Who's REALLY in Charge of your Mainframe Security?

Agenda

- Who is Julie-Ann Williams?
- z/OS Security
  - A little bit of history
  - Users
  - Stuff
  - Auditing
- So what's the problem?
  - Internal, product security
  - Exits
  - ISVs
    - Security bypasses
    - Advice
    - Additional functionality
- Conclusion

millennia...

Who is Julie-Ann Williams?

- 30 years in IBM Mainframes
- MVS Systems Programmer
  - with Security bias
- Author
  - CICS Essentials
  - z/Auditing Essentials
  - ISV Tech Docs
- Helping Customers to exploit bleeding edge technology on their IBM mainframes

millennia...

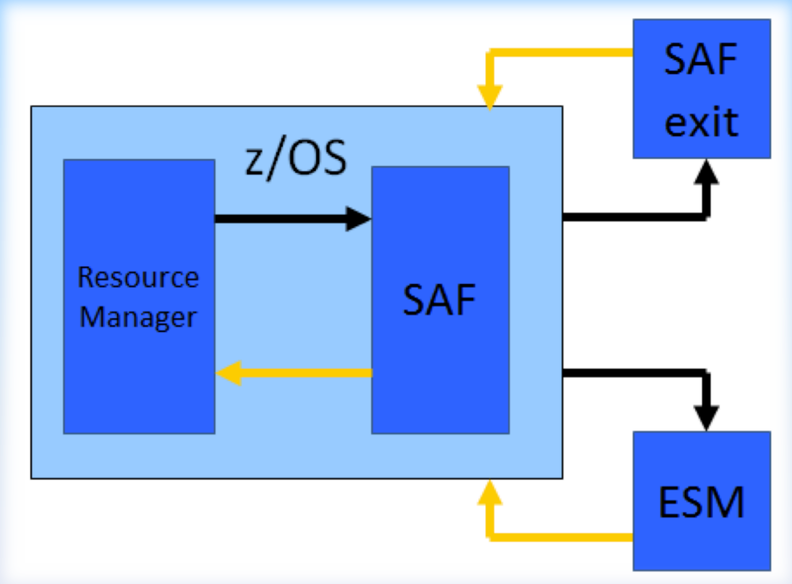
Who is Julie-Ann Williams?

- Life outside of work...
  - Kat 3 was a wedge-shaped robot with a pneumatic axe
  - We competed in Series 2-7 of Robot Wars
  - We were extremely proud to win the **Series 6 Sportsmanship Award**
  - Originally a double wedge with an overhead axe, the design was changed radically for the 6th series

millennia...

z/OS Security

- SAF (System Authorization Facility)
  - CA ACF2
  - CA Top Secret
  - RACF



millennia...

A Little Bit of History

- First mainframes as we recognise them today available from 1964
- There was no Internet to connect to!
- The concept of Data Security didn’t even occur to anyone until 1972!
- Barry Schrager
  - The Father of Data Security
  - University of Illinois
  - Systems “hacked” by students
  - Took those memories and skills into Mainframe World
  - SHARE VS/OS Security and Data Management Project
  - Wrote ACF2

A Little Bit of History

- z/OS is the most Securable Platform commercially available

- Most Important piece of enterprise software!
  - Without being able to guarantee system integrity nothing can be trusted
  - Without data security there can be no confidence in that data
  - Without authentication there is no way to control access

- Over reliance on defaults and lack of applied knowledge can leave the platform as open to “Hacker Attacks” as any other

millennia...

A Little Bit of History

- Cybersecurity
  - The state of being protected against the criminal or unauthorised use of electronic data, or the measures taken to achieve this

- Make sure “People” are who they say they are
  - Authentication
- Protect “Stuff” from “People”
  - Authorisation

millennia...

Users

- “People”
  - Not always a Carbon Based Life-Form
  - But mostly, real people

- Authentication
  - How can I know that you are who you say you are?

Something you have	e.g. Token
Something you know	e.g. Password
Something you are	e.g. finger print

  - Can I trust someone/thing else to vouch for you?

Stuff

- “Stuff”
  - Everything that isn’t “People”!
    - Data files
    - CICS transactions
    - Programs
    - Printers
    - etc

- Authorisation
  - Are you allowed to use that “Stuff”?

millennia...

Auditing

- Which “People” did what to your “Stuff” and when?

- Legislation
  - SAS 7.0
  - SOX
  - etc

- Internal vs External Audits

millennia...

So What’s the Problem?

- Internal, product security
  - e.g. DB2, Automation, MQ etc
  - Leaves non Security Specialist staff administering Security

?

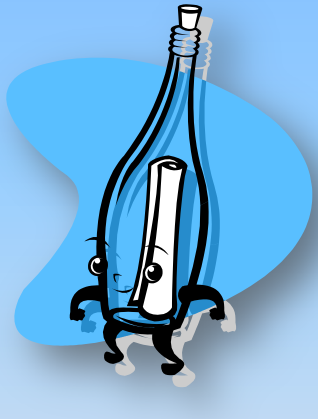
So What's the Problem?

- DB2
  - Not still using internal security are you?
  - Who's making your security policy decisions?
  - What's actually happening at the coal-face?
    - Are you doing the house-keeping?
    - Checking for 'alternate' routes to the data?
    - Are you tracking those accesses?
  - DB2 v10 introduced separation of admin rights from data access rights. At last!
  - DB2 v11 current GA version

millennia...

So What's the Problem?

- Automation
  - Are you using your ESM?
  - Are you sure?
    - What is being granted using default access levels?
  - Are you logging access to system critical infrastructure?
    - And not just failures!
    - By the automation product as well as the carbon based life forms?
      - Authority levels can be huge!



- MQ
  - Who's making your security policy decisions?
  - Do you know what/who is at the other end?
  - Can you prove it?

millennia...

So What's the Problem?

- Monitoring Tools
  - You are using your ESM to control access to **and** within aren't you?
  - Who's making your security policy decisions?

- USS
  - What / Who is in charge securing of all those USS and z/OS information highways?
    - Who is performing "Border Control"?
  - Who's making the decisions inside USS land?
  - Can you prove it?

- Workload Schedulers
  - Not still using internal security are you?
  - Not still using just the one userid for all batch are you?
    - What else can get done under its authority?
  - When was the last time you audited successes not failures?

millennia...

So What's the Problem?

- Home-grown utilities and applications
  - I bet you've all got one or two lurking around!
  - Are you protecting them?
  - Can you prove it?
  - Has the security been vetted?

millennia...

So What's the Problem?

- The Solution
  - Migrate all security to external implementation
  - controlled by ACF2, RACF or Top Secret

- Security Administration should always be done by Specialists

- Teach teams to be proactive and engage with the security team early
  - Needs to be a 2 way street!

millennia...

So What's the Problem?

- Exits
  - Often implemented for historic reasons
  - Often not understood by current staff
    - Written in Assembler with very rigid coding requirements

- The Solution
  - Review all exits regularly
  - Remove them where practical

- ACF2/RACF/Top Secret should be free to make security decisions

So What’s the Problem?

- ISVs
  - Security bypasses vs Performance options
  - Advice
  - Additional functionality
  - One last thing...

IBM®

MACRO4

bmcsoftware

VANGUARD
Integrity Professionals
Information Security Experts

EMC²

ca® technologies

INNOVATION® DATA PROCESSING

So What's the Problem?

- Polite suggestions to ALL software vendors
  - It's time to embrace the new security paradigm your customers have to work to
    - Assume they want/have to use an ESM
    - Don't provide samples of how to bypass controls
    - Do provide examples of how employ secure auditable controls
    - Separate Admin functions from user functions.
    - Separation of duties is the name of the game.
  - Yes UID(0) may fix it but it causes negative audit findings.
    - Please use the appropriate facilities.
  - Thank you ☺

- How safe are your dumps/debugging materials?

millennia...

So What’s the Problem?

- The Solution
  - Review all security requirements for new AND existing ISV products
  - Implement external security and switch internal security off

- ACF2/RACF/Top Secret should be free to make security decisions

millennia...

Conclusion

- Security should be controlled by Security
- Security Administration should always be done by Specialists
- Teach teams to be proactive and engage with the security team early
- ACF2/RACF/Top Secret should be free to make security decisions
- This is not always the case
- Check what happens at your site...

millennia...

Thank You

xxx

J

julie@sysprog.co.uk

07770 415102

millennia...