



OpenVMS
Security Update

1G03

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 V8.2 Security
- Security Roadmap

3N03 OpenVMS Security Update

2



OpenVMS: Security by Design

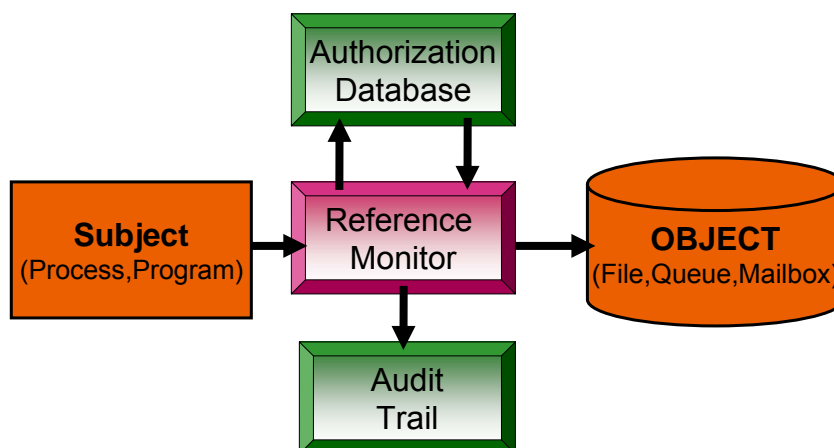
- Security was designed into VMS since V1.0
 - Subjects have UIC's (User Identification Code)
 - Objects have SOGW (Multiple levels of protection)
- The security model has been expanded encompassing new computing environments
 - Proxy access (to allow specific remote users in)
 - Captive Account (limiting 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 MUP (Feb 2005)
- OpenVMS Alpha 7.2-2, 7.3, 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 MUP (SSRT4866)

- Local authorized user can get unauthorized privileged access to data and system resources
- OpenVMS VAX and Alpha V6.* and V7.*
- MUP CD (shipping with OpenVMS V8.2) that includes a Mandatory Update for the supported version of OpenVMS:
 - V7.3-2 (Alpha)
 - V7.3-1 (Alpha)
 - V7.3 (VAX)
 - V6.2 (VAX and Alpha)
- 2 Installation Kits (VMSMUP and DNVOSIMUP)

3N03 OpenVMS Security Update

8

OpenVMS Alpha V7.2-2, V7.3 & V7.3-1 MUP (Nov 2003)



- 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

9

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


10



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 11



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 12



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



Security Products

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



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

15



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

16


OpenVMS V8.2



- 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 19

ACMELOGIN External Authentication



- For OpenVMS 8.2 the new ACMELOGIN External Authentication will remain as an SDK this includes the LDAP external authentication.
 - Kit & Documentation available in SYS\$EXAMPLES:
 - Integrity:
 - External authentication with NT Domains requires an Alpha Advanced Server in the cluster.
 - ACME Subsystem must be started manually. (See release note)
- With OpenVMS 8.n full functionality including
 - LDAP external Authentication
 - Kerberos

3N03 OpenVMS Security Update 20



Kerberos V2.1

- There are three significant changes to Kerberos 1.2 in OpenVMS V8.2:
- Additional security patches
 - MIT has released a number of additional security patches that have been included in the OpenVMS release
- Addition of "ktutil" utility
 - Kerberos for OpenVMS V2.0 was missing the ktutil program, which allows a user to read, write, or edit a keytab file.
- Kerberized Telnet supports forwarding credentials to an OpenVMS system with TCP/IP V5.5

3N03 OpenVMS Security Update

21




CDSA (Common Data Security Arch.)

- AES Encryption
 - CDSA now supports AES encryption in addition to the encryption types previously supported
 - A new example program in `SYS$COMMON:[SYSHLP.EXAMPLES.CDSA.AES]` shows how to use AES encryption with CDSA
- Secure Delivery ADK
 - The first pieces is being delivered as an Advanced Developer's Kit in OpenVMS V8.2
 - Secure Delivery allows the creation and verification of a "manifest" for any software kit
 - This manifest uses cryptographic digital signatures to ensure that the kit has not been tampered with in any way
 - A manifest can be created for any arbitrary file, although the full power of Secure Delivery is primarily focused on PCSI kits

3N03 OpenVMS Security Update

22




SSL for OpenVMS

- V1.1-B – port of OpenSSL 0.9.6G with Security Patches
 - Available now on hp VMS website
 - Download PCSI kit from the OpenVMS security website

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

- V1.2 – port of OpenSSL 0.9.7D – latest & greatest
 - Advanced Encryption Standard (AES)
 - Elliptical Curve Cryptography
 - Online Certificate Status Protocol (OCSP)
 - Install off-system disk
 - Ship with OpenVMS V8.2
 - Alpha & Itanium wt OpenVMS 8.2.

3N03 OpenVMS Security Update 23



Advanced Encryption Standard (AES)

- Replacement for Data Encryption Standard (DES)
- A.K.A. Rijndael
- RFC 3268 - Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)
- FIP Pub 197
- AES key lengths of 128, 192 and 256 bits.
- AES vs. DES
 - DES keys are 56 bits
 - 10^{21} times more AES 128-bit keys than DES 56 bit keys

If a DES 56-bit key is recovered in a second ...
... an AES 128-key recovered 149 trillion years

3N03 OpenVMS Security Update 24



Elliptical Curve Cryptography

- Public key encryption based on elliptical curve theory.
 - Keys generated from properties of elliptic curve equation
 - Instead of very large prime numbers
- Smaller keys
 - Faster, more efficient cryptographic keys
- Just as secure
 - 164-bit key same level of security as 1024 bit key
- Smaller numbers -> smaller keys -> less computing -> less power -> more battery life
 - Developed by Certicom, ECC used in mobile applications
 - (http://searchsecurity.techtarget.com/sDefinition/0,,sid14_g)

3N03 OpenVMS Security Update

25




Online Certificate Status Protocol

- Allows applications to determine the revocation state of a certificate.
- Allows for more timely status information vs. Certificate Revocation Lists (CRLs)
- Can act as an OCSP server (responder)
 - Process incoming requests
 - Issues responses
- Or as an OCSP client
 - Create and send requests to an OCSP server
 - Print requests and responses
- OpenSSL OCSP server and client for test and demo only

3N03 OpenVMS Security Update


26



Encryption for OpenVMS

- 56-Bit DES encryption that understands Backup
- Current Version 1.6 has been ported to I64.
- For OpenVMS V8.2 no license required
- Ships on LP CD

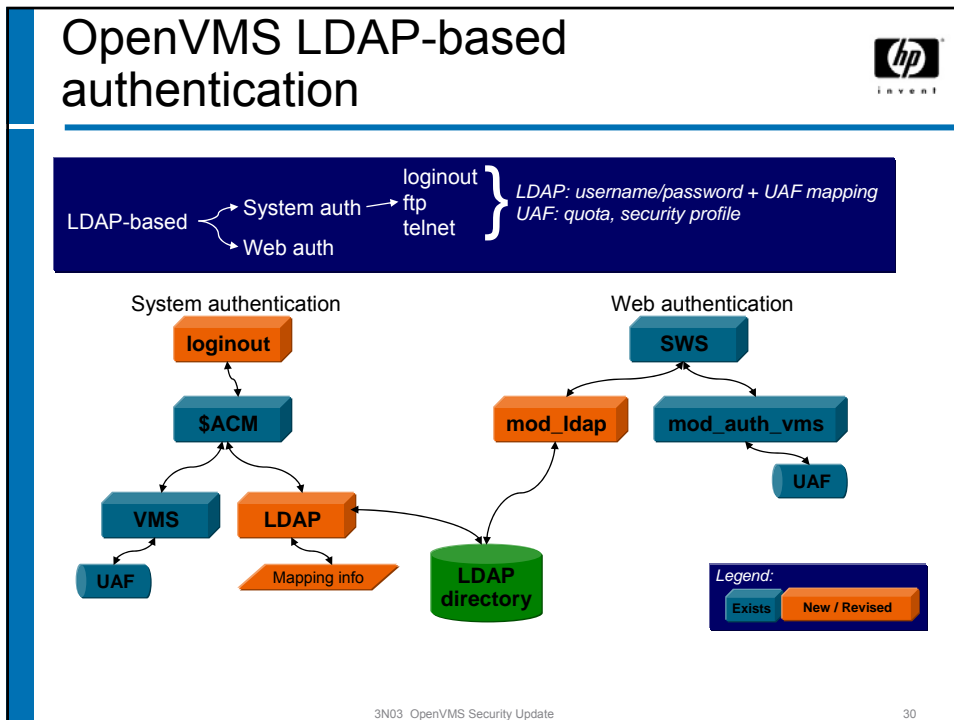
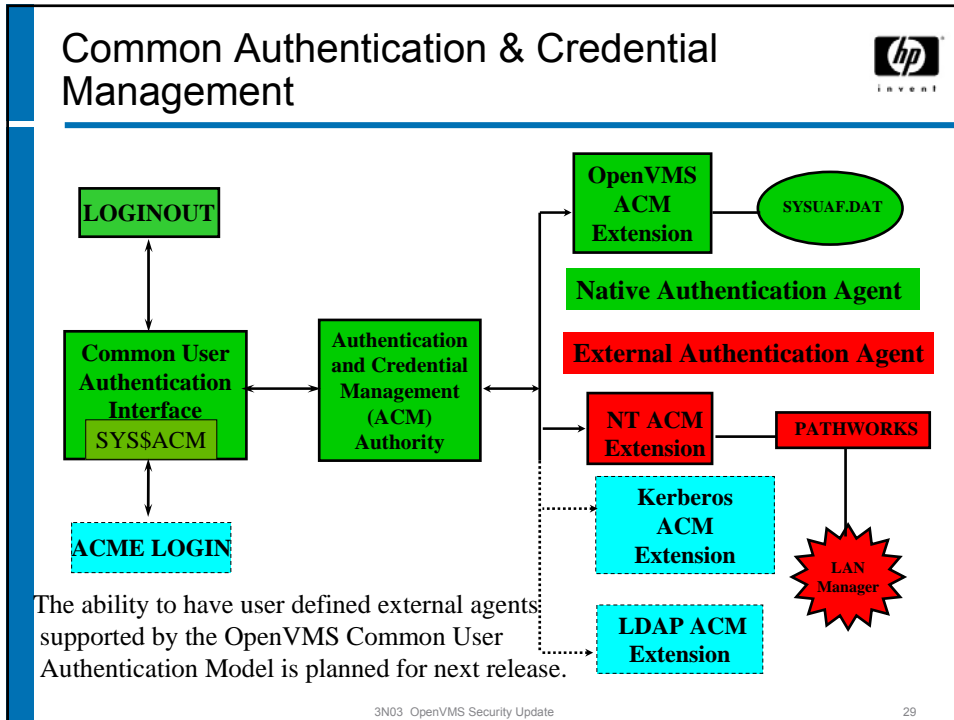
3N03 OpenVMS Security Update 27



OpenVMS Security Roadmap

2005	2006	2007	2008	2009
<p>OpenVMS V8.2</p> <ul style="list-style-type: none"> • ACME Login EAK wt LDAP • Kerberos 1.2 • OpenSSL 1.2 • CDSA (Secure Delivery SDK) • Buffer Overflow Protection (Integrity Servers only) 	<p>OpenVMS V8.3 *</p> <ul style="list-style-type: none"> • Production Quality ACME Login wt LDAP & Kerberos Agents • CDSA/Secure Delivery • VMS Encrypt Integration • IPSEC ships as part of TCP/IP • Kerberos version update 	<p>OpenVMS V8.4</p> <ul style="list-style-type: none"> • ACME Login is the default login with LDAP & and Kerberos Agents • Full function Secure Delivery 	<p>OpenVMS V8.n (Futures)</p> <ul style="list-style-type: none"> • Smart Card • Kerberized SSH • IPfilter 	
<p>Open Source Security Tools</p> <ul style="list-style-type: none"> • Stunnel (secure tunnel) • GnuPG V1.2.4 		<p>Open Source Security Tools</p> <ul style="list-style-type: none"> • SSLDump • SNORT for Network Intrusion Detection 		
		<p>IPSEC EAK</p>		

3N03 OpenVMS Security Update 28



Questions?

