z/TPF Security Enhancements

Jamie Farmer

IBM **z/TPF**

April 3rd, 2017

Agenda

- Addressing known OpenSSL security vulnerabilities that can affect z/TPF customers.
- Creating certificates with the SHA-256 digest algorithm, adhering to industry standards.

z/TPF OpenSSL Update

The OpenSSL package continues to be enhanced to address known security vulnerabilities that can affect z/TPF customers.

OpenSSL Upgrade to 1.0.2

- In January 2016, upgraded our existing OpenSSL support on z/TPF to the latest version
  - Version 1.0.2e
  - APAR PJ42982 and PJ43537
- Increased performance of the z/TPF OpenSSL processing by up to 12x
- Provided the following new function
  - Transport Layer Security versions 1.1 and 1.2
  - Secure Hash Algorithm 256 – SSL ciphers using SHA256
- Removed support of older SSL versions and ciphers
  - SSL version 2 and SSL version 3
  - RC2 and RC4 cipher algorithms

Addressing Known Security Vulnerabilities

- In March 2017, we upgraded the z/TPF OpenSSL package to address a known security vulnerability
  - Vulnerability could affect z/TPF customers
  - SSL Death Alert (CVE-2016-8610)
  - Upgraded OpenSSL to 1.0.2j version
  - APAR PJ44539 (PUT 14), available for download today
- APAR PJ44539 also disabled Heapcheck mode in shared SSL daemons to address memory depletion issues in z/TPF test systems

Creating z/TPF Certificates With The SHA-256 Digest Algorithm

To adhere to industry standards, z/TPF created certificates can be signed with the 256-bit Secure Hash Algorithm (SHA-256).

Creating z/TPF Certificates

- The z/TPF secure keystore can hold public/private key pairs used for RSA operations
    - The private key is never in the clear
    - The public key is usually distributed to remote systems in the form of a signed certificate.
- Self signed certificates or certificate requests can be created from z/TPF public/private key pairs using the ZPUBK REQCERT command.
    - Certificate requests are eventually signed by trusted third parties referred to as Certificate Authorities.
- Currently the certificates created on z/TPF can only be signed using the MD5 or SHA-1 digest algorithms

Digital Certificates Signed With The SHA-256 Digest Algorithm

- Industry security standards now recommend digital certificates be signed with the SHA-256 digest algorithm.
    - Many times, customer security audits require certificates to be signed with SHA-256 algorithm
- APAR PJ44481 provided the ability to issue ZPUBK REQCERT with an option for a SHA-256 digital signature.
    - PUT 14 APAR, closed in December 2016 and available for download today.
- The OpenSSL upgrade to 1.0.2 delivered in January 2016 made this possible and is required to use this support.

SHA-256 Digital Certificate Example

```
User:   ZPUBK REQCERT PATH-/tmp/tpfCertReq.pem KEYPAIR-tpf2048 CONFIG-/sslcfg/myssl.cnf DIGEST-SHA256

System: CSMP0097I 20.20.34 CPU-B SS-BSS  SSU-HPN  IS-01
        PUBK0004I 20.20.34 CERTIFICATE REQUEST GENERATED ON FILE /tmp/tpfCertReq.pem
```

```
Signature Algorithm: sha256WithRSAEncryption
        44:b1:b2:b7:2a:6e:ea:53:95:13:fe:d1:4f:05:18:71:a3:a8:
        01:06:c9:e6:84:ab:4c:46:47:72:3b:ef:42:c5:df:bc:a7:3b:
        cd:a3:87:2f:02:9a:05:a1:3b:45:71:57:ef:88:83:93:d8:71:
        61:a3:53:c2:98:f1:6a:96:79:7a:09:20:2b:e3:65:57:42:2a:
        57:de:d3:5f:31:9e:c1:7c:0e:55:2c:f9:7e:8f:69:81:aa:bc:
        76:a4:ce:12:33:31:c1:81:f6:2d:2c:df:c1:61:59:68:f6:23:
        85:68:1b:48:f3:f7:fc:22:60:63:90:1d:57:38:aa:36:10:32:
        31:34
```

Summary

- PJ43539 (PUT 14)
  - The OpenSSL package continues to be enhanced to address known security vulnerabilities that can affect z/TPF customers.
- PJ44481 (PUT 14)
  - To adhere to industry standards, z/TPF created certificates can be signed with the 256-bit Secure Hash Algorithm (SHA-256).

THANK YOU

Questions or comments?

Jamie Farmer

IBM **z/TPF**

April 3rd, 2017

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.

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.

This presentation and the claims outlined in it were reviewed for compliance with US law. Adaptations of these claims for use in other geographies must be reviewed by the local country counsel for compliance with local laws.