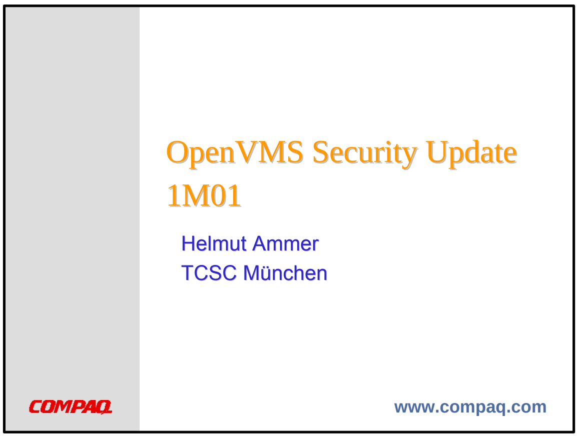
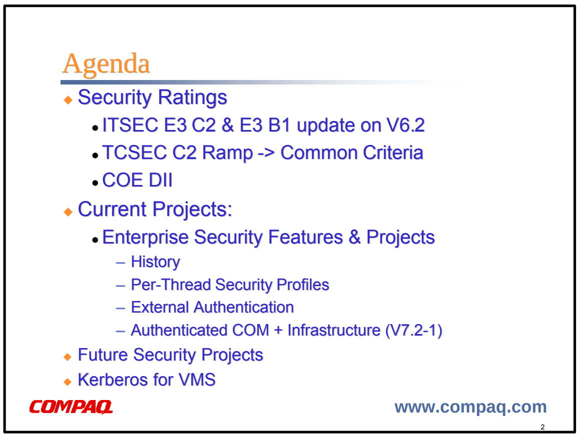


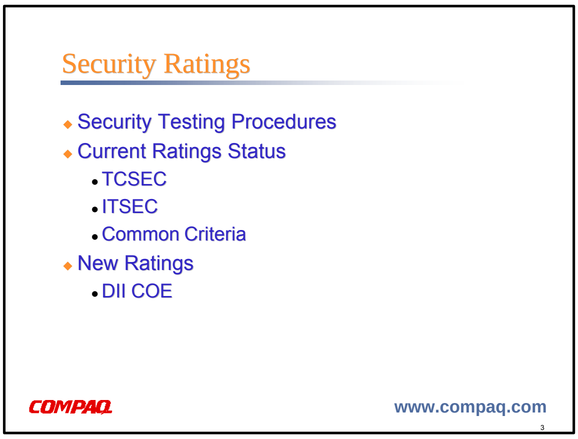
OpenVMS Security Update 1M01

Helmut Ammer
TCSC München



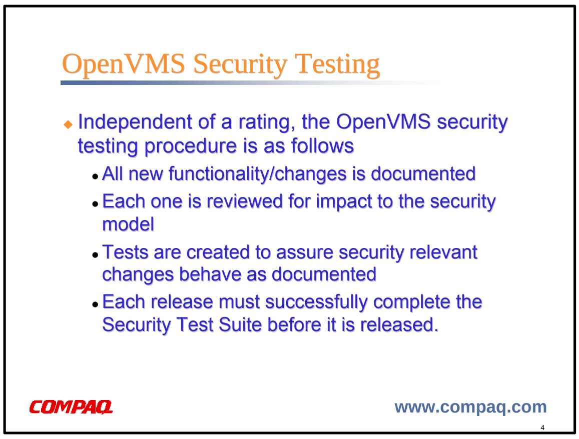
Agenda

- Security Ratings
  - ITSEC E3 C2 & E3 B1 update on V6.2
  - TCSEC C2 Ramp -> Common Criteria
  - COE DII
- Current Projects:
  - Enterprise Security Features & Projects
    - History
    - Per-Thread Security Profiles
    - External Authentication
    - Authenticated COM + Infrastructure (V7.2-1)
- Future Security Projects
- Kerberos for VMS



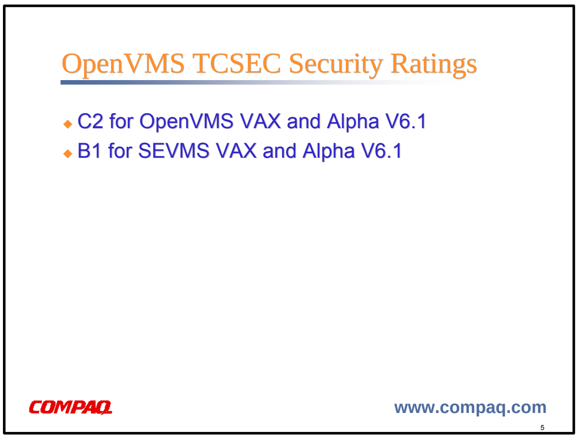
Security Ratings

- Security Testing Procedures
- Current Ratings Status
  - TCSEC
  - ITSEC
  - Common Criteria
- New Ratings
  - DII COE



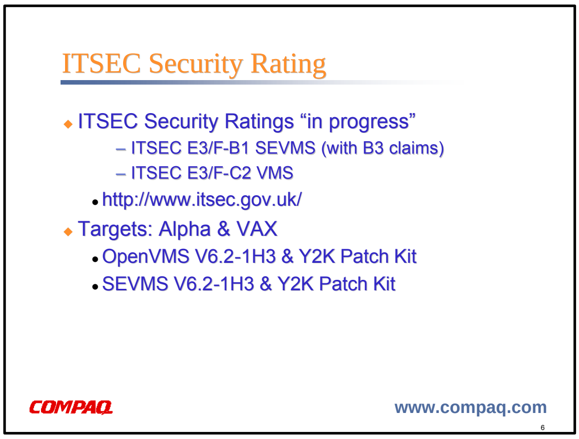
OpenVMS Security Testing

- Independent of a rating, the OpenVMS security testing procedure is as follows
  - All new functionality/changes is documented
  - Each one is reviewed for impact to the security model
  - Tests are created to assure security relevant changes behave as documented
  - Each release must successfully complete the Security Test Suite before it is released.



OpenVMS TCSEC Security Ratings

- C2 for OpenVMS VAX and Alpha V6.1
- B1 for SEVMS VAX and Alpha V6.1



ITSEC Security Rating

- ITSEC Security Ratings “in progress”
    - ITSEC E3/F-B1 SEVMS (with B3 claims)
    - ITSEC E3/F-C2 VMS
  - http://www.itsec.gov.uk/
- Targets: Alpha & VAX
  - OpenVMS V6.2-1H3 & Y2K Patch Kit
  - SEVMS V6.2-1H3 & Y2K Patch Kit

OpenVMS Future Security Ratings

- TCSEC/RAMP - Going Away
- OpenVMS 7.1 C2 RAMP Status

Common Criteria

- Independent 3rd party evaluations
  - CLEF (Commercially Licensed Evaluation Facility)
  - Common Criteria Profiles
    - C2? Industry Specific?

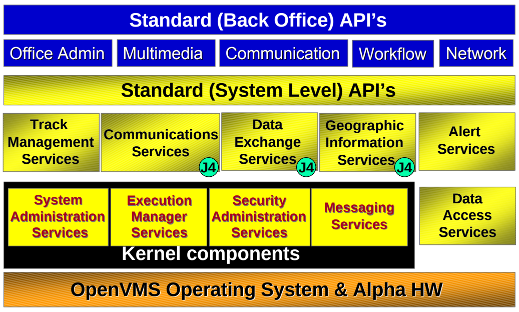
http://csrc.nist.gov/cc/

What is DII COE?

- The Defense Information Infrastructure Common Operating Environment (DII COE) provides a foundation for building open systems. It is a "plug and play" open architecture designed around a client/server model.

http://spider.osfl.disa.mil/cm/cm_page.html

DII COE 4.1.20 compliant OpenVMS



Standard (Back Office) API's

Office Admin | Multimedia | Communication | Workflow | Network

Standard (System Level) API's

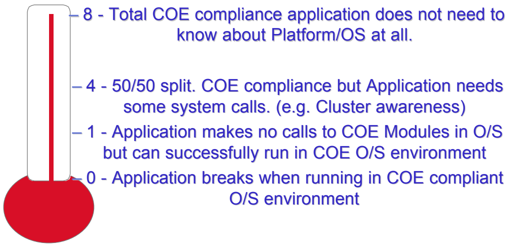
Track Management Services | Communications Services (J4) | Data Exchange Services (J4) | Geographic Information Services (J4) | Alert Services

System Administration Services | Execution Manager Services | Security Administration Services | Messaging Services | Data Access Services

Kernel components

OpenVMS Operating System & Alpha HW

COE Application Level's of Compliance



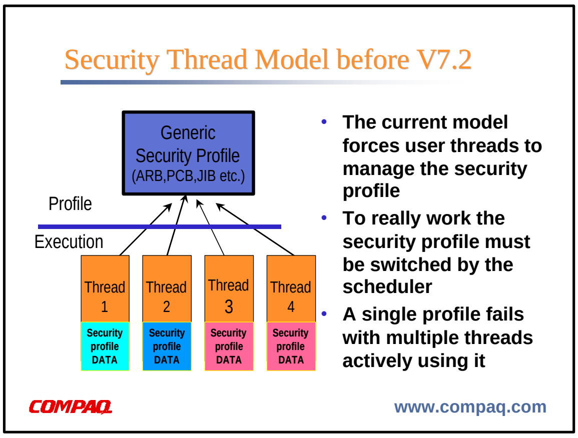
- 8 - Total COE compliance application does not need to know about Platform/OS at all.
- 4 - 50/50 split. COE compliance but Application needs some system calls. (e.g. Cluster awareness)
- 1 - Application makes no calls to COE Modules in O/S but can successfully run in COE O/S environment
- 0 - Application breaks when running in COE compliant O/S environment

Security MUPs

- OpenVMS Alpha V7.2
  - DEC-AXPVMS-VMS72_SYS-V0100-4.PCSI
  - DEC-AXPVMS-VMS721_SYS-V0100-4.PCSI
- OpenVMS Alpha Security MUP
  - ALPSMUP01_070 (Versionen V6.1, V6.2 & V7.0)
- OpenVMS VAX Security MUP
  - VAXSMUP03 (All Versions prior to V6.1)

OpenVMS V7.2 & V7.2-1 Projects

- Per-thread security
- V7.2-1 Authenticated COM
- Future Security Projects
  - LDAP Client investigation
  - Cluster Wide Intrusion Detection (A/V)
  - Kerberos V5
    - GSSAPI (Generic Security Services API)
  - $ACME Login
  - CDSA (Common Data Security Architecture) IR
  - IPSEC support



Security Thread Model before V7.2

Generic Security Profile (ARB,PCB,JIB etc.)

Profile

Execution

Thread 1

Thread 2

Thread 3

Thread 4

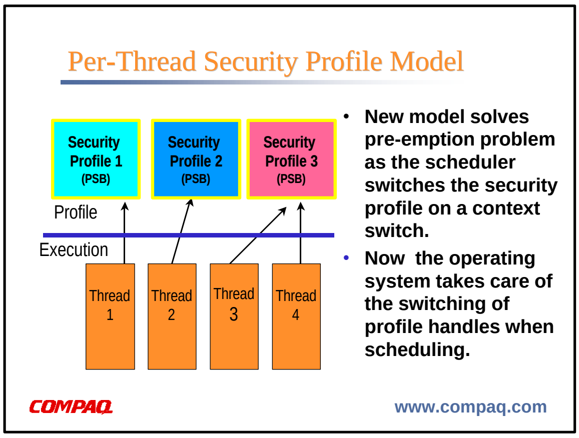
Security profile DATA

Security profile DATA

Security profile DATA

Security profile DATA

- The current model forces user threads to manage the security profile
- To really work the security profile must be switched by the scheduler
- A single profile fails with multiple threads actively using it



Per-Thread Security Profile Model

Security Profile 1 (PSB)

Security Profile 2 (PSB)

Security Profile 3 (PSB)

Profile

Execution

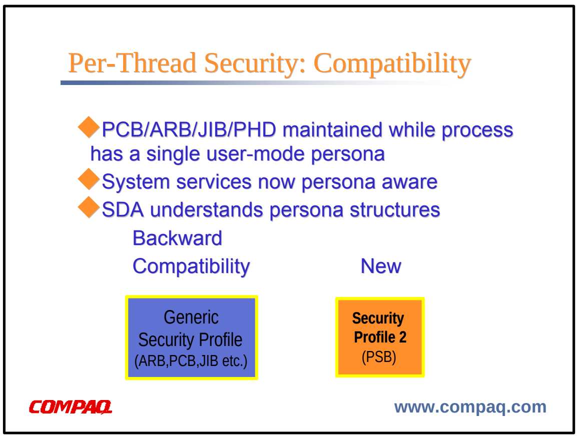
Thread 1

Thread 2

Thread 3

Thread 4

- New model solves pre-emption problem as the scheduler switches the security profile on a context switch.
- Now the operating system takes care of the switching of profile handles when scheduling.



Per-Thread Security: Compatibility

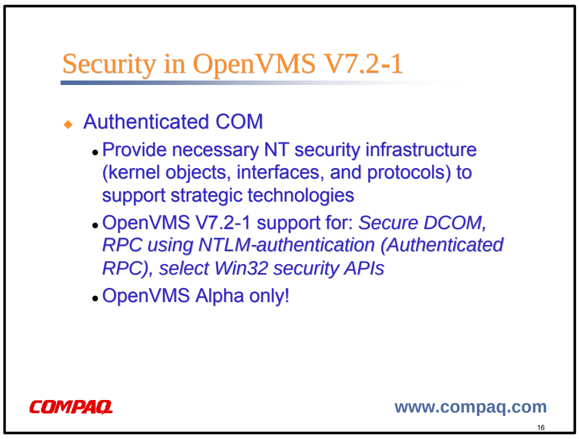
- PCB/ARB/JIB/PHD maintained while process has a single user-mode persona
- System services now persona aware
- SDA understands persona structures

Backward Compatibility

New

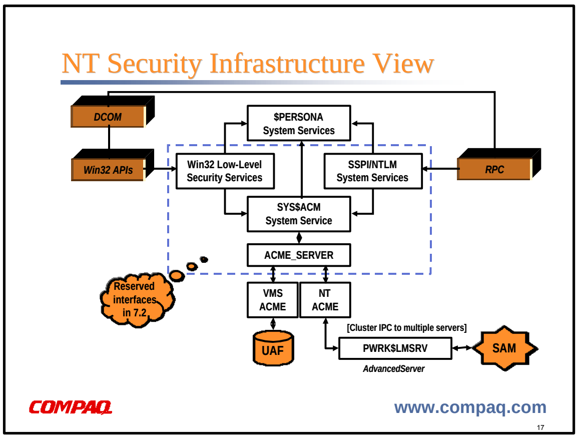
Generic Security Profile (ARB,PCB,JIB etc.)

Security Profile 2 (PSB)



Security in OpenVMS V7.2-1

- Authenticated COM
  - Provide necessary NT security infrastructure (kernel objects, interfaces, and protocols) to support strategic technologies
  - OpenVMS V7.2-1 support for: *Secure DCOM, RPC using NTLM-authentication (Authenticated RPC), select Win32 security APIs*
  - OpenVMS Alpha only!



NT Security Infrastructure View

DCOM

Win32 APIs

$PERSONA System Services

Win32 Low-Level Security Services

SSPI/NTLM System Services

RPC

SYS$ACM System Service

ACME_SERVER

Reserved interfaces in 7.2

VMS ACME

NT ACME

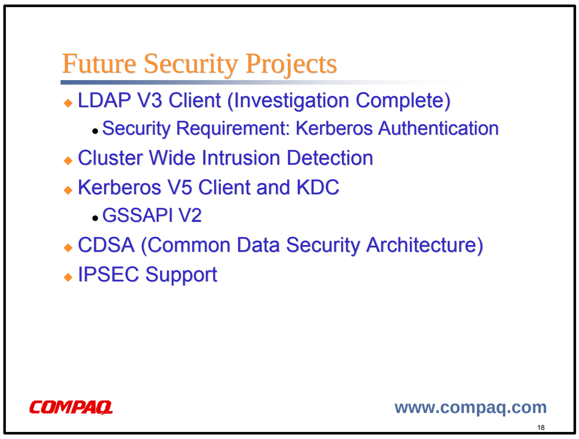
UAF

[Cluster IPC to multiple servers]

PWRK$LMSRV

AdvancedServer

SAM



Future Security Projects

- LDAP V3 Client (Investigation Complete)
  - Security Requirement: Kerberos Authentication
- Cluster Wide Intrusion Detection
- Kerberos V5 Client and KDC
  - GSSAPI V2
- CDSA (Common Data Security Architecture)
- IPSEC Support

Cluster Wide Intrusion Detection

Intrusion detection and breakin evasion is not applied cluster-wide. Intrusion detection and breakin evasion data are volatile.

- **CWID Requirements:**
  - **Intrusion and breakin events will be visible across the cluster (both VAX and Alpha)**
  - **Events from all nodes in the cluster will contribute to the detection and evasion mechanisms**
  - **Events must persist across system reboots**
  - **Only backwards-compatible changes will be made to the SYS$INTRUSION interfaces**

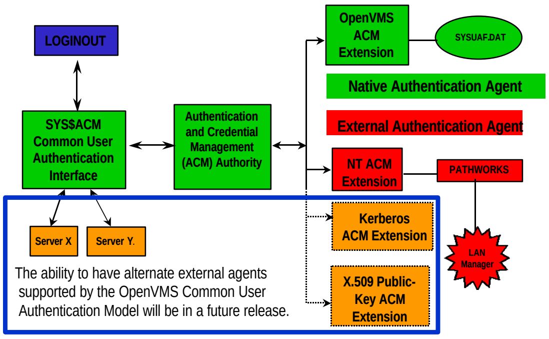
Kerberos VMS implementation

- Initially a separate installable kit featuring
  - Support available back to V7.1 (VAX & ALPHA)
  - GSSAPI V2
  - GUI & DCL interface
  - KDC & Client
- Ready for Field Test in CY2000

For more information on Kerberos see http://web.mit.edu/kerberos/www/

digital™

OpenVMS Common User Authentication and Credential Management Model


LOGINOUT
SYS$ACM Common User Authentication Interface
Authentication and Credential Management (ACM) Authority
OpenVMS ACM Extension
SYSUAF.DAT
Native Authentication Agent
External Authentication Agent
NT ACM Extension
PATHWORKS
LAN Manager
Kerberos ACM Extension
X.509 Public-Key ACM Extension
Server X
Server Y.

The ability to have alternate external agents supported by the OpenVMS Common User Authentication Model will be in a future release.

ACME Login

- SYS$ACM published
- Additional Loginout image
- How to write an ACME guide.
- Testing and Field Test exposure.

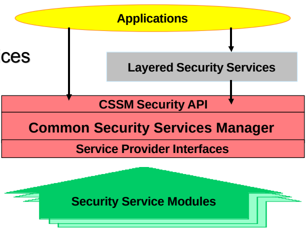
The CDSA Solution

Common Data Security Architecture (CDSA)

CDSA defines a four-layer architecture for cross-platform, high-level security services

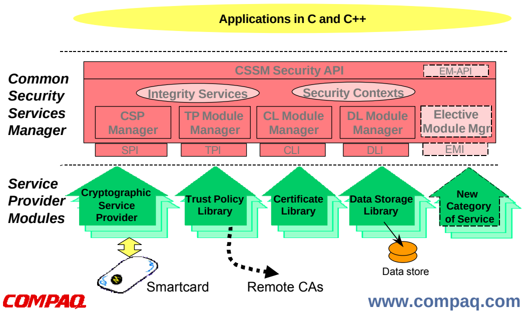
CSSM defines a common API & SPI for security services and integrity base

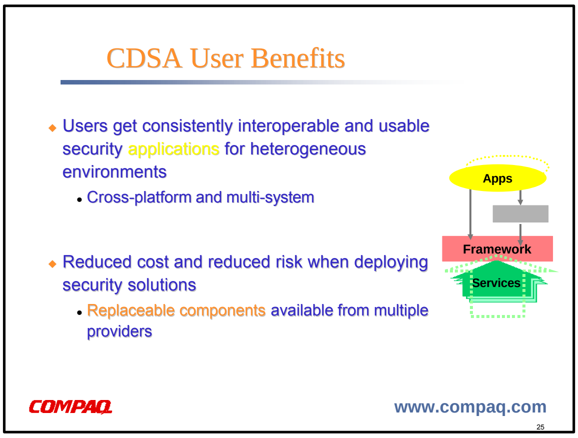
Service Providers implement selectable security services


Applications
Layered Security Services
CSSM Security API
Common Security Services Manager
Service Provider Interfaces
Security Service Modules

http://developer.intel.com/ial/security/

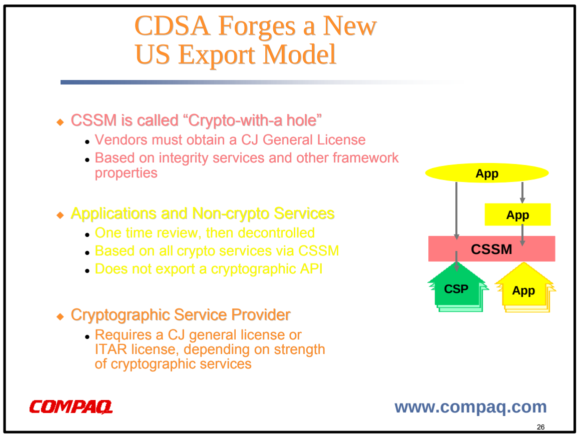
CDSA Framework





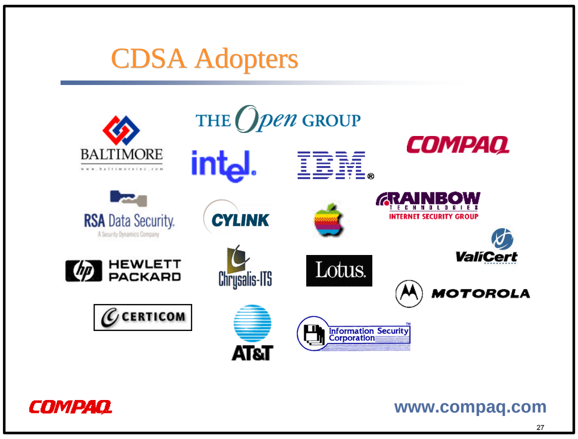
CDSA User Benefits

- Users get consistently interoperable and usable security applications for heterogeneous environments
  - Cross-platform and multi-system
- Reduced cost and reduced risk when deploying security solutions
  - Replaceable components available from multiple providers

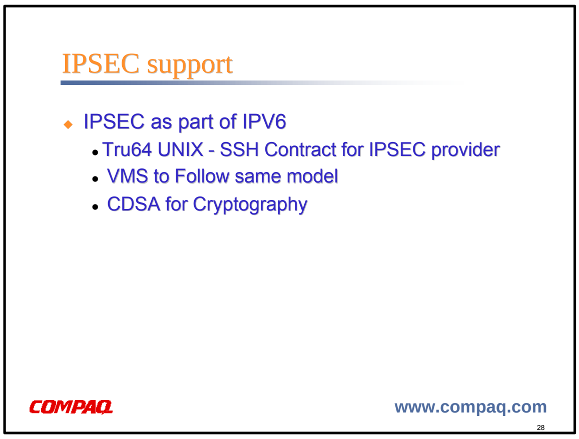


CDSA Forges a New US Export Model

- CSSM is called “Crypto-with-a hole”
  - Vendors must obtain a CJ General License
  - Based on integrity services and other framework properties
- Applications and Non-crypto Services
  - One time review, then decontrolled
  - Based on all crypto services via CSSM
  - Does not export a cryptographic API
- Cryptographic Service Provider
  - Requires a CJ general license or ITAR license, depending on strength of cryptographic services

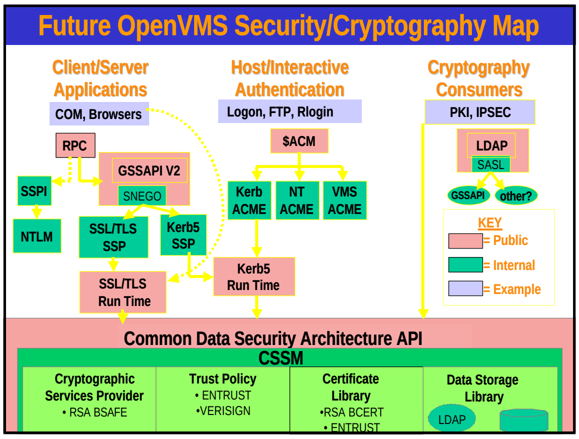


CDSA Adopters

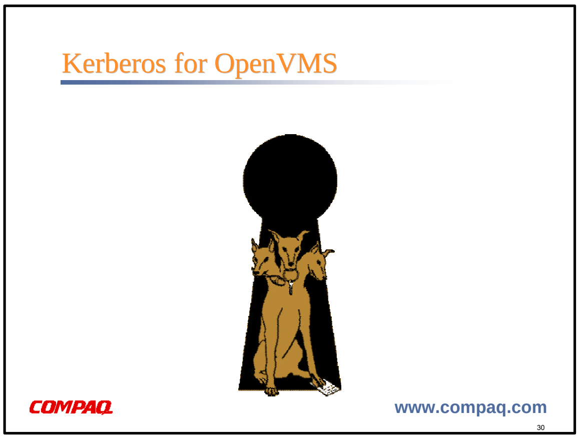


IPSEC support

- IPSEC as part of IPV6
  - Tru64 UNIX - SSH Contract for IPSEC provider
  - VMS to Follow same model
  - CDSA for Cryptography



Future OpenVMS Security/Cryptography Map



Kerberos for OpenVMS

Keberos Agenda

- What is it?
  - *– A Cryptographic Authentication protocol*
- History
- Benefit
- How it works
- OpenVMS Specific details

Kerberos Authentication
What's in a name?

- 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

Authorization vs. Authentication

- A system administrator **Authorizes** someone to use a computer by creating them an account.
  - Example: UAF> CREATE ASTRO
- The person proves that they are the authorized user of the account by **Authenticating** themselves typically with a password.

  Example:

  Username: ASTRO

  PASSWORD: *itsadogeatdogworld*

So what's the problem?

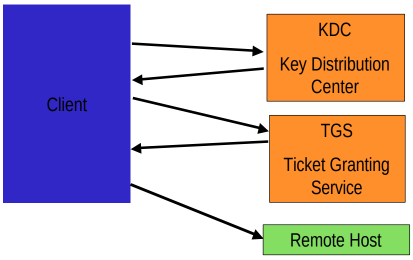
- Distributed computing forces the user to authenticate themselves to remote machines by having their passwords travel over the network.
  - A simple packet sniffing tool on a PC could read the password on it's way to the destination system

So how can you solve the Remote Authentication problem?

- Solutions:
  - Standards: IPSEC (Part of the IPV6 protocol)
  - SSH Secure Shell
    - SSH server for VMS
      http://kcgl1.eng.ohio-state.edu/~JONESD/ssh/DOC/
    - SSH client for VMS
      http://www.free.lp.se/fish/
    - Info on SSLEay
      http://www.free.lp.se/openssl/
- Kerberos for OpenVMS

How does Kerberos work?

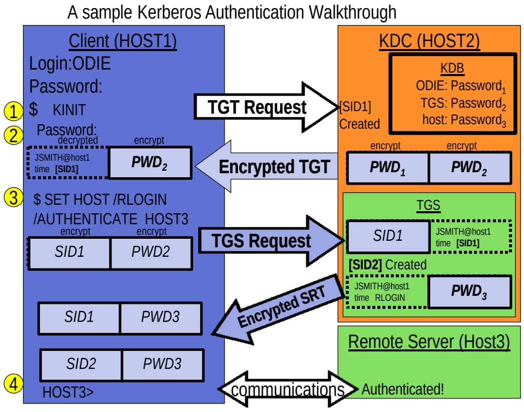
Authentication using cryptographic tickets.



Kerberos Components

- Key Components:
  - KDC (Key Distribution Center)
    - Grant Principle Account & Service Account
    - Administration of the Kerberos Users
    - Keytab files (Securely distributed to every node)
  - TGT (Ticket Granting Ticket)
  - TGS (Ticket Granting Service)
  - Valid account on the Remote Host

A sample Kerberos Authentication Walkthrough



Client (HOST1)

Login:ODIE
Password:

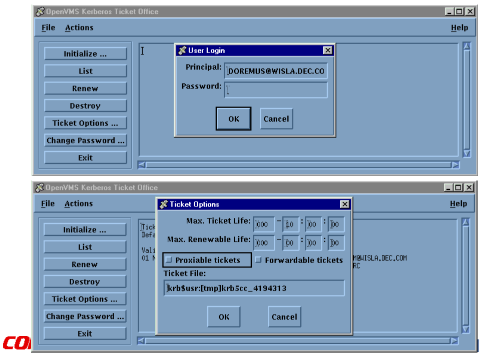
1 $ KINIT
2 Password:

3 $ SET HOST /RLOGIN /AUTHENTICATE HOST3

4 HOST3>

COMPAQ

VMS GUI User Features



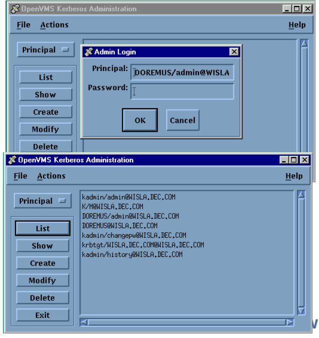
Principal: DOREMUS@WISLA.DEC.CO
Password:

Max. Ticket Life: 000 - 10 : 00 : 00
Max. Renewable Life: 000 - 00 : 00 : 00
□ Proxiable tickets □ Forwardable tickets
Ticket File:
krb$usr:[tmp]krb5cc_4194313

```
Tick
Defa

Vali
01 N
M@WISLA.DEC.COM
RC
```

VMS GUI KDC



Principal: DOREMUS/admin@WISLA
Password:

```
kadmin/admin@WISLA.DEC.COM
K/M@WISLA.DEC.COM
DOREMUS/admin@WISLA.DEC.COM
DOREMUS@WISLA.DEC.COM
kadmin/changepw@WISLA.DEC.COM
krbtgt/WISLA.DEC.COM@WISLA.DEC.COM
kadmin/history@WISLA.DEC.COM
```