z/TPF Network Security Compliance

2022 TPF Users Group Conference
March 27-30, Dallas, TX
Communications

—

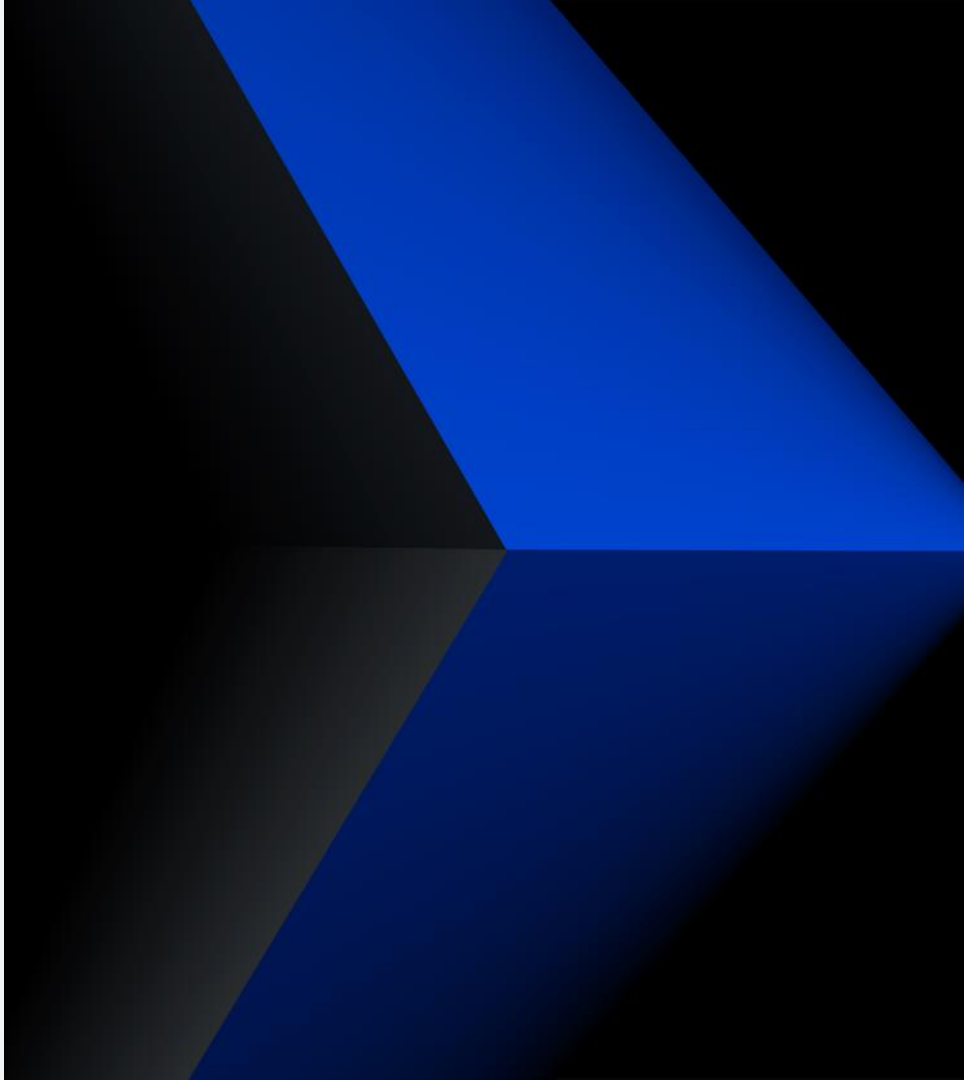
Angel Baez

IBM Z

IBM

Disclaimer

Any reference to future plans are for planning purposes only. IBM reserves the right to change those plans at its discretion. Any reliance on such a disclosure is solely at your own risk. IBM makes no commitment to provide additional information in the future.



Problem Statement

- How can I reduce the time and effort it takes to supply a security auditor with the necessary network security compliance information for the z/TPF system?
- How can I determine what TLS ciphers or TLS versions are in use on my system today?
- How can I determine what TLS certificates are in use by my z/TPF applications and whether they are nearing expiration?

Problem Objectives

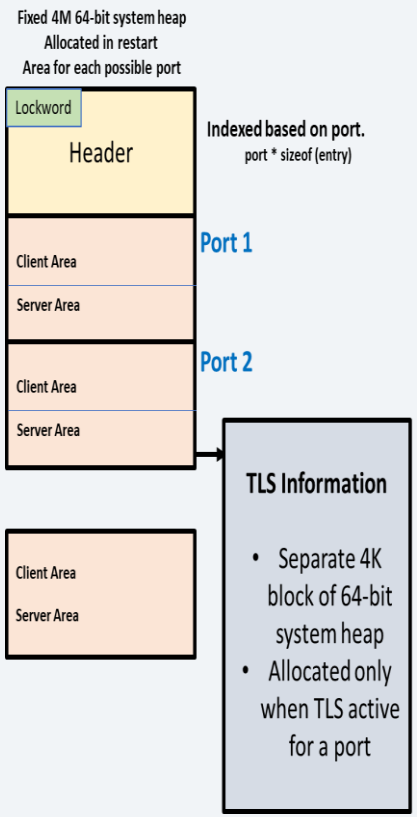
- The z/TPF system will now collect security compliance related information to reduce the time and resources needed to provide z/TPF security compliance information to a security auditor.
- Initial deliverable is focused on compliance information related to z/TPF networking
  - Which network ports are in use on the z/TPF system?
    - Which network ports are secure and which ports are not?
    - What security credentials (TLS ciphers, TLS versions, etc) are used to secure the port?
  - Which z/TPF applications or network ports are using an older TLS version or TLS cipher?
  - Which TLS certificates are in use by applications on z/TPF?

Technical Details

- z/TPF network compliance information saved in 64-bit system heap
  - The information is separated by port and model (whether the z/TPF application is acting as client or a server)

- The information is displayable using the new ZDCOM command
  - Ability to clear information for an individual port or all ports.
    - Existing active sockets are repopulated the next time the socket sweeper is run
    - Existing shared TLS sessions are repopulated the next time the shared SSL sweeper is run.

- The information is kept in core only and consists of compliance information for any TCP/IP sockets or TLS sessions started on the system since:
  - The last system IPL
  - The last ZDCOM CLEAR command was issued



As-Is Scenario

Supplying z/TPF Network Compliance Information for a Security Audit

- Christine, a Security Administrator for the z/TPF system, is asked to identify all various network traffic into and out of the z/TPF system.
  - She is also asked to supply evidence that the network traffic containing sensitive data flowing into and out the z/TPF system is secure.
  - Proving it is secure is not enough, she needs to provide the TLS credentials (TLS ciphers, TLS versions, Certificate Information, etc.) for the secure connections.
- Christine knows this will be a time consuming, manual process in z/TPF with information spread across many configuration files (if she is lucky) and other times embedded in application code.

Christine
Security Administrator

To-Be Scenario
Supplying z/TPF Network Compliance Information for a Security Audit

- With the new z/TPF ZDCOM compliance command, Christine is a couple of keystrokes away from providing a security auditor the information they need.

```
ZDCOM DISPLAY ALL

PORT     APPLNAME    PROTO TLS MODEL
-----  ----------  ----- --- ------
53       DNS          UDP   N  CLIENT
443      HTTPS        TCP   Y  CLIENT
443      HTTPS        TCP   Y  SERVER
520      RIP          UDP   N  SERVER
1000     RES_APP      TCP   Y  SERVER
1010     SCHED        TCP   N  SERVER
```

Christine issues the ZDCOM DISPLAY ALL summary command to identify all the active network traffic as well as which ports are secure.

The auditor was concerned that the SCHED application is insecure, until Christine explained that schedule information is publicly available and does not require security.

To-Be Scenario
Supplying z/TPF Network Compliance Information for a Security Audit

- The security auditor would like to understand how the RES_APP traffic is secured.

```
ZDCOM DISPLAY PORT-1000 SERVER

DCOM0001I 11.06.22 NETWORK COMPLIANCE SERVER DISPLAY FOR PORT 1000
 PORT-1000        MODEL-SERVER     TLS-Y
 PROTO-TCP        NAME-RES_APP
 TLS INFORMATION:
  TLS VERSIONS USED       : TLS 1.2
  TLS VERSIONS ALLOWED    : TLS 1.1, TLS 1.2
  TLS CIPHERS USED        : AES256-SHA256, AES128-SHA256
  TLS CIPHERS ALLOWED     : AES256-SHA256, AES128-SHA256,
                            AES128-SHA
  PRIVATE KEY KEYSTORE NAME    : RESKEY
  SERVER PRIVATE KEY SIZE      : 2048
 TPF CERTIFICATE:
  PUBLIC KEY LENGTH   : 2048
  SIGNATURE ALGORITHM: sha256WithRSAEncryption
  SUBJECT INFO        : /C=US/ST=New York/L=Poughkeepsie/O=IBM/OU=TPF/CN=
                        tpf.pok.ibm.com/emailAddress=johndoe@example.com
  ISSUE DATE          : Jan 24 14:41:15 2022 LST
  EXPIRATION DATE     : Jun 08 14:41:15 2022 LST
 CLIENT AUTHENTICATION: NO
END OF DISPLAY
```

Christine issues the ZDCOM DISPLAY PORT-1000 SERVER detailed display command to show the TLS credentials used to secure that server port.

The security auditor is concerned of the possibility of using TLS 1.1 version and AES128-SHA cipher, even though they have not been used.

As-Is Scenario
Determining Usage of TLS Ciphers on z/TPF

- Christine, a Security Administrator for the z/TPF system, is asked to ensure that the AES128-SHA cipher is no longer used on the z/TPF system and should be replaced with AES256-SHA256.
  - She needs to identify which applications are using AES128-SHA and which applications can use AES128-SHA.
- Christine knows this will be difficult to determine. She needs to identify all the applications that are using TLS, and then must determine if the AES128-SHA cipher is being used by any of the secure z/TPF applications.

To-Be Scenario
Determining Usage of TLS Ciphers on z/TPF

- With the new z/TPF ZDCOM compliance command, Christine can obtain all the ports that can use AES128-SHA, including the ports that have negotiated a sessions using AES128-SHA.

```
ZDCOM USAGE CIPHER-AES128-SHA

DCOM0006I 13.33.16 NETWORK COMPLIANCE USAGE
DISPLAY FOR CIPHER AES128-SHA

  PORT    MODEL     CIPHER USED
  ----- -------   -------------
  443     CLIENT          N
  443     SERVER          Y
  1000    SERVER          N

  END OF DISPLAY
```

The HTTPS server is negotiating sessions with remote partners to use the AES128-SHA cipher algorithm. This may require updates to the remote side as well.

You can use ZDCOM USAGE VERSION-xx to identify ports that are using a particular TLS version as well.

To-Be Scenario

Determining Which Remote Clients are Using a Given Cipher

Christine has identified server port 443 (HTTPS) server is using the AES128-SHA cipher. Christine uses the ZDCOM USAGE detailed display to identify which remote systems are negotiating the use of the AES128-SHA cipher algorithm.

```
ZDCOM USAGE CIPHER-AES128-SHA PORT-443 SERVER

REMOTE IP ADDRESSES USING AES128-SHA FOR PORT 443 AS SERVER

   REMOTE IP              LAST CONNECTION
 ----------------      --------------------
  100.100.100.100       2021-03-05 12:28:47
  200.200.200.200       2021-03-04 11:38:37
  9.57.13.50            2021-03-03 10:48:27
  10.10.10.10           2021-03-02 09:58:17

END OF DISPLAY
```

Lists up to the last 10 remote IP addresses that negotiated the use of AES128-SHA cipher organized by connection time since the last system IPL or ZDCOM CLEAR command.

Now Christine can determine if the remote systems need to be updated. She can reach out to those remote systems directly or analyze connections established in IP trace to determine what ciphers they are negotiating to determine if updates on the remote systems are required.

Note: For secure z/TPF server applications using the new server cipher preference option (APAR PJ46661, January 2022), it becomes easier to determine which remote clients will require changes

As-Is Scenario
Determining when Certificates are Nearing Expiration

- A recent incident occurred on the z/TPF system when the certificate used by the HTTPS server unknowingly expired. This caused disruption of service on the z/TPF system as new connection attempts to that server failed.
- Christine was asked to investigate how this can be prevented in the future.
- Christine realizes the only way to monitor the z/TPF certificates is to periodically manually display them using the ZPUBK DISPCERT command.
  - This requires knowing all the certificates that are in use on the z/TPF system as well as their location.
- Christine is concerned the manual certificate expiration monitoring process is difficult for her, and it is error prone. For example, what if a new certificate is added?

To-Be Scenario
Determining when Certificates are Nearing Expiration

- With the new z/TPF ZDCOM compliance command, Christine can use the ZDCOM CERTIFICATE SUMMARY command to summarize all the known certificates on the z/TPF system.

```
ZDCOM CERTIFICATE SUMMARY

DCOM0010I 08.35.38 CERTIFICATE SUMMARY DISPLAY

  PORT   MODEL       ISSUED          EXPIRES        DAYS
  ----- -------  -------------  -------------  ------
  443    CLIENT   Feb 19 2022    Jul 14 2022      109
  443    SERVER   Dec 24 2021    Apr 11 2022       15
  1000   SERVER   Feb 24 2022    Jun 12 2022       77
```

Christine sets up automation to periodically issue the ZDCOM CERTIFICATE SUMMARY command to summarize the in-use certificates along with their expiration information.

To-Be Scenario
Using the Certificate Expiration Monitor User Exit

Christine realizes that she can use the Certificate Expiration Monitor User exit to also monitor the certificates on the z/TPF system.

User Exit ucmp.cpp (UCMP) Prototype:

```
extern "C" void UCMP(unsigned short port_num, bool is_client, struct tm cert_issued,
                     struct tm cert_expiration, int days_to_expire)
```

- Port and model for which the certificate is used
- The time and date the certificate was issued
- The time and date the certificate expires
- The number of days remaining before expiration

The certificate expiration monitor user exit is invoked every day for every known certificate (~8PM local time).

Christine updates the UCMP user exit to send an email to herself anytime a z/TPF certificate will expire in less the 30 days. She also will WTOPC a console message when the certificate reaches 7 or less days before expiration.

Value Statement

This project makes it easier for customers to gather z/TPF security compliance information for z/TPF networking:

- Customers can determine all the active network ports on the z/TPF systems and whether they are secure or not.
- Customers can see the TLS credentials (TLS version, ciphers, key exchange, certificate information, etc.) for the secure ports.
- Customer can determine what TLS versions or TLS ciphers are currently being used to know when it's safe to drop support of older ciphers or versions.
- Customers can determine when a z/TPF TLS certificate is nearing expiration.

Delivered with **APAR PJ46476** (Sept 2021)

Possible Follow Ons

Where do we want to see the lab focus next on z/TPF compliance?

- **Focus on cipher / key usage (outside of TLS and networking)**
  - Which applications are using ciphers to encrypt / decrypt data?
    - For example, which applications are using tpf_encrypt_data (secure key encryption)
  - Which secure keys within the keystore are using a specific cipher, date of last usage?
  - Which z/TPFDF databases are encrypted and with which cipher?

- **Focus on vulnerabilities (OpenSSL, Java, Log4j, and so on)**
  - Which vulnerability patches are loaded to the z/TPF system from the available z/TPF vulnerability patches?

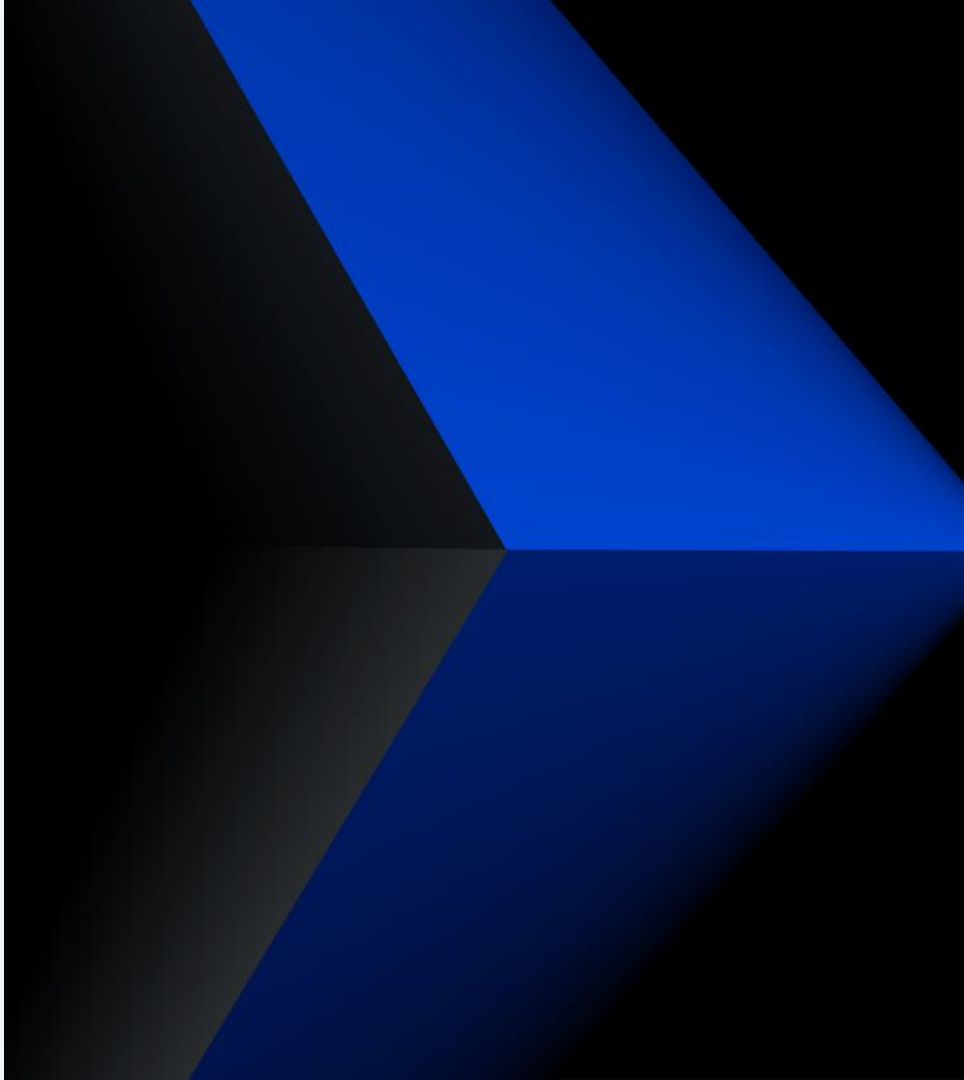
We want sponsor users!

Our development cycle is driven by your feedback.

We are looking for sponsor users to assist in design and implementation of future z/TPF Security Compliance related work.

If you are interested in participating as a sponsor user, please contact:

Angel Baez (angel.baez@ibm.com)



Thank you

Questions? Comments?