OpenVMS Security - What Technologies Are Provided
Session #: 3845

Leo Demers

OpenVMS Security Product Manager
Hewlett-Packard

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

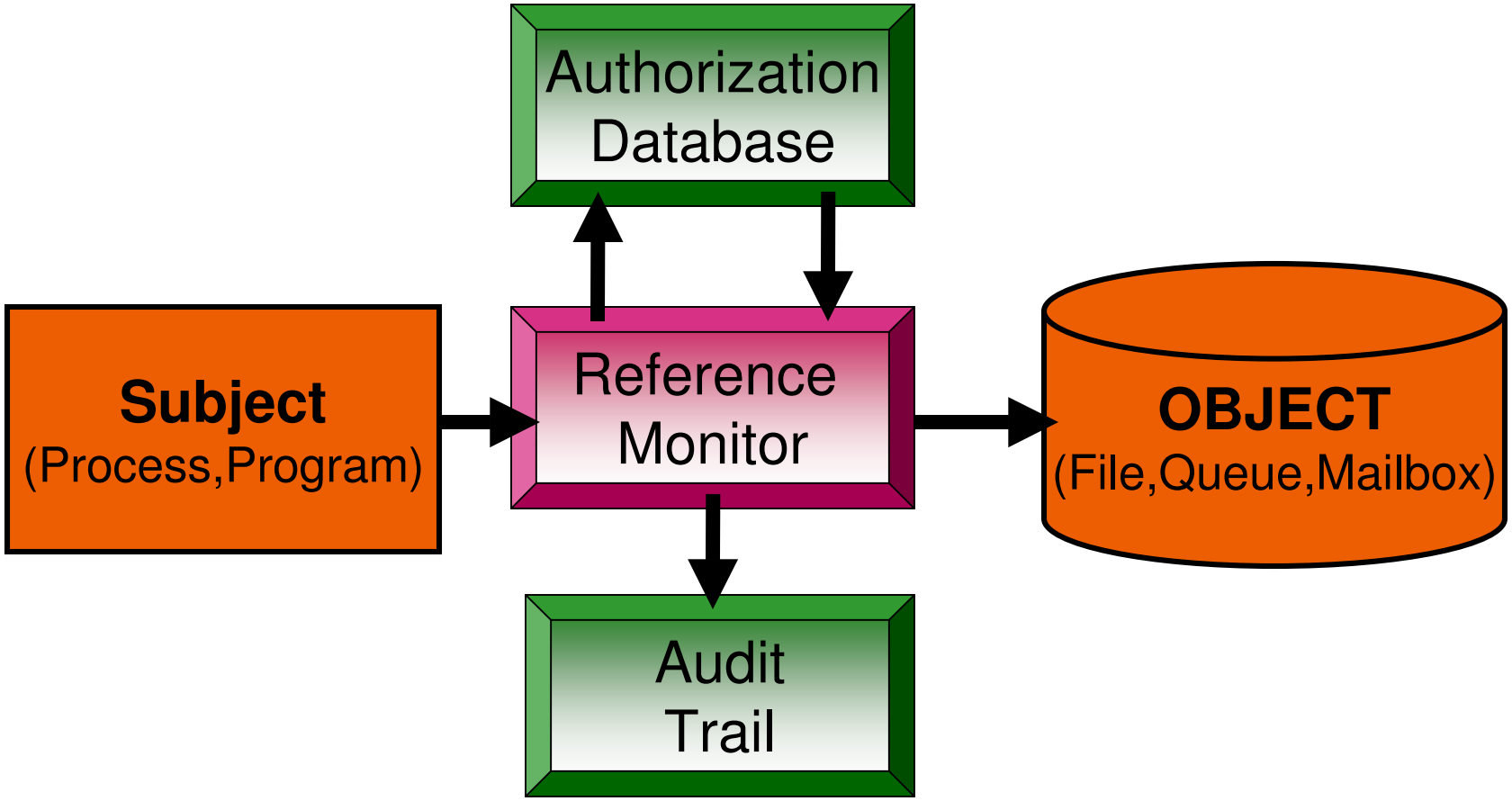
Agenda

- OpenVMS security Why it's so secure
- Security Management Basics
- Connecting to the world Securely
  - SSH
  - SSL
  - Kerberos
  - External Authentication
- Roadmap Review
- What's next

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)
  - ACLs (Access Control lists)
  - Protected Subsystems
  - Intrusion detection – Clusterwide

The OpenVMS Security Model



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

Securing OpenVMS
”It’s the Data”

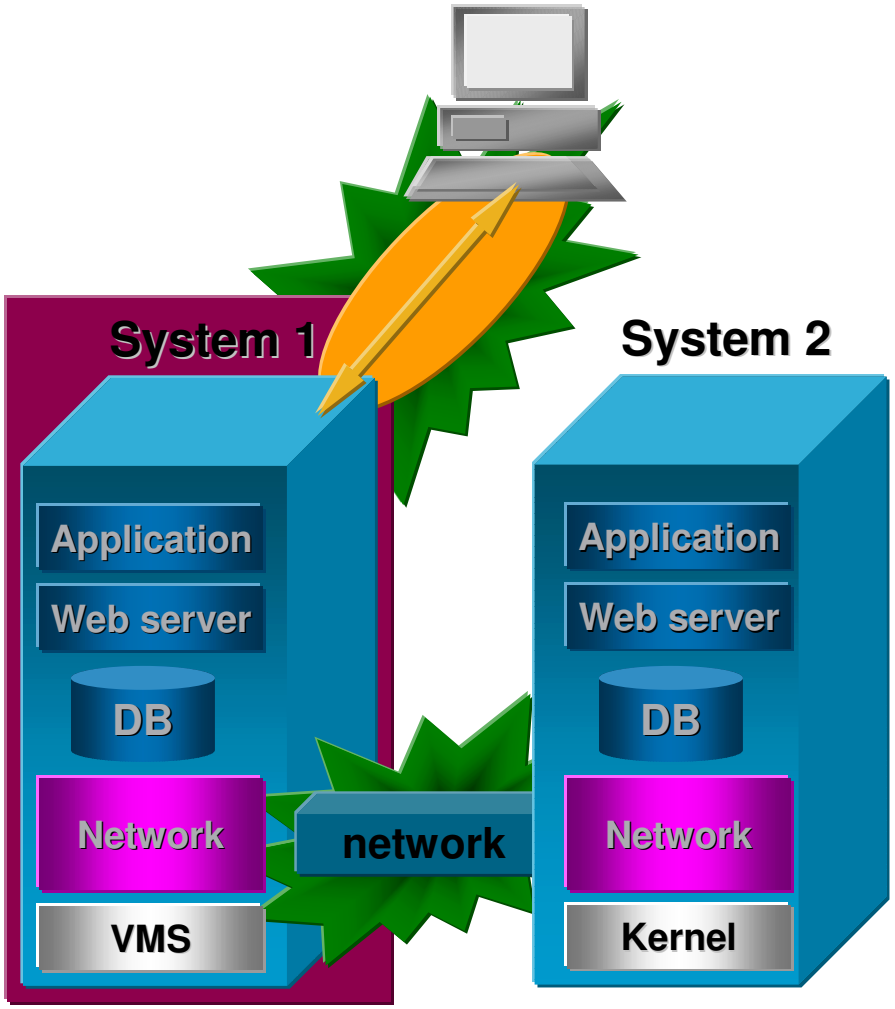
Server Security

- Authentication
- Authorization
- Access control

Transport Security

- Confidentiality
- Integrity

- Non-repudiation



The OpenVMS Security plan

- Support standards based security technologies for secure heterogeneous communication
  - CDSA (common data security architecture)
  - Kerberos V5 API's, KDC (key distribution center) and GSSAPI V2
  - OpenSSL (secure socket layer)
  - SSH V2 (secure shell
- Provide Open Source security tools
  - Stunnel (secure tunnel)
  - GnuPG (encryption for mail/digital signatures)
- Expand OpenVMS authentication
  - SYS$ACM API is a single API call simplifying application authentication
  - An ACME (authentication and credential management extensions) SDK will be available with OpenVMS 7.3-2
    - An LDAP ACME agent SDK will also be provided

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.

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.
- Is 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.

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

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.
- The MUP is in OpenVMS Alpha SYS kit.

O/S Version	Minimum SYS kit version
– 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

- CD ALPSMUP02 is included with the OpenVMS 7.3-2 distribution media kit.

DCE / COM Denial of Service

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

DCE / COM DoS (Resolution)

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	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

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

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

OpenVMS 7.2 MUP details

Non-Privileged System Crasher…

- Affects these OpenVMS Alpha releases.
  - V7.2-1
  - V7.2 with UPDATE V1.0
  - V7.2 with HARDWARE V1.0
- Which ECO do you need to apply
  - V7.2, V7.2-1 SYS ECO kits… or...
  - V7.2 UPDATE V2.0 ECO kit or higher
    - Merges UPDATE, HARDWARE, SYS

More MUP Details

- ALPSMUP01_070
- “Applications that creates accounts during installation may have those newly created accounts passwords compromised.
- VAXSMUP03
- “Many known exploits were corrected with the kit”
- Has VAXSMUP03 been applied to my system?
- IfSYS$COMMON:[SYSUPD]VAXSMUP03_060_IMAGE.DAT exists, Yes it has.

Security Update (SSL)

http://h71000.www7.hp.com/openvms/security.html

- HP SSL Version 1.1-B for OpenVMS Alpha is based on OpenSSL 0.9.6g, and includes the latest OpenSSL fixes
- Details on these fixes can be found at
  - 17-Mar-2004 http://www.openssl.org/news/secadv_20040317.txt
  - 30-Sept-2003 http://www.openssl.org/news/secadv_20030930.txt
  - 19-Mar-2003 http://www.openssl.org/news/secadv_20030319.txt
  - 17-Mar-2003 http://www.openssl.org/news/secadv_20030317.txt
  - 19-Feb-2003 http://www.openssl.org/news/secadv_20030219.txt
  - If you are running SSL for OpenVMS Version 1.0, V1.0-A, V1.0-B, V1.1 or V1.1-A please install SSL for OpenVMS version 1.1-B as soon as possible.

Security Update (Kerberos)

- http://h71000.www7.hp.com/openvms/security.html
- Kerberos Version 2.0 for HP OpenVMS, based on MIT Kerberos V5 Release 1.2.6 (plus security patches provided in Release 1.2.7 and 1.2.8). Kerberos Version 2.0 runs on OpenVMS Alpha Version 7.2-2 and higher.
  - MIT has found security vulnerabilities in all releases of MIT Kerberos V5 earlier than 1.2.5. Kerberos Version 1.0 for OpenVMS is based on MIT Kerberos V5 Release 1.0.5, and is affected by these security vulnerabilities.
  - If you are running Kerberos Version 1.0 for OpenVMS, install Kerberos Version 2.0 for OpenVMS ASAP!

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.

POP Server TCP/IP Services

- 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: 5.3, 5.1,5.0a, 4.2
- Install: HP TCP/IP Services for OpenVMS V5.3 ECO 2

Secure Web Server

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.

Security & Audit Service

Services

- Comprehensive security check of the OpenVMS physical, network, and remote applications access
- Installation and configuration of the PointSecure software to meet your companies security policies
- Training on the PointSecure solutions to enforce and maintain your companies security policies

Products

- Perpetual License for both System Detective and PointAudit
- 1st years maintenance for both System Detective and PointAudit

Deliverables

- State of system security report
- Customized reports
- List of identified vulnerabilities and suggested solutions

Securing OpenVMS Basics

- Have a Security Policy!
  - Apply OpenVMS MUP's & patches
  - Communicate & train everyone!
- Resources:
  - Guide system security (appendix C)

http://h71000.www7.hp.com/doc/731FINAL/6346/6346PRO.HTM

  - The OpenVMS security web page

http://h71000.www7.hp.com/security/

  - SANS Institute is excellent policy resource

http://www.sans.org/newlook/resources/policies/policies.htm

Auditing your OpenVMS Security

- $ANAL/AUDIT/SINCE=TODAY –
- SYS$MANAGER:SECURITY.AUDIT$JOURNAL;1
- $TYPE/TAIL=60 SYS$MANAGER:OPERATOR.LOG
- $TYPE/TAIL=60 APACHE$COMMON:[SPECIFIC.SS1.LOGS]-ACCESS_LOG
- $TYPE/TAIL=60 APACHE$COMMON:[SPECIFIC.SS1.LOGS]-ERROR_LOG

Security Technologies

Authentication

Validate who you are...

- Kerberos
- External Authentication (SDK)
  - LDAP ACME agent
  - *Kerberos ACME agent

Encryption

Keeping data secure…

…on the system

- CDSA
- (Common Data Security Architecture)
- GnuPG

…over the network

- SSL (Secure Socket Layer)
  - Stunnel (Secure Tunnel)
- SSH (Secure Shell)

*IPSEC

* Future projects

Are Some RISC Clusters More Secure Than Others?

A whitepaper Comparison of Potential Vulnerabilities and Security-Related Cluster Crashes for Three Different RISC-Based Platforms.

HP OpenVMS

IBM AIX

Sun Solaris

Respondent Comments About the Importance of Security

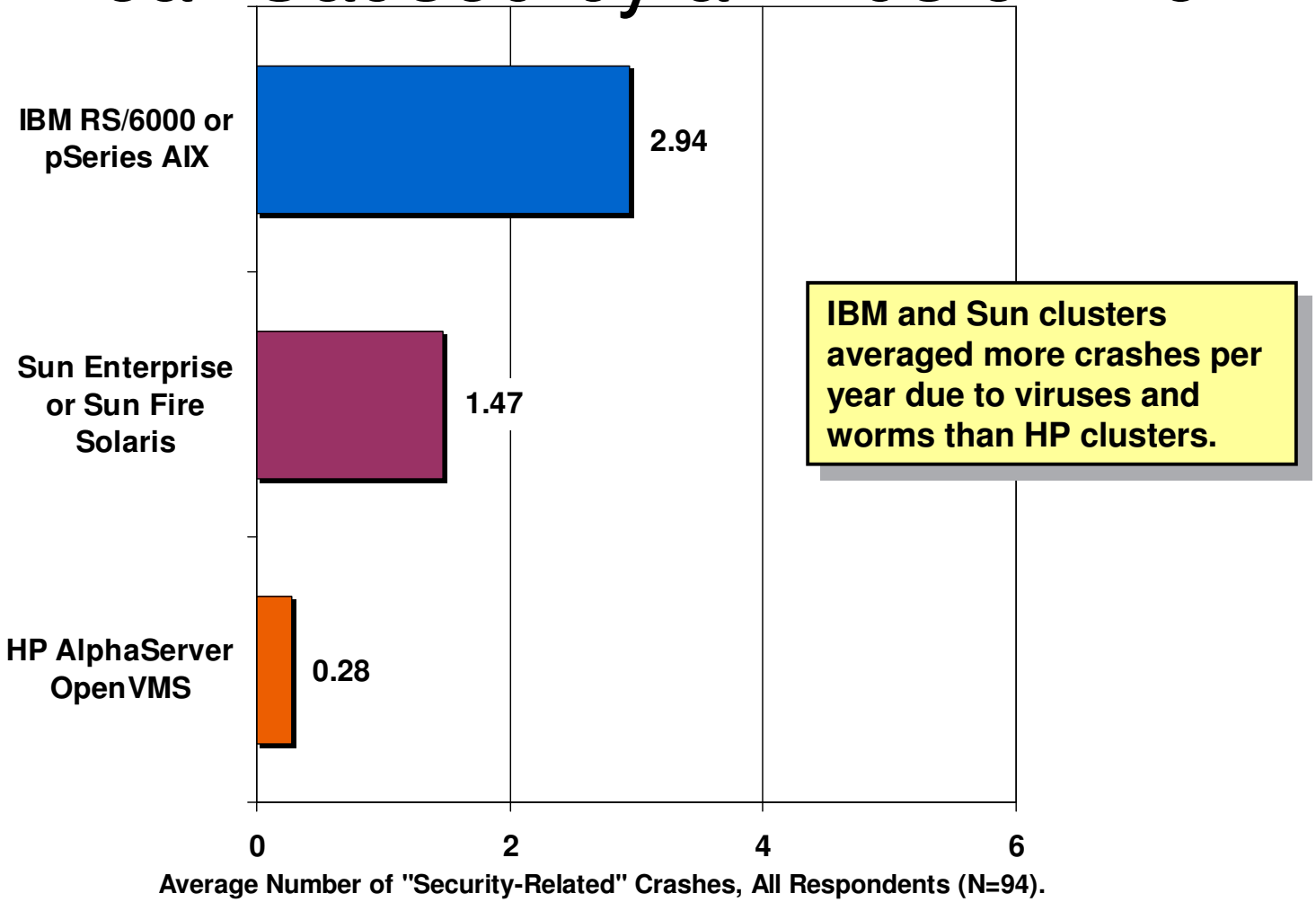
"Viruses and worms are much more of a threat now than they were 18 months ago. We have assigned someone to focus on this full-time."

"We formed a team that meets once a month to discuss our security strategy."

"We set up a dedicated team 12 months ago to focus on viruses, worms and other security threats."

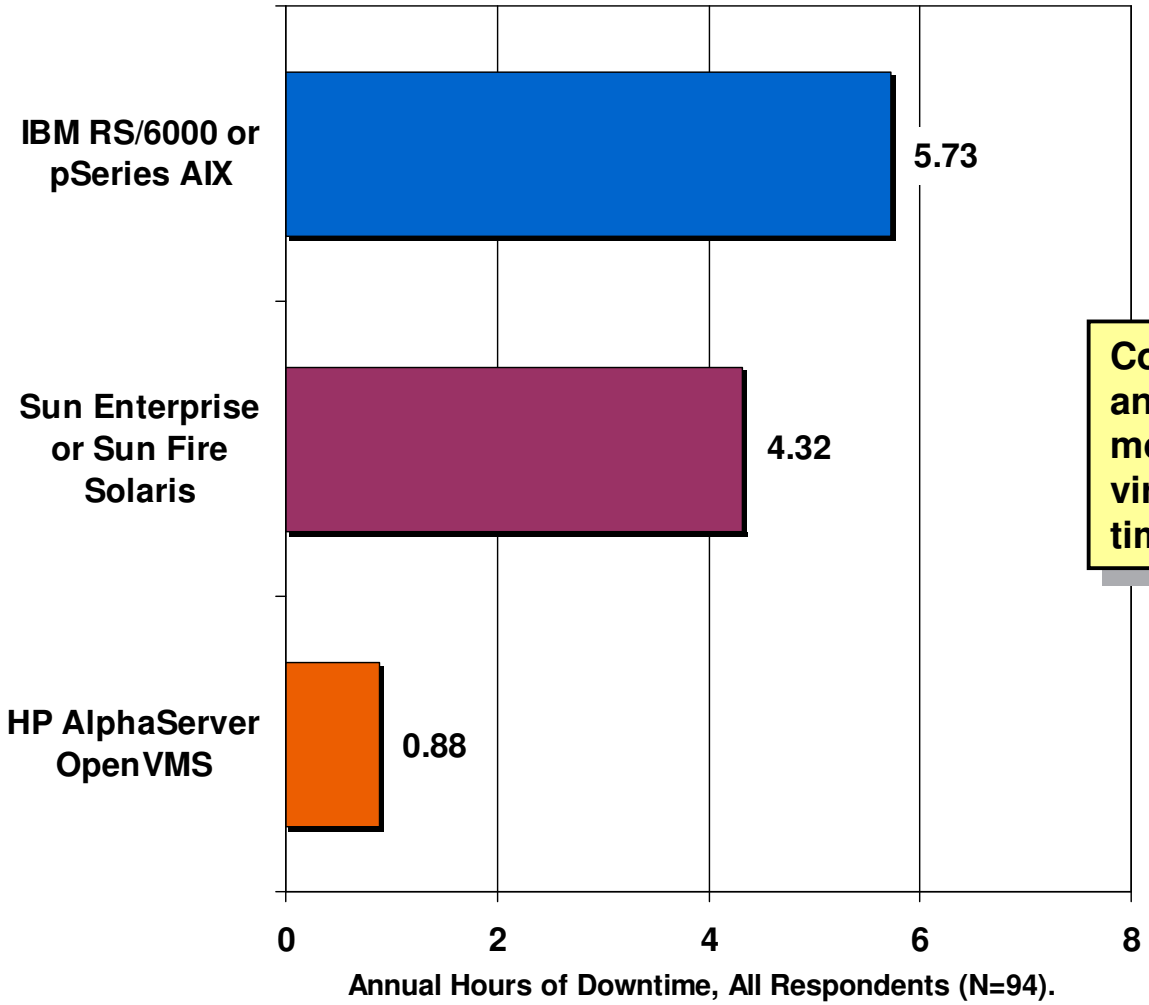
"Cost used to be the number one factor we considered when evaluating new servers. Now it is number two or three behind security."

Average of Cluster Crashes Per Year Caused by a Virus or Worm



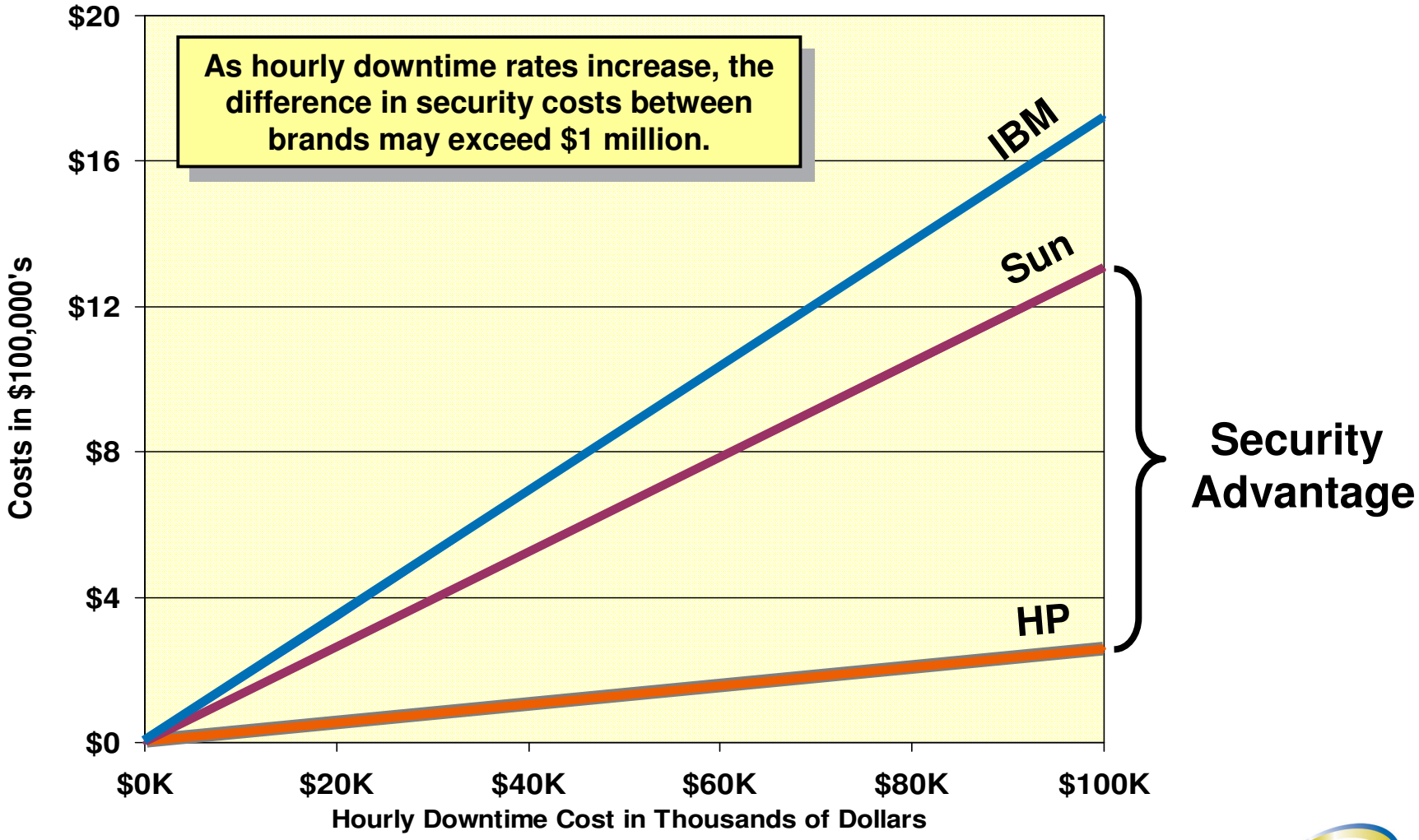
IBM and Sun clusters averaged more crashes per year due to viruses and worms than HP clusters.

Average Annual Cluster Downtime Due to a Virus or Worm



Compared to HP clusters, IBM and Sun averaged substantially more hours of downtime due to viruses and worms (5 and 7 times more, respectively).

Three-Year Security Costs by Cluster Brand At Different Downtime Rates



Comments on Differences in Server Security Vulnerabilities

"UNIX is a good operating system, but it is open and is vulnerable to hacking. All the flavors of UNIX use portions of open source code that hackers have access to."

"Unfortunately, we have to constantly apply patches to our UNIX and Windows servers to make sure we are as safe as possible."

"The Sun servers seem to be more vulnerable to viruses than some others I have worked with previously. But maybe they crash more often because they are overloaded."

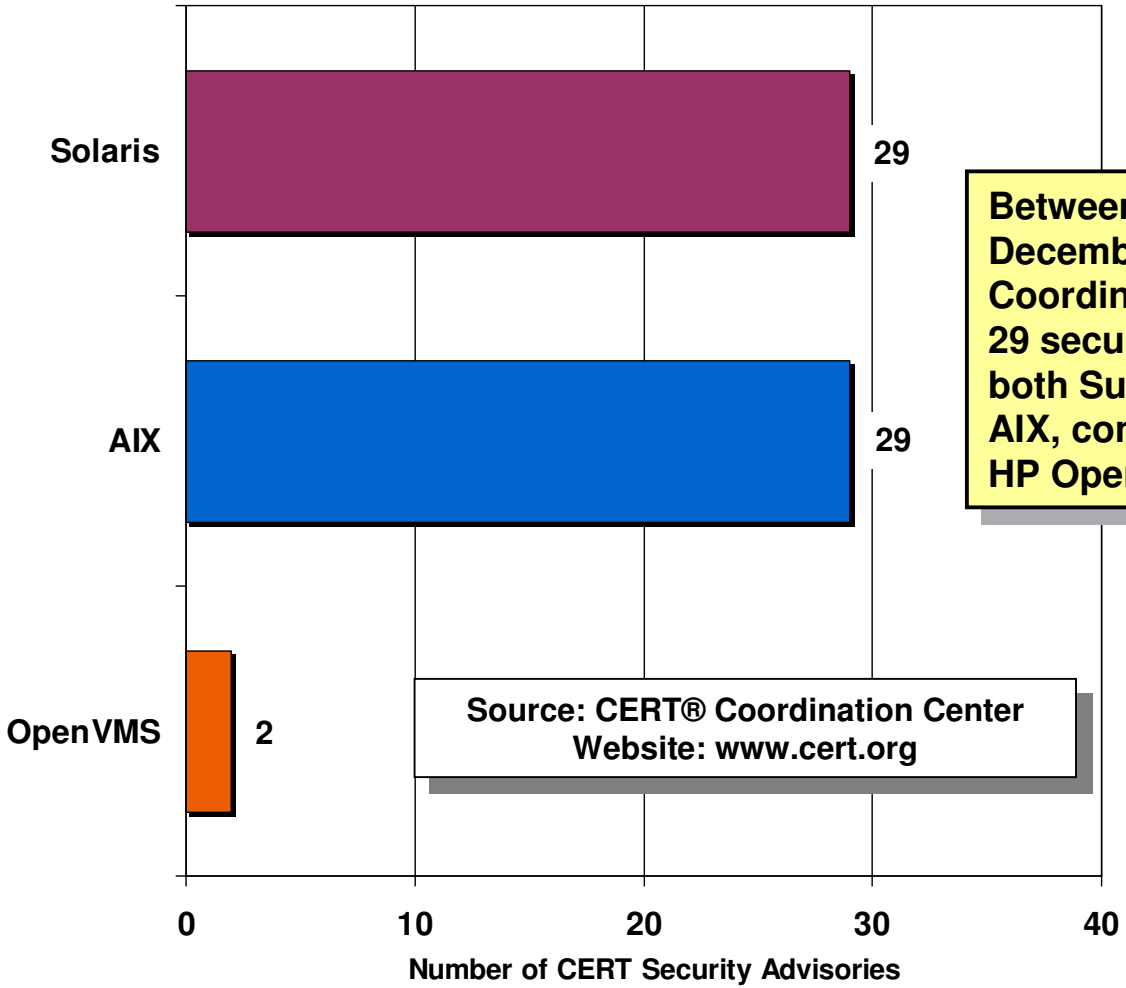
"If you do not keep your IBM cluster updated, you will run into security problems."

"IBM sends us a set of CD's roughly once a month with security information, updates and patches. I like the fact that the CD is customized for the IBM systems I have."

"OpenVMS is a pretty secure system. I can only recall two patches being released over the past few years - and one did not apply to us based on how we use our cluster."

"OpenVMS is definitely more secure. Less exploits are written for it. A single UNIX exploit could be tweaked to work across multiple UNIX variants."

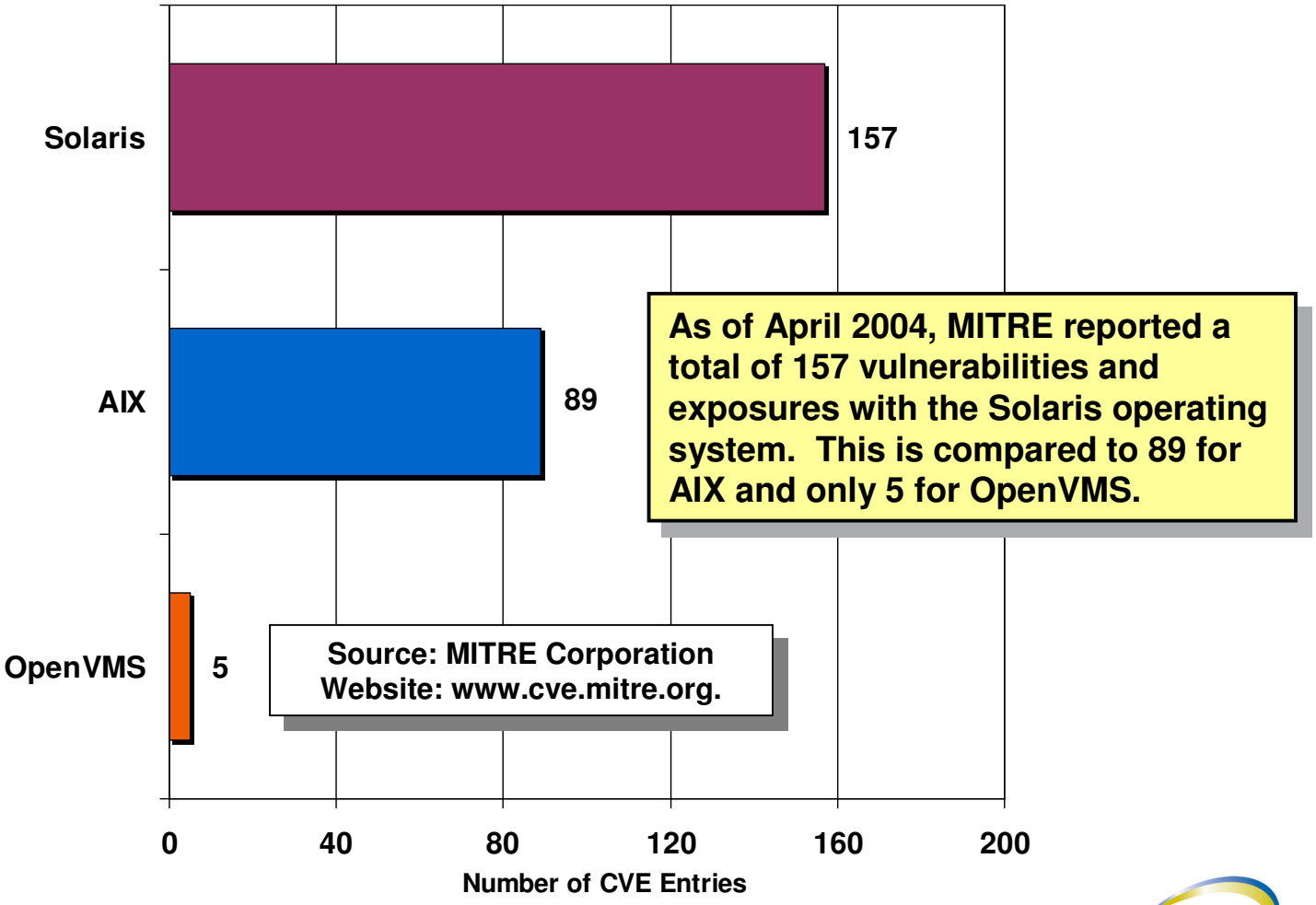
Security Advisories Issued Between 2000 – 2003 CERT© Coordination Center



Between January 1, 2000 and December 31, 2003, CERT Coordination Center issued 29 security advisories for both Sun Solaris and IBM AIX, compared to only 2 for HP OpenVMS.

Source: CERT® Coordination Center
Website: www.cert.org

Common Vulnerabilities and Exposures (CVEs)MITRE Corporation



Customer Comments Regarding the Security of HP OpenVMS Clusters

"OpenVMS is hard to hack into. Even if you log in as a user, it is hard to hack into other areas."

"OpenVMS has a high rating in security from the U.S. Department of Defense… If someone is worried about security and stability, I highly recommend OpenVMS."

"OpenVMS was designed from the ground up as a time sharing operating system. Security was not an afterthought."

"I wish all the rest of our IT environment were as reliable as our OpenVMS cluster. It would make my life a lot easier."

Why HP OpenVMS Clusters Have the Lowest Security Costs

- Solaris and AIX contain open source code that hackers can access. OpenVMS is designed with security in mind.
- Between Jan. 1, 2000 and December 31, 2003, HP clusters required far fewer security patches than IBM and Sun.
  - Only 2 for HP compared with 29 for IBM and 29 for Sun.
    - Source: CERT® Coordination Center.
- OpenVMS has far fewer security vulnerabilities than the other two operating systems.
  - Only 5 for HP compared with 89 for IBM and 157 for Sun.
    - Source: MITRE Corporation.

OpenVMS and Industry standard Security: Setting it up!

- Setting up Security technologies on OpenVMS.
  - SSH
  - Kerberos
  - External Authentication (LDAP Authentication)

Configuring SSH (1 of 5)

```
$ @sys$manager:tcpip$config

  Checking TCP/IP Services for OpenVMS configuration database files.

  HP TCP/IP Services for OpenVMS Configuration Menu

  Configuration options:

       1  -  Core environment
       2  -  PowerTerm client components
       3  -  Server components
       4  -  Optional components

       5  -  Shutdown HP TCP/IP Services for OpenVMS
       6  -  Startup HP TCP/IP Services for OpenVMS
       7  -  Run tests

       A  -  Configure options 1 - 4
      [E] -  Exit configuration procedure

Enter configuration option: 3
```

Configuring SSH (2 of 5)

```
HP TCP/IP Services for OpenVMS Server Components Configuration Menu
Configuration options:

  1 - BIND          Disabled Stopped     12 - NTP           Enabled  Started
  2 - BOOTP         Disabled Stopped     13 - PC-NFS        Enabled  Started
  3 - DHCP          Disabled Stopped     14 - POP           Enabled  Started
  4 - FINGER        Enabled  Started     15 - PORTMAPPER    Enabled  Started
  5 - FTP           Enabled  Started     16 - RLOGIN        Enabled  Started
  6 - IMAP          Enabled  Started     17 - RMT           Enabled  Started
  7 - LBROKER       Enabled  Started     18 - SNMP          Enabled  Started
  8 - LPR/LPD       Enabled  Started     19 - SSH           Enabled  Stopped
  9 - METRIC        Enabled  Started     20 - TELNET        Enabled  Started
 10 - NFS           Enabled  Started     21 - TFTP          Enabled  Started
 11 - LOCKD/STATD   Enabled  Started     22 - XDM           Enabled  Started

  A  -  Configure options 1 - 22
 [E] -  Exit menu

Enter configuration option: 19
```

SSH Configuration (3 of 5)

```
SSH Configuration

Service is not defined in the SYSUAF.
Service is not defined in the TCPIP$SERVICE database.
Service is not enabled.
Service is stopped.

        SSH configuration options:

                1 - Enable service on this node

                2 - Enable & Start service on this node

               [E] - Exit SSH configuration

Enter configuration option: 1
```

SSH configuration (4 of 5)

```
%TCPIP-I-INFO, TCPIP$AUX identifier (uic=[3655,*]) already exists
        Creating SSH Service Entry
Create a new default server host key? [YES]
   Creating private key file: TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]HOSTK
   Creating public key file:
  TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]HOSTKEY.PUB

The SSH CLIENT is enabled.

Do you want to configure SSH CLIENT [NO]: yes
```

OpenVMS configuration (5 of 5)

```
SSH CLIENT Configuration

Service is defined in the SYSUAF.
Service is enabled on specific node.
Service is stopped.

        SSH CLIENT configuration options:

                1 - Enable service on this node

                2 - Enable & Start service on this node

               [E] - Exit SSH_CLIENT configuration

Enter configuration option: 1
```

OpenVMS startup

```
$ @sys$startup:TCPIP$SSH_STARTUP
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$SSH_SSHD2.EXE installed
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$SSH_SFTP-SERVER2.EXE
%TCPIP-I-INFO, logical names created
%TCPIP-I-INFO, service enabled
%TCPIP-S-STARTDONE, TCPIP$SSH startup completed
$ @sys$startup:TCPIP$SSH_client_startup
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$SSH_SCP2.EXE installed
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$SSH_SFTP2.EXE installed
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$SSH_SSH-ADD2.EXE
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$SSH_SSH-AGENT2.EXE
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$SSH_SSH-KEYGEN2.EXE
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$SSH_SSH-SIGNER2.EXE
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$SSH_SSH2.EXE installed
%TCPIP-I-INFO, logical names created
%TCPIP-S-STARTDONE, TCPIP$SSH_CLIENT startup completed
```

SSH client connection

```
$ ssh secdem
Host key not found from database.
Key fingerprint:
xekeg-romec-dokyl-siset-dofys-vaveh-dehof-bares-gygis-ricyc-nexax
You can get a public key's fingerprint by running
$ ssh_keygen "-F" publickey.pub on the keyfile.
Host key saved to ssh2/hostkeys/key_22_secdem.pub
host key for secdem, accepted by STUDENTn Tue Nov 04 2003 14:43:31
Passphrase for key "ssh2/STUDENTn" with comment "1024-bit dsa,
  system@secdem.bootcamp.com, Fri Oct 31 2003 16:33:34": garbage
STUDENTn@secdem's password: garbage
Passphrase for key "ssh2/STUDENTn" with comment "1024-bit dsa,
  system@secdem.bootcamp.com, Fri Oct 31 2003 16:33:34": PASSWORD

Authentication successful.
 Welcome to OpenVMS (TM) Alpha Operating System, Version E7.3-2

$secdem>logout
Connection to secdem closed.  4-NOV-2003 09:52:05.93
```

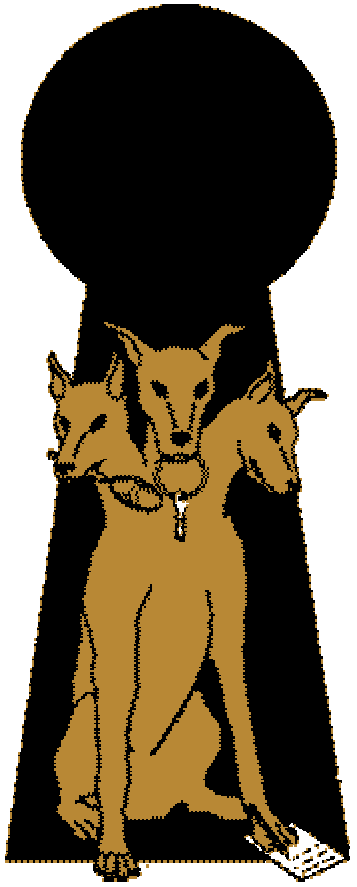
scp client connection scp

```
$ scp secdem:hello.exe *.*
Passphrase for key "ssh2/STUDENTn" with comment "1024-bit dsa,
  system@secdem.bootcamp.com, Fri Oct 31 2003 16:33:34": PASS
hello.exe                 |  3.5kB |   3.5 kB/s | TOC: 00:00:01 | 100%
$ scp secdem:test.txt  *.*
Passphrase for key "ssh2/STUDENTn" with comment "1024-bit dsa,
  system@secdem.bootcamp.com, Fri Oct 31 2003 16:33:34 ": garbage
STUDENTn@secdem's password: PASS
test.txt                  |   187B |   0.2 kB/s | TOC: 00:00:01 | 100%
$ directory
Directory SYS$SYSDEVICE:[STUDENTn]
hello.exe;1          SSH2.DIR;1           test.txt;1
Total of 3 files.
```

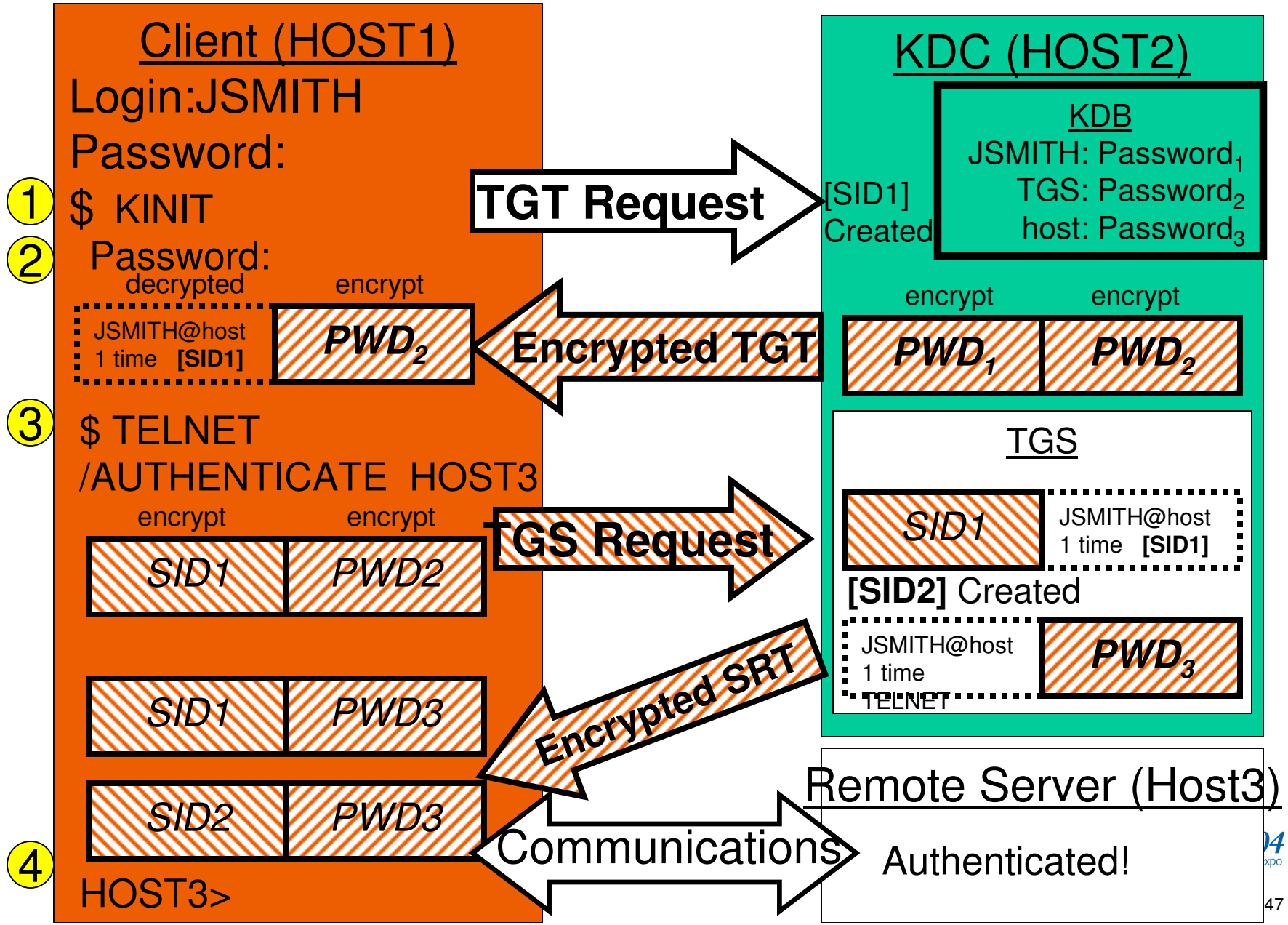
SSH remote execution

```
$ dir/full test.txt
Directory SYS$SYSDEVICE:[STUDENTn]
test.txt;1                          File ID:   (14278,2,0)
Size:              1/3              Owner:     [STUDENTn]
Created:       4-NOV-2003 10:45:34.33
Revised:       4-NOV-2003 10:45:34.43 (1)
Expires:      <None specified>
…
Record format:        Stream_LF, maximum 0 bytes, longest 32767
  bytes


$ run hello
Hello, world, from host: VMSn

$ ssh secdem run hello
Hello, world, from host: SECDEM
```

Kerberos for OpenVMS



Kerberos Ticket Process



Installing Kerberos On OpenVMS

- Kerberos V2 ships as part of OpenVMS V7.3-2
  - No installation is necessary on OpenVMS V7.3-2
  - Configuration must be done prior to use
  - Supported on OpenVMS V7.2-2 and up
    - Installation on earlier versions of OpenVMS is via a PCSI kit available on the web

    http://h71000.www7.hp.com/openvms/products/kerberos/

  - Installation documentation and OpenVMS Kerberos sources can be found at the same site
    - The sources are complete, and include build files
      - Unless you have a special need to build Kerberos yourself, use the standard distribution rather than building from sources
      - No differences except version number

Configuring Kerberos on OpenVMS

- The initial step in setting up a Kerberos system on OpenVMS is running the configuration utility

```
$ @SYS$STARTUP:KRB$CONFIGURE
```

  - This will
    - Create the Kerberos server database (server)
    - Set up the administrative entries (client & server)
    - Define logical names

Configuring A Kerberos client

$ set process/privileges=all
$ @sys$startup:krb$configure

Kerberos V2.0-6 for OpenVMS Configuration Menu

Configuration options:

1 - Setup Client configuration
2 - Edit Client configuration
3 - Setup Server configuration
4 - Edit Server configuration
5 - Shutdown Servers
6 - Startup Servers

E - Exit configuration procedure

Enter Option: 1

Where will the OpenVMS Kerberos 5 KDC be running [VMSxx]:secdem

Configuring A Kerberos client (continued)

What is the OpenVMS Kerberos 5 default domain [bootcamp.com]:
What is the OpenVMS Kerberos 5 Realm name [VMSxx.BOOTCAMP.COM]:
    SECDEM.BOOTCAMP.COM
Press Return to continue ...

Kerberos V2.0-6 for OpenVMS Configuration Menu

Configuration options:

1 - Setup Client configuration
2 - Edit Client configuration
3 - Setup Server configuration
4 - Edit Server configuration
5 - Shutdown Servers
6 - Startup Servers
E - Exit configuration procedure

Enter Option: 6

Configuring A Kerberos client (continued)

Press Return to continue …

Kerberos V2.0-6 for OpenVMS Configuration Menu

Configuration options:

1 - Setup Client configuration
2 - Edit Client configuration

3 - Setup Server configuration
4 - Edit Server configuration

5 - Shutdown Servers
6 - Startup Servers

E - Exit configuration procedure

Enter Option: e
$

Kerberos Startup and Shutdown

System Management Tools

SYS$STARTUP:KRB$STARTUP. COM

SYS$STARTUP:KRB$SHUTDOWN.COM

Definitions should be added to system files

Add @SYS$MANAGER:KRB$LOGICALS and

@SYS$STARTUP:KRB$STARTUP to

SYS$MANAGER:SYSTARTUP_VMS.COM

Optionally add @SYS$MANAGER:KRB$SYMBOLS to

SYS$MANAGER:SYLOGIN.COM

Kerberos Utilities

Kerberos DCL support is available through:

$ KERBEROS [/ADMIN] -
[/INTERFACE=[DECWINDOWS | CHARACTER_CELL]]

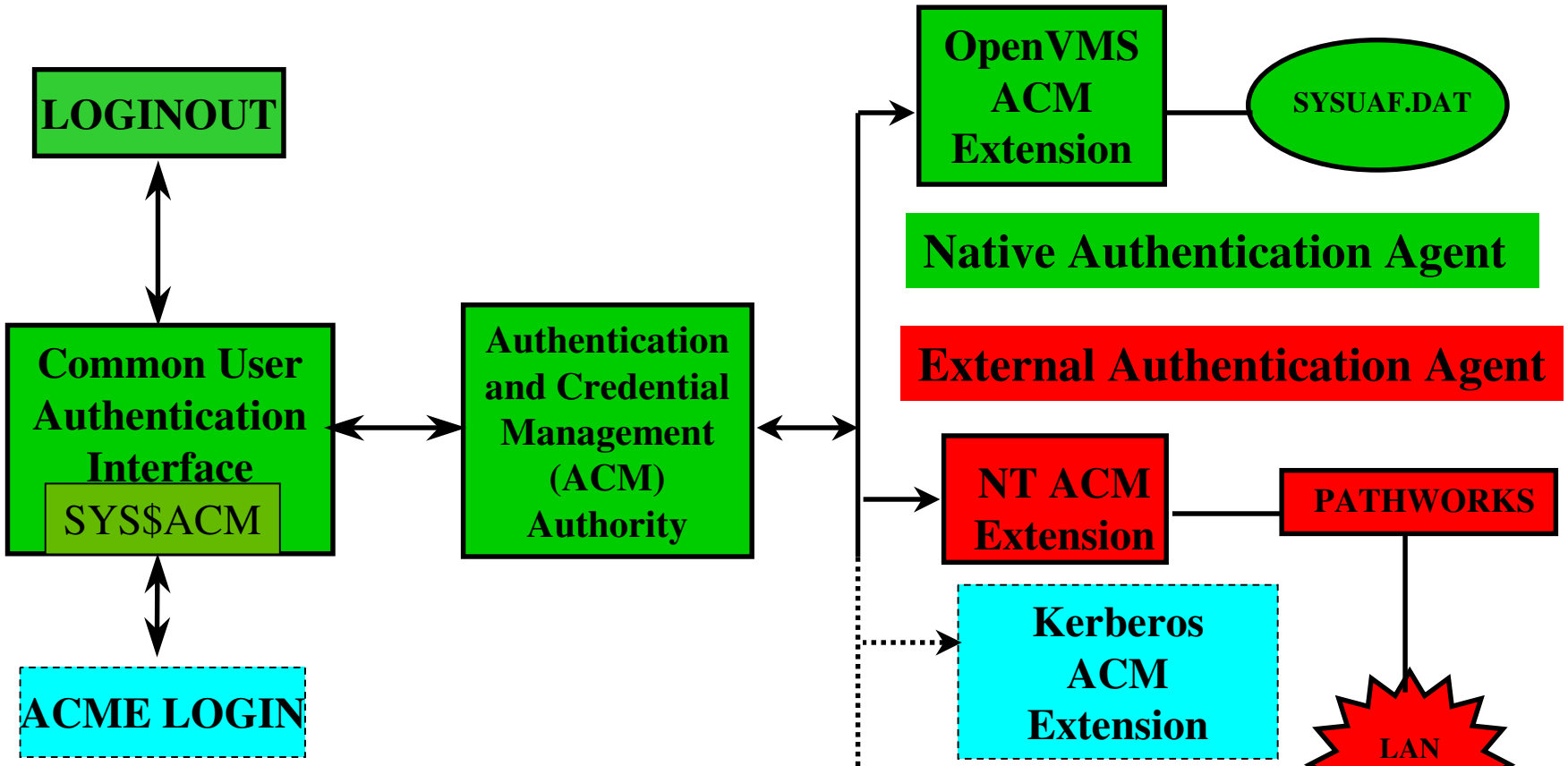
- Kerberos ticket manipulation programs available through symbols (created using @SYS$MANAGER:KRB$SYMBOLS):

Symbol	Function
kinit	Generate ticket granting ticket
klist	List tickets
kdestroy	Destroy tickets
kpasswd	Change Kerberos password
kadmin	Perform Kerberos administrative functions

Using Kerberos Client Programs (Unix Style)


```
$ @sys$manager:krb$symbols
$ kinit “STUDENTxx”
Password for STUDENTxx@SECDEM.BOOTCAMP.COM: bootcamp
$ klist
Ticket cache: krb$user:[tmp]krb5cc_2293763
Default principal: STUDENTxx@SECDEM.BOOTCAMP.COM

Valid starting          Expires                 Service principal
11/11/03 13:13:28  11/11/03 23:13:28  krbtgt/secdem.bootcamp.com@
   SECDEM.BOOTCAMP.COM

Kerberos 4 ticket cache: krb$user:[tmp]k4_tkt_cache2293763
KRB$KLIST: You have no tickets cached
$ kdestroy
$ klist
KRB$KLIST: No credentials cache file found (ticket cache
FILE:krb$user:[tmp]rb5cc_2293763)
```

Common Authentication & Credential Management

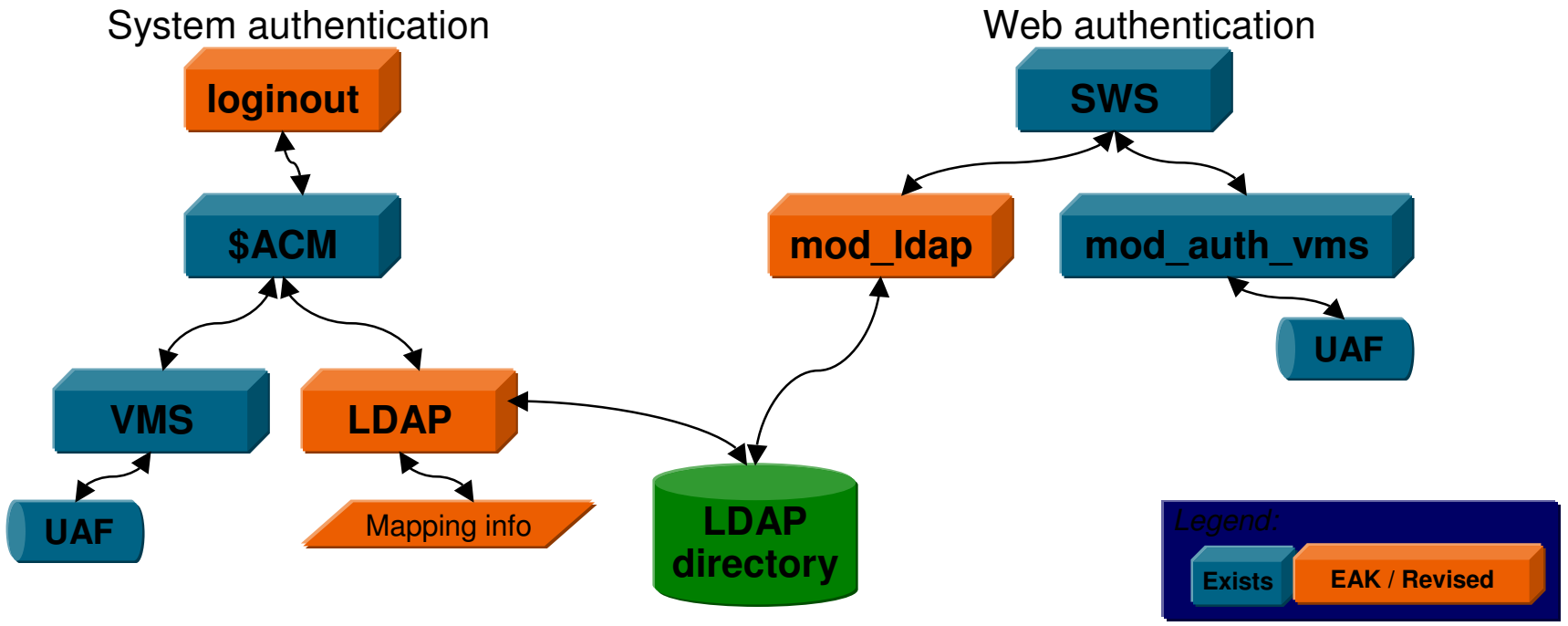


The ability to have user defined external agents supported by the OpenVMS Common User Authentication Model is planned for next release.

OpenVMS LDAP authentication

LDAP-based
- System auth → loginout, ftp, telnet
- Web auth

LDAP: username/password + UAF mapping
UAF: quota, security profile



Install LDAP ACME

```
$ PRODUCT INSTALL V732_ACMELOGIN
$ PRODUCT  INSTALL  V732_ACMELDAP
```

Starting The LDAP ACME

```
$ @SYS$STARTUP:LDAPACME$STARTUP
$ SHOW  SERVER  ACME  /FULL
```

Testing the LDAP ACME

```
$ MCR AUTHORIZE -
    COPY  SYSTEM  STUDENTn  /PASS=FOO -
    /NOPWDEXP  /UIC=[555,555]  /DEV=DKA0 -
    /DIR=[STUDENTn]  /FLAG=EXTAUTH
```

Then using the associated username and password,

```
$ TELNET 0
```

Username: student.n@bootcamp.com

Password: is now the one in the directory

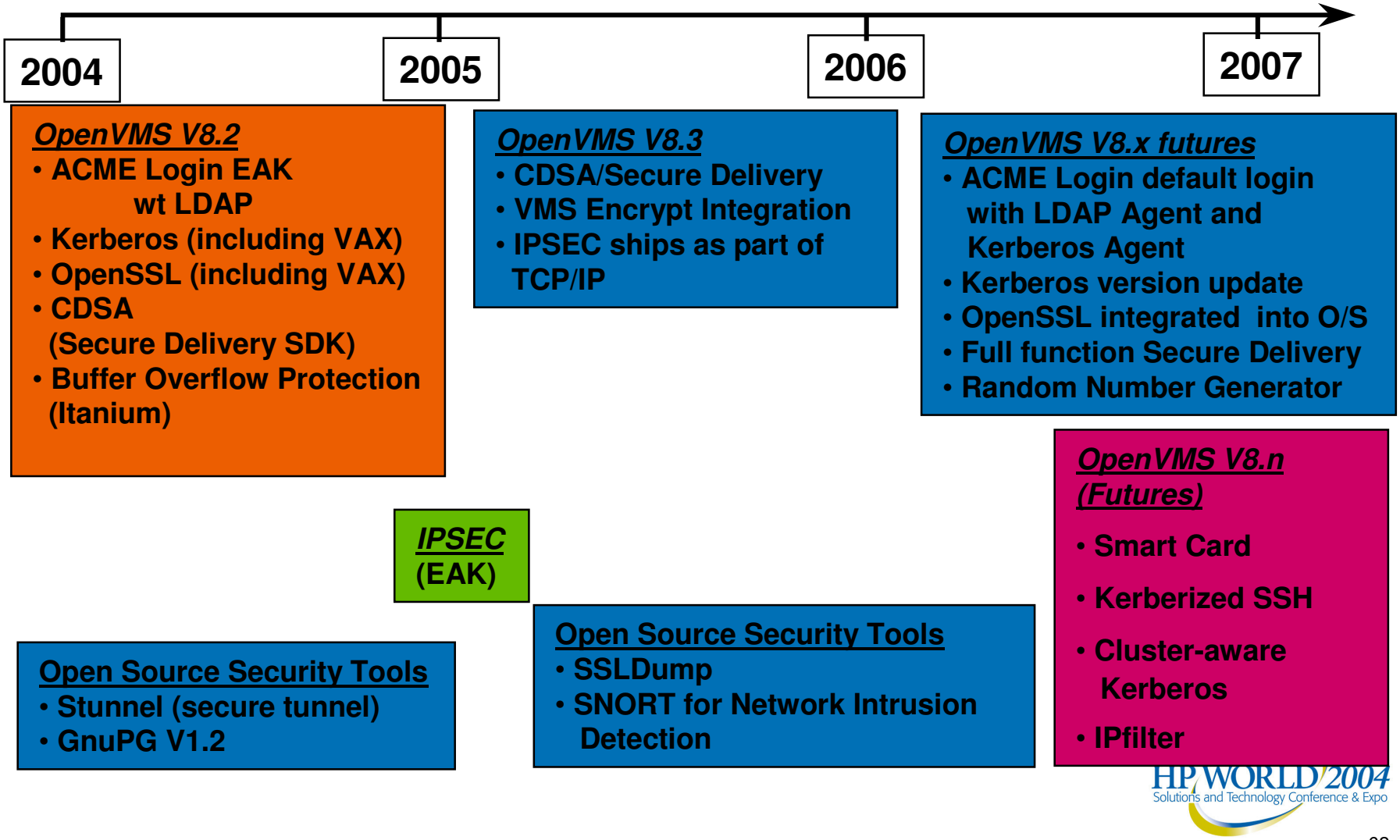
LDAPACME$AUTHORIZE

- The LDAPACME$AUTHORIZE tool targets the directory system to add a new directory entry, or to change the user's password:
  - $ MC LDAPACME$AUTHORIZE
  - Option 4 to Change Password
  - Option 5 to Select User (student.n@bootcamp.com)
  - $ telnet 0 and try new password

Uninstalling ACME LOGIN

- $ PRODUCT INSTALL V732_LOGIN
  - Press <RET> to accept the [YES] answer to both questions

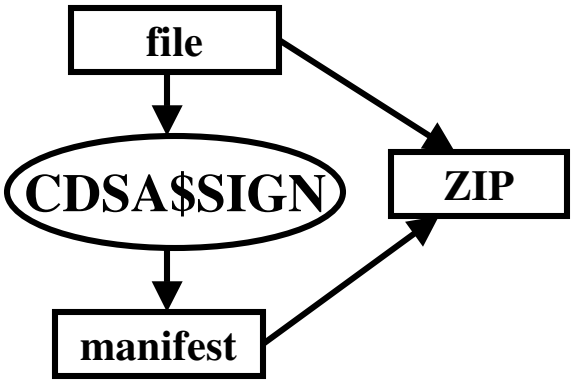
OpenVMS Security Roadmap



OpenVMS Secure Delivery (Future)

OpenVMS Signing Process

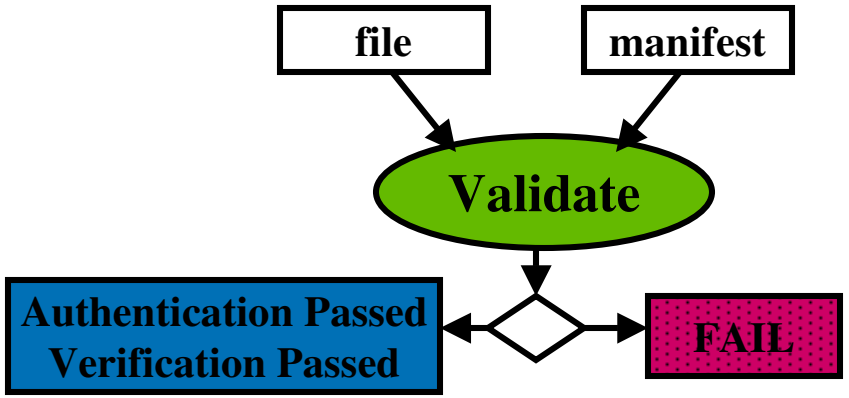
- Any file type (e.g. file.pcsi)



- Manifest encapsulates:
  - X509 Certificates
  - Digital Signature

Customer Validation Process

- Easily Incorporated into PCSI or as a standalone image



- Validation:
  - Authenticates Signer
  - Verifies file contents

Transport Independent
- HTTP, FTP, CD

PCSI dialog with Secure Delivery

```
$ product install kerberos /source=sys$kits:[kerberos]

The following product has been selected:
     HP AXPVMS KERBEROS V2.1-69                    Layered Product

%PCSIUI-W-NOMANIFEST, No manifest was found matching KERBEROS
Do you want to continue [YES]:?

(installation then continues normally)
-------------------------------
$ product install kerberos /source=sys$kits:[kerberos]

The following product has been selected:
     HP AXPVMS KERBEROS V2.1-69                    Layered Product

%PCSIUI-I-VALIDATED, kit has been validated successfully
Do you want to continue [YES]:?
```

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP

RECOMMENDED TRAINING VENUE FOR THE

HP Certified Professional

Grid