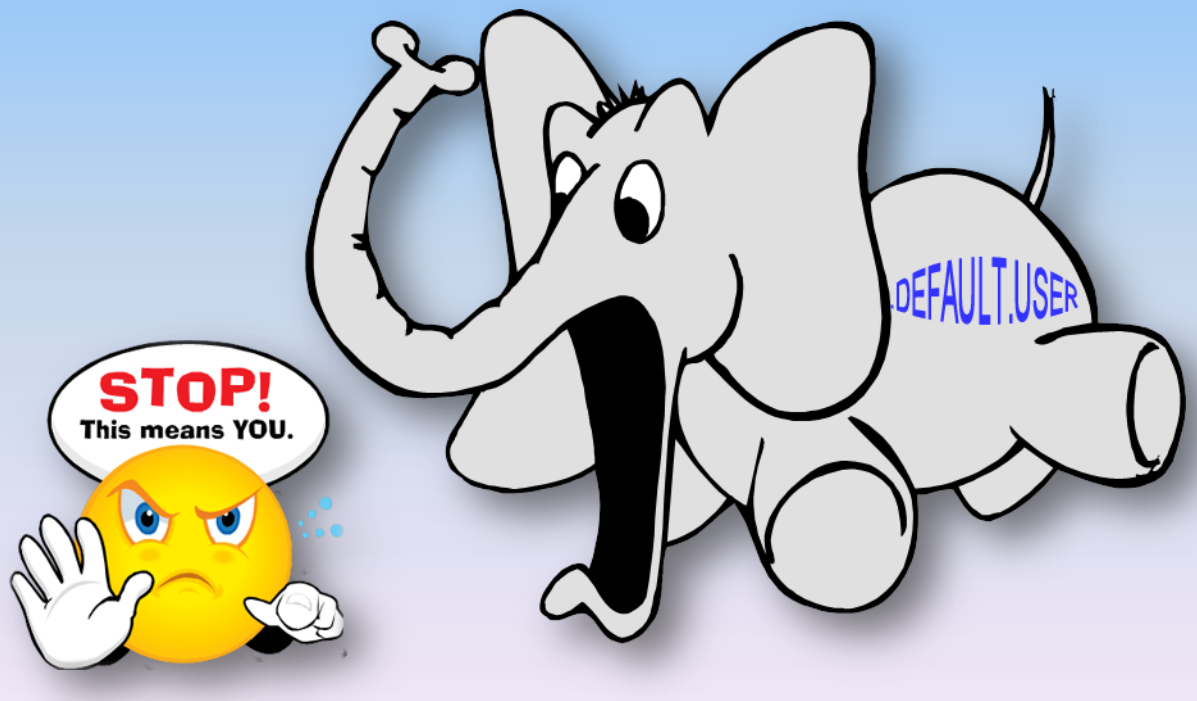
Is USS the Elephant in the Room?



Agenda

- USS – deprecation of BPX.DEFAULT.USER
  - What's the problem?
  - How did we get here?
  - What needs to be done to fix it?
- Q & A Session

millennia...

What is the Problem?

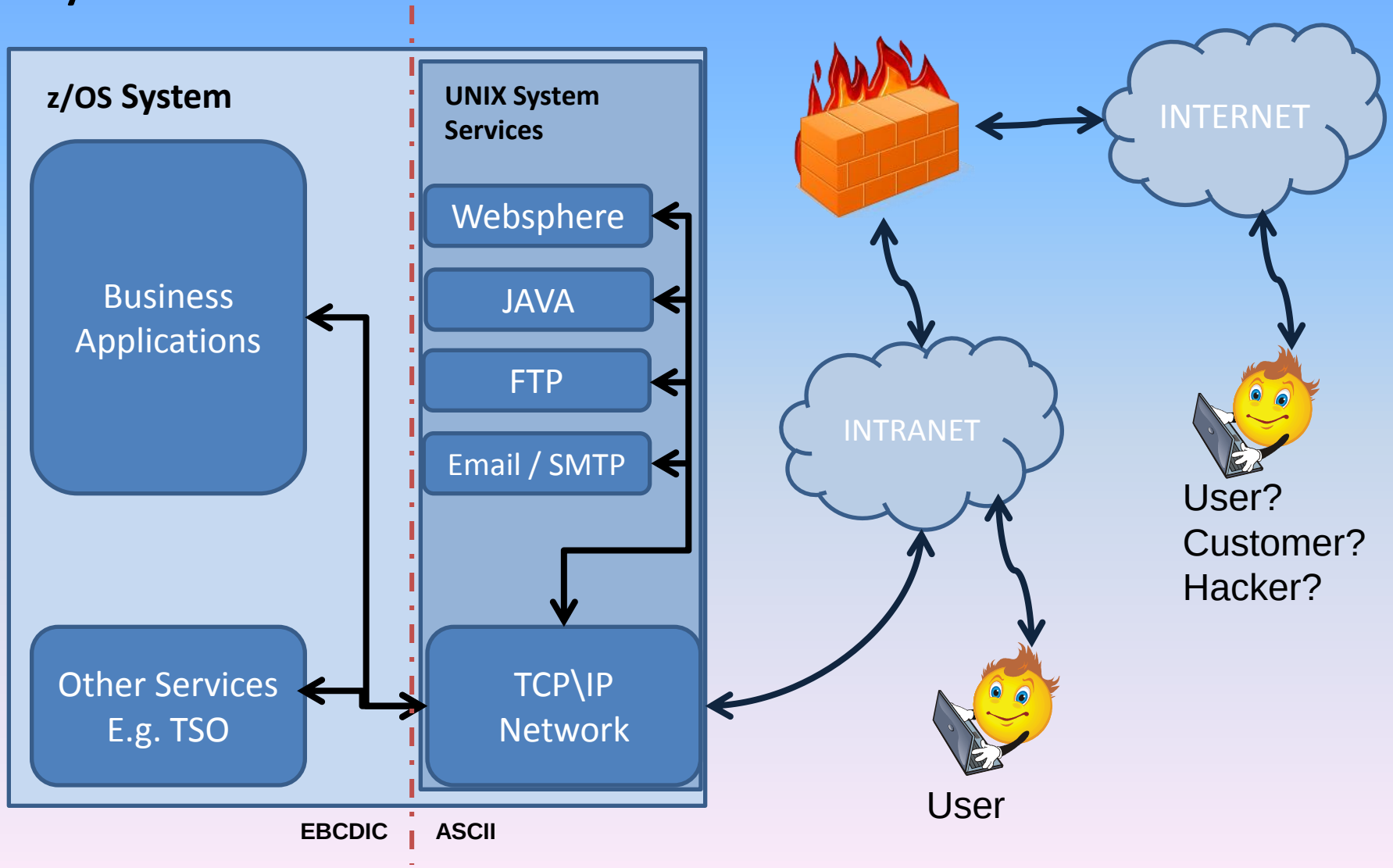
- Significant change in how default access to USS is granted on z/OS 2.1
- Potential show-stopper
- Why?
  - Essential z/OS services may not function
  - BPX.DEFAULT.USER resource is no longer supported
  - Replaced by new resources

What is USS?

- UNIX System Services
- POSIX compliant UNIX server emulation
  - Portable Operating System Interface for UNIX, a set of standards that define various aspects of the UNIX operating system.
- From the users perspective it's a UNIX server
- From the z/OS perspective just another supported service

A Little Bit of Background

System z



z/OS vs USS

- Logical boundary used to keep z/OS and USS processes separated
- Different File system structures
- Different data encoding
  - USS = ASCII
  - z/OS = EBCDIC
- Different security models

System Z Security

- People
  - Users
  - Groups
- Stuff
  - Files
  - Resources

Dual Security Model

- Fundamentally different security models
- In general
  - z/OS Security protects z/OS resources
  - USS Security protects USS resources
- Both security processes involved when action involves z/OS and USS resources

z/OS Security

- Userids
  - 8 Character limit, Alpha / Alpha-numeric
  - One userid per user
  - Each Userid has a default group
- Groups
  - 8 character limit, Alpha / Alpha-Numeric
  - Contains 1 or more Userids
- Access to ‘stuff’ controlled using profiles

z/OS Connecting Users to Stuff

- Profiles based on z/OS independent qualifier logic; e.g.
  - MY.DATA.*
  - MY.SECRET.DATA.*
- Access to profiles granted to multiple Userids and or Groups
  - Or by resource default (universal) access

USS Security

- UIDs
  - Numeric, 0 – 2,147,483,647
  - One UID per user
  - UID(0) = Superuser = Godmode
- GID
  - Numeric, 0- 2,147,483,647
  - Contains 1 or more UIDs
- Access to ‘stuff’ controlled using resources UNIX “File Security Packet” contents

USS Connecting Users to Stuff

- Hierarchical structure for all resources including files
- UNIX FSP includes:
  - Permission bits Owner : Group : Other
    - Only 1 Owner (UID), 1 Group (GID)
    - Other = Default (universal) Access
  - UNIX Access Control List
    - Individual Group / User access
  - Stored with resource in USS File system
  - Values inherited from parent resource, system defaults or set manually

Connecting z/OS & USS Security

- USS security UID's & GID's mapped to z/OS security Userid's & Groups
- Nominally 1 to 1 mapping
- User must have valid UID and Default GID to access USS
- Allocated explicitly or inherited via USS default access facility
- UID, Default GID & up to 300 supplementary group GIDs used for authority checks (256 for CA-TSS)

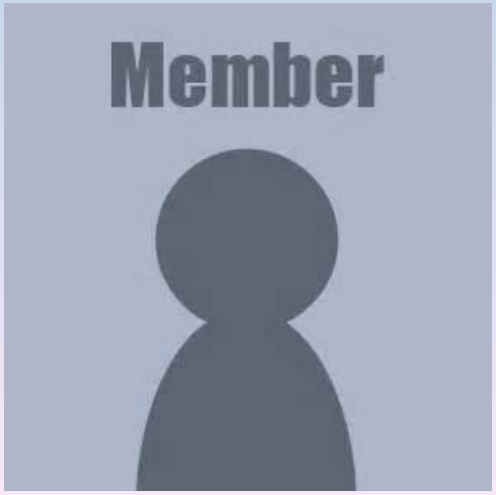
Access to USS – Default vs Explicit

- Explicit Access
  - Specific unique UID & GID values assigned to Userids & Groups
  - Fixed auditable assignments
  - Simple to audit usage

- Default Access
  - Single UID & GID values assigned to all callers
  - **Allocated 'on demand'**
  - **Very** complex to audit usage

USS Default Access - Current

- BPX.DEFAULT.USER
  - Single fixed UID and GID values
  - Allocated to user if userid has no UID or GID values on access to USS
  - All users assigned the same numbers ☹



USS Default Access - NEW

- BPX.UNIQUE.USER & BPX.NEXT.USER
  - Range of UID & GID values
  - Next unique UID and or GID values automatically assigned to USERID and Default Group if none found
  - Permanently assigned on first access to USS

USS Default Access – NEW cont.

- BPX.NEXT.USER
  - Unique ranges per database
  - RACF database AIM(2) or higher required
    - Max 129 users or groups sharing a single UID or GID
- BPX.UNIQUE.USER
  - RACF database AIM(3)
  - UNIXPRIV class active and SHARED.IDS profile defined
- USS Security Polices and procedures updated to match new process

CA-ACF2 & USS

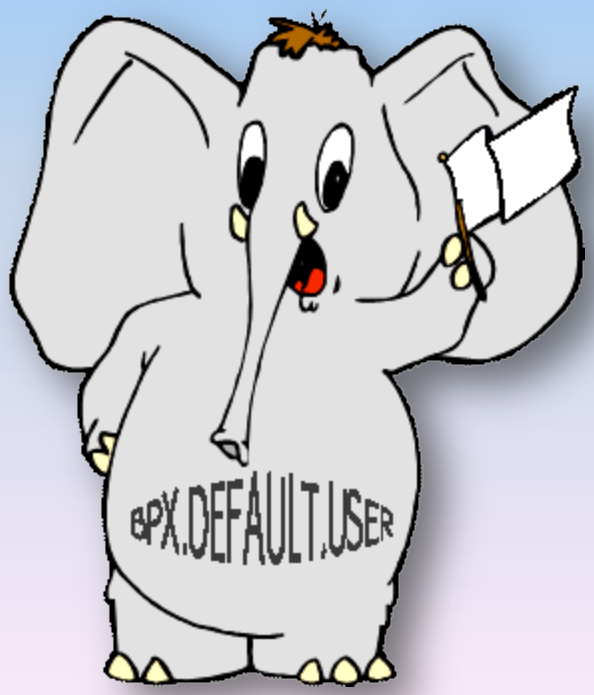
- UNIXOPTS GSO DFTUSER & DFTGROUP no longer used
- BPX.NEXT.USER
  - UID & GID ranges set via AUTOIDOM GSO record
- BPX.UNIQUE.USER
  - MODLUSER & UNIQUSER (UNIXOPTS GSO)
- RO55702 - create facility resource rule that will trace any requests to BPX.DEFAULT.USER

CA-TSS & USS

- OMVSUSR & OMVSGRP control options no longer used
- BPX.NEXT.USER
  - UID & GID ranges set via DFLTRNGU / DFLTRNGG control options
- BPX.UNIQUE.USER
  - MODLUSER & UNIQUSER control options
- RO58980 adds the ability to cut trace records for BPX.DEFAULT.USER usage

Default Access to USS?

- How are you justifying this to your auditor?
  - ‘on demand’ access to a business critical service?
  - Hackers know how to misuse it!
  - And who else?



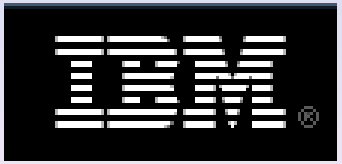
Implications of USS Default Access

- **Any** z/OS Userid can access USS ‘on demand’ **not** just those that need it
- Can access any USS resource where ‘OTHER’ value is READ or above
- Can access **any** z/OS dataset with uacc of READ or above
- **Very** complex to audit accurately
  - Multiple compensating controls required
  - USS Security policy must justify its usage

What's wrong with using BPX.DEFAULT.USER?

IBM* Presentation to RACF User Group 2013:

- *"Shared UID produces audit non-conformances*
  - *No accountability for who did what, who owns what, etc."*
- *"If a Unix service creates a resource while running with a shared UID, that resource is available to all users running with that shared UID"*



**ftp://public.dhe.ibm.com/.../nyrug_2013_03_default_user_removal.pdf*

What's wrong with using BPX.DEFAULT.USER?

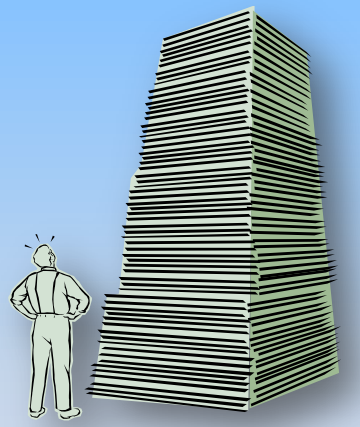
Robert Hansel*, RSH Consulting, presentation to SHARE in 2013:

- *"Shared ID - accountability difficult to establish - frequent audit finding"*
- *"UID becomes OWNER of File System objects created by a user using the Unix Default User"*
- *"UID becomes OWNER of File System objects when "chown" specifies a USERID that does not have an OMVS segment"*

**https://share.confex.com/.../RSH%20Consulting%20-%20BPX.DEFAULT.USER%20-%202013-08%20-%20SHARE%20-%2013393.pdf*

USS Security Policy

- Whatever happens your z/OS USS Security Policy will need updating
  - New procedures
  - Changes to auditing
- You **do** have one….?



- millennia… can help you create one or help you update your existing policy
  - Range of fixed price offerings are available from £15,000 (+VAT and expenses)

Conversion to Unique Users

- Multi-Step process
  - Baseline current configuration
  - Identify who is using the default access facility
  - Identify and resolve conflicts
  - Design new configuration, processes, mitigating controls etc.
  - Implementation
  - Ongoing monitoring and compliance

Baseline and Usage

- What UID & GID values are you using
- Are any being shared between multiple userids / groups?
- Do the additional resources required by BPX.NEXT.USER exist?
- Who is using BPX.DEFAULT.USER?
- millennia… have a fixed price service to identify the answers to these questions for you that comes in at £2,500 (+VAT and exes) per LPAR

Resolving Conflicts

- Implement unique UID and GID values as required
- Resolve any Shared values
- millennia… can perform the work required to achieve these goals for you at a fixed price of £9500* (+ VAT and exes) per security database

*except where the UID is shared by more than 129 users, this also applies to GIDs

Complex Conversions

- Resolving excessive sharing
  - Fix UID or GID values shared by > 129 IDs
  - Correct USS file system FSP permission bits and ACLs
- Correcting z/OS ACLs
  - RACF via FSSEC
  - CA-ACF2 via CA SAF HFS security
  - CA-TSS via HFSACL
- Achieving multi-system or site-wide UID / GID uniqueness
- Maintaining Uniqueness

Complex Conversions

- millennia… offers additional conversion services to assist with these complex conversions

- Additional analysis of your environment will be required before we can offer a price

millennia…

Monitoring and Compliance

- Monitoring USS activity
  - Update existing processes
  - Additional processes
- Compliance with USS Policy
  - Checking for the ‘human’ factor
- millennia… can provide help to bring your USS monitoring and compliance processes to the required levels
  - Fixed price service or Time and Materials offerings available, requires additional analysis before we can offer a price

One last thought…

From a computerworld.dk interview in 2013 with Peter Kruse from CSIS Security Group discussing the successful 2012 mainframe hacks in Sweden and Denmark.

"Hackerne er 100 procent gået efter mainframes og 100 procent efter zOS (operativsystemet i mainframes, red.), og man kan sige, at med disse angreb in mente har mainframen i hvert fald mistet sin uskyldighed" siger Peter Kruse

"The hackers are 100 percent gone after mainframes and 100 percent after zOS (operating in mainframes, ed.), And one can say that with these attacks in mind, the mainframe certainly lost its innocence" said Peter Kruse (sic)**

*http://www.computerworld.dk/art/227172/efter-det-store-csc-hack-flere-sager-paa-vej

** Google translate

What could you lose?

- Swedish Breach reported to include:
  - RACF database with 120k userids
  - 10,000+ datasets
  - Entire '/'
  - Sensitive personal data including financial details
- Danish Breach reported to include:
  - Large number of files from the Danish Police
  - Drivers license data including 4 million* social security numbers
- Both breaches were initially undetected

* CIA World Factbook - Denmark; pop 5.6 million (Est April 2014)

Any Questions?

millennia...

Contact Details:

Web site: www.sysprog.co.uk

Julie-Ann Williams

Email: julie@sysprog.co.uk

Mobile: ++44 (0) 7770 415102

Land Line: ++44 (0) 1932 887489

Linda McGrath

Email: linda.mcGrath@sysprog.co.uk

Mobile: ++353 (0) 86 2888772

Land Line: ++353 (0) 21-4374509

millennia...