RSH
CONSULTING

The Role of IBM Mainframes in Cybersecurity

MIT - CAMS

February 2023

RSH Consulting - Robert S. Hansel

RSH Consulting, Inc. is an IT security professional services firm established in 1992 and dedicated to helping clients strengthen their IBM z/OS mainframe access controls by fully exploiting all the capabilities and latest innovations in RACF. RSH's services include RACF security reviews and audits, initial implementation of new controls, enhancement and remediation of existing controls, and training.

- www.rshconsulting.com
- 617-969-9050

Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc. He began working with RACF in 1986 and has been a RACF administrator, manager, auditor, instructor, developer, and consultant. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He is a leading expert in securing z/OS Unix using RACF. Mr. Hansel has created elaborate automated tools to assist clients with RACF administration, database merging, identity management, and quality assurance.

- 617-969-8211
- R.Hansel@rshconsulting.com
- www.linkedin.com/in/roberthansel

Mainframe Users

- Two thirds of the Fortune 100
- 45 of the world's top 50 banks
- 8 of the top 10 insurers
- 7 of the top 10 global retailers
- 8 out of the top 10 telcos
- 70% of global transactions, on a value basis

  Source: IBM - April 2022

  https://newsroom.ibm.com/2022-04-05-Announcing-IBM-z16-Real-time-AI-for-Transaction-Processing-at-Scale-and-Industrys-First-Quantum-Safe-System

Mainframes reliably (and securely) process very high volumes of transactions

- ATM, credit cards, electronic payments, policy/account management

Design philosophy of backwards-compatibility

- Pre-existing features and functions are rarely changed or removed
  - Applications written decades ago still run under the latest OS releases
- New features and functions are typically added as optional

Topics

- Mainframe Operating Systems
- Mainframe Services
- z/OS Integrity
- z/OS Security
- Resource Access Control Facility (RACF)

RACF, z/OS, z/VM, z/VSE, z/TPF, IMS, DB2, and CICS are Trademarks of the International Business Machines Corporation

IBM Mainframe Operating Systems

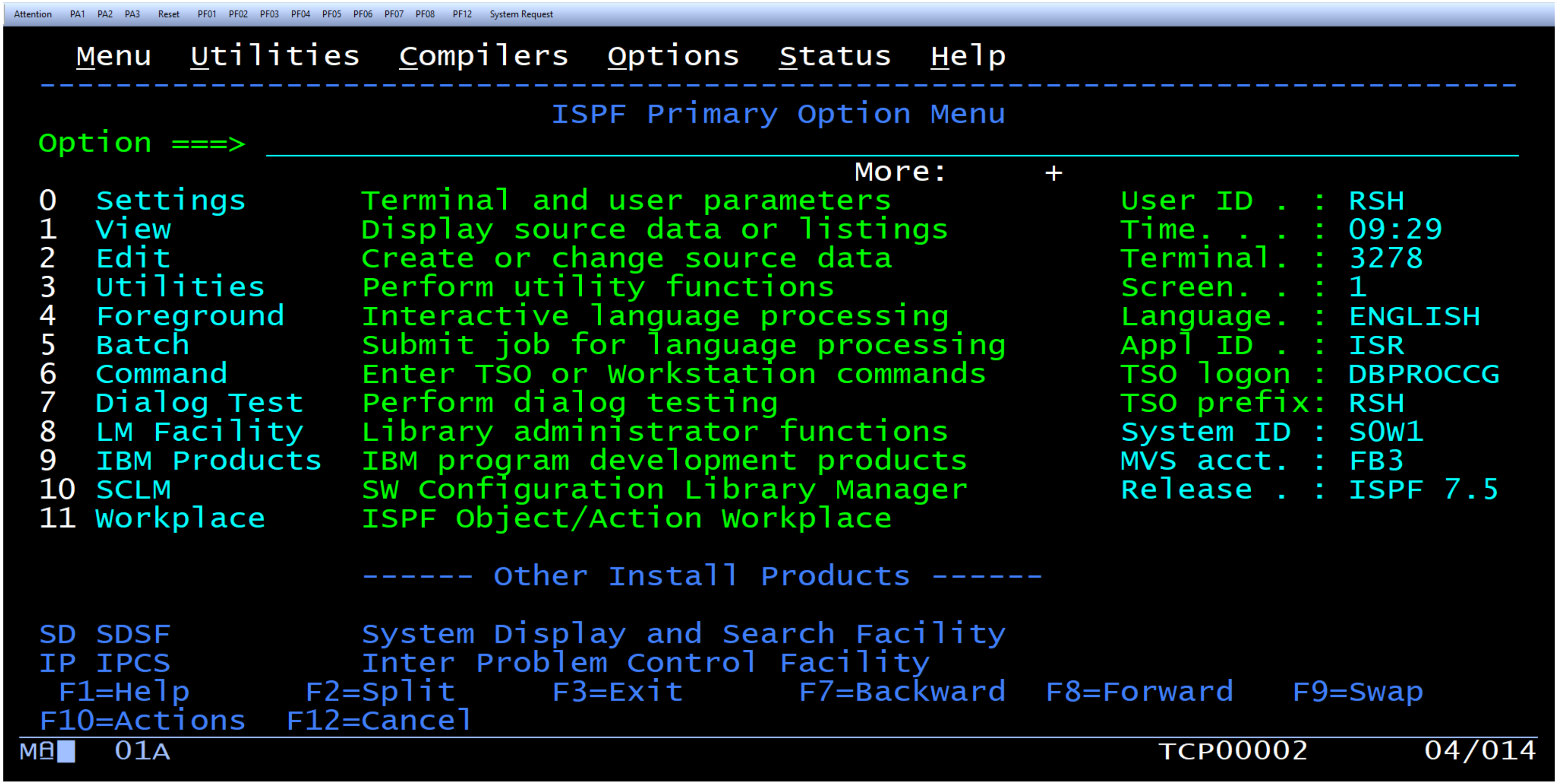
z/OS	1964	z = zero downtime
z/VSE	1965	Virtual Storage Extended
z/VM	1967	Virtual Machine
z/TPF	1979	Transaction Processing Facility
Linux on IBM Z	1999	

Mainframe OSs run on z Series mainframe computers with a unique hardware architecture

Mainframe Services - z/OS

- Job Entry Subsystem (JES) - Batch execution (1966?)
- Time Sharing Option (TSO) - Interactive menus and command execution (1971)
- User application processing
  - Customer Information Control System (CICS) - On-line transaction processing (1969)
  - Information Management System (IMS) - Hierarchical database system (1968)
  - Database 2 (DB2) - Relational database system (1983)
  - Message Queue (MQ) - Message communication and processing (1993)
- Data communications
  - Virtual Telecommunications Access Method (VTAM) (1974)
    - System Network Architecture (SNA) protocols
  - TCP/IP (1993?)
    - Applications - ftp, http, ldap, Kerberos, ssh, telnet, …
- z/OS Unix (1993) - POSIX compliant - Supports TCP/IP and Unix applications
- System management software products, such as …
  - Automated operations
  - Tape Management

Mainframe Services - TSO/ISPF menus

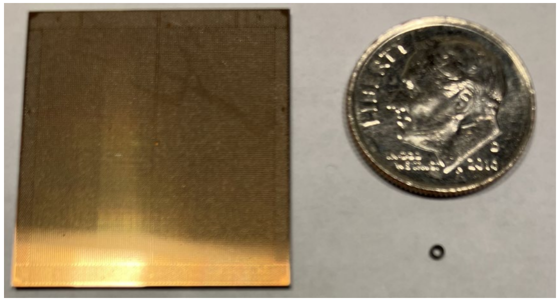


```
   Menu  Utilities  Compilers  Options  Status  Help
 ------------------------------------------------------------------------------
                            ISPF Primary Option Menu
 Option ===> __________________________________________________________________
                                            More:     +
 0   Settings      Terminal and user parameters            User ID . : RSH
 1   View          Display source data or listings         Time. . . : 09:29
 2   Edit          Create or change source data            Terminal. : 3278
 3   Utilities     Perform utility functions               Screen. . : 1
 4   Foreground    Interactive language processing         Language. : ENGLISH
 5   Batch         Submit job for language processing      Appl ID . : ISR
 6   Command       Enter TSO or Workstation commands       TSO logon : DBPROCCG
 7   Dialog Test   Perform dialog testing                  TSO prefix: RSH
 8   LM Facility   Library administrator functions         System ID : SOW1
 9   IBM Products  IBM program development products        MVS acct. : FB3
 10  SCLM          SW Configuration Library Manager        Release . : ISPF 7.5
 11  Workplace     ISPF Object/Action Workplace

                   ------ Other Install Products ------

 SD  SDSF          System Display and Search Facility
 IP  IPCS          Inter Problem Control Facility
  F1=Help      F2=Split     F3=Exit      F7=Backward  F8=Forward   F9=Swap
 F10=Actions  F12=Cancel
MA     01A                                                   TCP00002      04/014
```

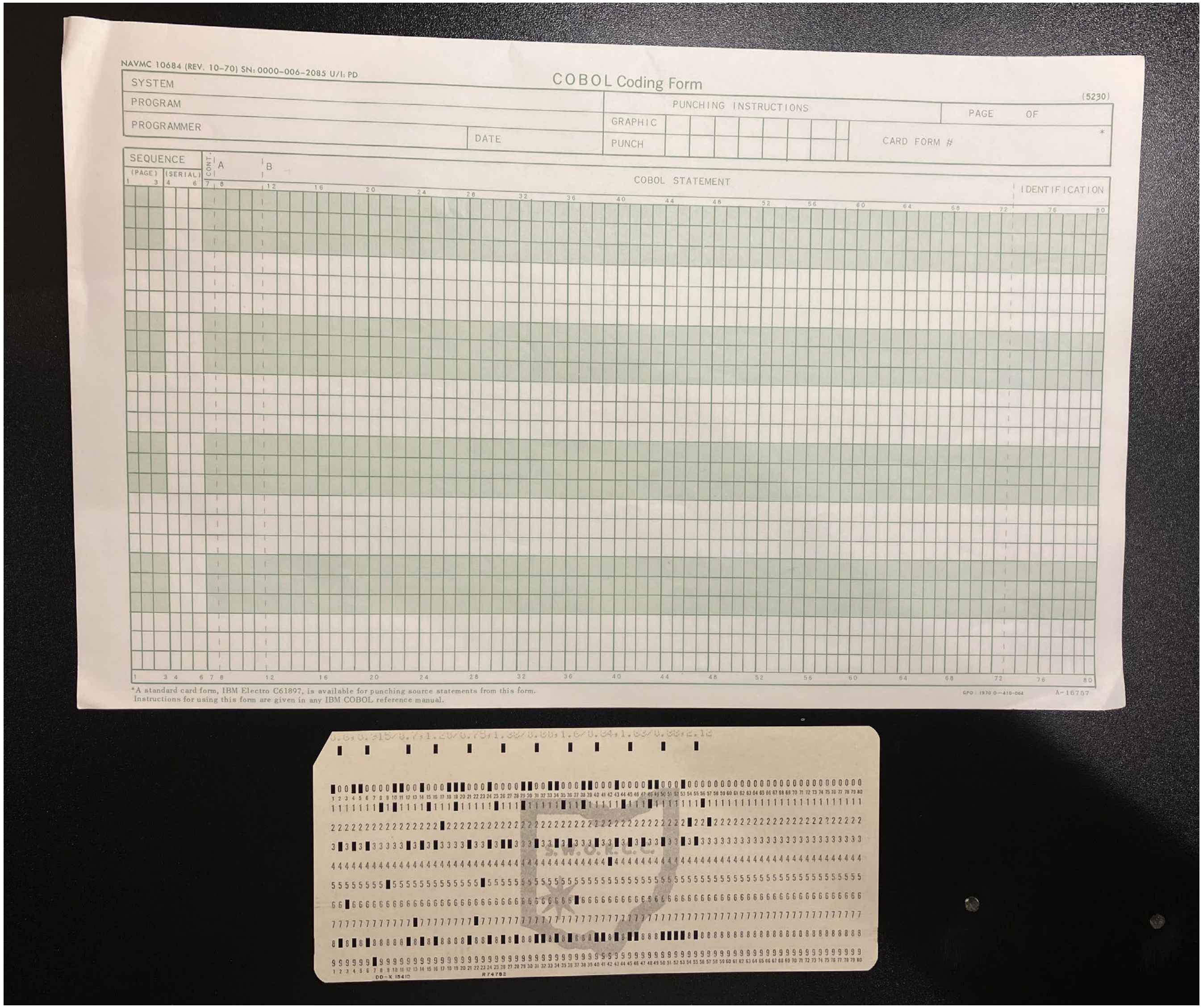
Mainframe Services - z/OS Unix

```
RSH:/S0W1/etc: >ls -al
total 840
drwxr-xr-x  17 OMVSKERN OMVSGRP      8192 Feb  8 13:31 .
drwxr-xr-x   6 OMVSKERN IPGROUP      8192 Oct  4  2018 ..
drwxr-xr-x   2 OMVSKERN OMVSGRP      8192 Oct  5  2018 IBM
drwxr-xr-x   2 OMVSKERN OMVSGRP         0 Apr 27  2017 PFA
drwxr-xr-x   2 OMVSKERN OMVSGRP         0 Apr 27  2017 Printsrv
-rw-r--r--   1 OMVSKERN OMVSGRP      2163 Oct  5  2018 csh.cshrc
-rw-r--r--   1 OMVSKERN OMVSGRP      8644 Oct  5  2018 csh.login
-rw-r--r--   1 OMVSKERN OMVSGRP      8644 Oct  5  2018 csh.login
drwxrwxr-x   2 OMVSKERN IPGROUP      8192 Sep  7  2021 dbb
-rw-r--r--   1 OMVSKERN OMVSGRP      1162 Oct  5  2018 inetd.conf
-rw-r--r--   1 OMVSKERN OMVSGRP        10 Nov 27  2018 inetd.pid
-rw-r--r--   1 OMVSKERN OMVSGRP      2587 Oct  5  2018 init.options
-rw-rw-rw-   1 OMVSKERN OMVSGRP      3645 Sep 20  2017 ipnodes
drwxrwxr-x   3 OMVSKERN OMVSGRP      8192 Sep 29  2017 kc4z
drwxr-xr-x   2 OMVSKERN OMVSGRP         0 Apr 27  2017 ldap
-rw-r--r--   1 OMVSKERN OMVSGRP      3834 Feb  6 12:47 log
-rw-r--r--   1 OMVSKERN OMVSGRP     19808 Oct  5  2018 magic
-rwxr-xr-x   1 OMVSKERN OMVSGRP      1072 Oct  5  2018 mailx.rc
-rw-r--r--   1 OMVSKERN OMVSGRP      1216 Sep 20  2017 osnmpd.data
```

z/OS and Mainframe Security Timeline



1964	OS/360 - Real Storage (i.e., memory) - 24 bit address
1966	MFT - Multi-programming Fixed Number of Tasks
1969	MVT - Multi-programming Variable Number of Tasks
196x	System product and Application "Internal" Security
1972	OS/VS2 R1 - SVS - Single Virtual Storage - 24 bit address
1972	SHARE Security Project
1973	IBM System Integrity Statement
1974	OS/VS2 R2 - MVS - Multiple Virtual Storage - Introduced Address Spaces
1976	IBM - Resource Access Control Facility (RACF)
1977	SKK - Access Control Facility 2 (ACF2) - now Broadcom / CA
1979	MVS/SE - System Extension
1980	MVS/SP - System Product
1981	CGA - Top Secret Security (TSS) - now Broadcom / CA
1983	MVS/XA - eXtended Storage - 31 bit address
1983	System Authorization Facility (SAF) - RACROUTE Macro - Common API
1988	MVS/ESA - Enterprise System Architecture
1996	OS/390 - bundling sets of like-products for new releases and maintenance
2001	z/OS - 64 bit address



NAVMC 10684 (REV. 10-70) SN: 0000-006-2085 U/I: PD

COBOL Coding Form

(5230)

SYSTEM

PROGRAM

PROGRAMMER

DATE

PUNCHING INSTRUCTIONS

GRAPHIC

PUNCH

PAGE OF

CARD FORM # *

SEQUENCE (PAGE) 1 3 (SERIAL) 4 6 CONT. 7 A 8 B 12

COBOL STATEMENT

IDENTIFICATION

*A standard card form, IBM Electro C61897, is available for punching source statements from this form. Instructions for using this form are given in any IBM COBOL reference manual.

GPO : 1970 O—410-064

A-16757

z/OS System Integrity

- Integrated hardware and z/OS software architecture (storage = memory)
  - Instruction State 0=Supervisor 1=Problem
  - Storage Protect Key 0-7=System (0=Master), 8=User (Virtual), 9-15 (Real)
  - Storage Fetch Protect bit - On/Off
  - Authorized Program Facility (APF) - "APF-authorized" program attribute
    - Programs fetched from APF designated libraries (require strict update control)

- Govern the ability of programs to …
  - Execute privileged instructions
  - Modify a memory page - requires key 0 or matching key
  - View a fetch protected memory page - requires key 0 or matching key
  - Invoke a privileged Supervisor Call (SVC)
  - Cross Address Space application isolation boundaries

- A program is consider to be "unauthorized" if it is not in Supervisor state, does not have a storage protect key less than 8, and is not APF-authorized

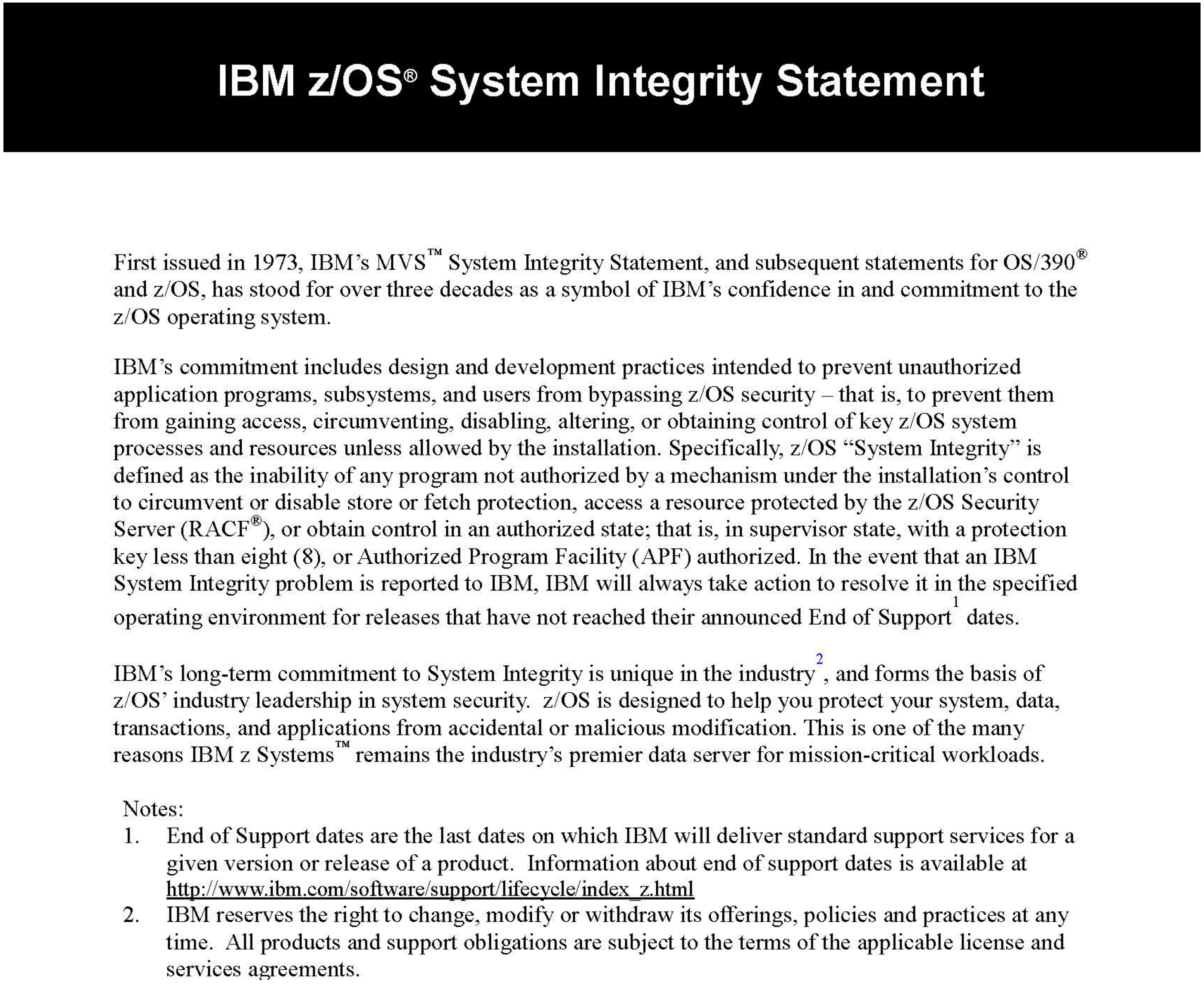
z/OS System Integrity

https://www.ibm.com/downloads/cas/OWGOKG40?mhsrc=ibmsearch_a&mhq=statement%20of%20system%20integrity

When IBM discovers an integrity or security issue, they publish it's existence on an IBM webpage that requires special permission to access. Often only post after a patch is available.

IBM generally does not provide any details about the nature of an issue, only that it exists.

When IBM provides patches to fix an issue, the documentation related to the patches often has few if any details on what the patch contains.



IBM z/OS® System Integrity Statement

First issued in 1973, IBM's MVS™ System Integrity Statement, and subsequent statements for OS/390® and z/OS, has stood for over three decades as a symbol of IBM's confidence in and commitment to the z/OS operating system.

IBM's commitment includes design and development practices intended to prevent unauthorized application programs, subsystems, and users from bypassing z/OS security – that is, to prevent them from gaining access, circumventing, disabling, altering, or obtaining control of key z/OS system processes and resources unless allowed by the installation. Specifically, z/OS "System Integrity" is defined as the inability of any program not authorized by a mechanism under the installation's control to circumvent or disable store or fetch protection, access a resource protected by the z/OS Security Server (RACF®), or obtain control in an authorized state; that is, in supervisor state, with a protection key less than eight (8), or Authorized Program Facility (APF) authorized. In the event that an IBM System Integrity problem is reported to IBM, IBM will always take action to resolve it in the specified operating environment for releases that have not reached their announced End of Support[1] dates.

IBM's long-term commitment to System Integrity is unique in the industry[2], and forms the basis of z/OS' industry leadership in system security. z/OS is designed to help you protect your system, data, transactions, and applications from accidental or malicious modification. This is one of the many reasons IBM z Systems™ remains the industry's premier data server for mission-critical workloads.

Notes:

1. End of Support dates are the last dates on which IBM will deliver standard support services for a given version or release of a product. Information about end of support dates is available at http://www.ibm.com/software/support/lifecycle/index_z.html
2. IBM reserves the right to change, modify or withdraw its offerings, policies and practices at any time. All products and support obligations are subject to the terms of the applicable license and services agreements.

z/OS Security

- Physical security
- Dataset Passwords - Specified in batch (196?); superseded by external security
- "Internal" security - developed pre-external security - external often optional
  - TSO User Attributes Dataset (UADS) - User identification and TSO authority
  - CICS Sign-on Table (SNT) and transaction protect keys (externalized in 1994)
  - DB2 DB2 Catalogs - database resource protection
  - SDSF ISFPARMS - SDSF function protection (externalized in z/OS 2.5 2021)
  - Other System Software Products - User identification and/or resource protection
  - User Applications - User identification and/or resource protection
- "External" security - RACF, ACF2, TSS, SAF - use optional in many cases
- Encryption
  - Crypto cards
  - Private key, Public key, PKI services, CA services
  - Data communications - Application Transparent / Transport Layer Security (AT/TLS)
  - Data encryption - datasets, DB2 tables - at rest and in use
  - Use of Crypto keys and functions are SAF / RACF-protected

z/OS Security

z/OS Security Evaluation

- Common Criteria Protection Profile for General Purpose Operating Systems Version 4.2.1 (OSPP), dated April 22, 2019 (ISO 15408)
  - Evaluation Assurance Level (EAL)
  - z/OS 2.4 - EAL4
  - RACF - EAL5
  - Requires specific configuration to meet the designated EAL
- Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD (Orange Book) - MVS/ESA V3R1 held B1 rating
  - Introduction of new features, especially z/OS Unix, precluded evaluation
  - IBM has continued to adhere to B1 specifications even though not evaluated

Introduction to RACF

- Resource Access Control Facility (RACF)
- RACF Functions
  - User Identification and Authentication
  - Dataset and General Resource Access Authorization
  - Monitor User Activity (i.e., logging)
  - Access Administration
- RACF Components
  - Database (Primary and Backup Pair)
    - Options - SETROPTS (SET Racf OPTionS) configuration options (e.g., password length)
    - Profiles - User, Group, Dataset, General Resource
  - Software
    - Programs - Query Database and make security decisions (extension of z/OS)
    - Tables - Specify the Databases and define resource Classes
    - Exits - Optional Installation-written programs that modify RACF's behavior
    - Commands - TSO programs used to create and administer options and profiles
    - Utilities - Programs used for backup, maintenance, unload, and control reports

RACF Functions

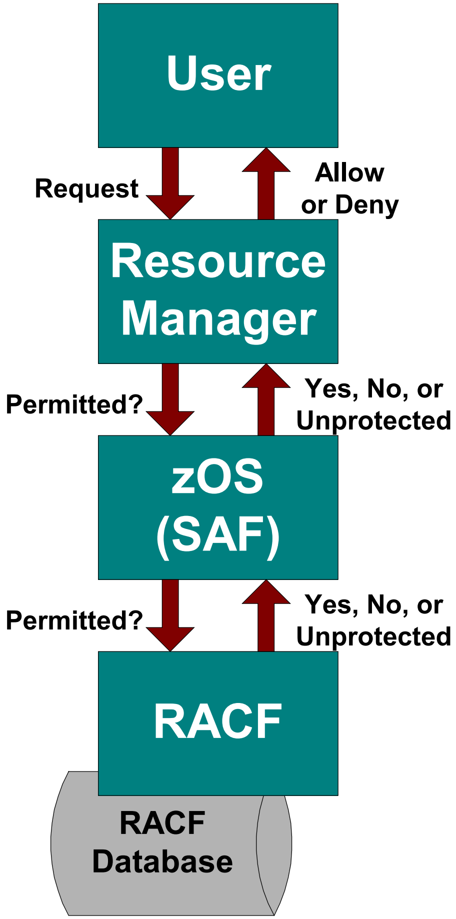
- RACF is called by a system resource manager (e.g. CICS, JES, MQ) whenever a user tries to logon or attempts to access a resource
  - Most calls are made using the RACROUTE macro, which invokes the System Authorization Facility (SAF)

- RACF looks for a matching profile in its database and determines whether the action is authorized

- RACF *advises* the resource manager to allow or disallow the action using a return code (0 - 4 - 8)

- The *resource manager* decides what action to take based on what RACF advises

- Common finding - Resource managers not configured to call RACF



Resource Profiles

```
RLIST FACILITY STGADMIN.ADR.STGADMIN.COPY ALL

 CLASS      NAME
 -----      ----
 FACILITY   STGADMIN.ADR.STGADMIN.* (G)

 LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS  WARNING
 -----  --------   ----------------  -----------  -------
  05    SECADMIN        NONE               READ    YES

 AUDITING
 --------
 ALL(READ)

 USER      ACCESS
 ----      ------
 STGGRP    READ
 SYSPROGS  ALTER
 #STORBAT  READ
 JOESMTH   UPDATE

    ID     ACCESS  CLASS               ENTITY NAME
 -------- ------- -------- ---------------------------------------
 NO ENTRIES IN CONDITIONAL ACCESS LIST
```

RACF - User Authentication

- Authentication options
  - Password: 1-8 characters - letters, numbers, and national characters ($, #, @)
    - SETROPTS options for mixed-case and additional special characters
  - Password Phrase: 9-100 characters - mixed-case letters, numbers, and special characters
  - Pass-Ticket: One-time password generated by an application at logon time
  - Digital Certificate: Public Key x509 certificate
  - Multifactor Authentication (MFA): PIN and dynamic token
- Password/Phrase encryption governed by SETROPTS option
  - LEGACY - Data Encryption Standard (DES) (1984)
  - KDFAES - Key Derivation Function with Advanced Encryption Algorithm (2014)

Mainframe Security - Hacking Incidents

- Very rare and mainframe's involvement often never publicized
  - Attack vector often via other internal systems (e.g., Identity Management)
  - Mainframes are rarely directly accessible via the Internet
  - No known mainframe ransomware incidents
  - Email attacks unable to install and APF-authorize mainframe programs

- 2010 Logica - UK mainframe service provider with datacenter in Sweden
  - Hacker entered z/OS Unix via FTP - used stolen unprivileged-user credentials
  - Discovered a Unix program that erroneously granted Superuser authority
  - Modified inetd.conf to set up reverse shell with Superuser authority
  - Exfiltrated improperly protected RACF database
    - Cracked RACF DES-encrypted passwords
  - Exfiltrated large quantity of very sensitive data

- Greatest threat to mainframe services availability - "Oops!"
  - Curtailing excessive authority helps guard against nefarious activities

Mainframe Security - Future Challenges

- Overcoming set-and-forget mentality
  - Maintaining strong security requires constant assessment of system configuration changes and software upgrades (e.g., ensuring new APF libraries are protected)
  - Implementations are often found to be incomplete or inadequate
  - Replacement of "Internal" security with "External" security still needed
  - Failure to leverage RACF's latest enhancements and features
    - KDFAES password encryption
    - Passphrase and MFA authentication
    - Dataset encryption
- Ensuring "authorized" system products adhere to integrity specification
- Ensuring TCP/IP applications do not have the same vulnerabilities as their non-mainframe equivalents
- Loss of mainframe talent due to aging mainframe population
  - Difficult to recruit younger staff due to perception mainframe is obsolete
  - Employers no longer invest in training as they once did
  - Outsourcing is not a good solution because outsourcers cannot find staff either

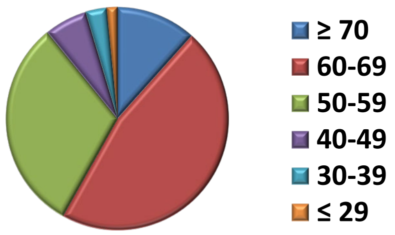
Mainframe Security - Survey - November 2022

RACF-L Demographics

At the time of this survey, RACF-L had approximately 1,500 subscribers in one form or another (regular, digest or index), of which about 300 were set to 'no mail'. Excluding the latter, this survey represents roughly 11% of the active RACF-L population.

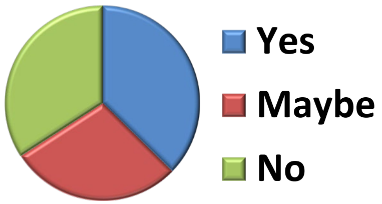
What is your age group?

Responses	Count	Percent %
70 and above	15	11.6%
60-69	60	46.5%
50-59	40	31.0%
40-49	8	6.2%
30-39	4	3.1%
29 and below	2	1.6%
Total	**129**	**100%**



Are you planning to retire in the next 5 years?

Responses	Count	Percent %
Yes	47	37.3%
Maybe	36	28.6%
No	43	34.1%
Total	**126**	**100%**


Yes
Maybe
No