What’s New with CICS Security

Leigh Compton

Consulting IT Specialist
CICS and z/OS Connect
lcompton@us.ibm.com

Continuous Delivery and Feature Toggles

- New deliveries between product releases through the service channel or as separate downloads
- No need to wait for the next major release
- No need to completely reinstall the CICS environment
- Selectively roll out new function
- Reduce the risk of introducing change

- Feature Toggle Files
  - Introduced in CICS TS V5.4
- Group Level Configuration Files
  - Control the features that you want to enable in a group of CICS regions
  - Optional parameter finalize locks specific settings
- Region Level Configuration Files
  - Enables feature in a single region
  - Can override features in group level files
    - Unless finalize was specified

NIST SP800-131A and FIPS 140-2

- CICS can check and report on conformance to the NIST SP800-131A standards
- National Institute of Standards Special Publication 800-131A
  - Provides cryptographic key management guidance
  - Specific guidance for transitions to the use of stronger cryptographic keys and more robust algorithms
- FIPS 140-2
- Federal Information Processing Standards Publication 140-2
  - Specifies the security requirements that will be satisfied by a cryptographic module

- Conformance to NIST SP800-131A
  - Delivered in CICS TS V5.2
  - Requires TLS 1.2
    - With FIPS 140-2 standards
  - Dictates stronger cryptographic keys and more robust algorithms
- NISTSP800131A=CHECK
- MINTLSLEVEL
- CIPHERS

IBM Health Checker

- Three health checker rules that define best practice for CICS TS security
  - Introduced in CICS TS V5.4
  - Added to V5.1 thru V5.3 via PTF
- If a CICS region becomes non-compliant a warning message is issued
- CICS health checker rules run every 30 minutes in the IBM Health Checker for z/OS address space
- Three health checker rules:
  - CICS_CEDA_ACCESS
  - CICS_JOBSUB_SPOOL
  - CICS_JOBSUB_TDQINTRDR

- CEDA Access
  - Checks whether CEDA is accessible to unauthenticated users
    - Accessible to the default user
    - SEC=NO
- Job Submission
  - Checks whether the system spool is accessible to unauthenticated users
    - SPOOL=YES
    - Accessible to the default user
    - SEC=NO
  - Checks whether any transient data queue that writes to the internal reader is accessible to unauthenticated users
    - TD Queue to INTRDR
    - Accessible to the default user
    - SEC=NO

Passtickets

- Request an external security manager to build a PassTicket
  - PassTicket is a password substitute
- Originally only available in context of FEPI programming
- PassTicket is for the user ID associated with the task that issues the command
- XPTKT=YES
  - A check is made that the user ID has update authority for the profile IRRPTAUTH.applid.userid

- EXEC CICS FEPI REQUEST PASSTICKET
- EXEC CICS REQUEST PASSTICKET
  - Introduced in CICS TS V5.3
- SIT parm XPTKT
  - Introduced in CICS TS V5.4
  - Added to CICS TS V5.2 and V5.3 via PTF

Security for Web Services

- Initial support in CICS TS V3.1; enhancements in subsequent releases
  - Web Services Security (WSS): SOAP Message Security 1.0 specification
  - Security tokens for authentication
    - Username Token
    - X.509 Certificate Token
  - Digital signatures for privacy and integrity
- Web Services Trust Language (WS-Trust) specification
- SAML Token
  - Supported in Provider and Requester pipelines
- Kerberos Token
  - Supported in Provider pipeline

- SAML
  - Added in CICS TS V5.2
  - Requires CICS Security Token Service
  - Supports the SAMLCore1.1 and SAML Core2.0 standards (without protocols)
- CICS Security Token Service
  - Added in CICS TS V5.2
  - Parse and validate SAML tokens
  - Rebuilding and re-signing modified SAML tokens
- Kerberos
  - Added in CICS TS V5.2

Kerberos

- CICS supports Kerberos using the external security manager
  - RACF based on Kerberos Version 5 and Generic Security Services (GSS)
- Verify a Kerberos token by configuring a service provider pipeline or by using the API command VERIFY TOKEN
- KERBEROSUSER
  - Default is region user ID
  - Must not be a protected user ID
  - Region user ID should be protected
  - ... not recommended to take default
- Mutual authentication
  - Token is returned to the client that supplied the Kerberos token to allow authentication of the CICS region

- EXEC VERIFY TOKEN
  - Introduced in CICS TS V5.2
- SIT parm KERBEROSUSER
  - Introduced in CICS TS V5.4
  - Added to CICS TS V5.2 and V5.3 via PTF
- 3270 Sign-on with Kerberos Token
  - Introduced in CICS TS V5.3
- Kerberos Mutual Authentication
  - Introduced in CICS TS V5.4
  - Added to CICS TS V5.3 via PTF

Support for AT-TLS

- SSL/TLS support provided by AT-TLS feature of IBM Communications Server
- AT-TLS: Application Transparent TLS
  - Socket enabled with AT-TLS sends and receives data in the clear while encrypted data flows over the network
  - Most applications do not need awareness of the security negotiations and encryption
  - Some applications need to be aware of AT-TLS or have control over the security functions
- TCPIPSERVICE can be configured as AT-TLS aware

- AT-TLS support for inbound HTTPS requests
  - Introduced in CICS TS V5.3
- CICS functions as AT-TLS Aware application
- CICS can obtain security information from AT-TLS
  - Query returns information, such as the cipher suite used for the TLS session and client certificate (if present).
- ATTLSAWARE attribute on TCPIPSERVICE resource

Additional Security for Job Submission

- **User ID under which the job submitted to the internal reader runs if USER= is not specified on the JOB card**
  - **Prior to CICS TS V5.5, the default is the region user ID**
  - **In CICS TS V5.5, default depends on security settings:**
  - **For WRITEQ TD, new attribute JOBUSERID specifies a user ID for the job**
    - **If not defined, defaults to region user ID**
  - **For SPOOLWRITE, user ID is region or task, based on value in feature toggle**
  - **If not region user ID, CICS adds "USER=job_userid" to JOB card**
- **Surrogate checking for SPOOLWRITE or WRITEQ TD commands**

- **Surrogate user checking for spool commands in job submissions to the JES internal reader**
  - **Activated with a feature toggle**
    - *com.ibm.cics.spool.surrogate.check=true*
    - **Applies to both WRITEQ TD and SPOOLWRITE**
  - **SIT parameter XUSER=YES**
- **User ID used for job submissions via SPOOLWRITE when no user ID is specified on the job card**
  - **Default is region user ID**
  - **Override to user ID of current task with feature toggle**
    - *com.ibm.cics.spool.defaultjobuser=TASK*

Security for Liberty Applications

- Additional authentication methods
  - Oauth 2.0
  - OpenID Connect Client 1.0
  - OpenID Connect Server 1.0
  - JSON Web Token 1.0
- Support for multiple secure Liberty JVM servers within a single CICS region
  - Liberty JVM servers use the angel process to call z/OS authorized services
  - Prior to CICS TS V5.5, only one Liberty JVM server per region could connect to the angel
  - Bypass was to run additional Liberty JVM servers without security

- Oauth and OpenID
  - Introduced in CICS TS V5.5
  - Added to CICS TS V5.3 & V5.4 via PTF
- JSON Web Token (JWT)
  - Introduced in CICS TS V5.5
  - Added to CICS TS V5.3 & V5.4 via PTF
- Multiple Liberty JVM servers
  - Introduced in CICS TS V5.5
  - Added to CICS TS V5.4 via PTF

3270 Intrusion Detection Services

- Allows CICS to detect if a 3270 emulator has invalidly modified a protected field generated by a BMS map.
- Works with the 3270 IDS provided by IBM Communications Server
- When both are enabled
  - BMS generated 3270 data handled by CICS
  - Non-BMS 3270 data handled by IBM Communications Server

- VTAM 3270 Intrusion Detection Service
  - Handles all 3207 applications
- CICS BMS 3270 Intrusion Detection Service
  - Introduced in CICS TS V5.4
  - Implemented and configured by feature toggle
    - *com.ibm.cics.bms.ids*
    - *com.ibm.cics.bms.ids.action*
    - *com.ibm.cics.bms.ids.vtamignore*
- User-replaceable module DFHBMSX
  - 3270 data stream validation program
    - Introduced in CICS TS V5.4
    - Added to V4.1 thru V5.3 via PTF
  - Called when a 3270 data stream validation error has been detected

Multi-factor Authentication for CMCI and CICS Explorer

- CICS TS now supports CICS Explorer sign-in with MFA
- Higher levels of user authentication for some or all users
- Define Credential without password or passphrase
- At sign-on, user is prompted for password or passphrase
  - User supplies password or passphrase concatenated with authentication token

- Enhanced CICS Explorer sign-on security
  - Introduced in CICS TS V5.5
  - Added to CICS TS V5.4 via PTF
  - Supported by CICS Explorer Version 5.4.0.4 or higher
- Requires IBM Multi-Factor Authentication for z/OS or equivalent
- Requires permission to authenticate through CMCI server
  - Security profiles in SERVER and APPL classes
- Requires CMCI JVM server in WUI region
  - Implemented with feature toggle in WUI region
    - *com.ibm.cics.cmci.jvmserver*

Enhanced CICS Commands

- VERIFY PASSWORD and VERIFY PHRASE
  - Support for GROUPID
  - CICS can perform verification against the group ID in addition to a user ID and password
- QUERY SECURITY
  - Support query for another user ID

- GROUPID on VERIFY PASSWORD and VERIFY PHRASE
  - Introduced in CICS TS V5.5
- USERID on QUERY SECURITY
  - Introduced in CICS TS V5.5
  - Task user ID must have authorization to query another user's access
  - CICS performs surrogate user check

Miscellaneous Security Enhancements

- Enhanced Password Algorithm
  - Stronger encryption of passwords
- Offloading authentication requests to open TCBs
  - Reduces contention on resource-owning TCBs
- UEPSGTYP parameter passed to XSNON exit
  - Identifying token type used in sign-on
- Message DFHXS1206
  - Includes a count of the invalid authentication attempts that were made before the valid attempt
- PERFORM SSL REBUILD
  - Refreshs the certificates used by a CICS region for SSL handshakes.

Auditing of SPI commands

- Message DFHAP1900 to the transient data queue CADS

Specify full verification at least once per day

- Update last-used date
- Update user statistics
- SIT parameter SECVFYFREQ=USRDELAY

Extend identity propagation to started transactions

- ICRX is propagated for START commands without USERID or TERMID
- Only supported on MRO or IPIC connections

Identify cipher suites used on connections

- Written to CMF records
- Performance data field SOCIPHER in the DFHSOCK group

- New options on GMTRAN for CESN & CESL
  - Force disconnect if user fails to sign-on
- Preset user ID on terminal can share ACEE
  - Terminals with same user ID can use a single ACEE
  - New SIT parameter: SNPRESET

Notes: Miscellaneous Security Enhancements

- Introduced in CICS TS V5.1
  - Auditing of SPI commands
  - Specify full verification at least once per day
  - Extend identity propagation to started transactions
  - Identify cipher suites used on connections
  - PERFORM SSL REBUILD
- Introduced in CICS TS V5.3
  - Enhanced Password Algorithm
  - Offloading authentication requests to open TCBs
  - UEPSGTYP parameter passed to XSNON exit
  - Message DFHXS1206
- Introduced in CICS TS V5.4
  - Preset user ID on terminal can share ACEE
- Introduced in CICS TS V5.5
  - New options on GMTRAN for CESN & CESL

Thank you

Leigh Compton
Consulting IT specialist
—
lcompton@us.ibm.com
ibm.com