security Workshop

Agenda

Instructor: Linda Harrison (lharriso@us.ibm.com)

Acknowledgment to Gwen Dente for original course development

IBM Washington System Center
IBM Technical Sales Support

Course Description

- This workshop is designed to give the student:
- An introduction to z/OS Communications Security Solutions;
- Experience in designing and building x.509 digital certificates to provide security for TLS and IPSec;
- Experience in creating AT-TLS, IPSec, and IDS Policies with z/OS Configuration Assistant and installing the policies to protect network traffic to and from z/OS;
- Experience in implementing Syslog Daemon, Policy Agent, and Traffic Regulation Management Daemon on z/OS managing security policies on z/OS;
- Insight into the differences among various security technologies, including OpenSSH, IPSec, SSL/TLS, and IDS.
- NOTE: The focus of the class is on z/OS Communications Server security technologies, and not on Kerberos or OpenSSH. There are no exercises with Kerberos or SSH.
- Audience:
- Technical Customers, IBMers, and Business Partners who need hands-on experience in building and implementing security policies on z/OS Communications Server.
- Prerequisites:
- Experience in managing and editing file structures on z/OS
- Intermediate to Advanced Experience in the implementation of TCP/IP - in z/OS Communications Server or other platforms
- Course Duration:
  4 days:
  9:00 AM - 5:30 PM (Day 1)
  9:00 AM - 5:30 PM (Day 2)
  9:00 AM - 5:30 PM (Day 3)
  9:00 AM - 4:00 PM (Day 4)

Agenda

- 002_Security Architectures in IT
- 003_Overview of Security in z/OS Communications Server
- 004_Positioning SSH, TLS, and IPSec for Securing Traffic
  - Comparing File Transfer Methods: OpenSSH, TLS, IPSec, Managed File Transfer
  - LAB: L00_Lab Diagrams
  - LAB: L01_Intro to the Lab Environment
- 005_Implementation of Syslog Daemon
  - LAB: L02_Implementing SYSLOG Daemon on z/OS
- 006_Implementation of Policy Agent
  - LAB: L03_Implementing a Basic Policy Agent with QoS Policies on z/OS
- 007_The Role of x.509 Security Certificates in z/OS Communications Server
  - LAB: L04_Reviewing Certificate Repositories (z/OS, Workstation) and Cleaning Up Old Entries
  - LAB: L05_Analyzing x.509 Digital Security Certificates & Creating Certificates and Keyrings
  - OPTIONAL LAB: L06_Researching Common AT-TLS and x.509 Certificate Errors
- 008_Overview of SSL/TLS/AT-TLS: Concepts and Command Flows
  - LAB L07_Configuring an AT-TLS Policy for FTP Client and Server on z/OS with z/OS Configuration Assistant on Windows
    - Implementing FTP with preconfigured x.509 digital certificates
  - OPTIONAL LAB L08_Exporting Certificates, Configuring AT-TLS for TN3270, Testing TN3270 AT-TLS
    - Implementing labs with student-configured x.509 digital certificates
- 009_Protecting Traffic with IP Filtering
  - LAB: L09_Configuring Default Profile IP Filters and Policy Filters
- 010_Implementation of Traffic Regulation Management Daemon (TRMD)
  - LAB: L10_Implementing TRMD
  - LAB: L11_Implementing and Testing IP Filters in z/OS
- 011 Protecting Traffic with IPSec VPNs
  - LAB: L12_Configuring IPSec to Secure Traffic between Two z/OS Nodes Using RSA Signature Mode
    - Implementing labs using presconfigured x.509 Certificates
  - OPTIONAL LAB: L13_Researching Common IPSec and x.509 Certificate Errors
- 012_Overview of Intrusion Detection Services
  - LAB: L14_Configuring an IDS Policy to Protect z/OS Against Attacks, Scans, and Other Intrusions (Traffic Regulation)
  - OPTIONAL LAB: L15_IPSec VPN Using Preshared Key
  - OPTIONAL LAB: L16_Network Security Services Daemon (NSSD)
  - OPTIONAL LAB: L17_Defense Manager Daemon (DMD)

References

Acknowledgments

- Gwen Dente for original course development, (retired) IBM Washington Systems Center
- Marilyn Allmond, (retired) IBM Cryptography support
- Wai Choi, IBM (zOS RACF Development)
- Alfred Christensen, (retired) IBM z/OS Communications Server Development
- Alyson Comer, IBM (z/OS System SSL Development)
- Erin Farr, IBM z/OS Development
- Christopher Meyer, IBM z/OS Communications Server Development
- Lin Overby, IBM Enterprise Networking Solutions
- Vicente Ranieri, IBM (Advanced Technical Support, System z Security)
- Mary Sweat, (retired) IBM Washington Systems Center
- Richard Theis, IBM Cloud Development

Web Pages

- URLs for Publications
  - http://www.ibm.com/systems/z/os/zos/bkserv/index.html
  - http://www.redbooks.ibm.com
- URLs for z/OS Communications Server and GUI Download
  - http://www.ibm.com/software/network/commserver/zos/support/
  - http://www.ibm.com/support/docview.wss?rs=852&context=SSSN3L&dc=DB530&dc=D430&dc=D410&dc=D420&dc=DB510&dc=DB550&q1=Configuration+Assistant&uid=swg24013160&loc=en_US&cs=utf-8&lang=en
  - or better:
    - http://www.ibm.com/software/network/commserver/zos/support/
    - then select "IBM Configuration Assistant for z/OS Communications Server" in "Download" section of the page
- Main Security Web Pages:
  - https://www.pcisecuritystandards.org/
  - http://www.iss.net/
  - http://www.ibm.com/servers/eserver/zseries/zos/security
  - http://www.ibm.com/systems/z/security/
- IBM Mainframe Servers
  - http://www.ibm.com/servers/eserver/zseries
- IBM zEnterprise Servers Network Technologies
  - http://www.ibm.com/servers/eserver/zseries/networking/technology.html
- z/OS Communications Server and Performance Benchmarks
  - http://www.ibm.com/software/network/commserver/zos/
  - http://www.ibm.com/support/docview.wss?uid=swg27005524

Web Pages (cont.)

- Communications Server for Linux on System z
  - http://www.ibm.com/software/network/commserver
  - http://www.ibm.com/software/network/commserver/library
- Communication Controller for Linux on System z
  - http://www.ibm.com/software/network/ccl
- PKI Services web site:
  - http://www.ibm.com/servers/eserver/zseries/zos/pki
- PKI Services Red Book:
  - http://www.redbooks.ibm.com/abstracts/sg246968.html
- ITSO Redbooks
  - http://www.redbooks.ibm.com
- RACF web site:
  - http://www.ibm.com/servers/eserver/zseries/zos/racf
- IBM Washington Systems Center Technical Sales Support
  - http://www.ibm.com/support/techdocs/
- Request for Comment (RFC)
  - http://www.rfc-editor.org/rfcsearch.html
  - http://www.rfc-editor.org/
- Online Courses (search for cryptography)
  - http://coursera.org

IBM Manuals

- IBM z/OS and z/OS Communications Server Manuals
  - z/OS Communications Server IP Configuration Guide (z/OS V1.13 SC31-8775, z/OS V2.1+ SC27-3650)
  - z/OS Communications Server IP Configuration Reference (z/OS V1.13 SC31-8776, z/OS V2.1+ SC27-3651)
  - z/OS IP Diagnosis Guide (z/OS V1.13 GC31-8782, z/OS V2.1+ GC27-3652)
  - z/OS IP System Administrator Commands (z/OS V1.13 SC31-8781, z/OS V2.1+ SC27-3661)
  - z/OS Four Volumes of IP Messages (z/OS V1.13 SC31-8783, SC31-8784, SC31-8785, SC31-8786, z/OS V2.1+ SC27-3654, SC27-3655, SC27-3656, SC27-3657)
  - z/OS Migration Manual (z/OS V1.13 GA22-7499, z/OS V2.1+ GA32-0889)
  - z/OS System SSL Programming Guide (z/OS V1.13 SC24-5901, z/OS V2.1+ SC14-7495)
  - z/OS Integrated Cryptographic Services (ICSF) System Programmer Guide (z/OS V1.13 SA22-7520, z/OS V2.1+ SC14-7507)
  - z/OS Cryptographic Services PKI Services Guide and Reference (z/OS V1.13 SA22-7693, z/OS V2.1+ SA23-2286)
  - z/OS Security Server RACF Security Administrator's Guide (z/OS V1.13 SA22-7683, z/OS V2.1+ SA23-2289)
  - z/OS Security Server RACF Command Language Reference (z/OS V1.13 SA22-7687, z/OS V2.1+ SA23-2292)
  - z/OS UNIX System Services Planning (z/OS V1.13 GA22-7800, z/OS V2.1+ GA32-0884)
  - z/OS UNIX System Services User's Guide (z/OS V1.13 SA22-7801, z/OS V2.1+ SA23-2279)
  - z/OS UNIX System Services Command Reference (z/OS V1.13 SA22-7802)
  - z/OS Management Facility (z/OSMF) Configuration Guide (z/OS V2.1+ SA38-0657)
  - z/OS Management Facility (z/OSMF) Programming (z/OS V2.1+ SA32-1066)
- z/OS Unix System Services OpenSSH
  - z/OS OpenSSH User’s Guide (SC27-6806)
- RACF Command Samples for TCP/IP on z/OS
  - SYS1.TCPIP.SEZAINST(EZARACF)

IBM Manuals (cont.)

- IBM RedBooks
  - Communications Server for z/OS V1R11 TCP/IP Implementation
    - Volume I: Base Functions, Connectivity, and Routing (SG24-7798)
    - Volume II: Standard Applications (SG24-7799)
    - Volume III: High Availability, Scalability, and Performance (SG24-7800)
    - Volume IV: Security and Policy-based Networking (SG24-7801)
  - Communications Server for z/OS V1R12 TCP/IP Implementation
    - Volume I: Base Functions, Connectivity, and Routing (SG24-7896)
    - Volume II: Standard Applications (SG24-7897)
    - Volume III: High Availability, Scalability, and Performance (SG24-7898)
    - Volume IV: Security and Policy-based Networking (SG24-7899)
  - Communications Server for z/OS V1R13 TCP/IP Implementation
    - Volume I: Base Functions, Connectivity, and Routing (SG24-7996)
    - Volume II: Standard Applications (SG24-7997)
    - Volume III: High Availability, Scalability, and Performance (SG24-7998)
    - Volume IV: Security and Policy-based Networking (SG24-7999)
  - Communications Server for z/OS V2R1 TCP/IP Implementation
    - Volume I: Base Functions, Connectivity, and Routing (SG24-8096)
    - Volume II: Standard Applications (SG24-8097)
    - Volume III: High Availability, Scalability, and Performance (SG24-8098)
    - Volume IV: Security and Policy-based Networking (SG24-8099)
  - Communications Server for z/OS V2R2 TCP/IP Implementation
    - Volume III: High Availability, Scalability, and Performance (SG24-8362)

End of Topic