Virtual CICS user group: Newsletter 55

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.

Virtual CICS user group presentation

The latest webinar from the Virtual CICS user group was entitled, “Providing system integrity for multiple LPARs with improved GDPR and PCI/DSS compliance”. It was presented by Al Saurette, Principal at MainTegrity Inc.

Al is a principal at MainTegrity Inc and is dedicated to improving security on mainframes and other platforms. For over 35 years, he has delivered innovative solutions for enterprise IT problem areas. With a strong Operations background, he is a regular speaker at international security conferences and has authored many IT industry thought-leadership papers.

MainTegrity is a member of the PCI Security Systems Council and works with client organizations to improve both application and system integrity, focusing on eliminating internal threats.

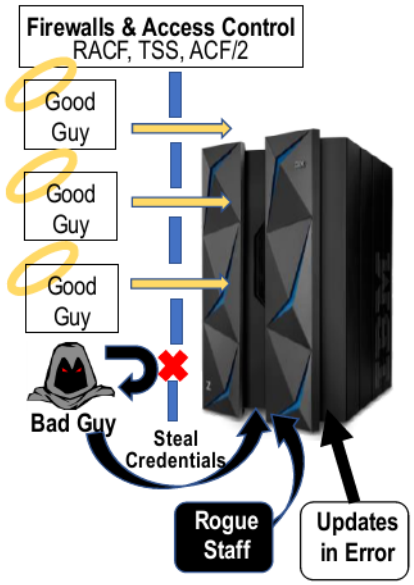

Figure 1: The security need

Al started off by identifying the business need for a software tool that could:

- Improve internal security and compliance (PCI/DSS, GDPR, NIST)

Contents:

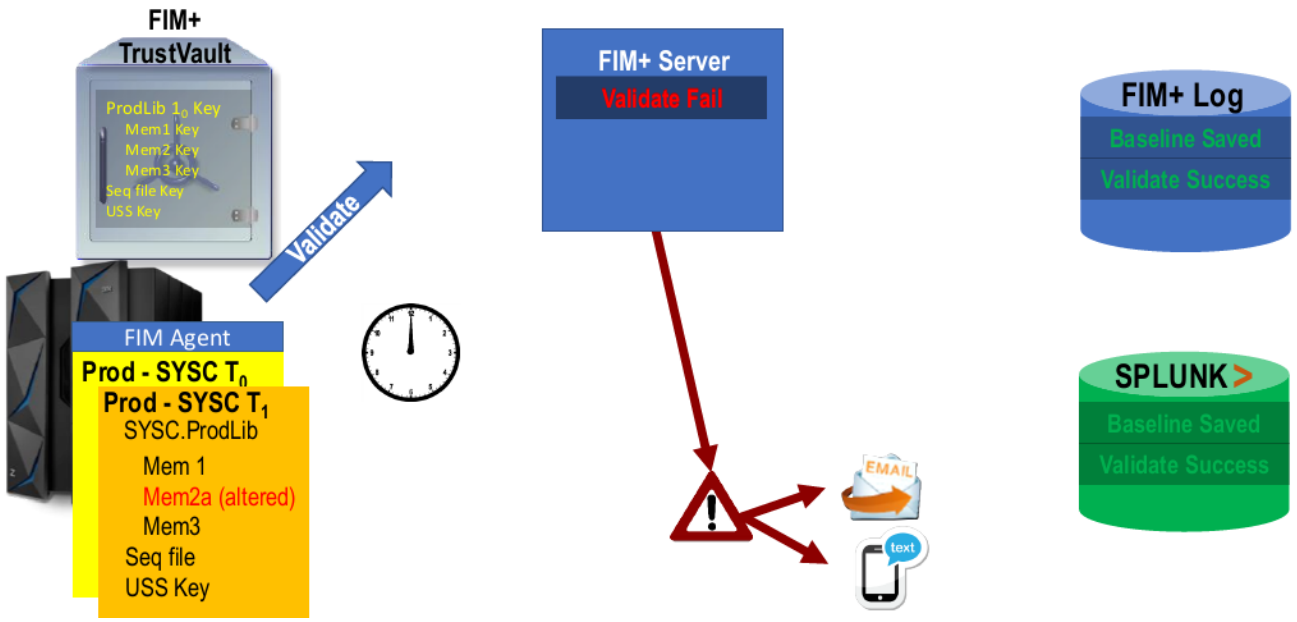

Figure 2: Change detected

- Manage system integrity across multiple clients, systems, or LPARs
- Audit/Certify that software is correct (on demand or continuous)
- Monitor system and configuration file changes (compare in stream)
- Give a new generation of support staff the tools to do things right
- Present info from differing tools (SMF, ServiceNow, Remedy, Splunk, QRadar, etc).

The 2019 IBM / Ponemon report, which surveyed over 500 organizations found that on average it took 206 days for a breach to be detected and a further 73 days to respond and recover. When they analysed the breaches, they found 51 percent were malicious attacks by outsiders, 25 percent were caused by human errors, and 24 percent were system glitches (corrupt files, bad configs, etc). On average, a breach cost $4.3 million, plus there was the impact on the reputation of the breached company, plus the IT guy (you) could lose his job.

As Figure 1 shows, traditional security products are designed to allow in the good guys and keep out the bad ones. However, bad guys can steal credentials (phishing, man-in-middle, guessing, etc) and get through the security. And trusted employees can go rogue (addiction, financial, health). Plus, well-meaning staff can make mistakes (deploy, update). You end trying to discover whether the changes were correct and whether all the LPARS are the same. This traditional monitoring is labour intensive and requires lots of z/OS-specific skills.

File Integrity Monitoring (FIM) creates a hash key for each file at a trusted level then saves the key in an encrypted vault. Later, it creates another hash key and compares the two keys. As well as IMS, it can monitor the z/OS system, CICS, Db2, TCP/IP, application executables, JCL, configs, USS files, Scripts, Clists, Log files, and encrypted data sets. If something is amiss, alerts can be sent via text or email to an admin or a central console. they can quickly

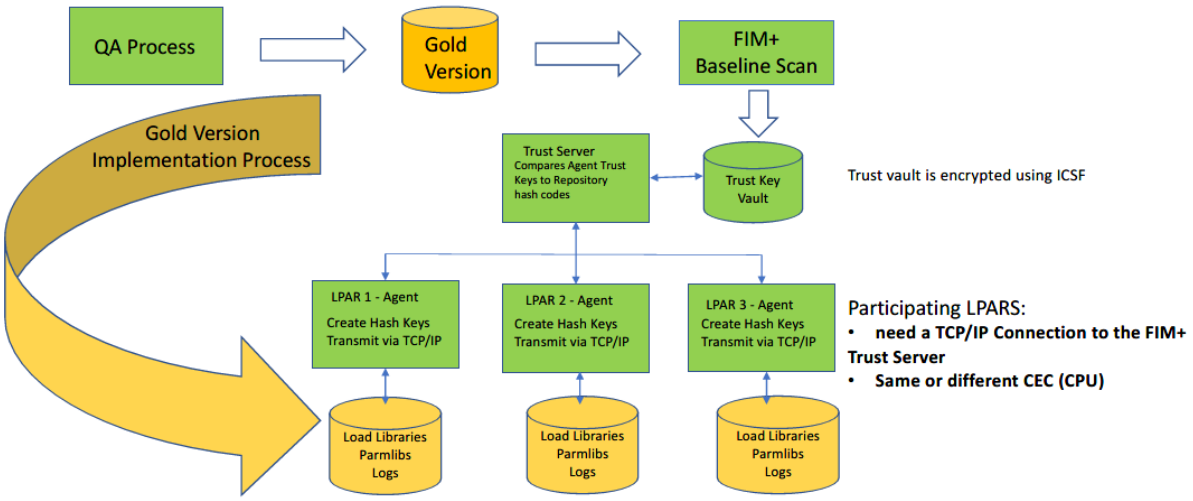

Figure 3: Integrity management

drill down to forensic info (SMF, change control, etc). To enhance performance, this can be offloaded to the crypto card, so it uses minimal CPU.

Figure 2 shows how a change to a file can be detected.

FIM+ validates a file's contents by scanning the actual file. No-one wants false alarms, so the software corroborates that alarms are real. It suppresses alarms from approved changes. And it can interoperate with change management systems. It can also ensure that code levels in all LPARS are the same and detect wrong versions, missed changes, and backout errors. It does this by using Before and After FIM+ snapshots to prove that everything was deployed correctly.

A problem at many sites is ensuring that systems and apps on multiple LPARS are rolled out correctly. And they need to accommodate the required LPAR-specific deviations. Sites need to know when people with legitimate credentials make unauthorized or inadvertent changes. Plus, code tends to drift from the base over time. The issue many sites face is that if a problem occurs in only one LPAR, how do you determine what is/should be different. It can be a daunting task. For most sites, ongoing audits to prove that production systems are correct are manual, so, typically, they are not carried out.

FIM+ can:

- Define a version of the application as the baseline and compare the code base in each LPAR to that baseline version.
- Identify any deviations from the baseline version.
- Continuous Audit is a consequence of implementing FIM+.
- Systems are protected from both inadvertent and malicious changes made using legitimate credentials.
- Advanced forensics are automatically generated to show you who, why, and what changes were made.

System Integrity Management is illustrated in Figure 3. Its features include:

- Baseline scan, which establishes a trusted "gold version" as a baseline release.

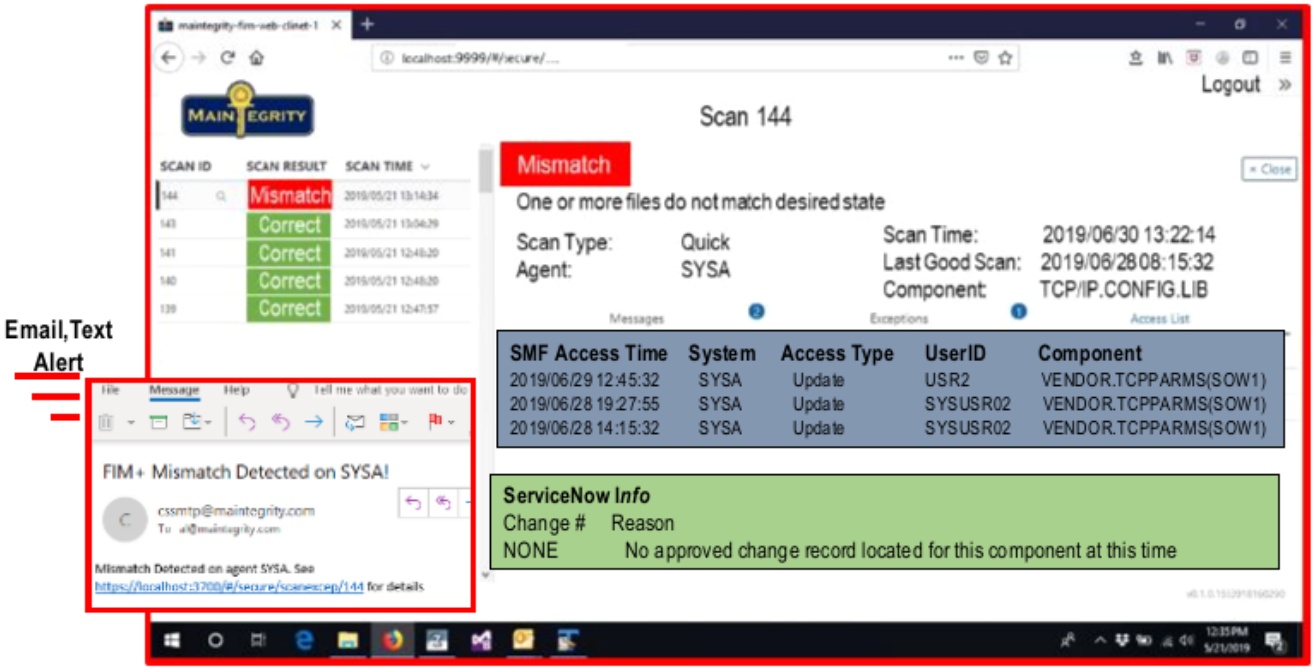

Figure 4: Human interface

- When a changed file is detected: the detection is logged; the proper authorities are notified; and complete forensics and compare functions are available through an easy-to-use GUI, so you know what changed, who changed it, when it was changed, and why it changed. It compares the file with the baseline version to show the actual lines that changed (text-based files).
- LPAR-specific files. This enables them to be excluded from comparison to the baseline version.
- Support for all log file types – GDGs, Date/Time Stamps, version numbers.

The human interface GUI is illustrated in Figure 4. Once an admin has received a text or email, one click opens the GUI in any browser and displays detailed information including SMF access data. A second click fetches change control information from ServiceNow or Remedy dynamically, without needing mainframe skills. A third click can invoke the instream file compare to show exactly what line changed. A complete restore can be accomplished by clicking the FIM+ Recovery Assistant to select and verify all the files required.

This automation means that a breach can be quickly identified (hours and minutes rather than months – according to the IBM/Ponemon report).

A copy of Al Saurette's presentation is available for download from the Virtual CICS user group website at virtualims.hostbridge.com/presentations/CICSFIMMar20.pdf.

You can see and hear the whole user group meeting at https://youtu.be/1GXptpe7P0k.

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

Meeting dates

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

- On 12 May, we have IBM's Stewart Francis. He will be discussing "CICS Bundles and Maven". Maven is a build automation tool used primarily for Java projects
- The following meeting is on 7 July, when Hostbridge will be discussing "Getting and Using CICS Integration Analytics".

We are using Webex for the user group meetings.

Recent CICS articles

Using the Liberty angel to access authorized z/OS services by Eric Phan on CICS Developer Center (2 March 2020): https://developer.ibm.com/cics/2020/03/02/using-the-liberty-angel-to-access-authorized-zos-services/.

An Integration Analytics Primer

There's an interesting blog at hostbridge.com/an-integration-analytics-primer/ looking at getting CICS performance data for composite applications in a hybrid IT environment. The blog suggests that it's often relatively simple to get data that shows how individual components of composite applications are performing, but it has been more problematic gaining a holistic set of analytics that reveal true end-to-end performance. Enterprises need comprehensive integration analytics.

Seemingly 'small' changes introduced at any layer of a hybrid IT application can have a major, ripple-through effect. They have seen three specific areas of interest emerge relating to integration analytics: end-to-end transaction tracking, application performance analytics, and RPA analysis.

HostBridge Transaction Analytics Connector (HTAC) is software that runs under CICS and extracts data and metadata from each external request to run a transaction/program. HTAC delivers this information to Splunk, along with the standard information that CICS keeps track of for all transactions. Splunk dashboards then correlate mainframe activity to non-mainframe activity, providing an end-to-end view of hybrid IT application performance.

About the Virtual CICS user group

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 virtualcics.hostbridge.com 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.