Virtual CICS user group: Newsletter 63

Welcome to the Virtual CICS user group newsletter. The Virtual CICS user group at virtualcics.hostbridge.com is an independently-operated vendor-neutral site run by and for the CICS user community.

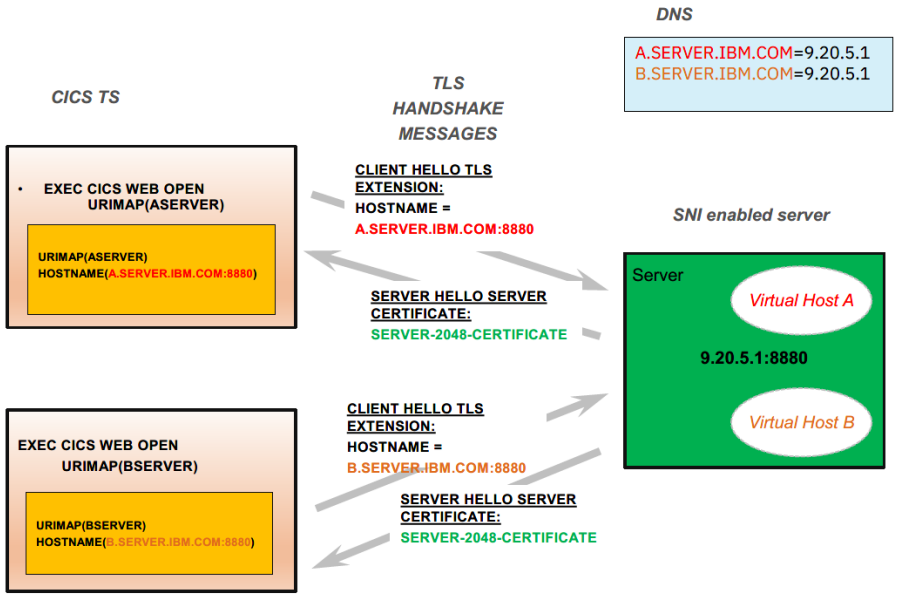

Figure 1: Without SNI support

Virtual CICS user group presentation

The latest webinar from the Virtual CICS user group was entitled, “What’s New in CICS Security”. It was presented by Colin Penfold, Technical Leader for IBM CICS Transaction Server Security.

Colin has been at IBM for almost 40 years, the last 30 in CICS. He has designed a number of features in CICS including Channels and Containers, the Link 3270 bridge, and CICS’s support for the IBM Health Checker for z/OS. For the last decade he has been the technical leader of CICS Security,

Contents:

Virtual CICS user group presentation	*1*
Meeting dates	*5*
CICS Modernization	*5*
About the Virtual CICS user group	*5*

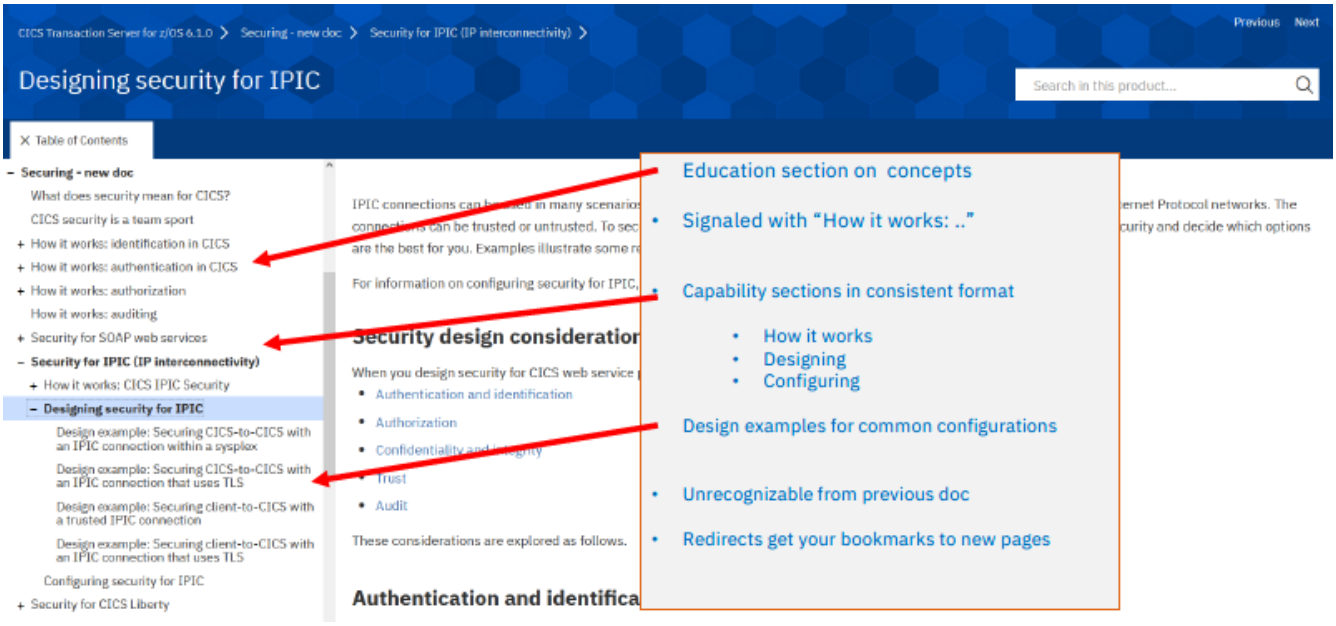

Figure 2: Rewrite and restructure of CICS security documentation

during which time he has designed security features in CICS including TLS enhancements, distributed identity support, and several new authentication mechanisms including MFA.

Colin Penfold started his presentation by saying that he would be talking about what's new in CICS TS 5.6 and the CICS TS Open Beta, which was released on 9 July.

He began by looking at enhancements to Transport Layer Security (TLS).

Server Name Indication (SNI) was introduced with Internet Engineering Task Force RFC 6066. SNI allows a server with a single IP address and port to host multiple secure websites, each with their own server certificate, eg Amazon (AWS). CICS TS supports SNI as a client. Note: SNI is supported rather than required. It's used if the server supports it, and there's no configuration.

The problem when accessing a server with multiple websites, as illustrated in Figure 1, is that, without SNI, the server certificate being returned doesn't match the calling URIMAP. With SNI, it does.

Moving to TLS 1.3 is a major change. There are three new ciphers for 1.3, and these ciphers are incompatible with TLS 1.2. There are also some performance changes. There's now a single handshake, more secure algorithms, and a change to cacheing.

That has required changes to the system initialization table (SIT) with the introduction of the parameter MAXTLSLEVEL and the removal of the parameter ENCRYPTION. ONLY has been removed as an option to the MINTLSLEVEL command. Numeric ciphers have been deprecated and will be removed.

The CIPHERS option on resources IPCONN, TCPIPSERVICE, and URIMAP now defaults to defaultciphers.xml rather than numeric ciphers. Also, USSCONFIG must have the file /security/ciphers/ defaultciphers.xml.

That means when MAXTLSLEVEL=TLS13 is specified, numeric ciphers are no longer supported, and all definitions must use

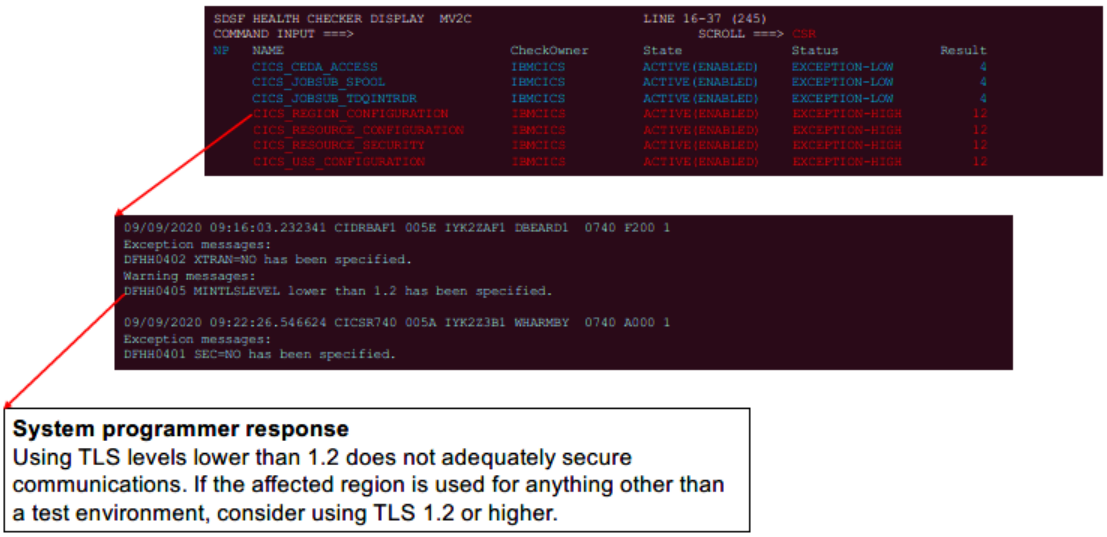

Figure 3: New CICS checks for IBM Health Checker for z/OS

xml files. People who try to change/install numeric ciphers will find that it fails.

To aid migration, currently with MAXTLSLEVEL<=TLS 1.2, where people specify:

```
EXEC CICS WEB OPEN CI-
PHERS(353839)
<URIMAP(urimap)>
```

A warning messages is issued once per program issuing the command. Existing requests are still honoured, but a new translate will fail.

Sites wanting to migrate to using TLS 1.3 will need to upgrade to z/OS 2.4, and upgrade to CICS TS Open Beta. They will then need to: copy and customize defaultciphers.xml; prepare RDO definitions, which means all resources must use xml files in CIPHERS, and TLS 1.3 ciphers must be included; and upgrade certificates, ie RSA key size must be at least 2048 bits, and ECC keys size at least 256 bits. Lastly, they must set MAXTLSLEVEL=TLS13. All ciphers will be defined in USSCONFIG. If any ciphers are found to have security flaws, they can now be changed in one place.

For users replacing outbound default ciphers, they must override the system supplied default 2-digit ciphers (a very limited set) used on:

```
EXEC CICS WEB OPEN
EXEC CICS INVOKE SERVICE
```

And replace them with defaultciphers.xml. The feature toggle to enable is: com.ibm.cics.web.defaultcipherfile=true.

Moving on to scenarios and best practices, Colin told the user group that CICS security documentation has been restructured. Education on concepts and terminology is aimed at new joiners. Advice on security in application architecture scenarios is aimed at application architects. Security configuration tasks for these scenarios is aimed at new systems programmers. The idea is that best practice advice and recommendations are absolutely clear to the reader. Figure 2 shows an example of some of the changes. Colin also showed some design example diagrams.

Colin then went on to talk about the IBM Health Checker for z/OS, which is designed to encourage best practice. It will report where sites are not conforming to advice. Basically, it helps to identify potential configuration problems before they impact availability or cause system outages. It programmatically checks the current active z/OS and sysplex settings

and definitions for a system. It them generates output with detailed messages to inform users of any potential problems and suggested actions to take to resolve them.

Health Check output is visible as option CK in SDSF. Checks are associated with a product or subsystem. In fact, IBM provides over 150 health checker checks. Each check tests configuration or state information. This results in a SUCCESS, WARNING, or EXCEPTION message.

New CICS Health Checks are based on best practice reviews of customers, and cover security configuration of Region definitions, CICS resources, and CICS zFS security. Best practice advice is aimed at production or production-like regions. Examples of checks include:

```
SEC=YES
XTRAN=YES|class
XUSER=YES
```

Figure 3 shows an example of the output. The lines coloured red highlight errors. In real life, they would be the same colour as the rest of the output.

Colin then moved on to monitoring and preventing threats. The new Open Beta shows the TLS protocol in monitoring records. This can be for in inbound and outbound performance records.

The enhanced security (XS) monitoring capability is available with CICS TS 5.6. Colin explained that the world has changed since this was first introduced. The XS security domain had no stats monitoring fields. That's because when it was introduced in 1992:

- Most requests were 3270 signon
- Only password/ passtickets
- Request on RO TCB
- Used DES encryption.

Nowadays, XS handles more authentication types, eg Password/Passphrases with KFDAES, MFA, Kerberos, and certificates. In addition, CPU and elapsed time authenticating has greatly increased. To avoid bottlenecks, requests cannot now all go through the RO TCB. Open TCBs are used or attached, increasing usage of TCBs. TCBs (and probably ESM requests) consume 24-bit storage.

There are new security statistics, and there are new areas being monitored, for example the total elapsed time that the user task spent verifying passwords, password phrases, PassTickets, and MFA tokens, the total elapsed time that the user task spent verifying basic authentication tokens, the total elapsed time that the user task spent verifying Kerberos tokens, and the total elapsed time that the user task spent verifying JSON web tokens.

Instruction Execution Protection (IEP) helps separate data storage from program storage, and prevents code from being executed on data storage, and therefore prevents buffer overflow exploits. In the past, it has been possible to hide code in data.

There are certain prerequisites for IEP: z/OS 2.4 or 2.3 with appropriate APARs. And users need to be using a z14 or higher. There are also new settings:

```
STORAGE OBTAIN and RELEASE
EXECUTABLE={YES|NO}
IARV64 GETSTOR
EXECUTABLE={SYSTEM_RULES|YES|NO}
```

EXECUTABLE is ignored if the hardware or software does not support IEP.

DSA storage in the new Open Beta is either executable or data (non-executable).

Where someone tries to execute code in a data area, there is a new IEP program check (0c4). The kernel ESTAE will identify 0c4 as an IEP program check with error code 0c4/akes. The PSW will be pointing to the next instruction and BEAR will contain the last branch address.

HostBridge is now offering services, support, expertise, and even free pilot software to help organizations rapidly make CICS applications available.

If sites really need to make data areas executable, there are API and XPI options, and definitions to allow this. It's primarily intended for ISVs and requires SYSEIB.

Lastly, Colin Penfold moved on to the simplified and improved diagnostics. The information for security failures has been improved. For example, problems can often occur where the userid is a functional userid or the transaction started on another region. It's difficult to identify the end user. A new DFHXS1117 message will accompany the DFHXS1111 message, giving the origin data information. The information will vary depending on entry point, but the distributed identity will be reported if available.

Security definitions for CAT 1 transactions have been removed. The situation is that only the region userid is allowed to run CAT 1 transactions. CICS already knows the region userid, the CAT 1 transactions, and how a transaction is started. Which makes asking an External Security Manager redundant. In addition, removing the ESM check makes it more secure. This is mentioned in the Auditor section of the CICS documentation to ensure auditors are aware.

A copy of Colin Pendold's presentation is available for download from the Virtual CICS user group website at virtualcics.hostbridge.com/presentations/CICSSecurityJul21.pdf.

You can see and hear the whole user group meeting at https://youtu.be/YmKVXT1WZpI.

Meeting dates

The following meeting dates have been arranged for the Virtual CICS user group:

- On 14 September, we have Colin Pearce, who will be discussing, "Collecting and Analysing CICS Statistics".
- The following meeting is on 16 November when Ezriel Gross, Principal Solutions Advisor, IBM Systems (CICS) at Rocket Software will be speaking.

We are using Zoom for the user group meetings.

CICS Modernization

HostBridge has produced a new eBook discussing CICS modernization. You can find it here: https://www.hostbridge.com/modernization-cics-apis-ebook/.

The new eBook, "Using APIs for CICS Modernization" explains the API modernization strategy and provides advice to help you get started.

On the eBook download web page, you'll also find a two-minute video that explains the difference between technology-based APIs and business-level APIs. Understanding this distinction is critical to success using APIs for modernization.

HostBridge has expertise and resources to advise you on strategy or deliver modernization services. If you'd like to discuss your modernization needs, please schedule a meeting by clicking on this calendar link.

The Virtual CICS user group is hosted at virtualcics.hostbridge.com. Anyone with an interest in CICS is welcome to join the Virtual CICS user group, which is free to its members.

To share ideas, and for further information, contact trevor@itech-ed.com.