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:

Date	Thursday 29th June 2023, 09:00 – 17:00 BST (Please note the time zone! The meeting is being run from the UK)
Venue	This is a hybrid meeting – you can attend in person or via Zoom. BMC Winnersh, 1020 Eskdale Road, 2nd Floor, Winnersh, RG41 5TS (click here for location map)
Registration	Click here
CPE/CPD hours	Up to a maximum of 7 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

Start	End	Topic	Who
09:00	10:00	**Welcome from our host, BMC Software** Kickoff welcome session and presentation from our host.	**David Lea** (BMC Software)
10:00	10:45	**Network Encryption Performance** There are many cryptographic dimensions that can impact the quality of the Network Encryption on IBM zSystems and LinuxONE platform. We have now all required technologies to help to measure and to understand impacts of cryptographic dimensions on both performance and security of the network encryption. The speaker will remind cryptographic dimensions and their impacts, share best practices, and explain how to achieve both security and performance objectives together.	**Guillaume Hoareau** (IBM)
10:45	11:00	**Coffee Break**	**All**
11:00	12:00	**What does a Zero Trust strategy mean to CICS** Zero trust isn't something you can buy or implement. It's a philosophy and a strategy. This presentation will show the features available in CICS TS which can help you with your Zero Trust strategy. The presentation will concentrate on a key principal of enabling the right user, to have the right access, to the right data, for the right reasons. It will cover the new content available in the CICS TS open beta, as well as some of the compliance enhancements in CICS TS 6.1.	**Colin Penfold** (IBM)
12:00	12:45	**Lunch Break**	**All**

12:45	13:15	**Hints & Tips** 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. This is a session for everyone to participate, so please come prepared with those questions.	**All, chaired by David Lea**
13:15	14:15	**Crypto Performance Update** This session will review the crypto speeds and feeds for IBM's z16 crypto hardware, including both the CPACF (internal to the CEC) and the new Crypto Express8S cards as reported in the latest IBM Benchmarks. We'll also talk about the performance reports that are available for crypto.	**Greg Boyd** (IBM)
14:15	14:45	**Afternoon tea and networking**	**All**
14:45	15:45	**Network Security Assessment with zERT** zERT aggregation is helpful to drive Network Security Assessment on z/OS. The generation of the SMF119-12 is very interesting and can be a masterpiece of the IBM zSystems security. Speaker to explain what we can do with SMF119-12 and how to perform a technical study to assess quality and quantity of network sessions flowing through z/OS environments, and how to connect this SMF119-12 with the rest of existing enterprise security functions (Dashboard, SIEM, Loghost …).	**Guillaume Hoareau** (IBM)
15:45	16:00	**Break while we switchover presenter**	**All**

16:00	17:00	**Understanding Mainframe Integrity Vulnerabilities** The integrity of mainframe data and software is critical in fundamentally securing your business. Understanding operating system integrity is a critical component of mainframe security strategies. It isn't just about user authentication and authorization. IBM's commitment to system integrity is one of the major reasons that z/OS is such a secure platform. z/OS, as well as the big three external security managers, (CA ACF2, CA Top Secret, and IBM's RACF), all rely on system integrity to function properly. An appropriate analogy for not having system integrity is like locking the front door to your house but leaving your windows open. Key takeaways include: • What is a Mainframe Integrity Vulnerability? • Why Should I Care About System Integrity? • What responsibilities do I have for my z/OS system with regards to integrity? • What is an IV based exploit? • What Can I Do About These IV's and Exploits?	**Ray Overby** (Rocket Software)
17:00		**End of meeting**	

Agenda and timings are subject to change.

About the speakers

Ray Overby, Technical Director, Rocket Software

Ray Overby is currently a Technical Director at Rocket Software, focusing on security strategies as it pertains to Modernizing the Mainframe. Ray was the CTO & Co-Founder of Key Resources, Inc., (KRI), purchased by Rocket Software in February of 2023. KRI was a security services and software development company specializing in mainframe security. Mr. Overby founded KRI in 1988. He has 40+ years of experience in IT security, including 8 years as a developer at SKK, Inc., specializing in CA ACF2 internals.

Mr. Overby continues to provide consulting services to Fortune 500 institutions focusing on configuration-based compliance audits, comprehensive z/OS pen tests and integrity vulnerability assessments, as well as mainframe security best practices.
Mr. Overby presents at SHARE, ISACA, numerous IT security conferences, security user group meetings, and RACF user group meetings. His focus continued to be on Mainframe Modernization, z/OS ethical hacking and mainframe vulnerability management. He has been published in z/Journal, HealthIT, TechTarget, InfoSecurity Magazine, CyberDefense Magazine, CIO Magazine, eWeek, InformationWeek, and IBM Enterprise Magazine.

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/