Who Should You TRUST?

NY RUG
Oct 9, 2007

Walt Farrell, CISSP, IBM
STSM
z/OS Security Development
IBM Poughkeepsie
wfarrell@us.ibm.com

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

DB2*
e-business logo
IBM*
IBM eServer
IBM logo*
OS/390*
RACF*
z/OS*
Consul Products

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.
UNIX is a registered trademark of The Open Group in the United States and other countries.
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- **What does TRUSTED mean?**
- **What Address Spaces does z/OS provide?**
- **Which do we recommend to TRUST?**
- **Alternatives to TRUSTing them?**
- **Other factors to consider**
- **Conclusion**

What does TRUSTED mean?

- Normally applies only to started tasks (STCs) and system address spaces
- Causes **most** RACROUTE REQUEST=AUTH requests to succeed
  - Not used by REQUEST=FASTAUTH
- Similar to PRIVILEGED, but allows auditing:
  - Via UAUDIT (just that user)
  - Via SETROPTS LOGOPTIONS for the class (everyone)

What Address Spaces does z/OS provide?

- MASTER*
- PCAUTH*
- RASP*
- TRACE*
- DUMPSRV
- XCFAS
- GRS*
- SMSPDSE*
- SMSPDSE1*
- CONSOLE*
- WLM
- ANTMAIN
- ANTAS000
- DEVMAN
- JESXCF
- ALLOCAS*
- IOSAS
- AXR
- CEA
- SMF
- VLF
- VTAM
- JES2
- JES2AUX*
- JES2MON
- CATALOG
- TCAS
- LLA
- And many more+

- * Limited Function
- + See MVS Initialization and Tuning Guide Chapter 1

Which do we recommend to TRUST?

- From RACF books (Security Administrator's Guide, System Programmer's Guide), candidates for TRUSTED include:
  - JES, LLA, CATALOG, DUMPSRV, IEEVMPCR, SMF, VLF, VTAM, APSWPROC, RACF (if RRSF used), IXGLOGR and XCFAS (“if sysplex communication is used”)
- Why?
  - Lack of TRUSTED might prevent IPL
  - Critical for system operation
  - Access unpredictable resources

Alternatives to TRUSTing them?

- Figuring out which resources each STC or system address space really needs
  - Can require a lot of reading in the books (scattered)
  - Or a lot of testing
- Problem with not TRUSTing them: You have a less robust z/OS system:
  - PTFs or new system release could change list of resources
  - Perhaps you missed something in your testing
- Result: Potential unexpected IPL

Other factors to consider

- Limited Function address spaces: Always run with TRUSTED
- z/OS System Integrity Statement: Applies to most (all?) of the system address spaces and “standard” z/OS STCs
  - Anything running APF-authorized, supervisor state, or system key
  - If they can be used to compromise security/integrity call the IBM Support Center
- Finally, if the System Integrity Statement applies, and IF they can be compromised, it does not matter if you have TRUSTED them or not!
  - the attacker can do anything to the system that he wants

Other factors to consider (continued)

- The system address spaces and “standard” z/OS STCs perform a standard set of functions
  - You may not know what they all are, and so may have a hard time figuring out what resource access to grant
  - But they are key to the proper operation of the system
  - If you want z/OS to work, whatever they want to do has to work, too.

Conclusion

- For all those reasons, it's simply better to
  - TRUST the ones we suggest that you should
  - And *perhaps* even the rest of the standard ones that belong to z/OS
- However:
  - IBM should do a better job of documenting what all the system address spaces are and the basics of what they do
  - IBM should consider making more suggestions for what to TRUST
  - We have a SHARE requirement related to that

System Integrity Statement

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

IBM's commitment includes designs 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 to, 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 8, or Authorized Program Facility (APF) authorized. In the event that an IBM System Integrity problem is reported, IBM will always take action to resolve it.

Questions ?