GSE UK Enterprise Security Working Group – Next Meeting

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

Date	Thursday 11th June 2020, 09:00 – 17:15 BST (Please note the time zone as the meeting is being run from the UK)
Venue	Due to the current situation with COVID-19, we are hosting this meeting via Webex only
Registration	Click here
CPE 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 knowledge and skills 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 CPEs (continuing professional education) to support maintenance of certifications, such as CISA, CISM, CISSP, CRISC

Please read on for the agenda line up.

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

Agenda

Please note: As all presenters will be working remotely, there will be a 10-minute gap between some sessions to allow for switchover to the next presenter. Agenda and timings are subject to change.

Start	End	Topic	Who
09:00	09:15	**Introduction from the Working Group Chairman** • Membership • GSE UK Conference 2020 & other Security events • CPEs • Future topics & venue • Feedback	**Jamie Pease** (Working Group Chairman)
09:15	10:15	**IoT & BYOD – The new security risks** In a world ever more connected to the internet, Security should be paramount. However, to keep pace with the new trends and technologies, companies and individuals, overlook the importance of security and the risks this poses. In this session we will be discussing the Internet of Things (IoT) and the concept of Bring Your Own Device (BYOD) and the security challenges and risks they can be to companies, systems, and ultimately to the mainframe.	**Mark Wilson** (RSM Partners)
10:15	10:25	**Break while we switchover presenter**	All

10:25	11:25	**ACF2 - A horse of a different colour** ACF2 demystified for people conversant in RACF! The presentation covers: • How ACF2 configuration differs from RACF • ACF2 power users and how they differ from RACF • ACF2 user definitions in RACF terms • Rules – explanation of how access is authorised • Activating classes in ACF2	**Ciara O'Connor** (RSM Partners)
11:25	11:35	**Break while we switchover presenter**	All
11:35	12:30	**The journey of two Mainframe Security Trainees** In this session, Beth and James from Lloyds Banking Group will share their experiences of entering the world of Mainframe as trainees and pursuing a career in Mainframe Security.	**Beth Newman-Jones and James King** (Lloyds Banking Group)
12:30	13:00	**Lunch Break**	All
13:00	13:30	**Mainframe Hacker Society – Defeating IBM's Attempt To Detect Privilege Escalation** In response to the well documented privilege escalation attacks against RACF/ACF2/TSS using an APF authorized Library, IBM recently released a new detection capability called ACEECHK to monitor users' privileges to alert the administrators if a low-level user managed to gain special and operations privileges. This novel detection capability was designed to give administrators the peace of mind that attacks they were seeing would be quickly mitigated through immediate notification. Unfortunately, ACEECHK fails to track and detect some critical components of users' privileges which enable a cautious hacker to continue executing privilege escalation attacks while staying far below IBM's radar. Attendees will gain a stronger understanding of IBM's new ACEECHK functionality and how attackers can bypass this new check.	**Chris Perry** (BMC)
13:30	13:40	**Break while we switchover presenter**	All

13:40	14:40	**Mainframes and the Moon** Few events in history caught the imagination of the world as did the first manned lunar landing in 1969. This session celebrates the 50th anniversary of that event and highlights the work done by IBM Mainframes in support of manned space program. Few events in history caught the imagination of the world as did the first manned lunar landing in 1969. This session celebrates the 50th anniversary of that event and highlights the work done by IBM Mainframes in support of manned space program. Few events in history caught the imagination of the world as did the first manned lunar landing in 1969. This session celebrates the 50th anniversary of that event and highlights the work done by IBM Mainframes in support of manned space program. In this session, Mark will tell the story of the role played by IBM Mainframes in the greatest technical achievement in the history of mankind.	**Mark Nelson** (IBM)
14:40	14:50	**Break while we switchover presenter**	All
14:50	15:50	**The importance of the z/OS Mainframe System Security Plan (SSP)** Cybersecurity is one of the most important concerns within the IT world. Auditors audit to the written policy and documentation of an organization. Too many organizations lack a z/OS mainframe System Security Plan (NIST Control PL-2) where the organization has formally documented: all standard controls (PCI, HiTrust, NIST, GDPR, PII, HIPAA), how those controls are implemented, standard definitions involving least privileged, authorized roles of users, authorized access for those standardized roles, and how other policy based controls are implemented within their Mainframe platform. Ask yourself: Where are all of the mainframe cybersecurity controls documented? If your organization has PCI, NIST, GDPR and other regulatory requirements - how have you documented the implementation within the Mainframe for each of those Controls? Where are your organization's Mainframe Platform Roles defined and allowed access for each role? Organizations with a Mainframe System Security Plan (SSP) have a documented roadmap from regulations to actual cybersecurity controls are implemented, how continuous monitoring is performed, how least privileged access is implemented, and how to review and audit (internal and external) and such.	**Steve Hosie** (Broadcom)
15:50	16:00	**Break while we switchover presenter**	All
16:00	17:15	**What keyring? What certificates? All I know is TLS doesn't work!** This session will cover the basic set up on keyring and certificates and the steps to figure out the problem.	**Wai Choi** (IBM)

17:15		**End of meeting**	

Future GSE UK Security meetings for your calendar

More details of our schedule can be found here: https://www.gse.org.uk/events/