Virtual IMS user group: Newsletter 71

Welcome to the Virtual IMS user group newsletter. The Virtual IMS user group at itech-ed.com/virtualims is an independently-operated vendor-neutral site run by and for the IMS user community.

Virtual IMS user group presentation

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

During his over 35 years in the IT industry, Gary has held senior management positions in a variety of IT companies that were engaged in both software development and IT services. Gary has held senior positions as a technician including as an IMS Systems Programmer, as a senior manager in IT delivery, and in a variety of business development roles.

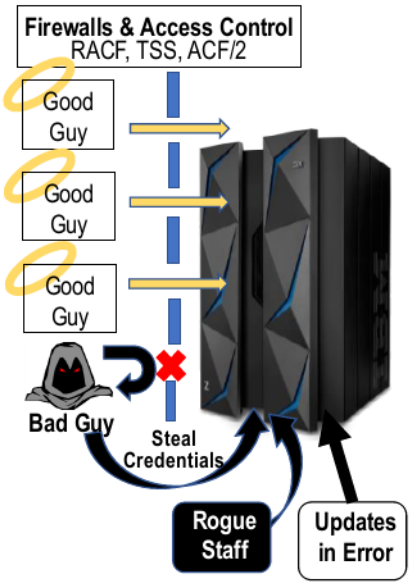
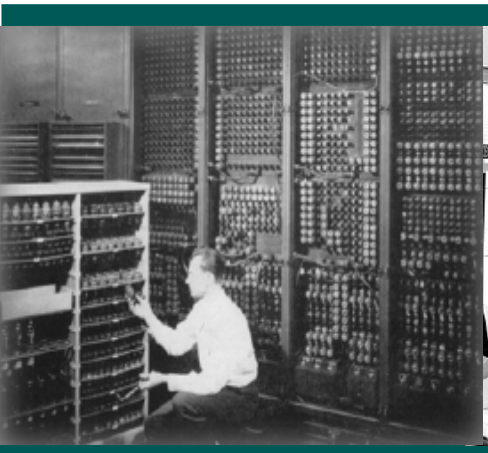


Figure 1: The security need

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

- Improve internal security and compliance (PCI/DSS, GDPR, NIST)
- Manage system integrity across multiple clients, systems, or LPARs

Contents:



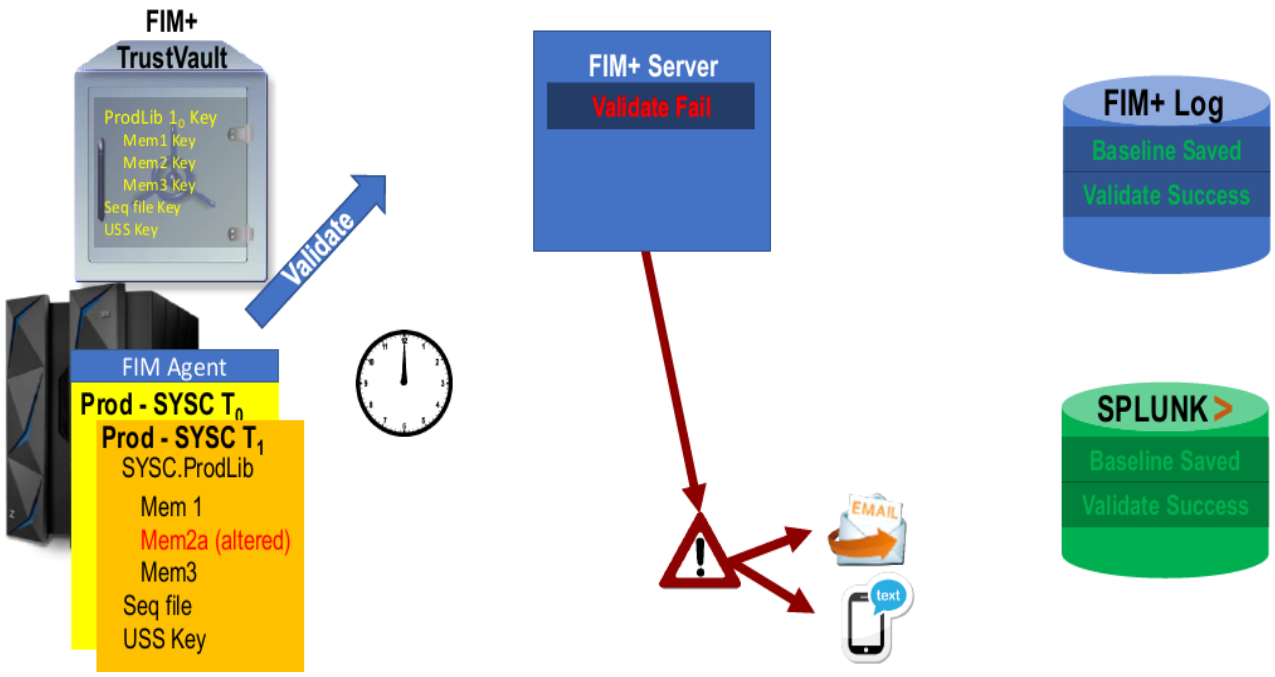


Figure 2: Change detected

- 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 analyzed 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 e-mail to an admin or a central console. they can quickly drill down to forensic info

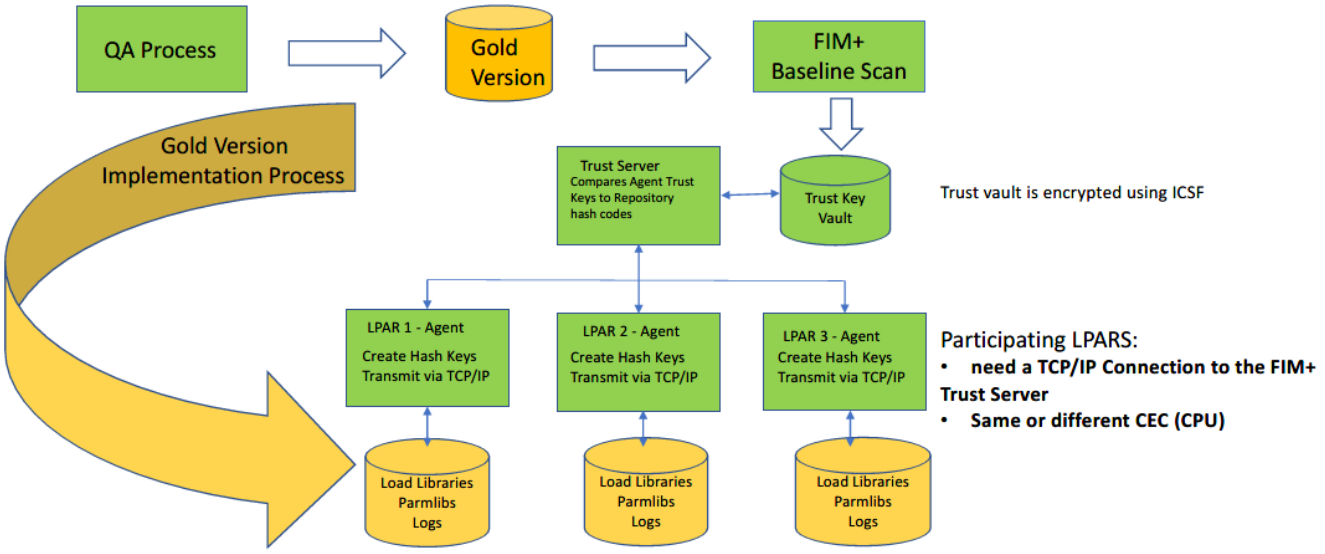


Figure 3: Integrity management

(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.

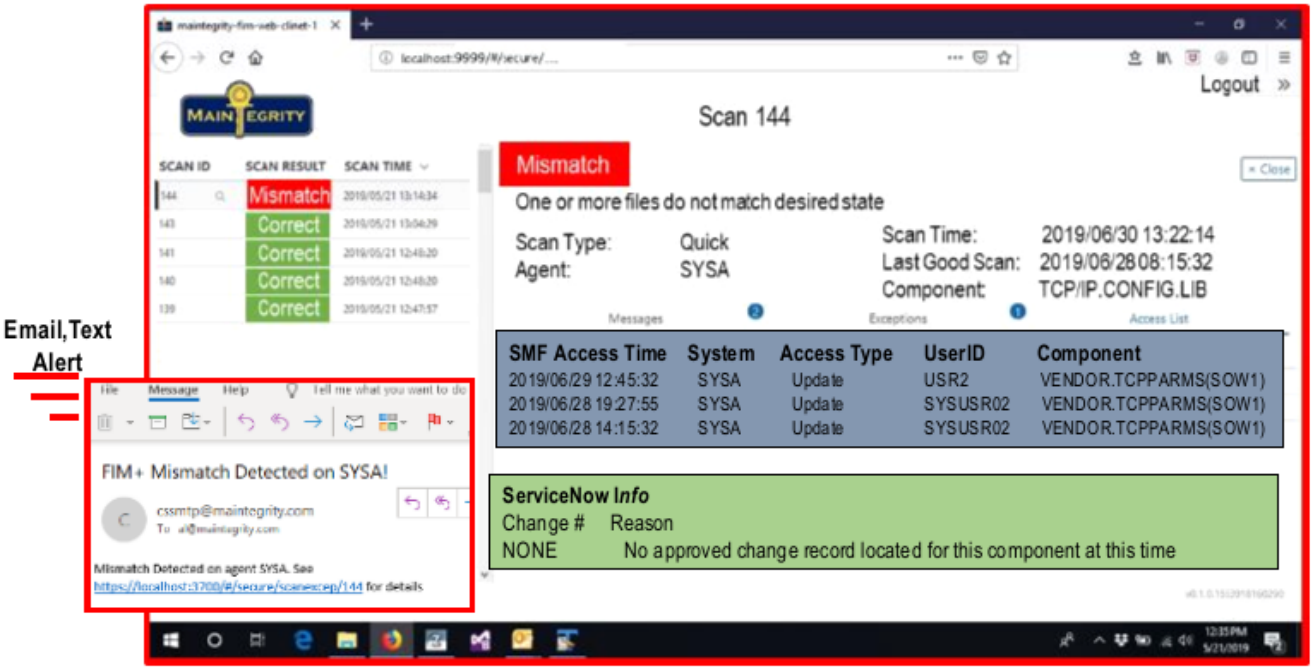


Figure 4: Human interface

- 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 had received a text or e-mail, 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 Gary Euler and Al Saurette's presentation is available for download from the Virtual IMS user group Web site at itech-ed.com/ virtualims/presentations/ FIM+Dec19.pdf.

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

Meeting dates

The following meeting dates have been arranged for the Virtual CICS user group providing we find a sponsor for 2020:

- On 7 April 2020, Radek Mrvec, Principal Software

Engineer at Broadcom will be discussing “Java and SQL in IMS for z/OS Applications”.

- The following meeting will be on 9 June 2020, when Haley Fung, Senior Software Engineer / Technical Lead at IBM will be discussing “4 Paths to Digital Transformation”.

Recent IMS articles

IMS 15 Member Online Change enhancement: OPTION(BLDPSBNO) by Hiroaki Katahira on z Systems Developer Community (20 February 2020). You can find the article at https://developer.ibm.com/zsystems/2020/02/20/ims-15-member-online-change-enhancement-optionbldpsbno/

How a CM1 SL0 Input Message Sent to IMS Connect Works by Subhasish Sarkar on Destination z (13 November 2019). You can find the article at https://destinationz.org/Mainframe-Solution/Application-Development/CM1-SL0-Input-Message-Sent-to-IMS-Connect

*5 IMS OTMA Enhancements You Don’t Want to Miss b*y Jack Yuan and Eric Su in IBM Systems Magazine (13 November 2019). You can find the article at https://ibmsystemsmag.com/IBM-Z/11/2019/5-ims-otma-enhancements

IMS 15 Managed ACB Enhancement: OPTION(NOCHECK) to IMPORT DEFN SOURCE(CATALOG) by Ken Nguyen on z Systems Developer Community (10 October 2019). You can find the article at https://developer.ibm.com/zsystems/2019/10/10/ims-15-managed-acb-enhancement-optionnocheck-to-import-defn-sourcecatalog/

Arcati Mainframe Yearbook

The brand new Arcati Mainframe Yearbook is now available. It includes an annual user survey, an up-to-date directory of vendors and consultants, a resources guide, a strategy section with papers on mainframe trends and directions, a glossary of terminology, and a mainframe evolution section.

Go to https://www.arcati.com/newyearbook20 to visit the download page. The Yearbook is available in PDF format and is completely FREE.

Our new website

itech-ed.com/virtualims

About the Virtual IMS user group

The Virtual IMS user group was established as a way for individuals using IBM’s IMS hierarchical database and transaction processing systems to exchange information, learn new techniques, and advance their skills with the product

The Web site at https://itech-ed.com/virtualims 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 IMS practitioners. Anyone with an interest in IMS is welcome to join the Virtual IMS user group and share in the knowledge exchange.

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

The Virtual IMS user group is free to its members.