



OpenVMS Security Update

3N03

Helmut Ammer
Technical Consultant OpenVMS
CCCSC



© 2004 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice



Überblick

- OpenVMS: Security by Design
- MUPs & Updates
- OpenVMS V7.3-2 Security
- Security Roadmap

3N03 OpenVMS Security Update

2

OpenVMS: Security by Design

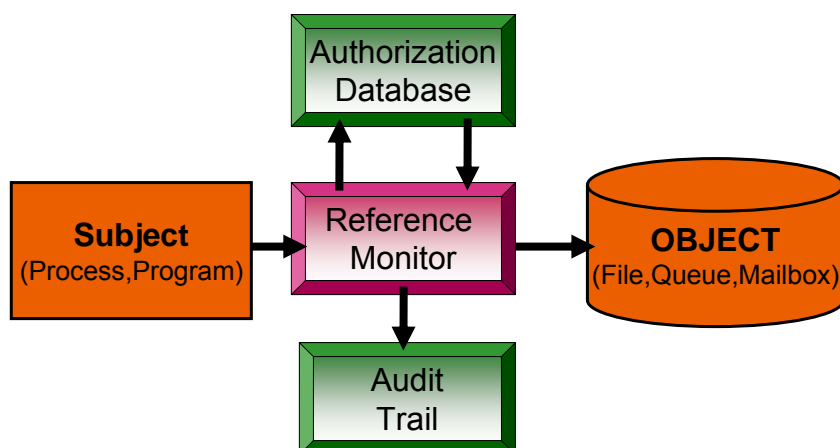


- Security was designed into VMS since V1.0
 - Subjects have UIC's (User Identification Code)
 - Objects have SOGW (Multiple levels of protection)
- The security model has been expanded encompassing new computing environments
 - Proxy access (to allow specific remote users in)
 - Captive Account (limiting access to specific uses)
 - Intrusion detection – Clusterwide!
 - ACLs (Access Control lists)
 - Protected Subsystems

3N03 OpenVMS Security Update

3

OpenVMS Security Model



Access from a Subject to an Object is mediated by the reference monitor to ensure it is authorized and audited.

3N03 OpenVMS Security Update

4

Security Defaults



- Discretionary Access Control Security (Commonly referred to as "C2") enabled by default
 - Including secure installation and password functions
- A single security domain encompasses:
 - System
 - Soft Partition (Galaxy)
 - Cluster
- Multiple-mode operating system
 - The operating system runs in a privileged mode protecting against modification by user level code.
- Secure File system
 - The OpenVMS file system can restrict non-privileged programs and processes from modifying system programs and files on disk.

3N03 OpenVMS Security Update

5


Viruses on OpenVMS



- It is possible for an OpenVMS system to be infected by a virus, but to do so, the program containing the virus would have to be run from a user account that has amplified privileges.
- As long as the system administrator is careful that only trusted applications are run from privileged accounts there is no known danger from viruses on OpenVMS.
- It is possible to store PC files on OpenVMS systems, so 3rd party virus scanners are available that run on OpenVMS and will scan these stored PC files for known PC viruses.
- There have been "Worms" on OpenVMS in the past a properly configured system minimizes this threat.

3N03 OpenVMS Security Update


6



MUPs & Updates

- OpenVMS Alpha 7.2-2, 7.3 7 7.3-1 MUP
- DCE/COM denial of service (all up to 7.3-2)
- DECWindows MUP (all up to 7.3)
- OpenVMS Alpha 7.2
 - DEC-AXPVMS-VMS72_SYS-V0100-4
 - DEC-AXPVMS-VMS721_SYS-V0100-4
- OpenVMS Alpha security MUP
 - ALPSMUP01_070 (versions 6.1,6.2 & 7.0)
- OpenVMS VAX security MUP
 - VAXSMUP03 (all versions prior to 6.1)
- Layered products:
 - New version of SSL and Kerberos
 - ACMS,POP and Secure Web Server updates

3N03 OpenVMS Security Update 7




OpenVMS Alpha V7.2-2, V7.3 & V7.3-1 MUP

- OpenVMS Engineering has determined that systems running OpenVMS Alpha V7.2-2, OpenVMS Alpha V7.3 or OpenVMS Alpha V7.3-1 have a potential security vulnerability. This vulnerability could be exploited to allow for unauthorized access to data and system resources.
- The Security MUP is included in the OpenVMS Alpha SYS kit and later

Version	SYS kit
OpenVMS Alpha V7.3-1	DEC-AXPVMS-VMS731_SYS-V0400-4.PCSI
OpenVMS Alpha V7.3	DEC-AXPVMS-VMS73_SYS-V0700-4.PCSI
OpenVMS Alpha V7.2-2	DEC-AXPVMS-VMS722_SYS-V0200-4.PCSI
- HP recommends that you apply this update to your systems immediately. After you apply this update, **you must reboot your system in order for the changes to take effect.**
- CD OVMSALPMUP3 is included with the OpenVMS 7.3-2 kit.

3N03 OpenVMS Security Update 8




DCE / COM Denial of Service

OpenVMS systems with DCE or COM installed or are using the RPC portion of DCE in the Base OpenVMS operating system are susceptible to a remote initiated Buffer Overflow, that hangs DCE or COM applications on OpenVMS.

Application	Architecture	Versions
COM	Alpha	V7.2-2, V7.3, V7.3-1
	VAX	N/A
DCE/RPC	Alpha	V6.2, V6.2-1H*, V7.1, V7.2, V7.2-* V7.3, V7.3-1
	VAX	V6.2, V7.1, V7.2, V7.3

3N03 OpenVMS Security Update 9



DCE / COM DoS (Resolution)

Application	Architecture	Patch Kit
COM	Alpha	DCOM_013_SSRT3608-V0100
	VAX	N/A
DCE/RPC	Alpha	ALP_DCE_030_SSRT3608-V0100
	VAX	VAX_DCE_030_SSRT3608-V0100

3N03 OpenVMS Security Update 10

DECwindows MUP



DECwindows Motif server has a potential security vulnerability that could be exploited to allow existing users unauthorized access to data and system resources

NOTE: This mandatory update required a reboot!

- Effected systems are only those that have DECwindows server installed on them
- Supported versions impacted:
 - OpenVMS Alpha version 6.2 7.1-2, 7.2-1h1, 7.2-2, 7.3
 - OpenVMS VAX version 6.2, 7.1, 7.2, 7.3
 - SEVMS Alpha version 6.2 & SEVMS VAX version 6.2

3N03 OpenVMS Security Update

11

TCP/IP V5.3 MUP



- A CD shipped with OpenVMS V7.3-1 that includes the TCP/IP data corruptor for NFS server.
- Part number: AG-RTBNA-BE
- The fix is included in the latest TCP/IP ECO kit

3N03 OpenVMS Security Update


12



Security Products

- Install always latest version of
 - HP SSL
 - HP Kerberos
- <http://h71000.www7.hp.com/openvms/security.html>

3N03 OpenVMS Security Update 13




ACMS Security Advisory

There is a potential security vulnerability involving ACMS processes having more privileges enabled than the privileges specified in the authorization file.

To protect against this potential security risk, HP is making available an update ECO for ACMS V4.3 customers running OpenVMS Alpha V7.2-1, V7.2-1H1, V7.2-2, and V7.3.

For ACMS V4.4 customers a new version ACMS V4.4A. ACMS V4.4 customers should upgrade to V4.4A immediately.

3N03 OpenVMS Security Update 14



POP Server

A potential vulnerability has been reported where a local authorized non-privileged user could gain unauthorized access to privileged files. The report is of a potential locally exploitable file corruption issue with HP TCP/IP services for OpenVMS POP server. This problem does not exist if the POP server is disabled.

To determine if the service is enabled, execute the following command:


```
$ tcpip show service pop
```

Service	Port	Proto	Process	Address	State
POP	110	TCP	TCPIP\$POP	0.0.0.0	Enabled

Effected HP TCP/IP services for OpenVMS versions:
V5.3, V5.1, V5.0a, V4.2

Resolution Install: HP TCP/IP Services for OpenVMS V5.3 ECO 2

3N03 OpenVMS Security Update 15



Secure Web Server

<http://h71000.www7.hp.com/openvms/products/ips/apache/>

Secure Web Server V1.3 or V1.2 security issues do not compromise the OpenVMS System Security but data compromised could be possible.

CSWSx_UPDATES: (New updates 29-Oct-2003)

For CSWS V1.3: [CSWS13_UPDATE V4.0](#)

For CSWS V1.2: [CSWS12_UPDATE V7.0](#)

CSWS_PHPx_UPDATE:

For CSWS_PHP V1.1: [CSWS_PHP11_UPDATE V1.0](#)

For CSWS_PHP V1.0: [CSWS_PHP10_UPDATE V1.0](#)

Note: these kits are cumulative and supersede previous kits.

3N03 OpenVMS Security Update 16




Security Advisories

HP's SSRT (Software Security Response Team) is the liaison to CERT organization <http://www.cert.org/>

Information on all of hps current security advisories can be mail to you.
See
<http://www.support.compaq.com/patches/mail-list.shtml>


3N03 OpenVMS Security Update 17



OpenVMS V7.3-2

- Documentation
 - Guide to System Security
 - Open Source Security for OpenVMS
 - Vol 1: Common Data Security Architecture
 - Vol 2: HP SSL (Secure Socket Layer)
 - Vol 3: Kerberos
 - HP TCP/IP Services for OpenVMS: Guide to SSH


3N03 OpenVMS Security Update 18



OpenVMS V7.3-2

- Mixed Case Passwords
 - UAF Flag: /FLAGS=PWDMIX
- Unix Portability Features
 - Support for UID and GUID UNIX security identifiers
 - CDE deadman (idle process killer)
 - CDE screen lock


3N03 OpenVMS Security Update 19



OpenVMS V7.3-2

- CDSA V7.3-2
 - Update to OpenSSL V0.9.6g
 - Automatically installed with V7.3-2
 - Do NOT remove
- CDSA must be initialized before use
\$ @SYS\$STARTUP:CDSA\$UPGRADE
- Symbol setup for CDSA
\$ @SYS\$MANAGER:CDSA\$SYMBOLS


3N03 OpenVMS Security Update 20



OpenVMS V7.3-2

- HP Kerberos V2.0 for OpenVMS
 - Mandatory SIP kit for OpenVMS V7.3-2
 - Can be installed on earlier versions of OpenVMS
- Kerberos V2.0 features
 - Fixes for CERT security advisories of MIT Kerberos
 - Support for triple DES encryption
 - Database enhancements
 - DNS support for locating Key Distribution Centers (KDCs)
 - Support for new Key Version Number utility (kvno)
 - Support for building 32-bit and 64-bit applications
 - Kerberos V4.0 interoperability
 - Many bug fixes from MIT

3N03 OpenVMS Security Update 21



OpenVMS V7.3-2

- HP Secure Socket Layer (SSL) V1.1-A
 - Port of OpenSSL V0.9.6g with several fixes
<http://www.openssl.org/news/>
 - HP homepage
<http://h71000.www7.hp.com/opensource/opensource.html#ssl>
- Layered product
- More information:
Session 2F06 DECUS Symposium 2003

3N03 OpenVMS Security Update 22

TCP/IP Services for OpenVMS V5.4


- Secure Shell (SSH) Client and Server
- Secure Socket Layer (SSL) for POP
- failSAVE IP

3N03 OpenVMS Security Update 23

What is SSL?

- Secure Sockets Layer
- Secures data communication between a client and server at the transport layer
- Authenticates the Server (by default) and the client (optionally)
- Provides data confidentiality
- Ensures data integrity


3N03 OpenVMS Security Update 24



SSL & OpenSSL

- Netscape developed SSL V2 & V3
- Transport layer security (TLS) is RFC 2246
- OpenSSL is a toolkit that provides:
 - SSLv2 & v3 protocols
 - TLS v1 protocol
 - Cryptographic algorithms
- OpenSSL is packaged to include:
 - An SSL library
 - A cryptographic library
 - A command line utility

3N03 OpenVMS Security Update 25




VMS changes to OpenSSL

- Ported 0.9.6G (V1.1-A)
- Added 64-bit API support.
- Added a menu-driven certificate tool.
- Removed static linking against UCX.
 - Allow DECC\$ calls to resolve to the installed IP stack.
- Added VMS PRNG support.
- Enhanced the documentation.
- Cleaned up VAX specifics & have PCSI kit available.
- And many more ... all of which are being sent back to the OpenSSL group - <ftp://ftp.openssl.org/snapshot/>.
 - openssl-VMS_64bit-snap-yyyyymmdd.tar.gz

<http://h71000.www7.hp.com/openvms/security.html#ssl>


3N03 OpenVMS Security Update 26



Kerberos? What's that?

- Kerberos is from Greek Mythology and is the three headed guard dog to Hades
 - Cerberus is the Roman spelling.
- Kerberos project History
 - Developed in 1984 at M.I.T. in Project Athena
 - Versions 1-3 M.I.T. Internal Athena use only
 - Version 4 (Available to the public) ~1988
 - Version 5 (Commercial ready) ~1997

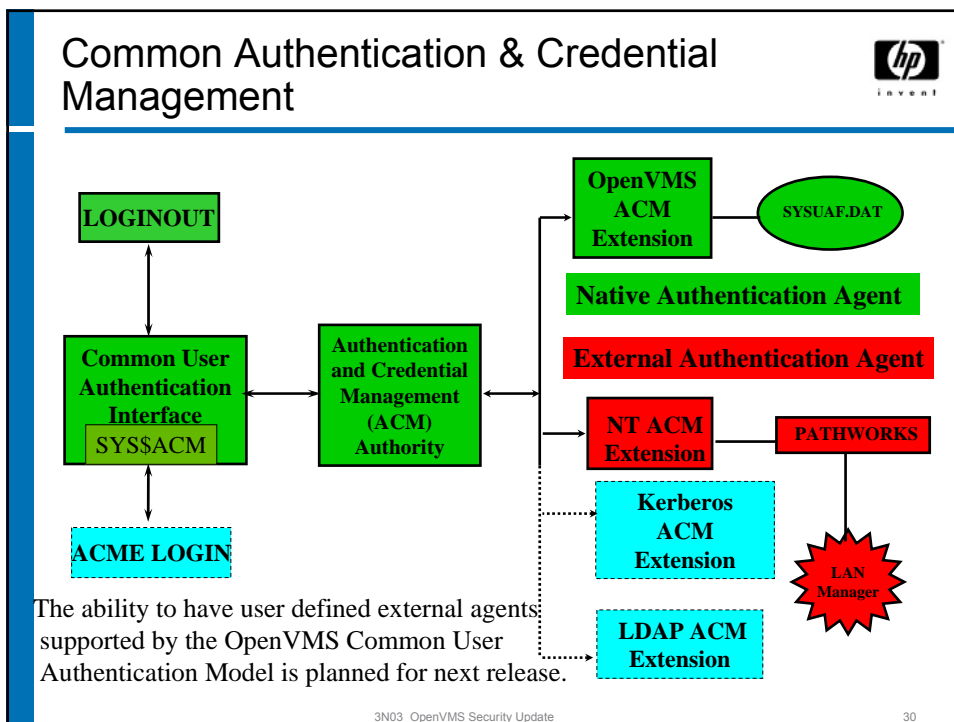
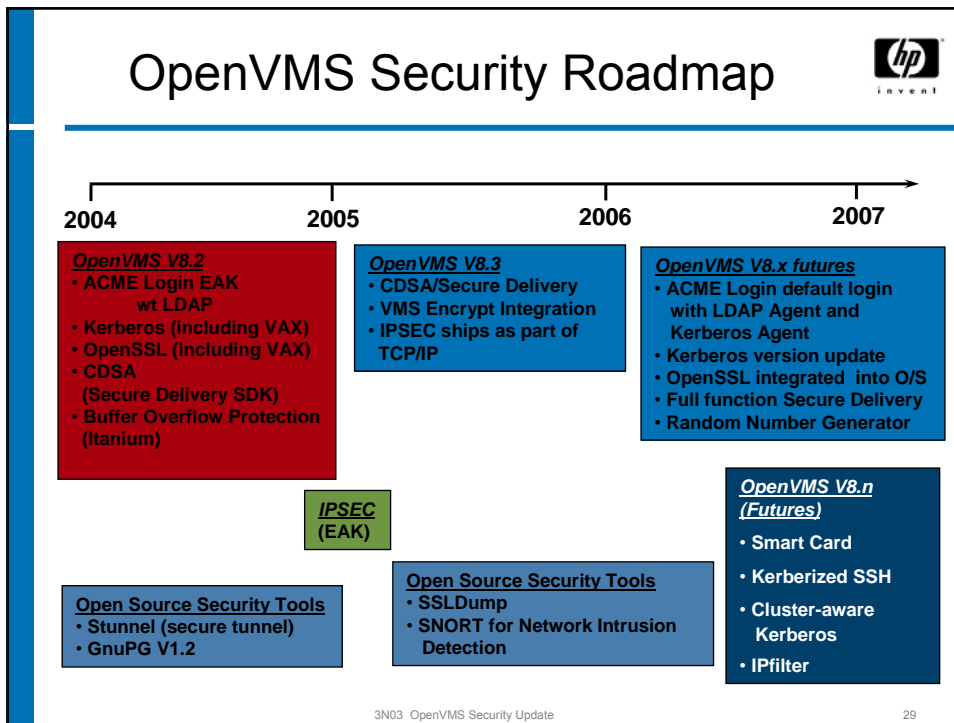
3N03 OpenVMS Security Update 27

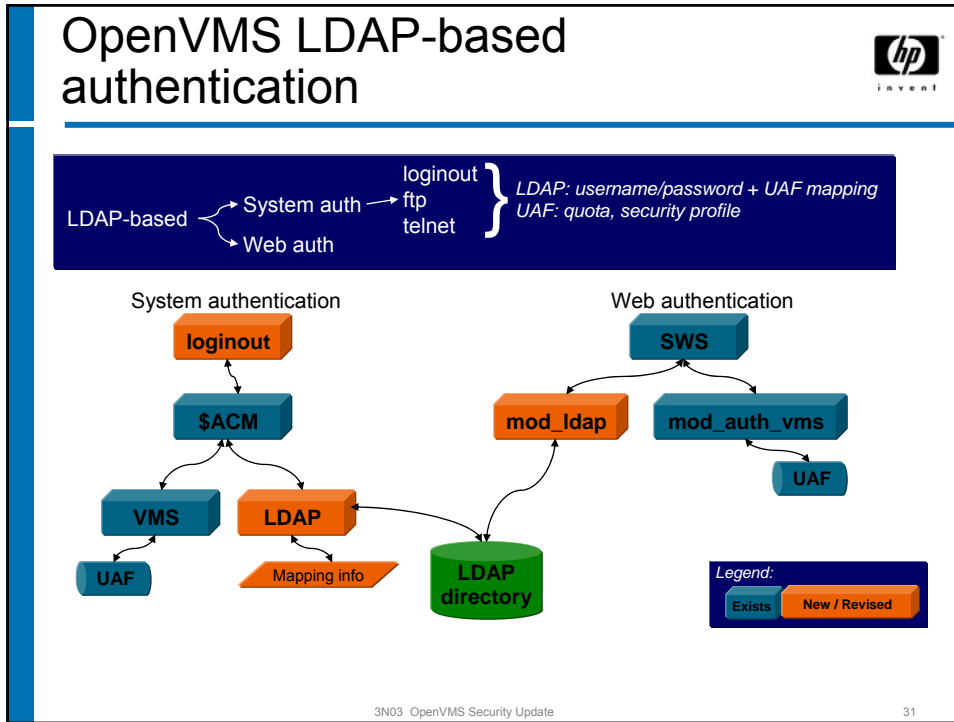


Kerberos Overview

- Kerberos was developed to provide a method of user authentication so that no password will cross the internet in a clear text or readable format.
 - Kerberos uses a series of cryptographic tickets to authenticate user requests, so that passwords are not transmitted in a clear text or easily readable form.
 - OpenVMS V7.3-1 provides both client and server support that is integrated into the operating system.

3N03 OpenVMS Security Update 28





Questions?

