z/OS 2.4 IBM Education Assistant (IEA)

Solution (Epic) Name: Change /dev/random to use TRNG

Element(s)/Component(s): z/OS UNIX System Services

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Session Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Session Objectives

- Explain the changes made to /dev/random.
- The behavior for /dev/random is that same as the behavior for /dev/urandom. Only /dev/random will me mentioned in this presentation.

Overview

- Who (Audience)
  - Any users of /dev/random or ssh.
- What (Solution)
  - When supported by the hardware, /dev/random will use the TRNG function of the PRNO instruction to generate random numbers.
- Wow (Benefit / Value, Need Addressed)
  - Removes the requirement of having to setup ICSF in order to access /dev/random.

Usage & Invocation

- Usage is transparent.
- Defaults to ICSF if TRNG is not supported.

Interactions & Dependencies

- To exploit this item, all systems in the Plex must be at the new z/OS level: No

- Software Dependencies
  - N/A
- Hardware Dependencies
  - TRNG support (z14 & above).
- Exploiters
  - N/A

Migration & Coexistence Considerations

- N/A

Installation

- N/A

Session Summary

- ICSF setup is no longer required to access /dev/random if TRNG is supported.
- TRNG is supported on z14 and above.
- Changes are transparent.

Appendix

- See the following publications for more information:
  - z/Architecture Principles of Operation
    - PRNO Instruction
  - z/OS UNIX System Services Planning
    - Creating special files: Random number files