Mark Wilson

Senior Director Consulting Services

The role of the systems programmer in protecting the mainframe from an accidental or malicious event

1

Agenda

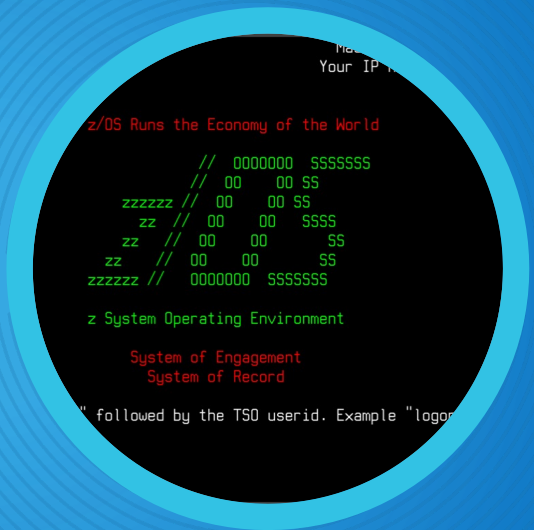
- Introductions
- The role of the sysprog
- What's missing
- What's going on in the real world
- What does this mean for us?
- My thoughts on the role of the modern day sysprog
- Questions

2

My Own Journey - Introduction

3

The Role of the Systems Programmer



4

What's a System Programmer?

- This is from an actual IBM Webiste: https://www.ibm.com/docs/en/zos-basic-skills?topic=world-who-is-system-programmer
- In a mainframe IT organization, the system programmer (or systems programmer) plays a central role
  - The system programmer installs, customizes, and maintains the operating system, and installs or upgrades products that run on the system
  - The system programmer might be presented with the latest version of the operating system to upgrade the existing systems. Or, the installation might be as simple as upgrading a single program, such as a sort application

5

What's a System Programmer?

- The system programmer performs such tasks as the following:
  - Planning hardware and software system upgrades and changes in configuration
  - Training system operators and application programmers
  - Automating operations
  - Capacity planning
  - Running installation jobs and scripts
  - Performing installation-specific customization tasks
  - Integration-testing the new products with existing applications and user procedures
  - System-wide performance tuning to meet required levels of service

6

What Do Sysprogs Really Do?

7

WHAT'S MISSING

8

9

9

Why?

10

10

What's going on in the world?

11

There is a lot going on

REGISTER NOW!

Call for Everything

Con Calendar

Room Reg Link

Official Swag

Speaker Index

Laura Abbott
Sylvain Afchain
Agent X
Austin Allshouse
Rick Altherr

Jacob Baines
Tomer Bar
Rotem Bar
Sylvain Baubeau

Crossover Episode: The Real-Life Story of the First Mainframe Container Breakout

45 minutes | Demo

Ian Coldwater Hacker
Chad Rikansrud (Bigendian Smalls) Hacker

Speaker(s) will be at DEF CON!

You've seen talks about container hacking. You've seen talks about mainframe hacking. But how often do you see them together? IBM decided to put containers on a mainframe, so a container hacker and a mainframe hacker decided to join forces and hack it. We became the first people on the planet to escape a container on a mainframe, and we're going to show you how.

Containers on a mainframe? For real. IBM zCX is a Docker environment running on a custom Linux hypervisor built atop z/OS - IBM's mainframe operating system. Building this platform introduces mainframe environments to a new generation of cloud-native developers- and introduces new attack surfaces that weren't there before.

In this crossover episode, we're going to talk about how two people with two very particular sets of skills went about breaking zCX in both directions, escaping containers into the mainframe host and spilling the secrets of the container implementation from the mainframe side.

When two very different technologies get combined for the first time, the result is new shells nobody's ever popped before.

REFERENCES: Getting started with z/OS Container Extensions and Docker: https://www.redbooks.ibm.com/abstracts/sg248457.html
The Path Less Traveled: Abusing Kubernetes Defaults: https://www.youtube.com/watch?v=HmoVSmTIOxM
Attacking and Defending Kubernetes Clusters: A Guided Tour: https://securekubernetes.com
Evil Mainframe penetration testing course :https://www.evilmainframe.com/
z/OS Unix System Services (USS): https://www.ibm.com/docs/en/zos/2.1.0?topic=system-basics-zos-unix-file
z/OS Concepts: https://www.ibm.com/docs/en/zos-basic-skills?topic=zc-zos-operating-system-providing-virtual-environments-since-1960s
Docker overview: https://docs.docker.com/get-started/overview/

• zOSFTPlib - python ftplib-like library specifically for Z/OS

12

Couldn't happen to me/us.. Really??

What if...

13

What's being done to help?

14

What's being done to help?

- Hardware
  - DELL/EMC
  - IBM
  - Others TBC
- Software
  - Maintegrity
  - KRI
  - BMC
  - IBM
  - Several Others

15

Hardware – What's Needed?

- Surgical recovery capability
  - Provide the ability to selectively restore a portion of data as required to repair only what was corrupted (example: one CKD volume, dataset/database)
- Catastrophic recovery capability
  - Providing a valid recovery point after an attack to restore 100% of the data
- Forensic analysis capability
  - Provide for inspection and determination to find a “known good state of data”
- Data validation capability
  - Provide a methodology for restoring data to the desired known good state

16

16

Hardware – Who's Doing What?

Dell Cyber Data Protection for mainframe data

- Dell EMC space-efficient snap innovation fortifies data protection against cyber attacks while minimizing recovery time and recovery capacity Dell EMC storage uses two-actor security and zDP definition persistence for system security and integrity.
- https://www.delltechnologies.com/en-gb/storage/mainframe.htm#tab0=0

- IBM z Cyber Vault
  - Reduce the time to recovery from days to minutes, by implementing a Data Corruption Protection solution as part of your D/R strategy
  - https://mediacenter.ibm.com/media/+IBM+Z+Cyber+Vault+Technical+Introduction/1_ug97n0p3
  - https://www.redbooks.ibm.com/abstracts/redp5506.html?Open

17

Software – Who's Doing What?

- Maintegrity
  - File Integrity Monitoring
  - https://www.maintegrity.com/
- KRI
  - Software Vulnerability Scanning
  - https://www.krisecurity.com/vulnerability-analysis/
- New Era Software
  - https://www.newera-info.com/

- BMC
  - Realtime Mainframe Threat Detection
  - https://www.bmc.com/it-solutions/bmc-ami-defender.html
- IBM
  - Security Admin & Reporting
  - https://www.ibm.com/products/zsecure-admin
- Many others
  - Vanguard, Beta Systems, Precisely, Broadcom, etc

18

What does it mean for us as Sysprogs?

19

What does it mean for us Sysprogs?

20

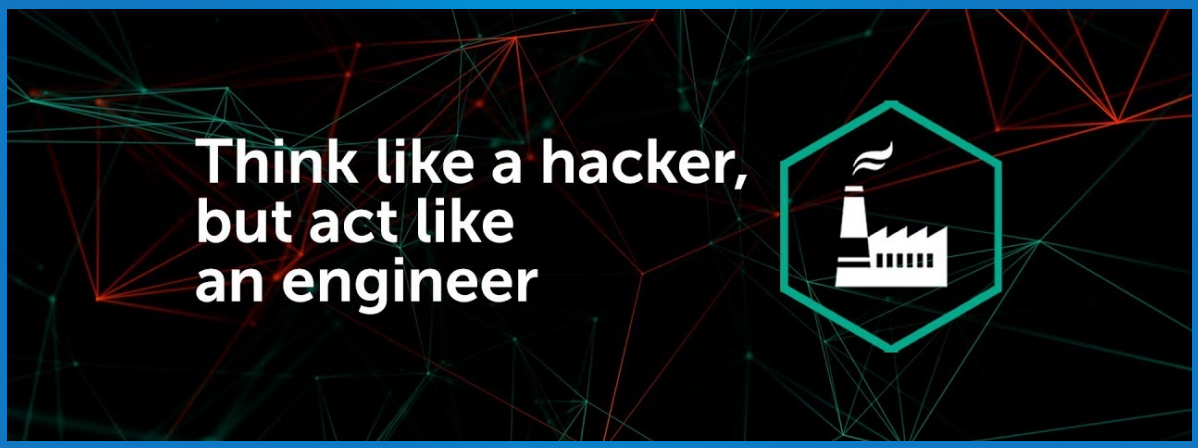
20

What does it mean for us as Sysprogs?

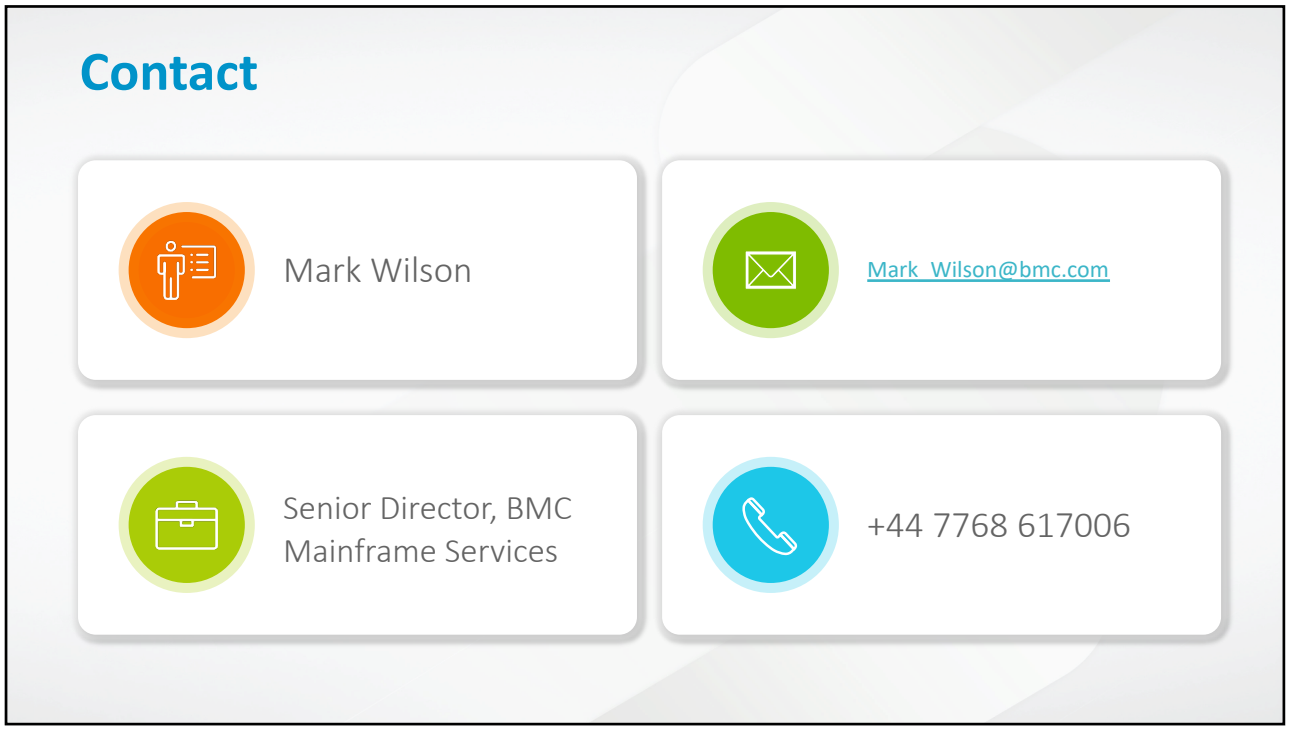
- Change our thinking
  - Its not always about APF or Security Privileges (Special, Operations, NON-CNCL, etc)
  - What about USS, FTP, SSH?
  - OMG what about containers on z and zLinux?
- Get involved and take ownership

My thoughts on the role of a modern day sysprog

The role of a modern day sysprog



Questions


Contact
Mark Wilson
Mark_Wilson@bmc.com
Senior Director, BMC Mainframe Services
+44 7768 617006

25


bmc
Customer Experience
26

26