IBM Security

The Privileged User – Your biggest vulnerability?

Jamie Pease CISA, CISM, CISSP, CITP, MBCS

zSecure Product Manager & Chairman of the GSE UK Security Working Group

IBM

Agenda

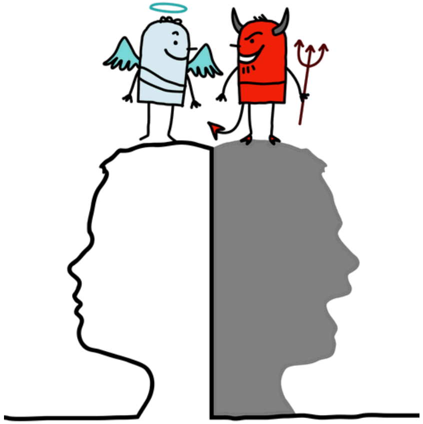
- Introduction
- What are privileged users
- Types of privileged users
- How are privileges typically managed
- Want to become privileged?
- Common audit concerns
- Practical steps to reduce risk
- Conclusions
- Useful resources

About me

- Based in London, UK (no Brexit questions please!)
- 20 years of experience in Mainframe Security
- I was a customer of IBM for many years, working for the UK's largest Insurance Company
  - I supported both RACF and ACF2 systems
- Joined IBM in 2007 as an IT Security Specialist, focusing on Mainframe Security
- Currently the Worldwide Product Manager for IBM zSecure
- Also Chairman of the Guide Share Europe UK Security Working Group

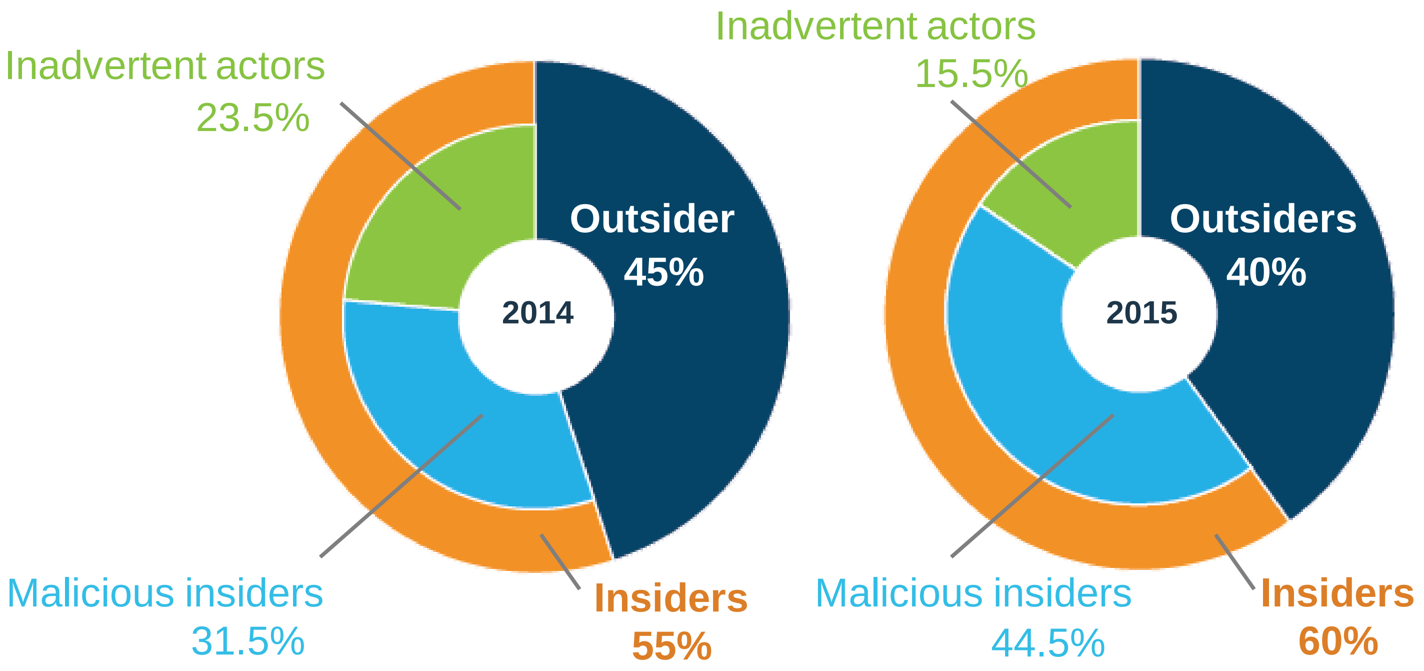
Introduction

- The privileged user is a blessing and a curse
  - They help keep our systems secure and available
  - Also come with a high risk tag
  - Can have direct or indirect privileges
  - Can be one of your biggest vulnerabilities
  - Often “used and abused” to get the job done
  - One of the top 10 recurring internal audit concerns

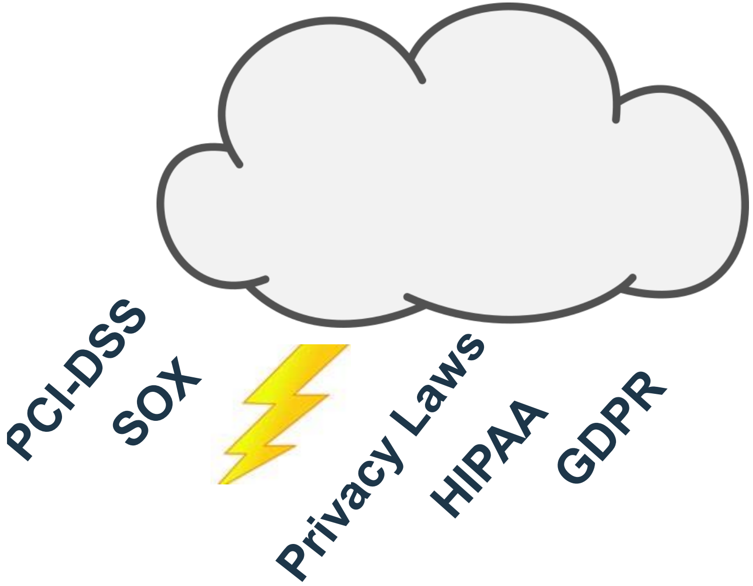


Who are the bad guys?

The growth of malicious insiders outpaced the reduction in inadvertent actors, pushing the insider total to 60%



Policies, Regulations, Legal requirements also apply for z Systems!



PCI-DSS

SOX

Privacy Laws

HIPAA

GDPR

What is a privileged user?

- Privileges apply to systems, applications, data, devices, hardware etc
- Think about it - if you have something extra than a normal user, are you privileged?
  - Ability to electronically transfer $100M?
  - Read access to IP / personal sensitive information?
  - Have RACF Special; Superuser etc?
  - Update access to the Trusted Computing Base?

Types of privileged users on the Mainframe

UNIX Process

Batch ID

Batch Management

RACF Admin

MVS Sysprogs

Storage Admin

CICS Sysprogs

Operator

Started Task ID

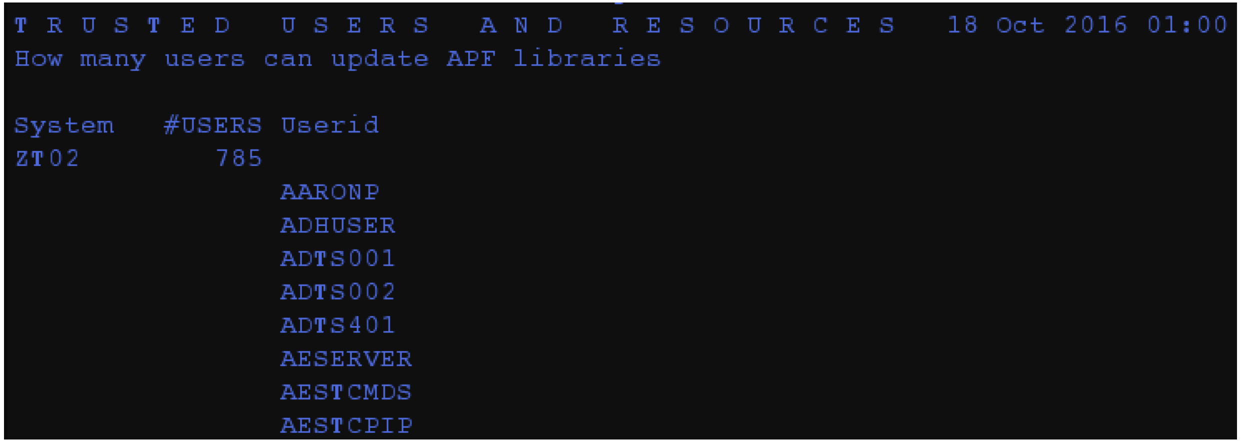
Auditor

DBAs

MQ Sysprogs

Types of privileged users - continued

- Or perhaps you are a normal user that can inherit?
  - Think SURROGAT
  - Switch to UID 0
  - Via an exit or SVC
  - Via PPT . . .
- 3000 users with update access to APF - Privileged?

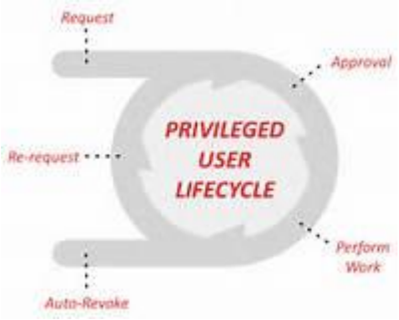


```
T R U S T E D   U S E R S   A N D   R E S O U R C E S   18 Oct 2016 01:00
How many users can update APF libraries

System    #USERS Userid
ZT02         785
                 AARONP
                 ADHUSER
                 ADTS001
                 ADTS002
                 ADTS401
                 AESERVER
                 AESTCMDS
                 AESTCPIP
```

How are privileges managed these days?

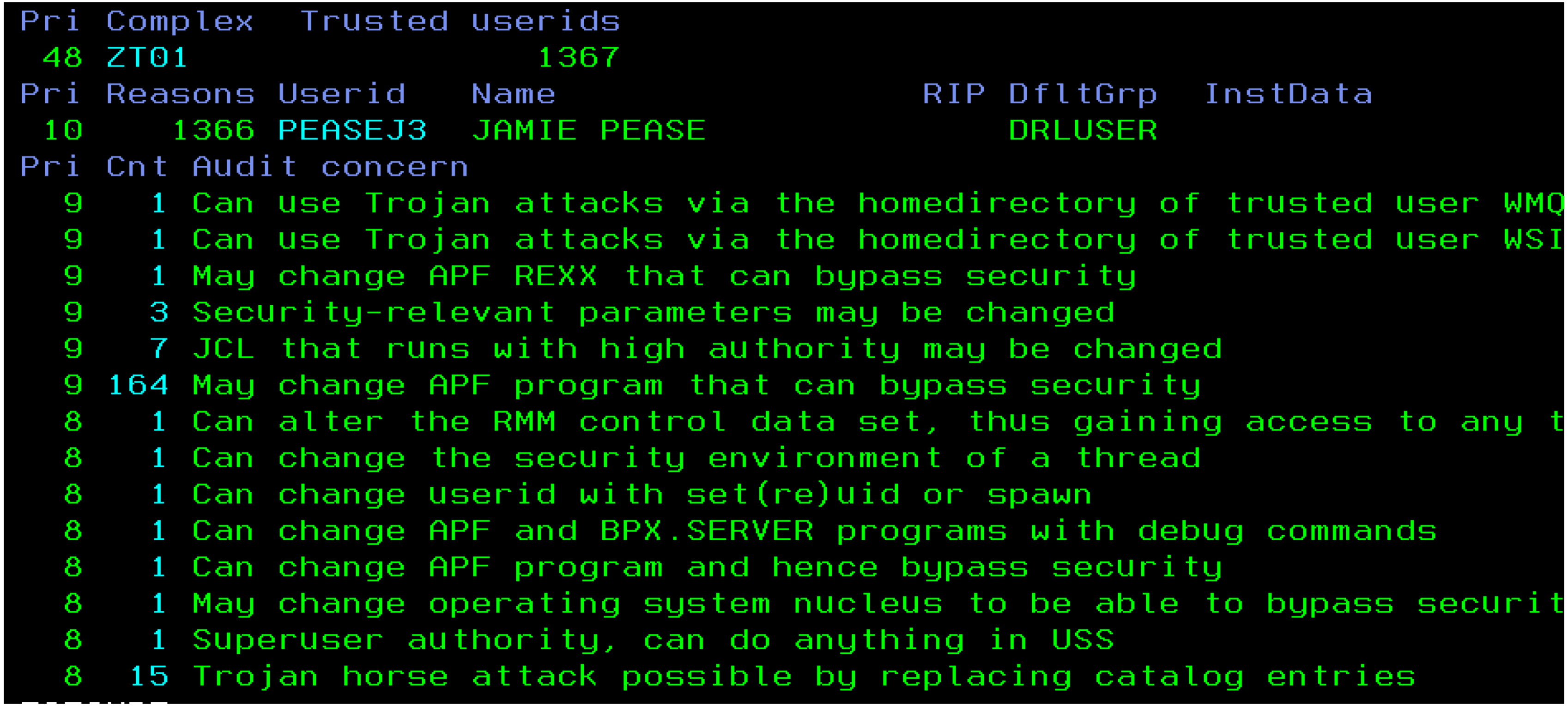
- Varies from organisation to organisation
- Most common method is still assigning privileges directly to an employee, contractor
- Emergency user ID with check-in / out is more main stream
- Logon with non-privileged user ID, then elevate privileges
- Change Management software handles some privileged functions, such as updating sensitive libraries



Want to become privileged or elevate?

- Who has update access to your APFs, RACF database, CLIST libs, PROCLIBs, UNIX files
- Read access perhaps to some SURROGAT profiles or maybe the RACF database?
- How about some code to do that?
- Maybe ask the RACF Admin to submit that deck of commands for you?

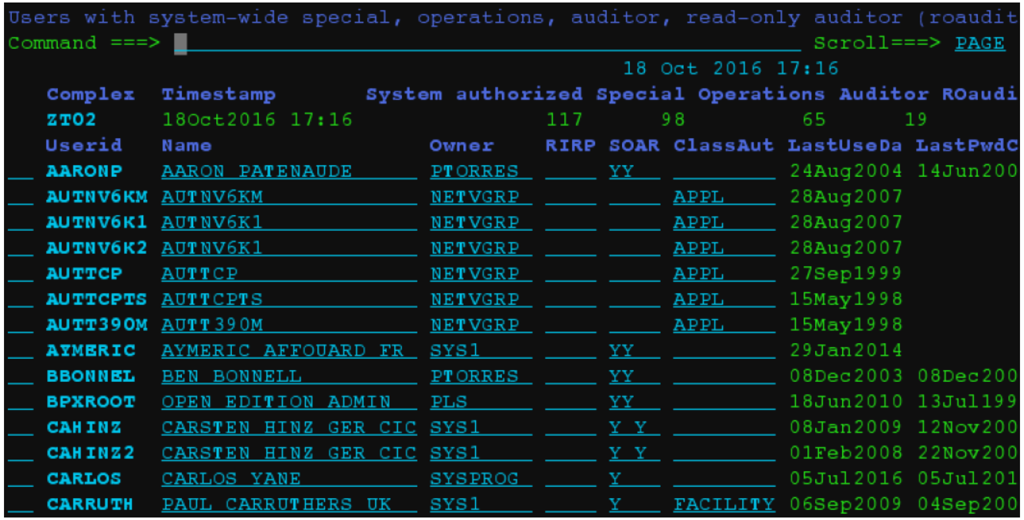
Example routes to elevating privileges



```
Pri Complex  Trusted userids
 48 ZT01                 1367
Pri Reasons Userid   Name                    RIP DfltGrp  InstData
 10    1366 PEASEJ3  JAMIE PEASE                 DRLUSER
Pri Cnt Audit concern
  9   1 Can use Trojan attacks via the homedirectory of trusted user WMQ
  9   1 Can use Trojan attacks via the homedirectory of trusted user WSI
  9   1 May change APF REXX that can bypass security
  9   3 Security-relevant parameters may be changed
  9   7 JCL that runs with high authority may be changed
  9 164 May change APF program that can bypass security
  8   1 Can alter the RMM control data set, thus gaining access to any t
  8   1 Can change the security environment of a thread
  8   1 Can change userid with set(re)uid or spawn
  8   1 Can change APF and BPX.SERVER programs with debug commands
  8   1 Can change APF program and hence bypass security
  8   1 May change operating system nucleus to be able to bypass securit
  8   1 Superuser authority, can do anything in USS
  8  15 Trojan horse attack possible by replacing catalog entries
```

Common audit concerns – 1/3

- A user with a combination of attributes
  - All in one Security Admin and Storage Admin
  - Often a conflict of interest = poor SoD
- Too many privileges
  - Does the RACF Admin really need update access to those APF libs or modify the TCP/IP stack?
- Temporary privileges still intact long after expiry date



```
Users with system-wide special, operations, auditor, read-only auditor (roaudit
Command ===>                                                   Scroll===> PAGE
                                                18 Oct 2016 17:16
   Complex  Timestamp       System authorized Special Operations Auditor ROaudi
   ZTO2     18Oct2016 17:16               117      98         65        19
   Userid   Name                 Owner    RIRP SOAR ClassAut LastUseDa LastPwdC
   AARONP   AARON PATENAUDE      PTORRES       YY            24Aug2004 14Jun200
   AUTNV6KM AUTNV6KM             NETVGRP            APPL     28Aug2007
   AUTNV6K1 AUTNV6K1             NETVGRP            APPL     28Aug2007
   AUTNV6K2 AUTNV6K1             NETVGRP            APPL     28Aug2007
   AUTTCP   AUTTCP               NETVGRP            APPL     27Sep1999
   AUTTCPTS AUTTCPTS             NETVGRP            APPL     15May1998
   AUTT390M AUTT390M             NETVGRP            APPL     15May1998
   AYMERIC  AYMERIC AFFOUARD FR  SYS1          YY            29Jan2014
   BBONNEL  BEN BONNELL          PTORRES       YY            08Dec2003 08Dec200
   BPXROOT  OPEN EDITION ADMIN   PLS           YY            18Jun2010 13Jul199
   CAHINZ   CARSTEN HINZ GER CIC SYS1          Y Y           08Jan2009 12Nov200
   CAHINZ2  CARSTEN HINZ GER CIC SYS1          Y Y           01Feb2008 22Nov200
   CARLOS   CARLOS YANE          SYSPROG       Y             05Jul2016 05Jul201
   CARRUTH  PAUL CARRUTHERS UK   SYS1          Y    FACILITY 06Sep2009 04Sep200
```

Common audit concerns – 2/3

- Inexperienced staff with powerful privileges
- Default (well known) or weak passwords
- Easy to inherit privileges (E.g. via SURROGAT, BPX.SUPERUSER)
- Generous allocation of attributes such as RACF AUDITOR or perhaps UID 0!
- Single batch user ID running all batch workloads
- Easy to elevate privileges – “basic user” turned privileged

Common audit concerns – 3/3

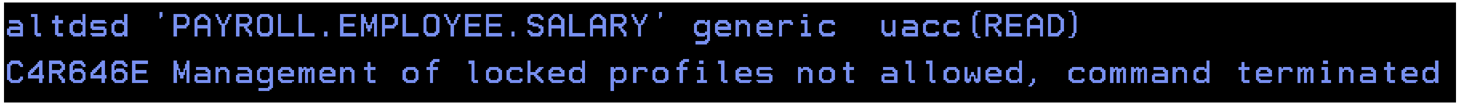
- Limited security monitoring, often performed by the (RACF) people that do the implementation work
- Recertification efforts do not extend to system type user IDs
- User IDs running with high privileges because that’s what the vendor documentation suggested
- Passwords of privileged accounts flowing around the network in the clear
- Accountability! Who used it and what did they do?

Practical steps to remediate those audit concerns – 1/4

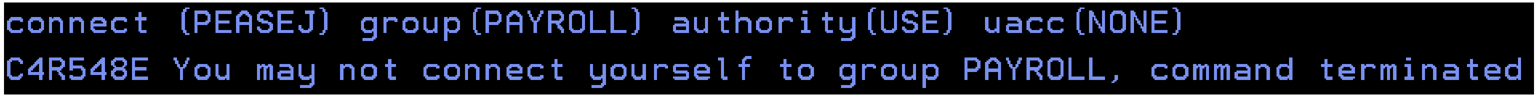
- Establish a baseline to determine who or what is supposed to have which privileges, including the purpose
- Adopt the principle of least privilege
- Start cleaning up – what’s not being used?
- Monitor and audit activities of privileged accounts
  - Both individual and shared accounts
- Establish session recording
  - Record privileged user activity in detail for forensics and compliance reviews – you might need it for legal proceedings!

Practical steps to reduce risk – 2/4

- Establish and follow a regular process for recertifying privileged users
- Understand how users could bypass system security
- Establish access controls that prevent privileged users from accessing sensitive resources or elevating privileges
- Implement an acceptable use policy for privileges
- Control which services a privileged user can use
  - E.g. RACF Special user ID cannot FTP



```
altdsd 'PAYROLL.EMPLOYEE.SALARY' generic  uacc(READ)
C4R646E Management of locked profiles not allowed, command terminated
```



```
connect  (PEASEJ) group(PAYROLL) authority(USE) uacc(NONE)
C4R548E You may not connect yourself to group PAYROLL, command terminated
```

Practical steps to reduce risk – 3/4

- Establish preventive controls that block inappropriate privileged user activities (E.g. SETROPTS NOSAUDIT)
- Implement strong authentication with Multi-Factor Authentication mechanisms
- Encrypt sessions for privileged users
- Challenge vendors who suggest the need for powerful privileges for their solutions

Practical steps to reduce risk – 4/4

- Education, education, education!
  - People are the weakest link in the chain
  - Remember, a Computer is told what to do by his master
  - We are all prone to making mistakes
  - Prevention is better than cure

Conclusions

Self-Destruction

Computer will blow up in...

- Privileged users are like a nuclear bomb
  - Can cause mass-destruction of your system in the wrong hands
- Just one misconfigured security setting can potentially mean that all users on the system are classed as privileged
- A privileged user should not be an “all-in-one” to accomplish all
- Perform audits, access reviews and monitoring frequently!
- Be proactive, take control of them before they take control of your business
- The insider is the one to watch! Remember that 60% statistic?

Useful resources

Interactive White Paper: Your biggest vulnerability: The privileged user

Video: Your Biggest Vulnerability – The privileged user

Questions?

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.