



## GSE UK Security Working Group – Next Meeting

We are pleased to confirm that the next meeting of the GSE UK Security Working Group, is scheduled as follows:

<b>Date</b>	Thursday 7th July 2022, 10:00 – 17:00 BST (Please note the time zone! The meeting is being run from the UK)
<b>Venue</b>	Via Zoom
<b>Registration</b>	<a href="#">Click here</a>
<b>CPE/CPD hours</b>	Up to a maximum of 6 hours (full attendance required to claim maximum number of hours)

This meeting is suitable for anyone with an interest in Mainframe Security, including Mainframe Security Professionals (newbies to experienced), Cyber Security Specialists, System Programmers, Auditors and Managers. Attending this meeting will grow your professional skills and knowledge in the following areas:

- Latest security innovations from vendors and how they help enhance security for your organisation
- Current threats, trends, including regulatory and compliance updates to help you prioritise security and compliance efforts
- Share problems, knowledge, best practices with working group members
- Give feedback to vendors on their offerings, including product direction
- Earn CPE/CPD hours to support maintenance of certifications or an education portfolio

Please [read on for the agenda](#) line up.

**Jamie Pease CISA, CISM, CDPSE, CISSP, CITP, MBCS**  
Chairman of the GSE UK Security Working Group

## Agenda

**Please note:** There will be a 15-minute gap between most of the sessions to allow for switchover to the next presenter. Agenda and timings are subject to change.

Start	End	Topic	Who
10:00	10:30	<p><b>Introduction from the Working Group Chair</b></p> <p>Kickoff session for the meeting, where the Chair will provide an update on working group business and news from the GSE UK Region, such as the annual conference.</p>	<p><b>Jamie Pease</b> (Working Group Chair)</p>
10:30	11:15	<p><b>Changes to Security in CICS TS 6.1 – Simplification and Compliance</b></p> <p>CICS TS 6.1 contains a large number of enhancements to simplify and improve security in CICS. The following are some of those that will be covered.</p> <p>Auditing of CICS can be a time consuming exercise for customers. The CICS TS 6.1 release has new capability to simplify this data collection.</p> <p>It also works with the new z Security and Compliance Center. The presentation will cover these changes, and associate changes in region tagging and new z/OS Health Checks which will make audits a faster and less painful process.</p> <p>Upgrading to new releases of CICS has always involved the time consuming definitions of CAT 1 transactions to security. An enhancement has been made making this unnecessary and more secure at the same time. This should reduce the time taken to upgrade CICS TS.</p> <p>To help application architects and junior system programmers navigate the complexities of security we have been restructuring the security documentation with educational material about how security works in CICS accompanied by design and configuration examples.</p> <p>There are also a number of enhancements to TLS including support for TLS 1.3. We are also providing new monitoring and stats to enable a simpler and safer upgrade to new TLS levels. These cover both CICS configured TLS and AT-TLS.</p>	<p><b>Colin Penfold</b> (IBM UK)</p>

11:15	11:30	<b>Break while we switchover presenter</b>	<b>All</b>
11:30	12:00	<p><b>Simplifying the Diagnosis of CICS TS related security problems</b></p> <p>Whilst the ICH408I and DFHXS1111 messages can diagnose some problems, they were designed at a time when problems were mainly 3270 based. Diagnosing more complex problems can stretch even senior system programmers.</p> <p>CICS TS 6.1 provides a number of enhancements simplifying the diagnosis of security problems which will be covered in this presentation.</p> <p>For some problems we have new messages which will enable more junior system programmers to diagnose a problem quickly. For more difficult to diagnose security problems, which often take many weeks to diagnose, we have a new diagnosis facility call security request recording (SRR). This is designed to help system programmers to diagnose complex multi-task sysplex wide CICS security problems, regardless of the security manager, even in production.</p> <p>The presentation will include a demo of how the SRR can be used by the help desk or a system programmer and how to diagnose problems using it's easy to use output.</p>	<b>Lewis James</b> (IBM UK)
12:00	12:45	<b>Lunch Break</b>	<b>All</b>
12:45	13:30	<p><b>How to Start your move to Zero Trust</b></p> <p>Today, as the mainframe enjoys renewed interest and priority around Hybrid IT, it also results in increased connectivity and risk exposure previously unheard of on the mainframe. This, in an ever increasing threat environment, has brought about a drive to achieving Zero Trust across the enterprise. In this session, we will outline an achievable approach to starting your journey to Zero Trust, while also modernizing your mainframe security. Not only will this result in your zero trust journey but it will also reduce exposures and audit failures.</p>	<b>Chip Mason</b> (Broadcom)
13:30	13:45	<b>Break while we switchover presenter</b>	<b>All</b>

13:45	14:30	<p><b>Hints &amp; Tips</b></p> <p>Do you have any questions, ideas, conundrums you would like to share with the group? This 'all hands' session is your opportunity to tap into a wealth of expertise! It could be a technical question, or maybe you are interested to know who has implemented a specific change and what were the challenges.</p> <p>This is a session for everyone to participate, so please come prepared with those questions.</p>	<b>All</b>
14:30	14:45	<b>Break while we switchover presenter</b>	<b>All</b>
14:45	15:45	<p><b>Detecting Changes in the RACF Database</b></p> <p>Tracking changes is an inherent part of z/OS Configuration Management, typically applied against System Datasets and Libraries with the added goal of providing reliable backups that can be used for auditing and recovery purposes. These Dataset and Library targets lend themselves to conventional processing as their records and formats are well defined and understood. We simply read them, process them and store copies with the goal of detecting changes. From this, reports and notifications follow.</p> <p>But what about other sources of configuration data that don't fit into this convenient, conventional processing model. For example, the RACF Database whose structure is anything but consistent across its major data elements – Classes, Profiles, Certificates. In this presentation and demonstration, using an innovative browser application, these elements will be extracted from the database in real-time, baselined with HASHed snapshots taken. Changes will be introduced to each element and subsequently the updated database will be compared against the snapshots to detect the changes and prepare an audit report all within the browser.</p>	<b>Paul Robichaux</b> (NewEra Software)
15:45	16:00	<b>Break while we switchover presenter</b>	<b>All</b>
16:00	17:00	<p><b>Reducing the use of UID(0)</b></p> <p>A look at tightening security by reducing the use of UID(0). I will cover a few mechanisms to find tasks that are running with UID(0) and show some of my recent findings. I will cover various tasks that need UID(0) and several that don't. I will also examine ways of keeping track of UID(0) use.</p>	<b>Lennie Dymoke-Bradshaw</b> (Independent Consultant)
17:00		<b>End of meeting</b>	



## About the speakers

### Chip Mason

Chip Mason has over 20 years of experience in the software industry. Chip leads strategy and product definition for Mainframe Security products in CA Broadcom. In this capacity, Chip works to guide integration and product development toward delivering valuable Security solutions, as well as acting as a subject matter expert assisting customers to ensure security and compliance. Chip has experience across many areas of Enterprise IT, including Security Management, Software Development, Service Management, and Event Management. Chip is certified in Scaled Agile Framework, ITIL, and is a Certified Information Systems Security Professional (CISSP).

Chip resides in Raleigh, NC where he enjoys his family and photography.

### Paul R. Robichaux

Paul is CEO and co-founder of NewEra Software, Inc. He served as the Chief Financial Officer of Boole and Babbage for the ten years immediately preceding his co-founding of NewEra in 1990. He holds a BS in Accounting and a Masters in Business Administration from a Louisiana State University, is a Certified Public Accountant and a frequent speaker at industry events. The corporate mission of NewEra Software is to provide software solutions that help users avoid z/OS noncompliance, make corrections when needed and in doing so, continuously improve z/OS integrity and Security.

**Future GSE UK Security meetings for your calendar**

More details of our schedule, including other events from the GSE UK Region can be found here: <https://www.gse.org.uk/events/>