Virtual CICS user group: Newsletter 46

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

Virtual CICS user group presentation

The latest webinar from the Virtual CICS user group was entitled, “Multi-factor authentication for z/OS and CICS: what, why and how – part of your GDPR compliance strategy”, and was presented by Keith Banham, Manager, Research and Development at Macro 4, a division of UNICOM Global.

Keith has worked in IT for over 35 years and is the mainframe R&D manager at Macro 4, a division of UNICOM Global. Keith started as an Assembler programmer at a major bank, and, during his 30+ years at Macro 4, he has worked on many of the company’s solutions for application lifecycle management, application performance management, document management, and session management. He is responsible for driving the modernization of these solutions by building Web, Eclipse, and mobile interfaces, and architecting cross-platform solutions utilizing UNICOM’s open systems and IBM i capabilities.

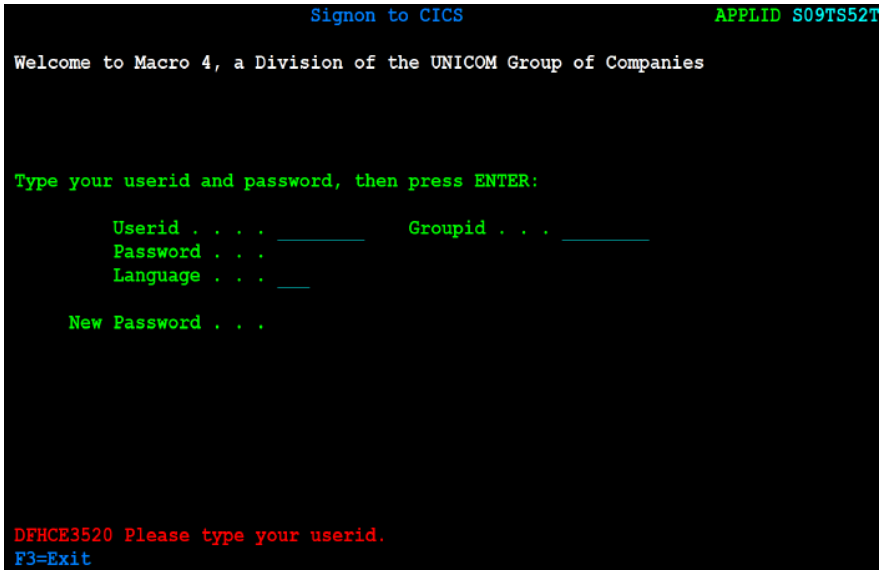

Figure 1: Standard mainframe security

Contents:

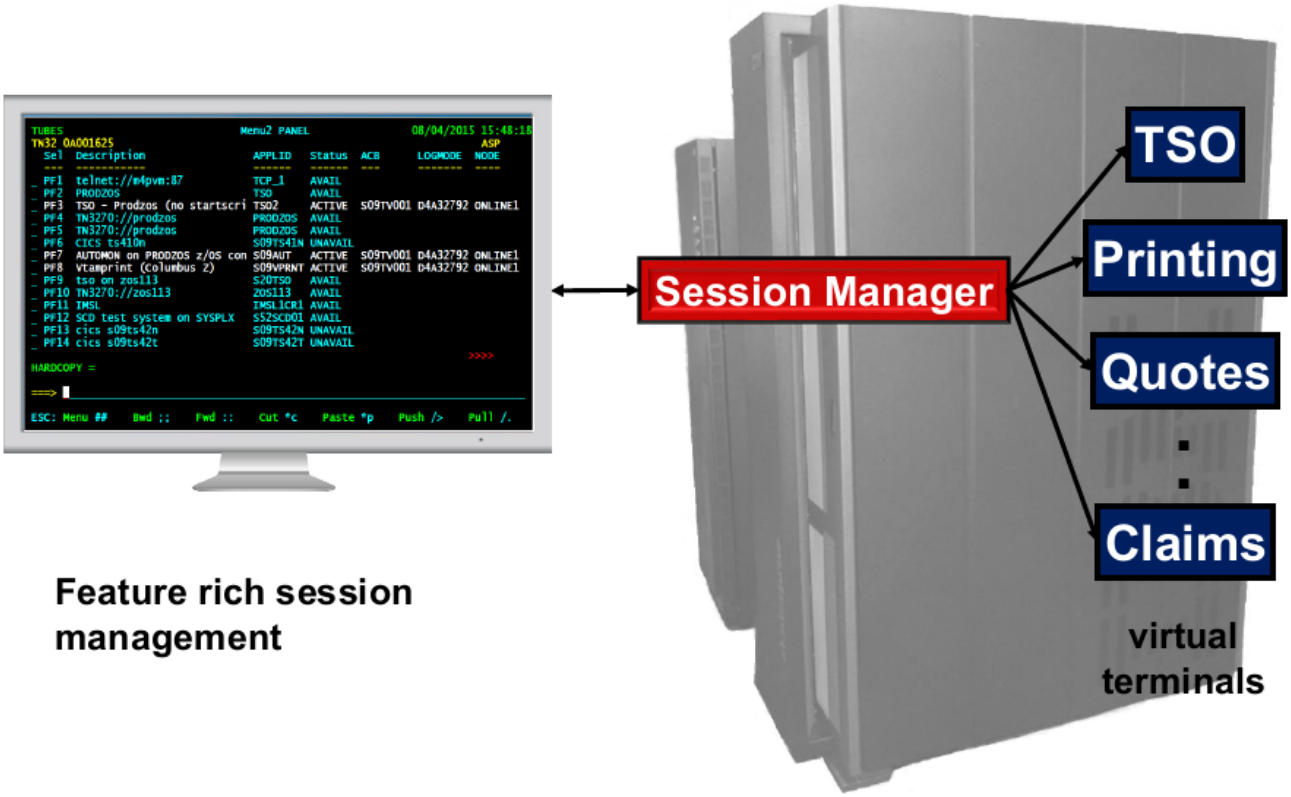

Figure 2: Mainframe session management

Keith Banham started his presentation by telling the group that security is a key feature of z/OS and CICS, but the weakest link is the use of user-IDs and passwords, making the system vulnerable to hacking and misuse. Multi-Factor Authentication (MFA) is not a new technology, but it is now available on z/OS and CICS.

Figure 1 shows the standard login page that has been with us for years. It expects an 8-character password.

Many people access the mainframe using devices other than green screens while they are on the move. And many non-IT people are accessing mainframes and could be accessing sensitive data.

General Data Protection Regulation came into force in May this year. It's meant to protect the personal data of all EU citizens and applies to companies globally that may have data on EU citizens. Before an organization can store data on EU citizens, those citizens must give informed consent. And they now have increased rights. They can access, correct, and delete the data held on them by a company, and they can do that free of charge. There can be tougher fines for organizations that don't comply with the regulations.

It means that mainframe sites now need (more than ever) to control access to data, and the way to do that is to use MFA.

At one time, biometrics were thought to be the answer to the security issue – things like fingerprints and retinal scans. The problem with biometric data is that once it's in the computer (as 0s and 1s) it's static data. It never changes and can therefore be sniffed, traced, and reused.

Multi-Factor Authentication for z/OS is integrated with RACF. It uses a One Time Password (OTP) generator, and is valid for a short period

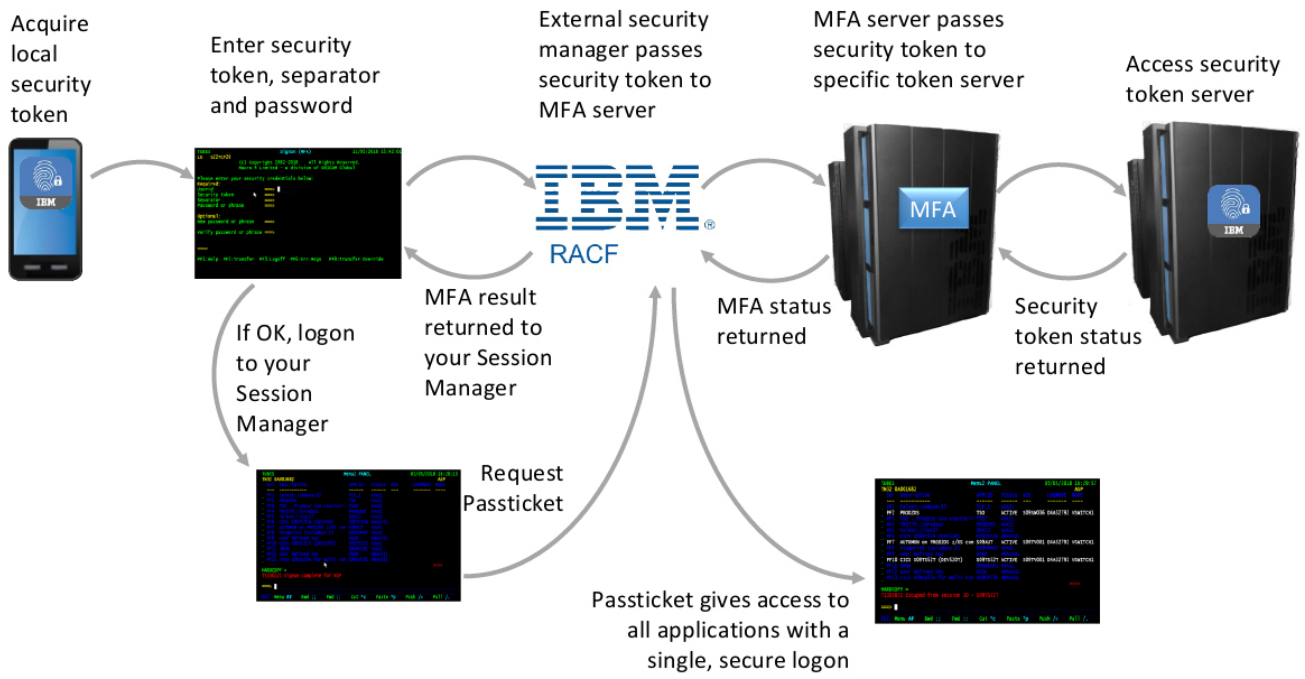

Figure 3: Example in-band and compound using RACF and IBM TouchToken

(eg 60 seconds). It does require additional hardware and software.

RSA SecurID (a fob) and RSA Authentication Manager (software) rely on a person having a fob (or equivalent) and two things they know, eg an RSA SecurIDPIN, and something else they know. Alternatively, Apple devices can be used. They require IBM TouchTokenfor z/OS and IBM TouchTokenApp on iOS device. Security requires the iOS device and App and your fingerprint. These are described as 'in-band'.

'Out-of-band' MFA uses IBM Multi-Factor Authentication for z/OS and a Web page where people enter their RACF credentials. The user's MFA policy may include RSA SecurID, IBM TouchTokenfor z/OS, or other devices.

In the USA, a lot of companies use the IBM MFA Certificate Authentication. This requires a Common Access Card (CAC) and Personal Identification Verification (PIV). You can use it 'out-of-band' only. It uses the approved certificate from the card and a PIN number.

True MFA is available with IBM Multi-Factor Authentication for z/OS V1.3. It uses additional factors and provides RADIUS (Remote Authentication Dial In User Service) support (eg SafeNet, RSA SecurID), and generic TOTP (Time-based One Time Password), which has Android and Microsoft Windows support. Compound Authentication for 'in-band' uses the PassPhrasefield field when logging in.

As illustrated in Figure 2, many people are accessing the mainframe using a session manager rather than logging in in the traditional way. Using a modern Session Manager provides a single logon and control. It simplifies the process by using PassTickets. And it allows sites to customize logon screens and add instructions (where this doesn't conflict with regulations, eg PCI).

Figure 3 illustrates 'in-band' and compound MFA using RACF and IBM TouchToken. RACF could be replaced by other security management products.

IBM Multi-Factor Authentication can be configured using the AZFEXEC command. Keith Banham went on to give more details of how MFA can be implemented.

Auditing is part of an organization's GDPR strategy. Auditors need to know who signed in, who used a specific application, and when, and for how long. What's needed is a way to push metrics into Business Analytic tools and combine them with other metrics. For example, JasperReports (an open source Java reporting tool) can be used to produce graphs showing user activity. Or Splunk (the SIEM tool) can be used to produce interactive reports.

A copy of Keith Banham's presentation is available for download from the Virtual CICS user group Web site at www.fundi.com/virtualcics/presentations/CICSMFASep18.pdf.

You can see and hear the whole user group meeting by downloading the WMV file from www.fundi.com/virtualcics/presentations/2018-09-11meeting.wmv.

Meeting dates

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

- On 13 November 2018, Jason Brosius, Senior Software Engineer at CA Technologies, will be presenting, "Provisioning CICS: Customize your CICS provisioning Using z/OS Provisioning Toolkit".
- The following meeting is on 15 January 2019, when Tom Dunlap, CTO at Themis, Inc, will be discussing, "The CICS / Db2 interface".

We will be using Citrix GoToMeeting for the user group meetings.

CICS news

Compuware has updated its Topaz for Total Test, automating mainframe unit testing software. It has acquired XaTester from Xact Consulting A/S. The software enables developers to create unit tests for both batch and CICS-based programs written in COBOL, PL/I, and Assembler. You can read the full press release at: https://resources.compuware.com/xatester_acquisition_parasoft_partnership.

Recent CICS articles

OSGi Demystified: 3.3 – Workarounds for exploiting OSGi Services effectively by Ivan Hargreaves on CICS DevCenter (31 August 2018). You can find the article at: https://developer.ibm.com/cics/2018/08/31/osgi-demystified-3-3-exploiting-osgi-services/

OSGi Demystified: 3.2 – Declarative Services by Ivan Hargreaves on CICS DevCenter (31 August 2018). You can find the article at: https://developer.ibm.com/cics/2018/08/31/osgi-demystified-3-2-declarative-services/

OSGi Demystified: 3.1 – Dynamic Class Loading by Ivan Hargreaves on CICS DevCenter (31 August 2018). You can find the article at: https://developer.ibm.com/cics/2018/08/31/osgi-demystified-3-1-dynamic-class-loading/

The Virtual CICS user group was established as a way for individuals using IBM's CICS TS systems to exchange information, learn new techniques, and advance their skills with the product.

The Web site at www.fundi.com/virtualcics provides a central point for coordinating periodic meetings (which contain technically-oriented topics presented in a webinar format), and provides articles, discussions, links, and other resources of interest to IBM CICS practitioners. Anyone with an interest in CICS is welcome to join the Virtual CICS user group and share in the knowledge exchange.

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

The Virtual CICS user group is free to its members.