z/OS 3.1 IBM Education Assistant

Solution Name: BCRYPT Hashing

Solution Element(s): ICSF

July 2023

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

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

Objectives

- Review high-level changes for BCRYPT hashing algorithm

Overview

- Who (Audience)
  - z/OS Application Programmers
- What (Solution)
  - BCRYPT hash generation and validation
- Wow (Benefit / Value, Need Addressed)
  - Parity with existing Java implementations

Usage & Invocation

- To utilize the new hashing algorithm, the existing One-Way Hash (CSNBOWH) callable service may be called with a new hashing method rule, "BCRYPT"
- When generating a BCRYPT hash, the callable service accepts the plaintext to be hashed along with a 'cost' parameter.
  - It returns a 'shadow password' containing a random salt, the cost, the algorithm version used, and the actual hash
- When validating a BCRYPT hash, the service accepts an existing hash and a plaintext.
  - It performs the hash on the plaintext using the same salt and cost present in the existing hash
  - It compares the result against the provided hash and determines if they match

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - None

Upgrade & Coexistence Considerations

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

Installation & Configuration

- No special installation or configuration actions are needed

Summary

- One-way hash callable service now supports the BCRYPT hashing algorithm

Appendix

- Publications
  - IBM Health Checker for z/OS User's Guide