Subject: ZFS Encrypted Datasets

Submitted by: Darren Moffat

File: PSARC/2007/261/opinion.ms

Date: February 6, 2008

Committee: Darren Moffat (opinion written by Garrett D'Amore), Kais Belgaied, Mark Carlson, Joseph Kowalski, Glenn Skinner.

Product Approval Committee:

Solaris PAC
solaris-pac-opinion@sun.com

1. Summary

ZFS Encrypted Datasets is a project to provide cryptographic security to ZFS datasets. Specifically, it is intended to protect against theft of physical storage, man-in-the-middle attacks on the SAN, and to provide dataset level secured deletion. Data is encrypted at the data set level, allowing a mix of encrypted and unencrypted data in the same ZFS storage pool. The ZFS command-line and graphical user interfaces will be updated accordingly.

2. Decision & Precedence Information

The project is approved as specified in reference [1].

The project may be delivered in a patch release of the ON consolidation.

The project depends on the following other project and may not be delivered before it.

PSARC/2007/266
AES CCM for kernel crypto framework

3. Interfaces

The project exports the following interfaces.

Interfaces Exported		
Interface	Classification	Comments
encryption	Committed	Dataset property
sha256+ccm	Committed	Dataset checksum property value
keyscope	Committed	Dataset property
keysource	Committed	Dataset/pool property
keystatus	Committed	Dataset/pool property
zfs key	Committed	ZFS dataset key command
zpool key	Committed	ZFS pool key command

The project imports the following interfaces.

Interfaces Imported		
Interface	Classification	Comments
Kernel Cryptographic subsystem	Consolidation Private	PSARC 2001/533

4. Opinion

4.1. Encrypted swap.

The project team noted that encryption of a dataset used for swap was possible, but suffers from several security limitations which prevent it from being fully secure. The project team recommended that a project be funded to investigate resolving these limitations, involving both the memory subsystem and the security teams.

4.2. Documentation of key compromise

During discussion, it was noted that documentation covering policy and procedures for handling of various forms of key compromise was required. The project team indicated that it plans to update the System Administration guide to cover this, but one member noted that it would be desirable to include at least a reference to the guide in the zfs and/or zpool manual pages.

5. Minority Opinion(s)

None.

6. Advisory Information

A project to investigate properly securing swap using cryptography should be funded, involving both the security and virtual memory teams.

7. Appendices

7.1. Appendix A: Technical Changes Required

None.

7.2. Appendix B: Technical Changes Advised

None.

7.3. Appendix C: Reference Material

Unless stated otherwise, path names are relative to the case directory PSARC/2007/261.

1. One pager
   File: 20070509_darren.moffat
2. Design document
   File: commitment.materials/zfs-crypto-design.pdf
3. Updated zfs manual page
   File: commitment.materials/zfs.1m
4. Updated zpool manual page
   File: commitment.materials/zpool.1m
5. Command line examples
   File: commitment.materials/cli-examples.txt
6. Notes from commitment review
   File: 20080206.2007.261.commitment
7. OpenSolaris Project web page
   URL: http://opensolaris.org/os/project/zfs-crypto/

