HP-UX Security Features

Doug Lamoureux, CISSP
Technical Consultant
Systems Networking and Security Lab
Hewlett-Packard

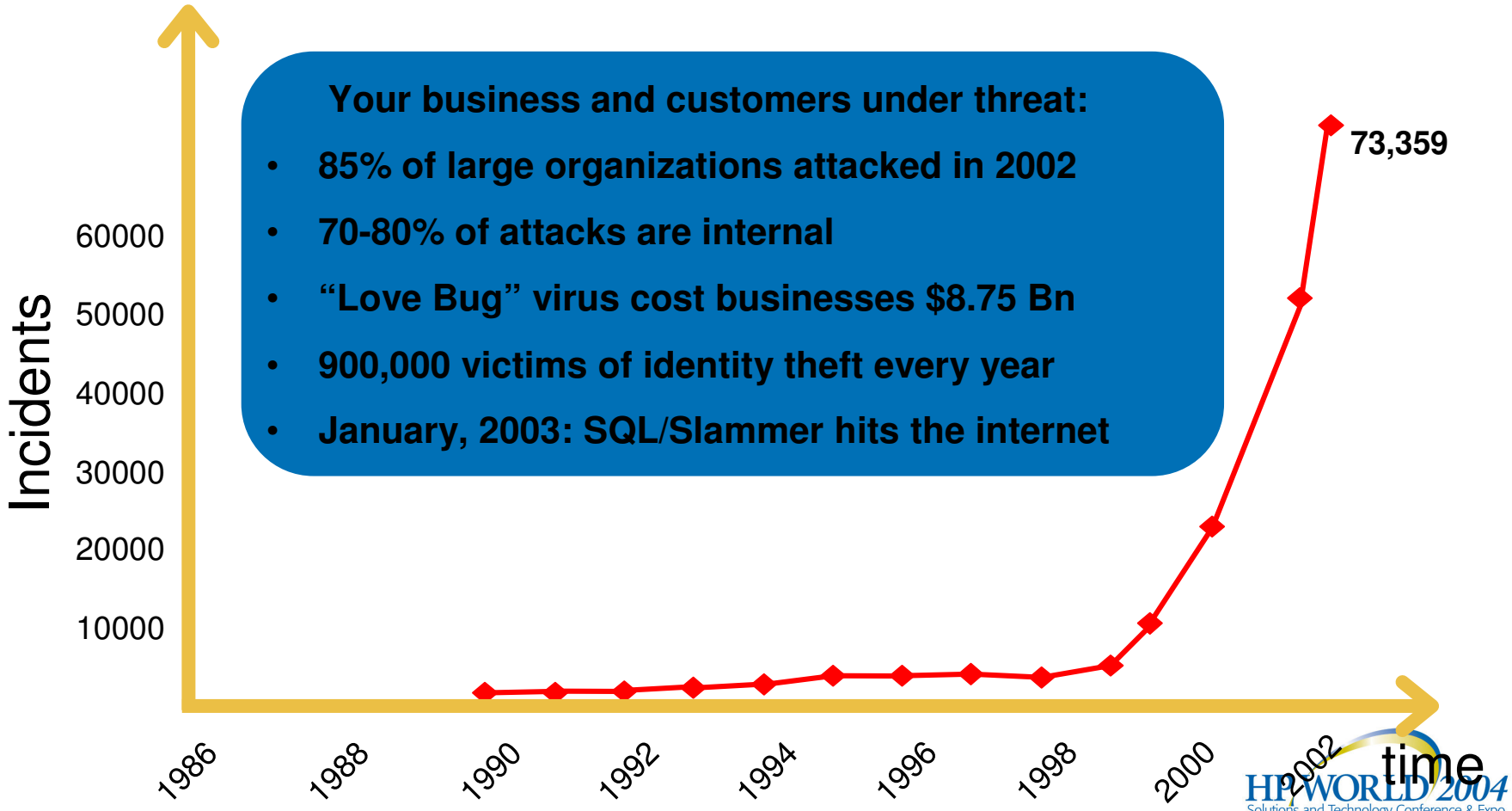
Agenda

- Motivation
- The “Big Picture”
- Host Security
- Network Security
- Authentication
- HP-UX Internet Express
- Security Solutions

Motivation: The increasing importance of security

Sources: www.cert.org
CSI – FBI Computer Crime Survey, 2002

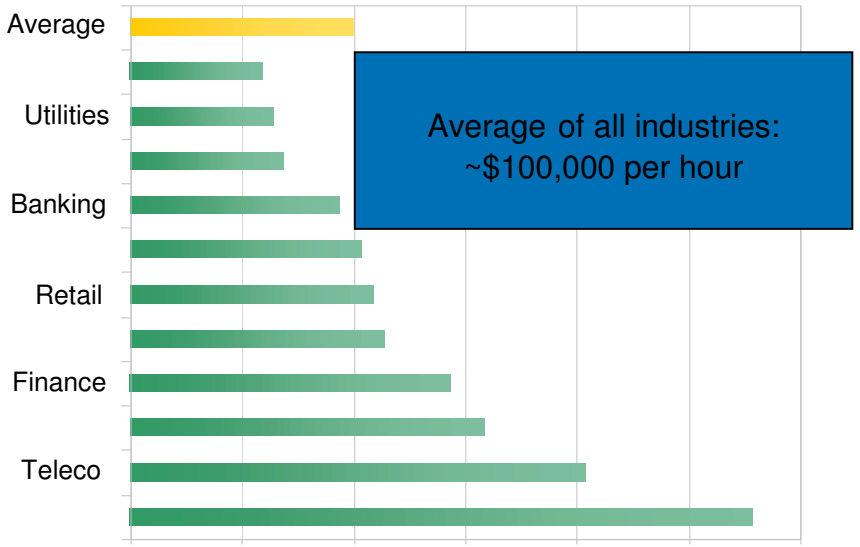
The number of security incidents is increasing exponentially



The consequences of an attack can be catastrophic

Major security incidents lead to serious business impacts

- Direct losses:
  - lost orders
  - loss of immediate revenues
  - lost IP or confidential info
  - liabilities from lost employee or customer data
  - theft/ fraud
- Indirect losses:
  - recovery costs
  - damaged competitiveness
  - damaged brand image



Source: Network Computing, April 2002
"Downtime Costs Money"

downtime is a key contributor to business losses

Motivation: **Regulations**

European Data Protection Directive

Sarbanes-Oxley

Privacy Act

Graham-Leach-Bliley

Insurance Information and Privacy Protection Model Act

Homeland Security Act

Cyber Security Research and Development Act

HIPAA

Government Information Security Reform Act

FERC

Child Internet Protection Act

SEC Regulation S-P

Family Educational Rights and Privacy Act

Network Advising Initiative

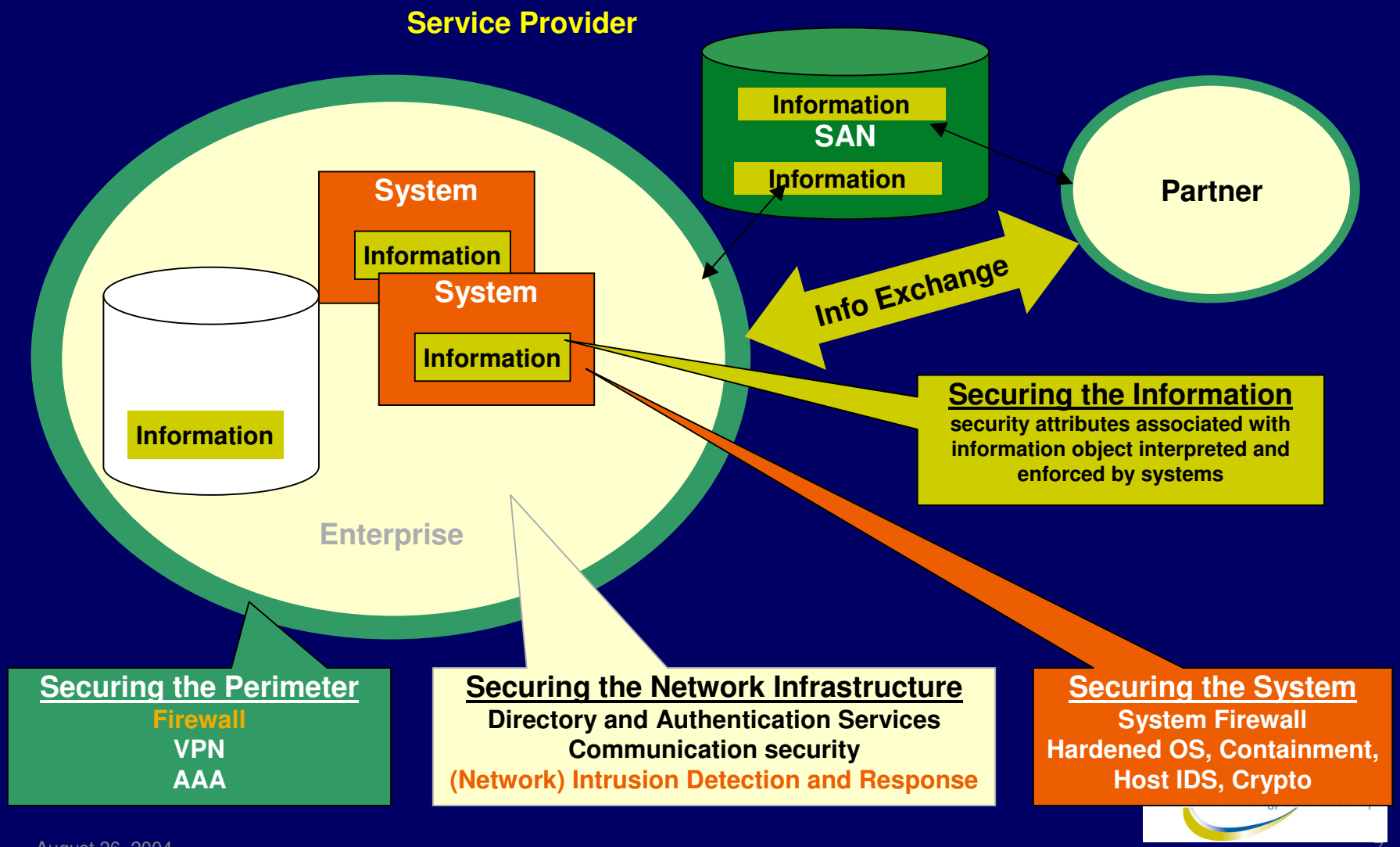
Consequences of Regulations

April 28th, CNET News

Nortel fires CEO, other top execs

"The actions taken by Nortel's board are about accountability for financial reporting"

Security: Big Picture



An Analogy

Physical Analogy: Bank Security

Network Security

- IPSec
- Secure Shell
- Kerberos
- AAA Server
- LDAP Directory Server

Intrusion Prevention

- IPFilter
- Bastille
- Pluggable Authentication
- LDAP-UX integration

Intrusion Detection & Analysis

- Host-Based Intrusion Detection
- Stack buffer overflow protection
- Audit

Mitigation

- Containment
- Role-based Access Control

Tools

- /dev/random
- Ethereal
- Snort
- MD5 Checksum
- Security Patch Check

Future Features

To learn more about future HP-UX Security features (NDA Required):

HP-UX 11i V2 Security Containment
Session #: 4066
Thursday 11:00am

Host Security on HP-UX 11i

Products and Features

- HP-UX Install-Time Security
- HP-UX Bastille
- Host Intrusion Detection System (HIDS)
- Trusted/Standard Modes
- Stack buffer overflow protection
- EAL4-CAPP Certification

Tools

- Security Patch Check
- HP-UX Strong Random Number Generator
- HP-UX MD5 Secure Checksum
- Sudo *(Internet Express)*

HP-UX Install-Time Security

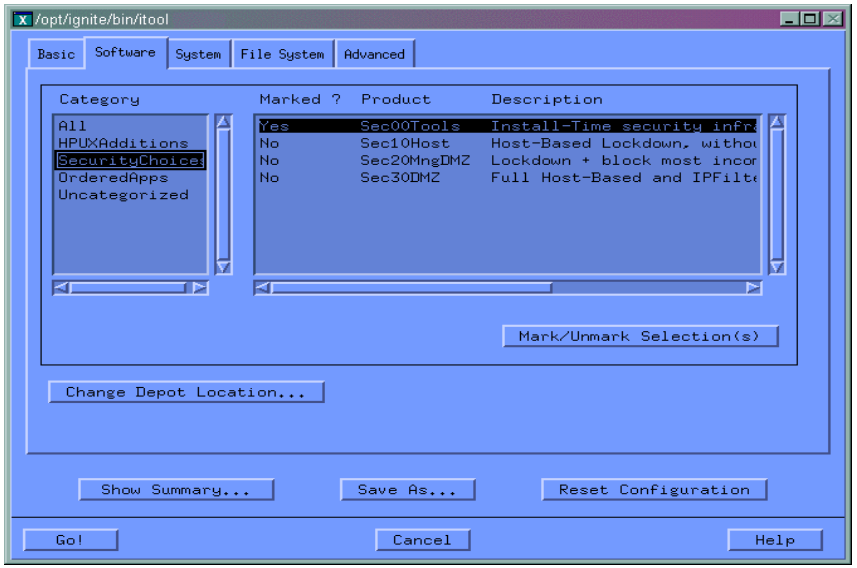
- Deploy HP-UX into high threat environments **quickly**
  - Make security or compatibility decisions suited to your needs
  - Security tradeoffs no longer configured for the “generic user”
- Customers can be “secure-by-default,” at installation,
  - Can later revise settings with Bastille

HP-UX Install-Time Security Options

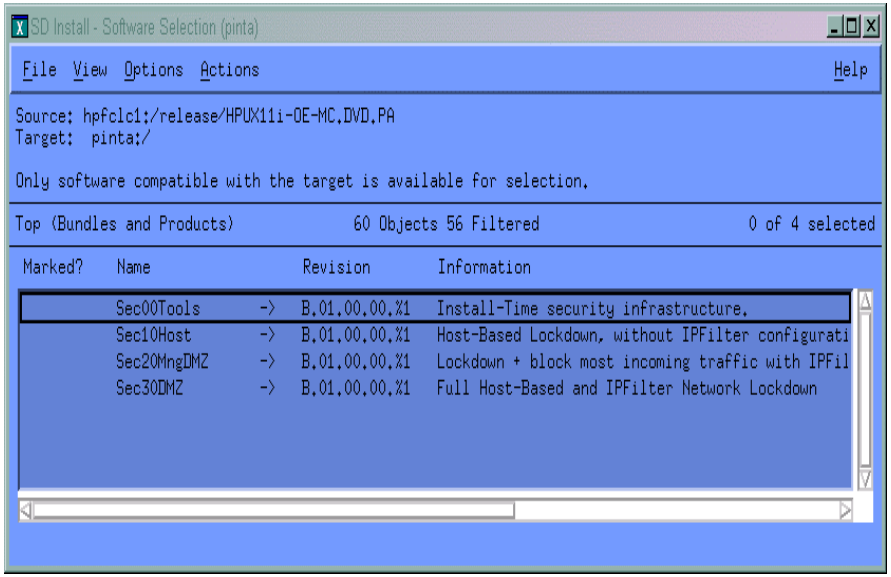
Security Level	Description
Sec00Tools	The install-time security infrastructure; no security changes
Sec10Host	Host-based lockdown: no firewall; networking runs normally, including non-root Telnet and FTP
Sec20MngDMZ	Lockdown uses IPFilter firewall to block incoming connections except common, secured, management protocols
Sec30DMZ	DMZ Lockdown: IPFilter blocks all incoming connections except SecureShell

Four Ways to Use HP-UX Install-Time Security

1) Ignite/UX



2) Software Distributor



2) Manual

```
# swinstall –s <depot> -x autoreboot=true <level>
```

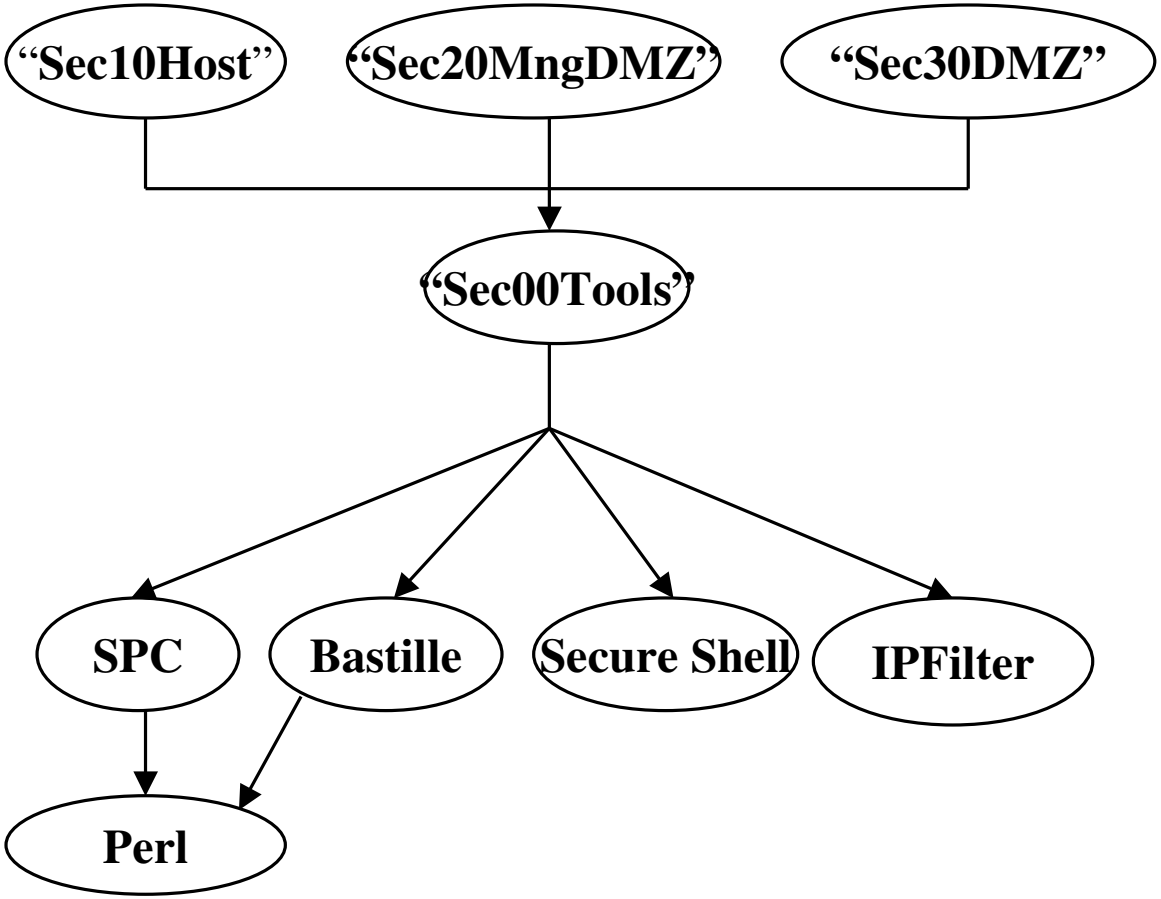
4) Update/UX

```
# update-ux –s <depot> <OE> <level>
```

Other Tools Used with ITS

- Security Patch Check (SPC)
  - Ensures security patches are current on a server
  - Bastille sets SPC to run regularly
- IPFilter
  - Host Firewall filters TCP, UDP and ICMP
  - Bastille configures to protect in two “DMZ” levels
- HP-UX Secure Shell
  - Log in securely to a locked-down system
  - Use as a secure substitute for rcp, ftp, remsh, and telnet

ITS “Under the Hood”



Host Security on HP-UX 11i

Products and Features

- ✓ HP-UX Install-Time Security
- **HP-UX Bastille**
- Host Intrusion Detection System (HIDS)
- Trusted/Standard Modes
- Stack buffer overflow protection
- EAL4-CAPP Certification

Tools

- Security Patch Check
- HP-UX Strong Random Number Generator
- HP-UX MD5 Secure Checksum
- Sudo *(Internet Express)*

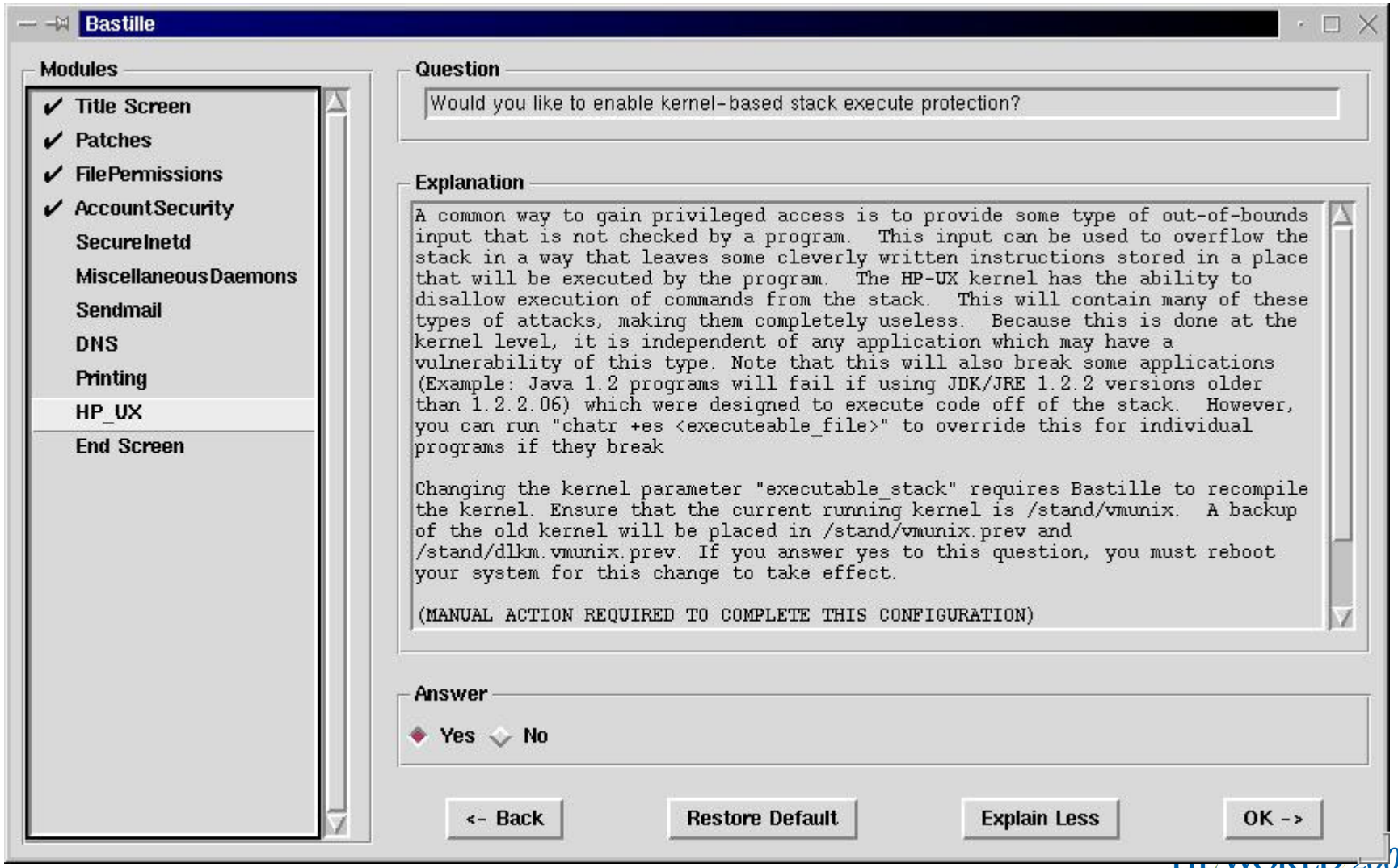
HP-UX Bastille

- An open source (GPL) security hardening and lockdown tool
- Available on Linux and HP-UX (HP-UX supported by HP)
- Configures system daemons, settings, and software, such as sendmail to be more secure

HP-UX Bastille Features

- Turns off unneeded services, such as echo and finger
- Helps create chroot “jails”
  - Additional security layer for Internet services such as web and Domain Name Service (DNS)
- Educational administrator interface
- Bastille configuration can revert to the Pre-Bastille state
- Configures conversion to Trusted Systems or Password Shadowing
- Security Patch Check can run automatically
- Configures the IPFilter firewall

Bastille Screenshot



Host Security – Products and Features

HP-UX Bastille's Modules

- Looking at HP-UX functionality
  - HP-UX modules list
    - Patches
    - File Permissions
    - Account Security
    - Secure Inetd
    - Miscellaneous Daemons
    - Sendmail
    - DNS
    - Apache
    - FTP
    - HP-UX
    - IPFilter

HP-UX Bastille's IPFilter Module

- Enables a basic stateful host-based firewall
  - Blocks incoming traffic by default requiring the explicit enablement of remote services on a per service basis
  - Allows all outbound traffic by default for ease of use
  - Configures incoming traffic for common services
    - Secure Shell remote terminal service
    - WBEM's multi-system management
    - HIDS (Host Intrusion Detection System) reporting and management
    - Common https web administration
    - DNS query connections and zone transfers
  - The custom-rules mechanism allows for easy server specific customizations

HP-UX Bastille's HP-UX Module

- Enables kernel-based stack execute protection
  - Requires kernel rebuild and reboot
- Restricts remote access to swlist
- Hardens "ndd" tunable parameters for network devices
  - ip_forward_directed_broadcasts disabled
  - ip_forward_src_routed disabled
  - ip_forwarding disabled
  - ip_ire_gw_probe disabled
  - ip_send_redirects disabled
  - ip_send_source_quench disabled
  - tcp_conn_request_max increased to mitigate DOS attacks
  - tcp_syn_rcvd_max increased to mitigate DOS attacks

Host Security on HP-UX 11i

Products and Features

- ✓ HP-UX Install-Time Security
- ✓ HP-UX Bastille
- **Host Intrusion Detection System (HIDS)**
- Trusted/Standard Modes
- Stack buffer overflow protection
- EAL4-CAPP Certification

Tools

- Security Patch Check
- HP-UX Strong Random Number Generator
- HP-UX MD5 Secure Checksum
- Sudo *(Internet Express)*

HP-UX Intrusion Detection System (HIDS)

Host-based security product for HP Operating Environments that enables security administrators to proactively monitor, detect, and respond to attacks within a network.

Many types of attacks that can bypass network-based detection systems, HIDS complements existing network-based security mechanisms, bolstering enterprise security.

Network-based vs. Host-based Intrusion Detection

	Pros	Cons
NID	• Non-intrusive • OS independent • Detects common, known network attacks	• Does not scale well • Ineffective against encrypted traffic • Does not detect unknown attacks (signature-based) • Does not detect insider attacks

HID	• Detects insider & outside attacks
	• Detects both known and unknown attacks
	  • Anomaly detection
	• Not impacted by:
	  • encrypted traffic
	  • high speed networks
		• Needs to be tailored
		• Can incur some overhead
		• Most are signature based

Host Security – Products and Features

How HP-UX Host IDS is Different

- Protects against unknown *vulnerabilities*
  - Templates look for patterns of misuse
  - Detects known and unknown attacks
- Near real-time detection & local response
  - Real time Tripwire
- Tightly coupled with HP-UX kernel
  - Auditing system tailored for IDS
- Built by those who know HP-UX the best (HP-UX R&D Lab)

Vulnerabilities Monitored by Host IDS

System critical

- Unauthorized access
- Privilege escalation
- Trojan horse
- “Root” exploits

HP-UX OS

- Race Condition
- Buffer overflow
- Password guessing

User security

- Failed logins
- Failed SU attempts
- Unauthorized modification of other users' files

Files

- Modification of critical system files and directories
- Creation of world writable files
- Creating "setuid" files
- File additions and deletions

How HP-UX Host IDS Works

- Host IDS agent process monitors HP-UX servers locally
  - Kernel audit data
  - System log files
- Correlates using an HP “correlation engine” (ECS)
  - Detection templates
- Logs and sends alerts
  - Alerts locally stored
  - Alerts sent to Host IDS Central Management Station (GUI)
- Supports near real-time response capability
  - Customized response scripts

e.g., sends to OpenView OVO, kill offending process, etc.…

Host Security – Products and Features

Performance

- Factors:
  - Type and number of system calls
  - Product configuration
  - Server class
  - Mode of operation
    - blocking vs non-blocking mode
- TPC-C benchmark, less than 2% degradation

Host Security on HP-UX 11i

Products and Features

- ✓ HP-UX Install-Time Security
- ✓ HP-UX Bastille
- ✓ Host Intrusion Detection System (HIDS)
- **Trusted/Standard Modes**
- Stack buffer overflow protection
- EAL4-CAPP Certification

Tools

- Security Patch Check
- HP-UX Strong Random Number Generator
- HP-UX MD5 Secure Checksum
- Sudo *(Internet Express)*

HP-UX Standard Mode Security

- Provides good basic security features
  - Standard UNIX file access control
  - File ACL's for finer grain permissions
- Many Authentication methods thorough PAM
  - LDAP
  - Kerberos
  - NTLM
- Defacto Standard Shadow Password (11i v1 and later)

HP-UX Standard Mode Security

- Restricted Administration tools
  - Service Control Manager
  - Restricted SAM
- Standard UNIX system logs
  - syslog, sulog
  - wtmp, btmp, utmp for accounting information
- Object Reuse
  - Memory buffers and files are initialized to known values before allocation to a user to prevent a previous user's data from being disclosed

HP-UX Standard Mode Security

Standard Mode HP-UX Feature Availability

	10.20	11.00	11i v1	11i v2
Industry-standard UNIX security	X	X	X	X
Object reuse	X	X	X	X
HFS access control lists	X	X	X	X
Restricted SAM	X	X	X	X
Servicecontrol Manager roles		X	X	X
Large (>60000) user IDs	X	X	X	X
Keberos v5 authentication	X	X	X	X
LDAP v3 authentication		X	X	X
Windows 2000 authentication		X	X	X
NIS manageability	X	X	X	X
Pluggable Authentication Module		X	X	X
NIS+ manageability		X	X	X
JFS access control lists			X	X
Encrypted password protection			X	X
Boot authentication				X
Long passwords				X
Password complexity checking			X	X
Password reuse checking				X
Password lifecycle management				X
Login controls				X
Auditing			X[2]	X[2]
Strong random number generator			X[3]	X
Boot authentication				X
Execute protected stack			X	X

1. Password reuse checking was delivered as part of Extension Pack 9804 and integrated into subsequesnt HP-UX releases.
2. Auditing in form of idds for Intrusion Detection.
3. Available only as a Web release, not part of the core OS release.

HP-UX Trusted Mode Security

Expanding on the fundamentals of Standard Mode:

- Trusted Mode gives the administrator or security officer additional features and options not available with standard UNIX security.
- When the system administrator invokes trusted mode conversion through SAM, the system creates the “Trusted Computing Base”(TCB), which provides the mechanisms and architecture to extend HP-UX security to be fully C2 Security compliant.
- Conversion to the TCB includes protected password database, system default files, terminal default files, device assignment files, and modified crontab entries

HP-UX Trusted Mode Security

- Boot authentication provides that only authenticated and authorized users can access the system in its maintenance ‘single-user’mode
(now available in Standard Mode)
- Encrypted password protection (~Shadow Password)
  - Encrypted passwords are not stored in the publicly readable /etc/passwd
- Long Password
  - A longer password, containing an increased amount of complexity also known as entropy, is harder to crack than a short password
- Password Complexity checking (password length, etc)
- Password History
- Password Policy (expiration time, etc)

HP-UX Trusted Mode Security

- Login Controls
  - Time based access
  - Device based access
  - Account lockouts
- Audit and Logging
  - Using the Audit ID extension of Trusted Mode to uniquely identify users, the audit system can be configured to audit any of over 100 security relevant system calls on a per-user basis
  - System call auditing is the most secure form of accountability. It is also the most resource intensive!
  - HP provides a tool through the System Administrator (SAM), to view the audit records. This tool can be configured to filter out audit records that are of no interest to the system administrator
- Co-existence support with LDAP-UX

HP-UX Trusted Mode Security

Trusted Mode HP-UX Feature Availability

	10.20	11.0	11i v1	11i v2
Encrypted passwords	X	X	X	X
Boot authentication	X	X	X	X
Long passwords	X	X	X	X
Password complexity checking	X	X	X	X
Password reuse checking		X	X	X
Password lifecycle management	X	X	X	X
Login controls	X	X	X	X
Auditing	X	X	X	X
C2 security compliance	X	X	X	X
JFS support	X	X	X	X
NIS+ manageability		X	X	X
LDAP-UX (3.3) support		X	X	X

Host Security on HP-UX 11i

Products and Features

- ✓ HP-UX Install-Time Security
- ✓ HP-UX Bastille
- ✓ Host Intrusion Detection System (HIDS)
- ✓ Trusted/Standard Modes
- **Stack buffer overflow protection**
- EAL4-CAPP Certification

Tools

- Security Patch Check
- HP-UX Strong Random Number Generator
- HP-UX MD5 Secure Checksum
- Sudo *(Internet Express)*

HP-UX Stack Buffer Overflow Protection

- Disabled the ability to execute code from the stack
- This feature prevents widely used buffer overflow against privileged programs
- The HP-UX stack overflow protection offers the advantage of a per-binary override to enable legitimate applications to operate without problem (Java for example)
- Available on both Standard and Trusted Mode

Host Security on HP-UX 11i

Products and Features

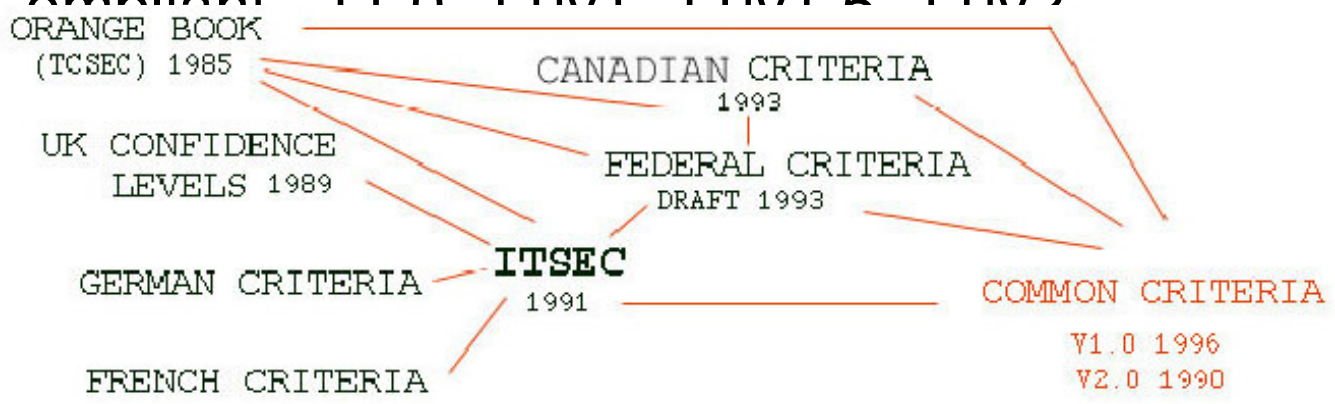
- ✓ HP-UX Install-Time Security
- ✓ HP-UX Bastille
- ✓ Host Intrusion Detection System (HIDS)
- ✓ Trusted/Standard Modes
- ✓ Stack buffer overflow protection
- **EAL4-CAPP Certification**

Tools

- Security Patch Check
- HP-UX Strong Random Number Generator
- HP-UX MD5 Secure Checksum
- Sudo *(Internet Express)*

EAL4-CAPP Certification

- Trusted-mode HP-UX 11iv1 has achieved Common Criteria EAL4-CAPP certification –the certificate of compliance was presented in March, 2003.
- TCSEC CT, ITSEC E3/F-C2
  - Certified –10.20
  - Compliant – 11.0, 11iv1, 11iv1.5, 11iv2



Host Security on HP-UX 11i

Products and Features

- ✓ HP-UX Install-Time Security
- ✓ HP-UX Bastille
- ✓ Host Intrusion Detection System (HIDS)
- ✓ Trusted/Standard Modes
- ✓ Stack buffer overflow protection
- ✓ EAL4-CAPP Certification

Tools

- **Security Patch Check**
- HP-UX Strong Random Number Generator
- HP-UX MD5 Secure Checksum
- Sudo *(Internet Express)*

HP Security Patch Check

- Supports 11.0, 11.04, 11.11, 11.22, 11.23, …
- Analyzes filesets and patches on an HP-UX system against the HP-UX Patch Catalog
- Generates a report of recommended security patches for the system
- Identifies patches with warnings present on the system
- Support is covered by HP-UX support contract
- Part of 11.23 and beyond OEs

HP Security Patch Check

```
# /opt/sec_mgmt/spc/bin/security_patch_check -r
WARNING: There are world-writable directories in your path
        to perl and/or your PATH environment variable.  This represents a
        security vulnerability (especially if running as root) that may
        compromise the effective use of this tool.  Please use the command:
        chmod o-w <directory name>
        to ensure this tool can be used safely in the future.  A list of the
        vulnerable directories follows:
              /var/opt/iplanet
              /var/opt/iplanet/servers
…
NOTE:    Downloading from
        ftp://ftp.itrc.hp.com/export/patches/security_catalog.sync.

NOTE:    ftp://ftp.itrc.hp.com/export/patches/security_catalog.sync
            downloaded to ./security_catalog.sync successfully.
```

HP Security Patch Check (cont.)

WARNING: ./security_catalog is group or world writable.

WARNING: /tmp/ is group/world writable and the sticky bit is not on.

NOTE: HP has issued Non-Critical warnings for the active patch PHCO_23413 on the target system. Its record, including the Warn field, is available from ./security_catalog, through the Patch Database area of the ITRC or by using the -m flag (security_patch_check -m ...).

WARNING: HP has issued Critical warnings for the active patch PHCO_27037 on the target system. Its record, including the Warn field, is available from ./security_catalog, through the Patch Database area of the ITRC or by using the -m flag (security_patch_check -m ...).

HP Security Patch Check (cont.)

*** BEGINNING OF SECURITY PATCH CHECK REPORT ***
Report generated by: /opt/sec_mgmt/spc/bin/security_patch_check.pl, run as root

Analyzed localhost (HP-UX 11.11) from hpatcux2
Security catalog: ./security_catalog
Security catalog created on: Mon Apr 26 18:47:16 2004
Time of analysis: Tue Apr 27 10:30:36 2004

List of recommended patches for most secure system:

#	Recommended	Bull(s)	Spec?	Reboot?	PDep?	Description
1	PHCO_25918	237	No	No	No	sort(1) cumulative
2	PHCO_26561	275	No	No	No	csh(1) cumulative
3	PHCO_27019	275	No	No	No	ksh(1)
4	PHCO_27345	275	No	No	Yes	cumulative sh-posix(1)

Host Security on HP-UX 11i

Products and Features

- ✓ HP-UX Install-Time Security
- ✓ HP-UX Bastille
- ✓ Host Intrusion Detection System (HIDS)
- ✓ Trusted/Standard Modes
- ✓ Stack buffer overflow protection
- ✓ EAL4-CAPP Certification

Tools

- ✓ Security Patch Check
- **HP-UX Strong Random Number Generator**
- HP-UX MD5 Secure Checksum
- Sudo *(Internet Express)*

HP-UX Strong Random Number Generator

- The Strong Random Number Generator provides a secure, non-reproducible source of true random numbers for applications with strong security requirements, such as generating encryption keys.
- Generating encryption keys from a non-random source constitutes a security risk

HP-UX Strong Random Number Generator

2 Interfaces to read random data

- /dev/random
  - standard blocking interface
  - read(2) system call will not return until the requested amount of random data, up to 256 bytes, has been collected internally
- /dev/urandom
  - standard non-blocking interface
  - Internal buffer is hashed using AES to provide high quality random data
  - Internal buffer is re-initialized at least every minute to guarantee that the output remains unpredictable

HP-UX Strong Random Number Generator

- Available on 11i v1 (11.11) from software.hp.com
- Bundled with 11i v2 (11.23)

Host Security on HP-UX 11i

Products and Features

- ✓ HP-UX Install-Time Security
- ✓ HP-UX Bastille
- ✓ Host Intrusion Detection System (HIDS)
- ✓ Trusted/Standard Modes
- ✓ Stack buffer overflow protection
- ✓ EAL4-CAPP Certification

Tools

- ✓ Security Patch Check
- ✓ HP-UX Strong Random Number Generator
- **HP-UX MD5 Secure Checksum**
- Sudo *(Internet Express)*

HP-UX MD5 Secure Checksum

- HP-UX MD5 Secure Checksum (a.k.a. md5sum or MD5 Checksum) is a popular approach for checking file integrity
- Helps verify that files downloaded over ftp/http have not been corrupted during transfer
- Checks whether file contents have changed
- Based on the standard MD5 Message-Digest Algorithm
- Consists of two separately installable components:
  - HP-UX MD5sum (md5sum Command)
  - HP-UX LibCryptX (MD5 Libraries)

Host Security – Tools

HP-UX MD5 Secure Checksum

- Compatible with open source md5sum output
- Command line tool (md5sum) and hashing libraries (libcryptx)
- Secure form of the Unix cksum command
  - md5sum = secure cksum
- 128-bit cryptographic strength hash generator
- High-performance and scalable md5sum command based on patented architecture*

* Patent Pending

HP-UX MD5 Secure Checksum Sample


```
# md5sum –k /stand/vmunix
fb74007d455c363530c2c30249026e99 27261520  /stand/vmunix

# cksum /stand/vmunix
4235960935 27261520 /stand/vmunix
```

Host Security on HP-UX 11i

Products and Features

- ✓ HP-UX Install-Time Security
- ✓ HP-UX Bastille
- ✓ Host Intrusion Detection System (HIDS)
- ✓ Trusted/Standard Modes
- ✓ Stack buffer overflow protection
- ✓ EAL4-CAPP Certification

Tools

- ✓ Security Patch Check
- ✓ HP-UX Strong Random Number Generator
- ✓ HP-UX MD5 Secure Checksum
- Sudo *(Internet Express)*

More…

Session #3180 (Mon 9:30am):

Maintaining HP-UX System Security

Network Security on HP-UX 11i

Products and Features

- HP-UX IPSec
- HP-UX IPFilter
- HP-UX Secure Shell
- Internet Services
- Directory Enabled Computing
  - Netscape Directory Server
  - LDAP-UX
  - OpenLDAP *(Internet Express)*

Tools

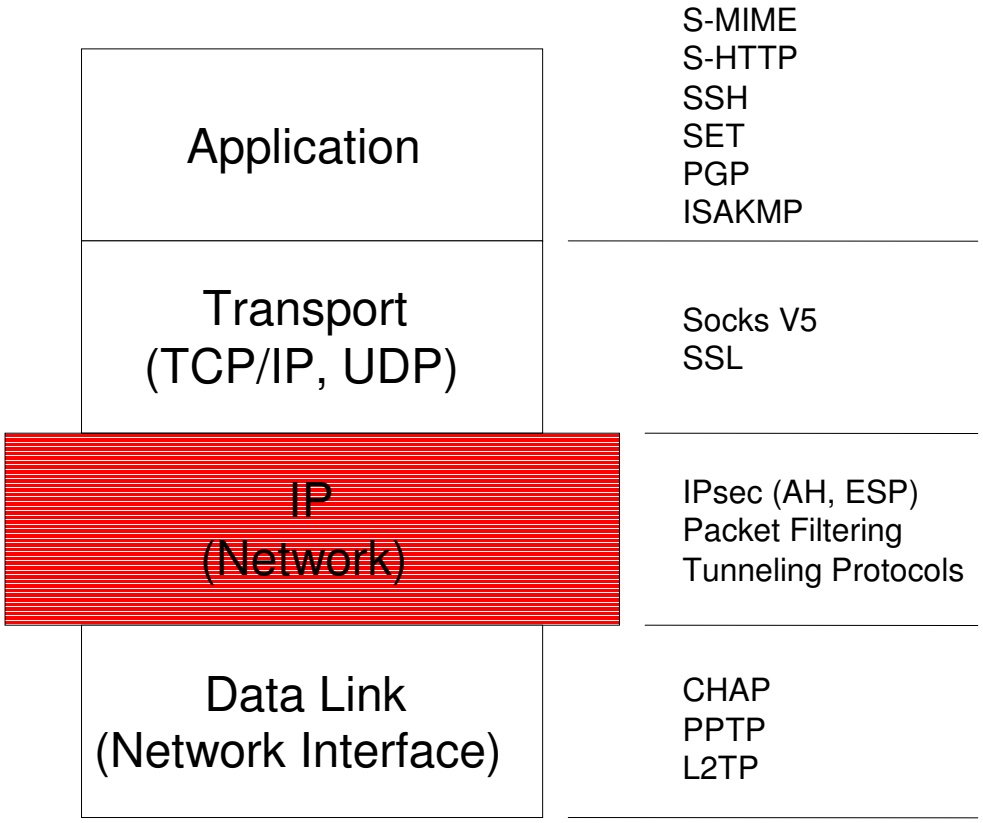
- LDAP SDK
- OpenSSL
- GSS-API
- SNORT *(Internet Express)*
- Ethereal *(Internet Express)*
- Nessus *(Internet Express)*

HP-UX IPSec

What is IPSec?

IPSec provides an infrastructure to allow secure communications (authentication, integrity, confidentiality) over IP-based networks between systems/devices that implement the “IPsec” set of protocols.

Where does IPSec fit?



HP-UX IPSec Features

- Adheres to all relevant IPsec standards, including IKE (Internet Key Exchange) for automated key generation.
- **Focused on end-system IPsec**. Can communicate with other end-systems (transport mode) or with VPN gateways (tunnel mode).
- Easy to adopt. Transparent to existing applications. Protects customer's investment.
- Tightly integrated with both IPv4 and IPv6 networking stacks (recently tested at MoonV6 project moonv6.com).
- Industry leading performance. Crypto performance is optimized for PA-RISC and IPF (IA64) architecture.
- Fully supported in an MC/ServiceGuard environment.
- Demonstrated multi-vendor interoperability.

HP-UX IPSec Features (continued)

- Host-based authentication: pre-shared keys or digital certificates (via Baltimore, OpenSSL, or Verisign PKI). Certificates are obtained programmatically (auto-enrollment) for Verisign and via “face-to-face” enrollment for Baltimore.
- CLI for IPSEC policy configuration.
- Includes policy defaults for ease of config.
- Flexible rule-based security attribute & access control policy configurations. Allows combinations of IP addresses, subnet mask, ports, protocols …
- Diagnostic & monitoring tool. Logging & audit trail for accountability & intrusion alerts

IPSec: The Basics

Authentication Header (AH)

- Provides data/packet integrity. Also prevents address spoofing and replay attacks.
- Authenticates the entire IP datagram using cryptographic hash algorithms (HMAC-SHA1 or HMAC-MD5).

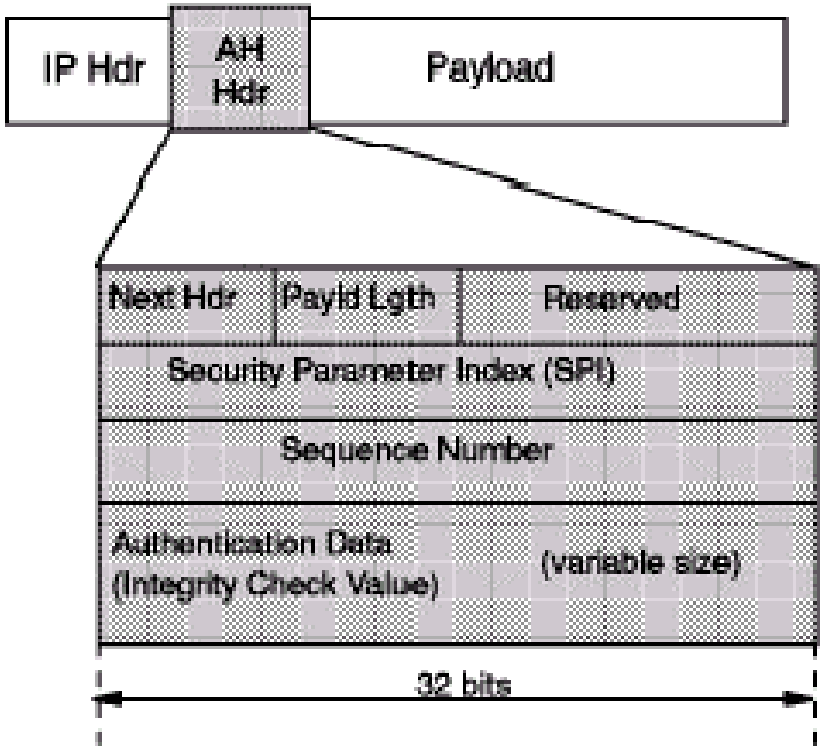
Encapsulating Security Payload (ESP)

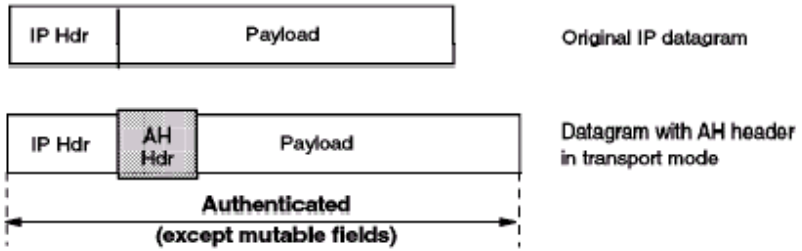
- Provides confidentiality via encryption. Can optionally provide the same authentication services that AH provides (also via HMAC-SHA1 or HMAC-MD5).
- Typical encryption algorithms: DES, 3DES, AES

Modes of Operation

- Transport mode: Used for end-end communication. Original IP header is not encrypted.
- Tunnel mode: Used for communication with a VPN gateway. New IP header is added and entire original packet is encapsulated/encrypted.

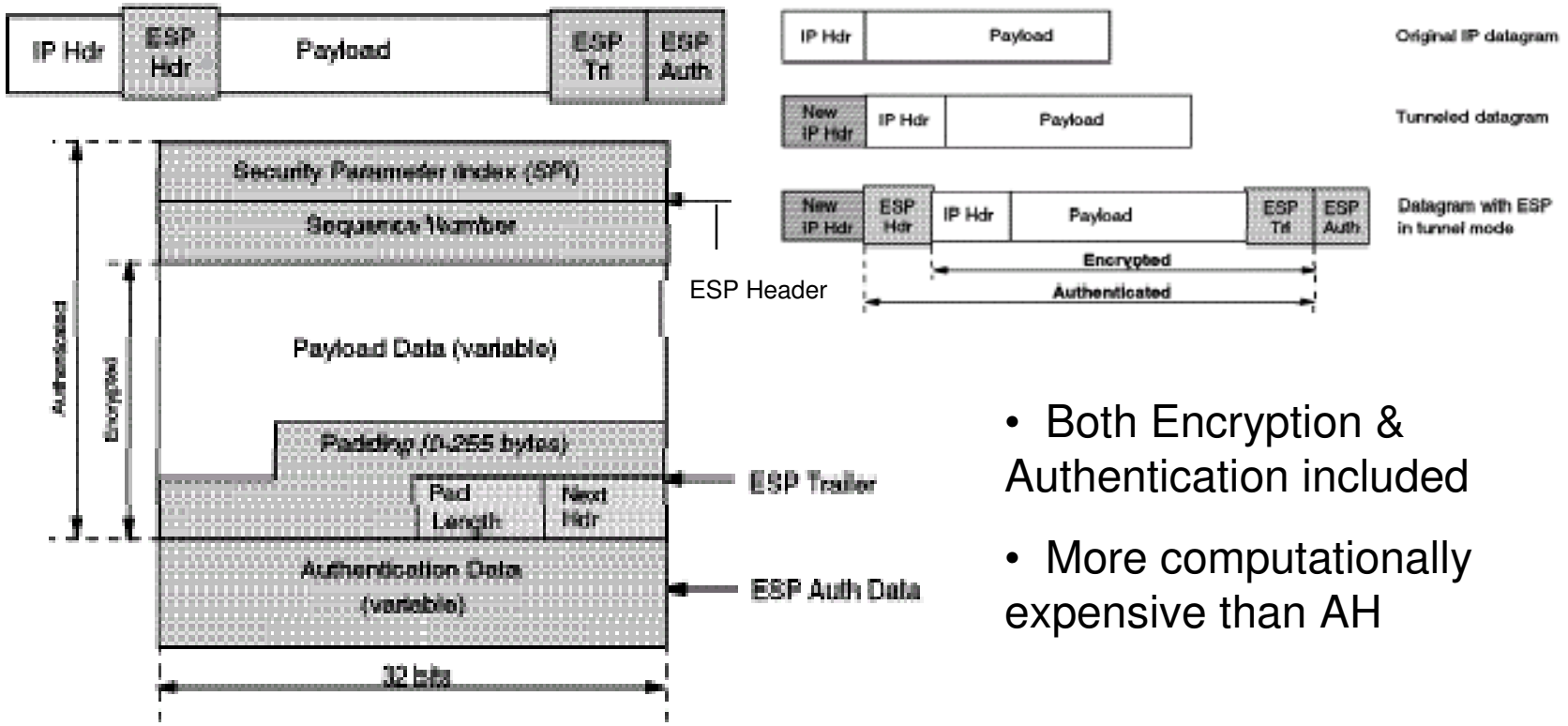
IPSec: Authentication Header





- **Simple format**
- **Low processing overhead**

IPSec: Encapsulating Security Payload (ESP)

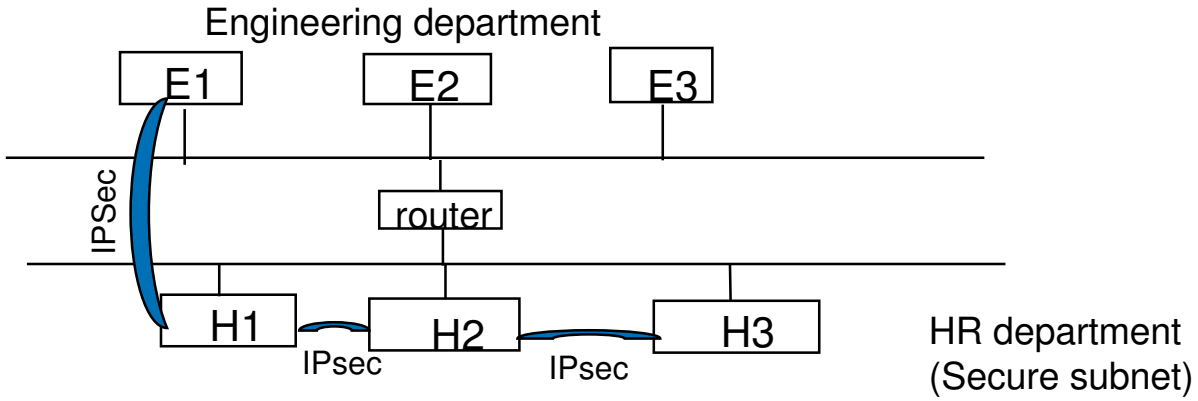


- Both Encryption & Authentication included
- More computationally expensive than AH

IPSec Scenario 1: End-to-end secure communication within Internal Network

According to FBI, 80% of security breaches came from internal attacks. Therefore, it is important to secure internal network traffic within the enterprise.

Example: Securing internal communication to the HR department



- Use IPsec to secure traffic within the HR department (Secure Subnet)
- Use IPsec to secure end-to-end communication between an engineering station to a HR server (client-server or server-to-server)

Network Security on HP-UX 11i

Products and Features

- ✓ HP-UX IPSec
- **HP-UX IPFilter**
- HP-UX Secure Shell
- Internet Services
- Directory Enabled Computing
  - Netscape Directory Server
  - OpenLDAP *(Internet Express)*
  - LDAP-UX

Tools

- LDAP SDK
- OpenSSL
- GSS-API
- SNORT *(Internet Express)*
- Ethereal *(Internet Express)*
- Nessus *(Internet Express)*

HP-UX IPFilter

What is IPFilter:

A “System Firewall” that provides firewall protection for **individual HP-UX hosts**, as opposed to a perimeter firewall that protects an entire network or subnet.

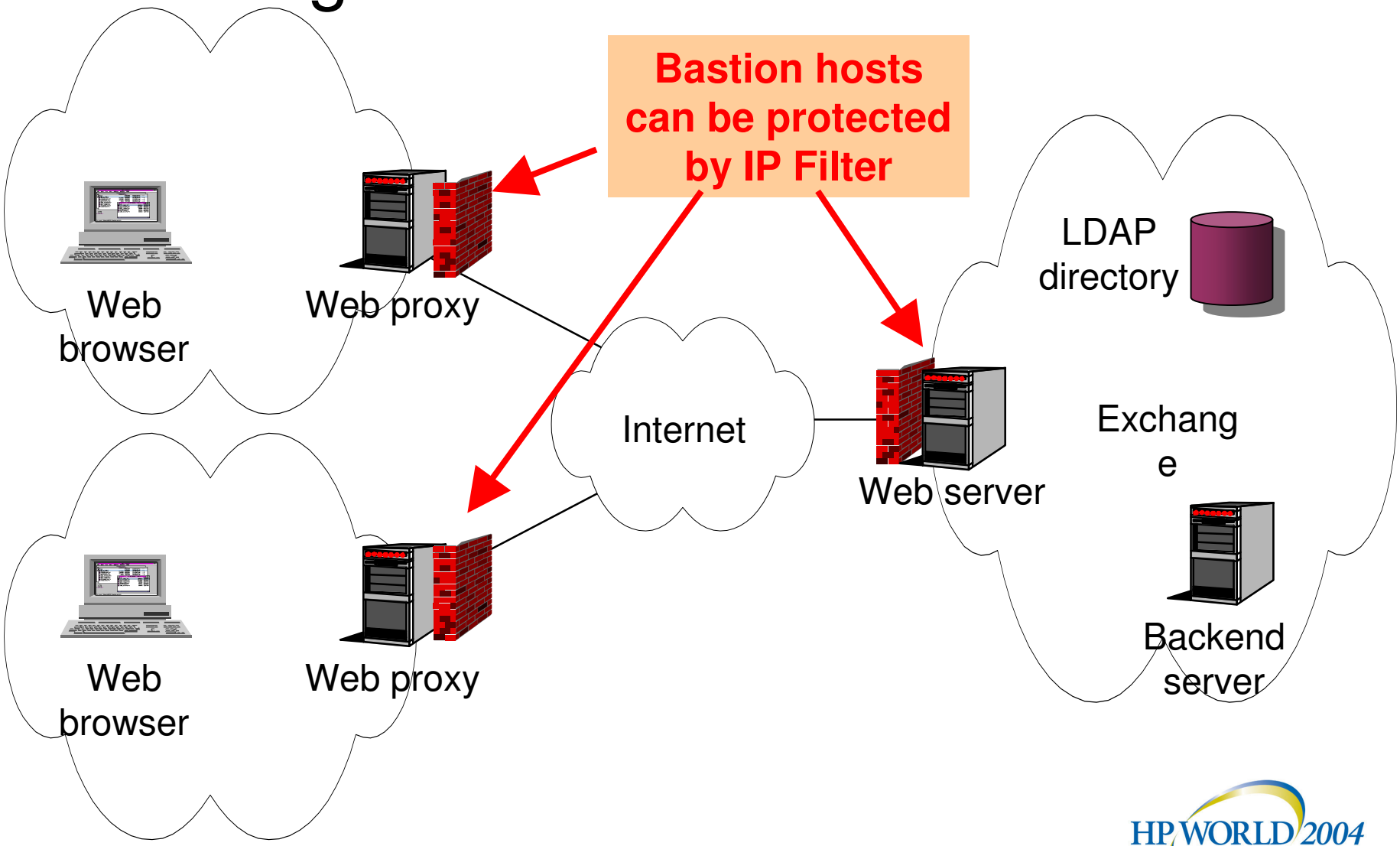
HP-UX IPFilter: Features

- Protection is based on inspection (stateless and stateful) of network traffic going to/from the system. Handles TCP, UDP, and ICMP packet flows.
- Uses a subset of features/technology used by perimeter firewalls:
  - Rules for allowing traffic in/out. Based on IP address, port #, protocol, interface, ICMP message type, etc.
  - Full-fledged stateful inspection firewall
    - Connection monitoring/Detection of potential attacks
    - Verify correct TCP behavior -> sequence numbers, flags, detects connection closing, etc.
  - Rule grouping for efficiency/clarity
  - Flexible command-line configuration and logging capabilities

HP-UX IPFilter: Features *(cont.)*

- Network Address Translation (NAT) support in 11i v2 and beyond
- Not for use with non-IP protocols (e.g. SNA, IPX)
  - Based on open source developed by Darren Reed for OpenBSD. Ported to HP-UX and supported/maintained by HP.
  - Contains perimeter firewall features as well, but these are not the focus of this product and are not supported by HP

HP-UX IPFilter Scenario 1: Protecting Bastion Hosts



Network Security – Products and Features

HP-UX IPFilter Dynamic Connection Allocation (DCA)

An IP-address based packet filtering system that can be used as an effective safeguard for IP based network services:

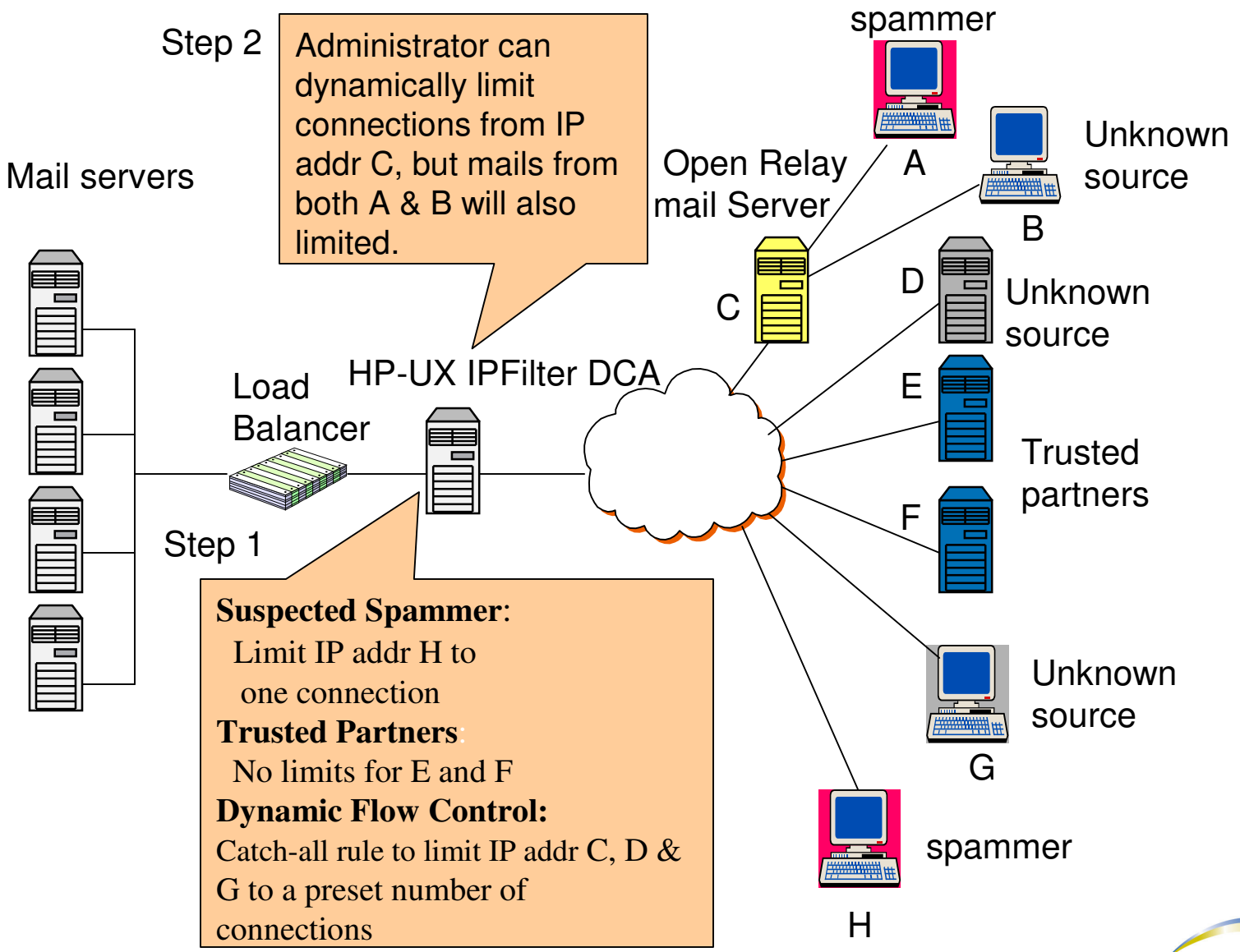
- Limit connect requests to slow down potential spammers
- Configurable connection limit per IP address, subnet or range of IP addresses
- Trusted partners can be configured to bypass connection limitations
- Hosts in an IP subnet can be assigned a cumulative limit

- Based on enhancements to current HP system firewall product (HP-UX IPFilter). DCA provides additional functionality within the HP-UX IPFilter product.

DCA Features

- Dynamically flow control untrusted network sources
- Reject excessive connect requests to slow down connection rates from unknown sources that exceed the flow control limit
- Flexible Rule-based filtering
- Support of IP address and port-based filtering
- Allow dynamic updates of filtering rules without the need of restarting DCA
- Configurable flow control limit
- Configurable action against connection request exceeding flow control limit. A connect request (SYN packet) can be dropped or terminated by sending RST.

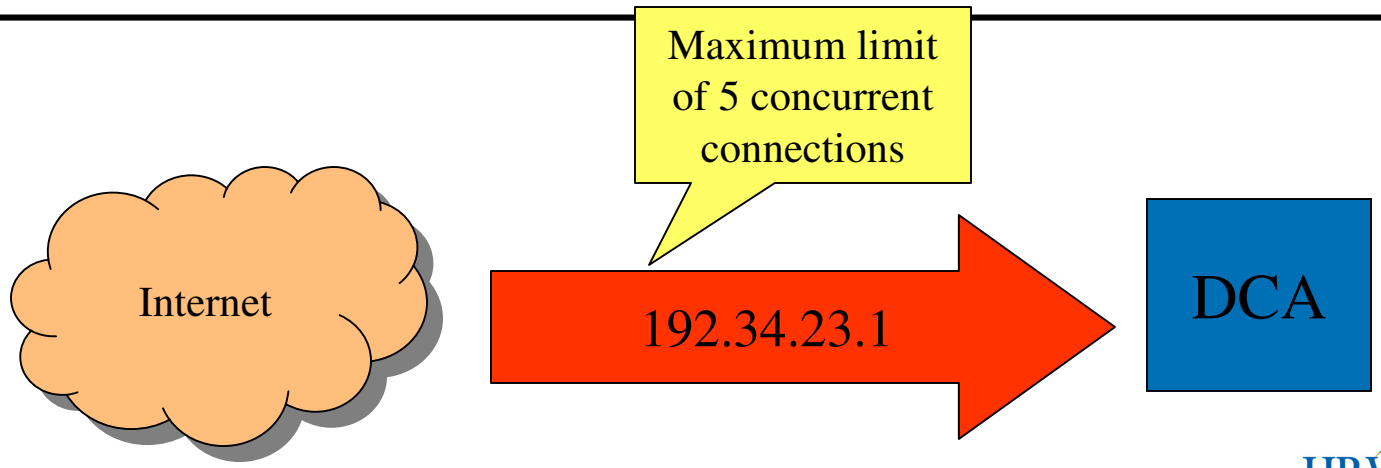
An example of HP-UX IPFilter DCA Configuration



Network Security – Products and Features

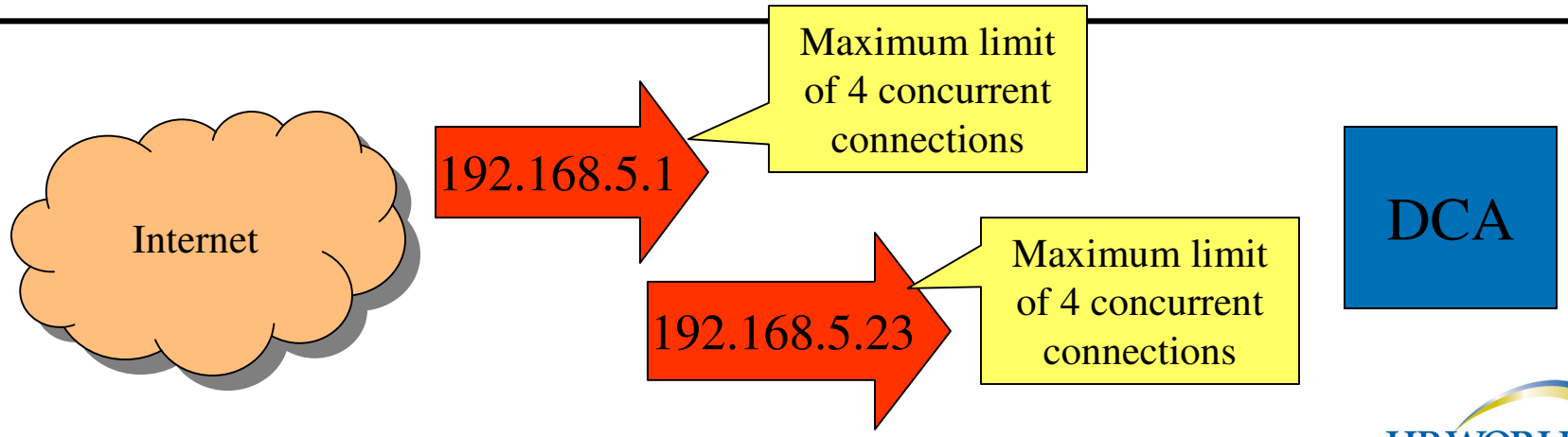
DCA Filtering Rule 1

Individual connection limit per IP address
pass [rtn-reset] in quick proto tcp from 192.34.23.1 to any port = 25 keep limit 5
This rule will limit maximum concurrent connections from host 192.34.23.1 to 5. If [rtn-reset] option is specified, reset will be sent for over limit connection.



DCA Filtering Rule 2

Connection limit for each individual IP address within a subnet
pass in quick proto tcp from 192.168.5.0/24 to any port = 25 keep limit 4
This rule will limit maximum concurrent connections from any individual host in subnet 192.168.5.0/24 to 4



HP-UX IPFilter Availability

- Supported Links:
  - Gigabit Ethernet (1000Base-T)
  - Fast Ethernet (100Base-T)
  - Ethernet (10Base-T)
  - APA (11i v2 when available)
  - VLANS (11i v2 when available)
  - PCI FDDI
  - PCI Token Ring
  - InfiniBand (HP-UX 11i v2)

More..

Session #3545 (Wed 8am):

IPFilter Dynamic Connection Control

Network Security on HP-UX 11i

Products and Features

- ✓ HP-UX IPSec
- ✓ HP-UX IPFilter
- **HP-UX Secure Shell**
- Internet Services
- Directory Enabled Computing
  - Netscape Directory Server
  - OpenLDAP *(Internet Express)*
  - LDAP-UX

Tools

- LDAP SDK
- OpenSSL
- GSS-API
- SNORT *(Internet Express)*
- Ethereal *(Internet Express)*
- Nessus *(Internet Express)*

HP-UX Secure Shell (SSH)

What is HP-UX Secure Shell?

SSH is a program for secure remote login, to execute commands on a remote machine, and to transfer files securely over an insecure network.

HP-UX Secure Shell Features

- Based on OpenSSH (current stable revisions)
- Provides strong encryption
- Secure tunneling capabilities
- Several authentication schemes
  - Kerberos 5/GSSAPI
  - PAM for password authentication
  - Public key
- IPv6 support
- Fully-tested HP product
- Support included with HP-UX Support Agreement
- Privilege separation
- Support for SSH-1 and SSH-2 protocols

More..

Session #3611 (Fri 9:30):

SSH Explained

Network Security on HP-UX 11i

Products and Features

- ✓ HP-UX IPSec
- ✓ HP-UX IPFilter
- ✓ HP-UX Secure Shell
- **Internet Services**
- Directory Enabled Computing
  - Netscape Directory Server
  - OpenLDAP *(Internet Express)*
  - LDAP-UX

Tools

- LDAP SDK
- OpenSSL
- GSS-API
- SNORT *(Internet Express)*
- Ethereal *(Internet Express)*
- Nessus *(Internet Express)*

Internet Services

- Bind 9.2.0
  - DNSSEC
  - TSIG
  - Dynamic DNS
  - IPv6 Support
  - Available on 11.0 & 11i v1 & v2
- WuFTP 2.6.1
  - Virtual Host
  - Guest users and groups
  - Restrict access (ftpaccess)
  - IPv6 Support
  - Available on 11.0 & 11i v1 & v2

Internet Services

- Sendmail 8.11.1
  - Antispam rule set
  - SMTP Authentication
  - LDAP Based routing
  - Spam control using Message Submission Agent
  - Virtual Hosting
  - IPv6 Support (11i v1 only) ??
  - Available on 11.0,11i v1 & v2

Internet Services

- TCP Wrappers
  - Used to restrict access to Internet Services (similar to inetd.sec)
  - Monitors and Logs incoming connections
  - Supports XTI as well as sockets based services
  - Protection against hostname and hostaddress spoofing
  - Supports RFC 931 (client name lookup)
  - Based on Opensource code
  - Available on HP-UX 11i v1 (11.11)

More..

Session #3390 (Wed 11am):

Internet Services on HP-UX: New Features and the Future

Network Security on HP-UX 11i

Products and Features

- ✓ HP-UX IPSec
- ✓ HP-UX IPFilter
- ✓ HP-UX Secure Shell
- ✓ Internet Services
- **Directory Enabled Computing**
  - Netscape Directory Server
  - OpenLDAP *(Internet Express)*
  - LDAP-UX

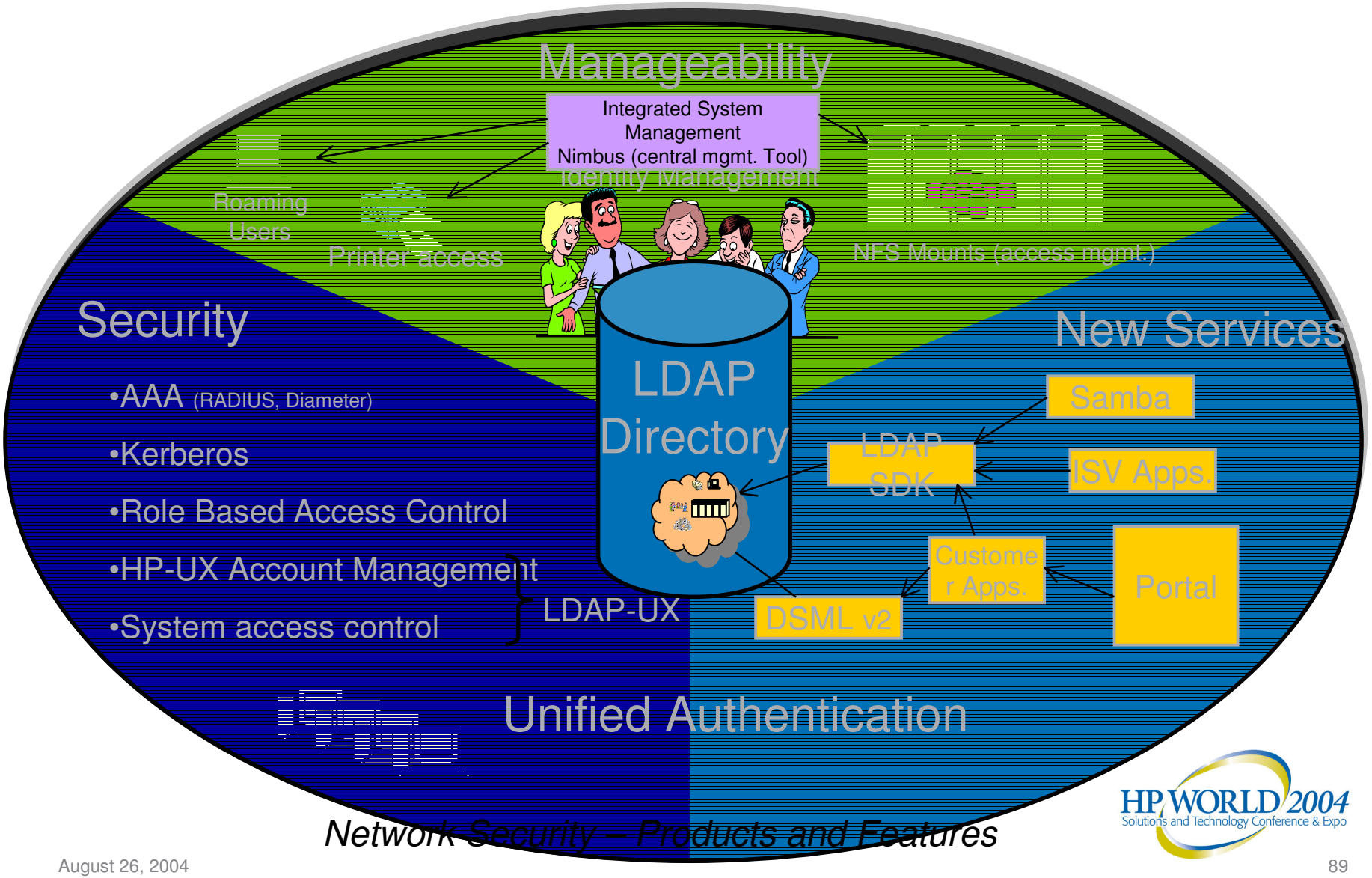
Tools

- LDAP SDK
- OpenSSL
- GSS-API
- SNORT *(Internet Express)*
- Ethereal *(Internet Express)*
- Nessus *(Internet Express)*

HP-UX & Directory-Enabled Computing

- HP's official program to promote directory-enabled applications and services for the HP-UX platform.
  - OS continues to see further integration with LDAP.
  - Additional services, and applications available from HP (CIFS, Kerberos, autofs…)
  - Developer kits and directory-enabled framework available to HP-UX developers
  - HP's strategy to integrate HP-UX into Identity Management deployments
  - Improve HP-UX's provisioning and configuration (zero configuration)
  - Top to bottom LDAP based management (Thanks to LDAP integration in Lights Out firmware)

Directory-Enabled Computing: Values



Network Security – Products and Features

Netscape Directory Server

- Netscape Directory Server v6.11 available on HP-UX 11.0, 11i (v1 & v2)
- Bundled with OE's on 11i and included in the Application CD's for 11.0 (also available for download from software.hp.com)
- No client licensing fee for internal (intranet) users.
- Licenses required for external (extranet) users stored in the Directory (first 250,000 free.)
- Full support from HP

Netscape Directory Server Features

- LDAP based Directory Server (RFC3377)
- Console Server configuration and Management tool (HP-UX and Windows)
- Multiple backend databases
- Multi-Master replication (NDS v6.2 includes 4-way multi-master.)
- Class of Service attribute
- SSL/TLS Support
- Password Policy
- Online Schema updates

Features of LDAP-UX Integration

NIS/LDAP Gateway

- Allows NIS clients to use LDAP (a migration tool.)
- Requires passwords be stored in directory server to be “visible” and in {crypt} format.
- Supports all NIS clients. Runs on 10.20 and later

LDAP-UX Native Client

- HP-UX 11.00+ can use LDAP as name service.
- NSS_LDAP library obtains info. for passwd, group and others.
- PAM_LDAP library provides LDAP based authentication.
- PAM_AUTHZ library restricts logins Flexible and scalable configuration.
- Digest-MD5 support.
- SSL Support.
- High Performance (single connection and caching daemon)
- X.500 group membership supported
- Windows integration
- Simple LDAP Data Management tools

Features of LDAP-UX Integration

- NIS/LDAP Gateway
  - Allows NIS clients to use LDAP (a migration tool.)
  - Requires passwords be stored in directory server to be “visible” and in {crypt} format.
  - Supports all NIS clients. Runs on 10.20+.

- LDAP-UX Native Client
  - HP-UX 11.00+ can use LDAP as name service.
  - NSS_LDAP library obtains info. for passwd, group and others.
  - PAM_LDAP library provides LDAP based authentication.
  - PAM_AUTHZ library restricts logins Flexible and scalable configuration.
  - Digest-MD5 support.
  - SSL Support.
  - High Performance (single connection and caching daemon)
  - X.500 group membership supported
  - Windows integration
  - Simple LDAP Data Management tools

HP-UX/LDAP Integration

- Provide network repository for:
  - Account Management
    - /etc/passwd, /etc/group
  - Access Management
    - /etc/netgroup, pam_authz
  - Network Configuration
    - /etc/services, /etc/hosts, /etc/protocols, /etc/networks
  - Service Configuration
    - /etc/rpc
  - Device Configuration
    - Printer configuration (as of B.03.20)
- Provide a Single Security Space
  - Single account/password for HP-UX and other organizational applications.

Schemas

- Network Information Service schema defined in RFC2307
  - posixAccount
  - posixGroup
  - others such as ipNetwork, nisNetGroup, etc…
- Other common schemas used with RFC2307:
  - inetOrgPerson (RFC2798) & groupOfUniqueNames (RFC2256)

LDAP-UX Integration with Active Directory

- Combining LDAP-UX with PAM Kerberos allows HP-UX to integrate account authentication and management with Windows 2000 Active Directory.
  - Share single user entry in ADS
    - Single account ID and single password (does not require password sync.)
  - Kerberos provides a base for Single Sign On
    - Either pam_kerberos or pam_ldap works with ADS, but kerberos is preferred.
  - Multi-domain support
    - Allows login to HP-UX for any user in the forest (requires that unique account id numbers be assigned across the domain.)
  - LDAP-UX supports X.500 group syntax (same as ADS)
    - Allows simpler group management
  - Either SFU 2.0 or 3.0 schema supported
    - Stores UNIX data in Active Directory

More…

Session #3202 (Wed 4pm):
Integrating HP-UX Authentication with Windows 2000 Active Directory

Authorization with PAM_AUTHZ

- With PAM_UNIX and NIS, system access control can be achieved using a special +/- syntax in the local /etc/passwd file
  - Only supported when using PAM_UNIX
  - Provides “deny” functionality by hiding a users password field.
- A module called PAM_AUTHZ, delivered with LDAP-UX, can be used to restrict login access to systems
  - Can be used with any PAM authentication module
  - Uses same /etc/passwd syntax traditionally used with NIS
  - Supports netgroups

Network Security on HP-UX 11i

Products and Features

- ✓ HP-UX IPSec
- ✓ HP-UX IPFilter
- ✓ HP-UX Secure Shell
- ✓ Internet Services
- ✓ Directory Enabled Computing
  - Netscape Directory Server
  - OpenLDAP *(Internet Express)*
  - LDAP-UX

Tools

- **LDAP SDK**
- OpenSSL
- GSS-API
- SNORT *(Internet Express)*
- Ethereal *(Internet Express)*
- Nessus *(Internet Express)*

LDAP C-SDK

The HP LDAP C SDK is a Software Development Kit that contains a set of LDAP Application Programming Interfaces (API) to allow you to build LDAP-enabled clients

- Bundled with LDAP-UX 3.2 and later
- Based on Netscape LDAP C SDK Version 5.10
- Closely follows the interface outlined in RFC 2251
- Supports SSL interfaces

Network Security on HP-UX 11i

Products and Features

- ✓ HP-UX IPSec
- ✓ HP-UX IPFilter
- ✓ HP-UX Secure Shell
- ✓ Internet Services
- ✓ Directory Enabled Computing
  - Netscape Directory Server
  - OpenLDAP *(Internet Express)*
  - LDAP-UX

Tools

- ✓ LDAP SDK
- **OpenSSL**
- GSS-API
- SNORT *(Internet Express)*
- Ethereal *(Internet Express)*
- Nessus *(Internet Express)*

OpenSSL

What is SSL?

Secure Socket Layer (SSL) is a network protocol that allows applications to securely transmit data over the network.

In addition to privacy SSL can (using certificates, public and private keys) provide authentication.

What is OpenSSL?

OpenSSL is a cryptography toolkit implementing the **Secure Sockets Layer** (SSL v2/v3) and **Transport Layer Security** (TLS v1) network protocols and related required cryptography standards. This **Open Source** toolkit **is licensed** under the Apache-style licence

OpenSSL on HP-UX

- OpenSSL has been removed from Internet Express and available as a standalone, fully supported, product on 11i v1 and v2
- Future HP-UX SSL enabled products will use this version of OpenSSL negating the need to update multiple products for a single OpenSSL fix
- Unsupported/Disabled Features:
  - Hardware accelerator
  - RC5 crypto
  - IDEA crypto

Network Security on HP-UX 11i

Products and Features

- ✓ HP-UX IPSec
- ✓ HP-UX IPFilter
- ✓ HP-UX Secure Shell
- ✓ Internet Services
- ✓ Directory Enabled Computing
  - Netscape Directory Server
  - OpenLDAP *(Internet Express)*
  - LDAP-UX

Tools

- ✓ LDAP SDK
- ✓ OpenSSL
- **GSS-API**
- SNORT *(Internet Express)*
- Ethereal *(Internet Express)*
- Nessus *(Internet Express)*

Generic Security Service API (GSSAPI)

- Allows programmers to write security related code without having to understand the underlying technology
- GSSAPI provides the framework for the security service, not the actual security service (similar to PAM)
- Applications pass Tokens to establish a security context between peers

Generic Security Service API (GSSAPI)

- GSSAPI is independent of the underlying Transport (TCP, UDP,SCTP, etc.)
- GSSAPI does NOT define the protocol used to pass data between endpoints:
  - FTP AUTH GSSAPI/ADAT <Token>
- Along with Authentication GSSAPI provides:
  - **Message Integrity:** Guarantee the data has not been corrupted
  - **Confidentiality:** Encrypt the data being passed between the sender and receiver (if the underlying mechanism supports it)

Network Security on HP-UX 11i

Products and Features

- ✓ HP-UX IPSec
- ✓ HP-UX IPFilter
- ✓ HP-UX Secure Shell
- ✓ Internet Services
- ✓ Directory Enabled Computing
  - Netscape Directory Server
  - OpenLDAP *(Internet Express)*
  - LDAP-UX

Tools

- ✓ LDAP SDK
- ✓ OpenSSL
- ✓ GSS-API
- SNORT *(Internet Express)*
- Ethereal *(Internet Express)*
- Nessus *(Internet Express)*

Authentication Services on HP-UX 11i

Products and Features

- Authentication on HP-UX
  - Pluggable Authentication Module (PAM)
  - Name Service Switch (NSS)
- HP-UX Kerberos Client and Server
- HP-UX AAA Server
- Shadow Password

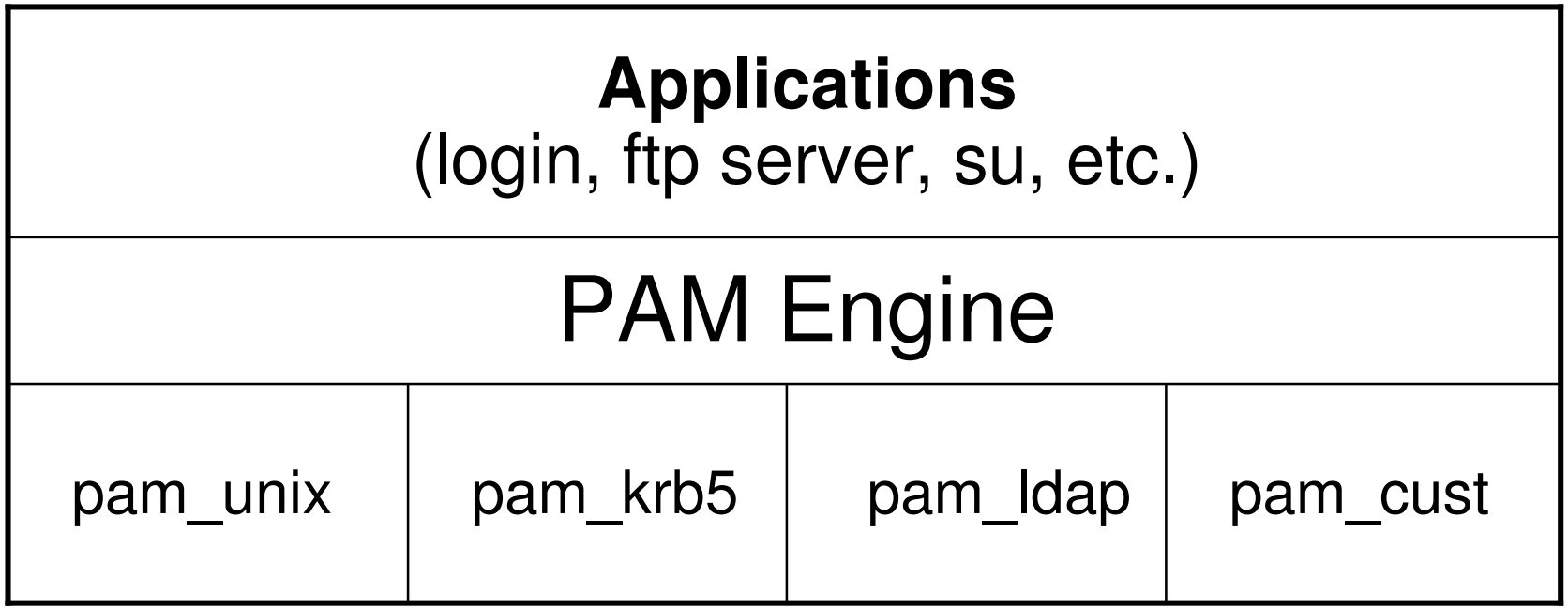
Authentication on HP-UX

- Typical (traditional) authentication on HP-UX requires 2 components that are “loosely” tied together:
  1. Username and Password
  2. A valid “password entry” for the user that includes a uid & gid number, home directory, login shell, etc.
- Authentication is handled through the Plugable Authentication Module (PAM)
- “Password Entry” retrieval is controlled using the Name Service Switch (NSS)

Plugable Authentication Module

- Allows server/service developers to write their authentication code to a standard API
- Allows system administrators to choose which authentication module(s) to authenticate users with
- By “stacking” modules a user can be authenticated by multiple modules

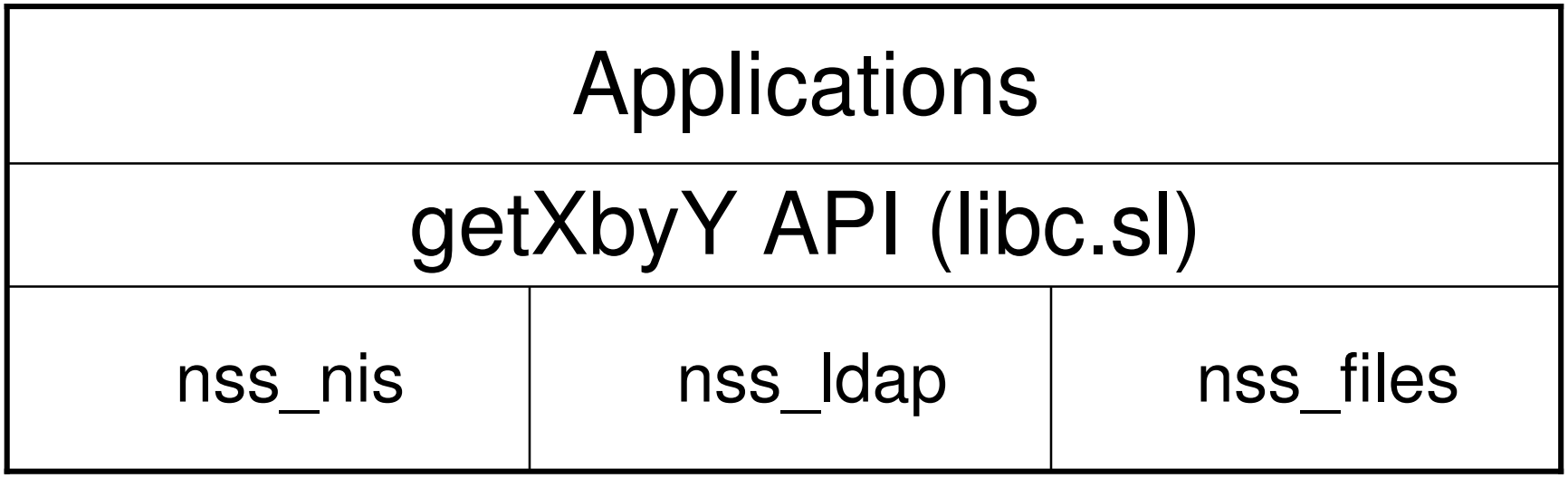
PAM Architecture



Name Service Switch (NSS)

- Used to determine the source from which various system calls will attempt to retrieve data from
- Multiple sources can be configured
- Possible to configure different actions for each status returned from each source

NSS Architecture



Authentication Services on HP-UX 11i

Products and Features

- ✓ Authentication on HP-UX
  - Pluggable Authentication Module (PAM)
  - Name Service Switch (NSS)
- **HP-UX Kerberos Client and Server**
- HP-UX AAA Server
- Shadow Password

Kerberos

Is

- A network authentication protocol
- Uses a trusted 3rd party (KDC) to distribute "tickets"
- Can be used to encrypt data between clients and servers

Is not

- A network authorization protocol
- A repository for user account information

HP Kerberos Client

- Bundled with the Core-OS on 11i v1 (11.11) and later
- Available on the Application CD for 11.0 or bundled with PAM-Kerberos on software.hp.com
- Includes
  - Kerberos client libraries (including Kerberos GSS-API)
  - Kerberos utilities (kinit, klist, etc)
- Required by PAM-Kerberos
- Secure Internet Services (Kerberized telnet, ftp, r-commands) built-in into standard binaries; enabled with “inetsvcs_sec enable” command

HP Kerberos Server

- The Trusted 3rd Party
- Stores User and Server/Service Keys
- Grants Tickets to clients
- Handles remote user/password administration
- Authentication Server (AS) and Ticket Granting Server (TGS) are separate processes (usually run on the same server)

HP Kerberos Server (cont.)

- Open source distributions:
  - MIT (http://web.mit.edu/kerberos/www)
  - Heimdal (http://www.pdc.kth.se/heimdal)
  - Bones (Kerberos Version 4)
- Commercial Distributions:
  - HP Kerberos Server (Free: http://www.software.hp.com)
  - Microsoft Windows 2000 Server – Active Directory
  - Cybersafe TrustBroker (http://www.cybersafe.ltd.uk)

HP Kerberos Server

- Supports RFC 1510 (The Kerberos Network Authentication Service (V5)) specification
- GUI and CLI administration interface
- Multithreaded for high performance
- Support for LDAP backend to store Kerberos principals (new for version 3.1)
- Secondary Servers used for HA
  - Kpropd for C-Tree backend (incremental)
  - Multiple LDAP Servers for LDAP backend
- Version 3.x available on 11i v2 (11.23)
- Version 2.1 available on 11.0 and 11i v1 (11.11)

Configuring HP Kerberos Server

- krbsetup tool
  - Configure Server
  - Remove Server
  - Start/Stop Server
- kadmin/kadminl
  - Command line tool to manage principal database
  - Can be scripted
- kadmin_ui/kadminl_ui
  - Graphical tool to manage principal database

Authentication Services on HP-UX 11i

Products and Features

- ✓ Authentication on HP-UX
  - Pluggable Authentication Module (PAM)
  - Name Service Switch (NSS)
- ✓ HP-UX Kerberos Client and Server
- **HP-UX AAA Server**
- Shadow Password

HP AAA (Authentication Authorization & Acounting)

HP-UX AAA Server (RADIUS) for

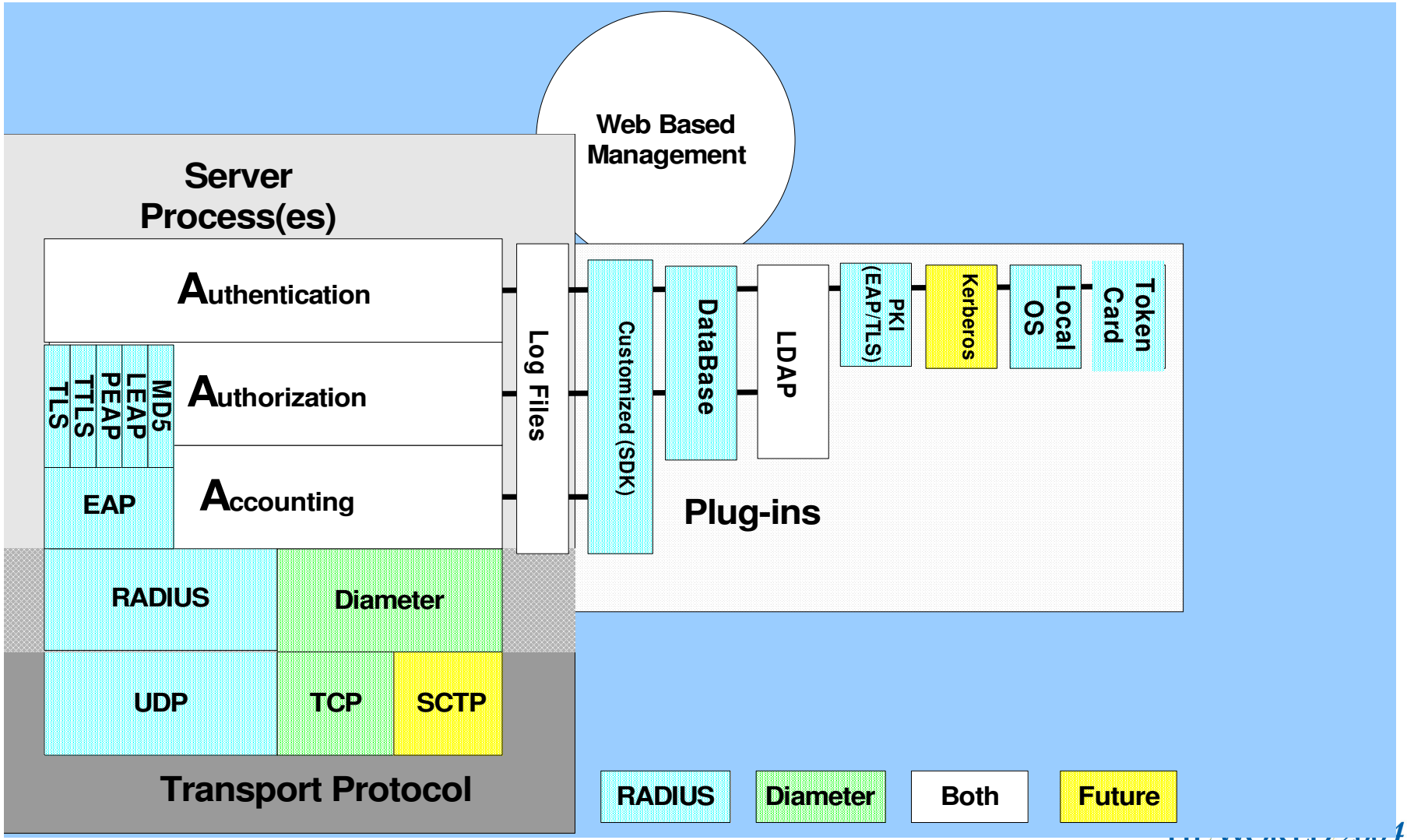
- Wireless and wired LAN Security (hot spot/hot zone, enterprise)
- Securing enterprise remote access (VPN)
- Carrier grade service providers (ISP/Telecom)
- Interoperability with existing devices and applications
- Typical Markets:
  - Telecom
  - Enterprise
  - Service Providers
- Emerging Environments:
  - WLAN/Mobile convergence
  - Integrated Enterprise security (Network access & existing authentication services)

HP AAA (Authentication Authorization & Acounting)

HP-UX Mobile AAA Server (Diameter) for

- Standards based support of future AAA functionality
- Features to support new usage/revenue models.
- Mobile IP
- Typical Markets:
  - Telecom
  - Service Providers
- Emerging Environments:
  - Mobile IP Billing
  - Customer Care/Billing

Architecture: RADIUS & Diameter Server Products



RADIUS Server Features

- Scalability/Availability
  - LDAP (directory) and Oracle external data stores
  - Integrate with existing directories/data bases
  - Load balance/failover with external data stores
  - Tested into millions of users
  - Industry leading performance (1000 trans/sec)
  - SNMP Support
  - DHCP Interface for IP address assignment
- Flexibility
  - Plug-in architecture allows customized authentication and authorization processes
  - SDK for developing proprietary plug-ins
  - Configurable policy engine/state machine to further customize behaviors (e.g. time of day restrictions)
  - Configurable vendor specific attributes
  - Supports both Livingston and Merit accounting log formats

RADIUS Server Features (Cont)

- Manageability
  - Web based secure (https) management console can manage multiple AAA servers and view logs ands statistics
  - SNMP support
  - Session management (concurrent access control)
  - Command line utilities
- 802.1x Features
  - EAP/MD5 (Wired LAN security)
  - LEAP (Cisco interoperability)
  - EAP/TLS (PKI interoperability)
  - EAP/TTLS (secure password – integrate with other services)
  - PEAP (Microsoft interoperability)
- Non 802.1x Features
  - PAP, CHAP

Authentication Services on HP-UX 11i

Products and Features

- ✓ Authentication on HP-UX
  - Pluggable Authentication Module (PAM)
  - Name Service Switch (NSS)
- ✓ HP-UX Kerberos Client and Server
- ✓ HP-UX AAA Server
- **Shadow Password**

Shadow Password

- De-facto standard to provide a secure local password storage and password policy
- Allows the password field of a user entry in /etc/passwd to be hidden from non-privileged users
  - Encrypted password is replaced by ‘x’ in /etc/passwd and stored in the root only readable file /etc/shadow
- Implements password aging policy for users stored in local /etc/passwd file
  - Defaults defined in /etc/default/security file
  - Policy parameters:
    - **PASSWORD_MAXDAYS** - maximum number of days that passwords are valid
    - **PASSWORD_MINDAYS** - minimum number of days before a password can be changed
    - **PASSWORD_WARNDAYS** - number of days before password expiration that a user is to be warned that the password must be changed

Shadow Password

- Encrypted passwords and password aging policy information stored in /etc/shadow file, readable by root only
- Format of shadow entry:
  <login name>:<encrypted password>:<last changed>:
  <min>:<max>:<warn>:<inactivity>:<expiration>:<reserved>
- Shadow Password fields are accessed using the getspent(3c) API

Shadow Password Installation and Configuration

- Shadow Password is available on 11i v1, v1.6, v2 (11.11/22/23)
- Part of the standard OS for 11i v1.6 & v2
- Bundle of patches for 11i v1, downloadable from software.hp.com:
  http://www.software.hp.com/ISS_products_list.html
- By default Shadow is NOT configured
- Enabling Shadow on a Standard Mode System is done using the pwconv tool (run pwchk FIRST)
- Disabling Shadow on a Standard Mode System is done using the pwunconv tool
- Trusted Systems can not be converted to Shadow directly, must be un-Trusted first

Shadow != Trusted Systems

Shadow

Is

- Password Hiding
- Password Aging Policy
- Support LDAP-UX co-existence
- De-facto standard compliant

Is NOT

- Support all Trusted Systems features, such as auditing, password history, etc.
- C2 Level Certified
- Completely binary compatible with applications that don't use PAM for authentication
  - Encrypted passwords in /etc/shadow are readable only by root
  - Encrypted passwords are not returned in getpwent() API's

Authentication Services on HP-UX 11i

Products and Features

- ✓ Authentication on HP-UX
  - Pluggable Authentication Module (PAM)
  - Name Service Switch (NSS)
- ✓ HP-UX Kerberos Client and Server
- ✓ HP-UX AAA Server
- ✓ Shadow Password

HP Internet Express for HP-UX 11i

- A collection of over 50+ popular open source Internet, Web, and Security services tested and qualified on HP-UX
- Many components included a Webmin module for use with the Webmin (Included with the HP Webserver Suite)
- Internet Express media is included in hp-ux OE Media Kit and http://software.hp.com
- Support model:
  - Components in HP-UX 11i OE are fully supported.
  - Components in the Internet Express media are unsupported. However, HP will report the defects to the open source community and incorporate the appropriate defect repairs for each new release.

HP Internet Express for HP-UX 11i

Security related products and tools

- **Snort –** Network Intrusion Detection
- **OpenLDAP –** LDAP Server
- **SUDO –** Restricted “Super User”
- **Ethereal**/TCPdump/libpcap **–** Network packet capture
- DanteSOCKS – SOCKS Server
- **Stunnel** – SSL tunneling
- **Nessus** – Remote Security Scanner
- CyrusIMAP – IMAP Server
- CyrusSASL – Simple Authentication and Security Layer (SASL)
- Xinetd – Inetd replacement

SNORT

- Network Intrusion Detection System & packet capture tool
- Realtime capture and analysis of IP networks using:
  - protocol analysis
  - content searching/matching
- Detects
  - buffer overflows attempts
  - stealth port scans
  - CGI attacks
  - SMB probes
  - OS fingerprinting attempts
- 3 modes of operation
  - packet sniffer
  - packet logger
  - full blown network intrusion detection system

SNORT

- Rules are being generated and posted as attacks and vulnerabilities are discovered
- Most up-to-date contributed rules can be found at: http://www.snort.org/dl/rules/
- Currently 2376 rules have been contributed
- Custom rules can be generated easily:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP MyFile";
flow:to_server,established; content:“MyFile"; reference:arachnids,328;
classtype:suspicious-filename-detect; sid:335;  rev:4;)
```

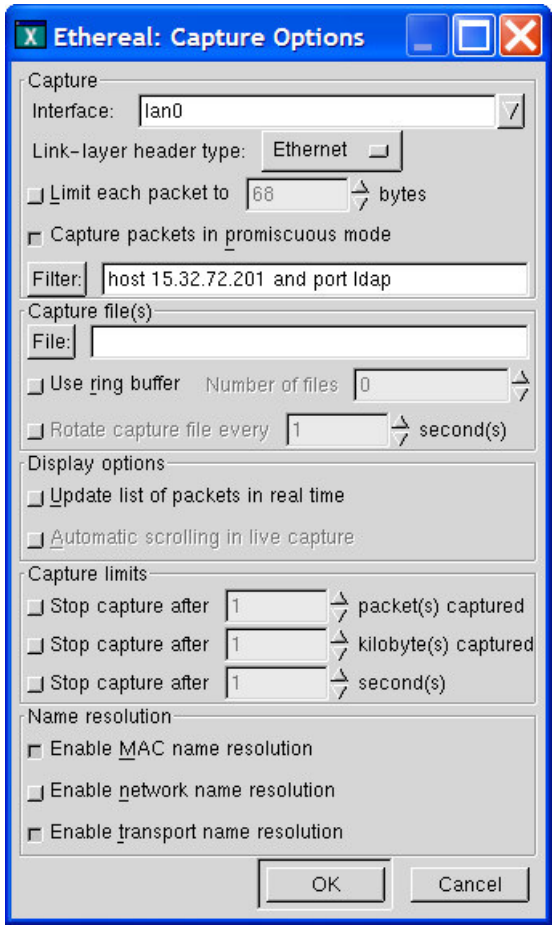
Ethereal

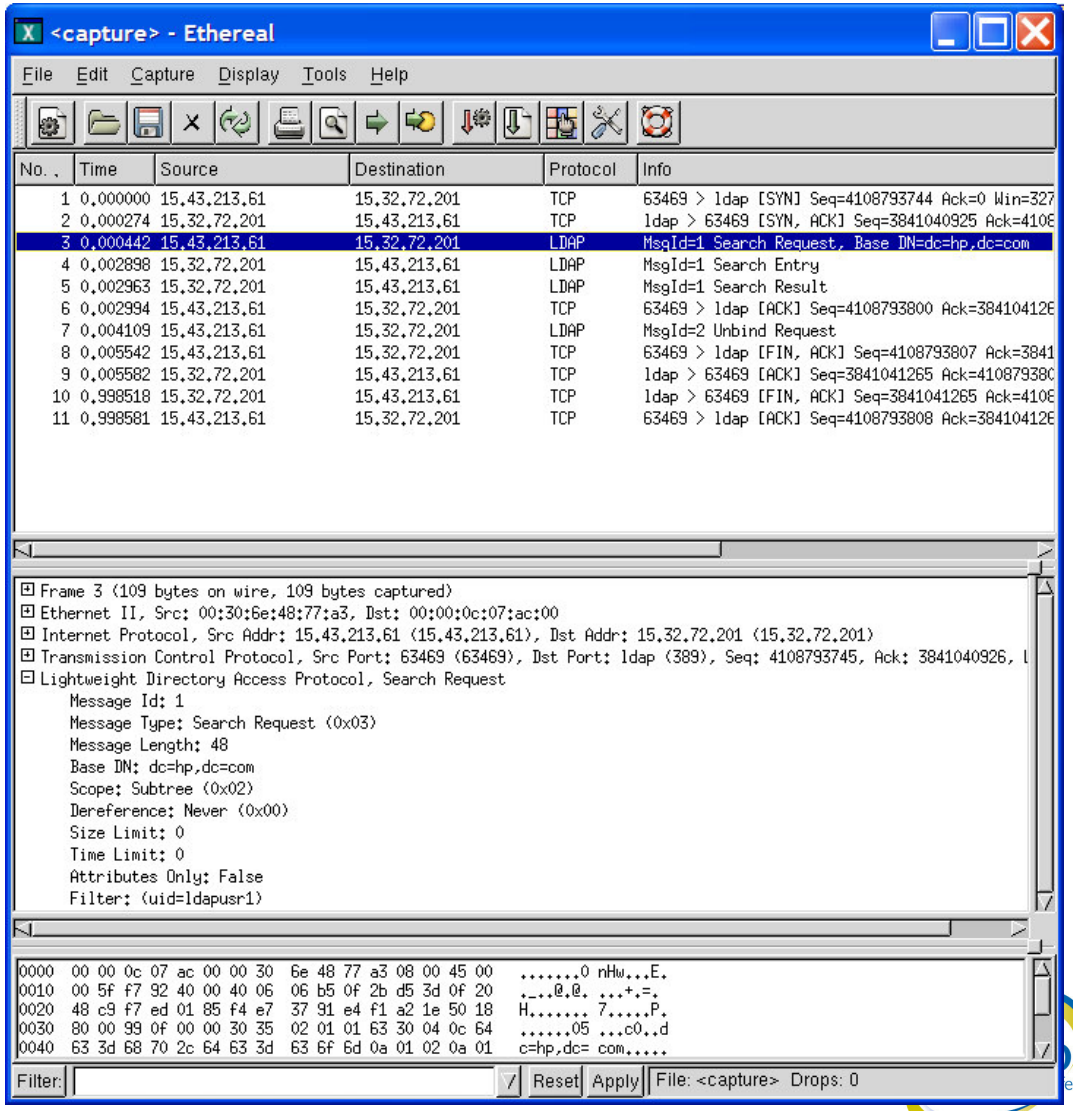
- Packet Sniffer and Viewer
- Available on many different OS's
- Able to read many different trace formats:
  - nettl (HP-UX)
  - tcpdump
  - iptrace (AIX)
  - LANalyzer
  - snoop (Solaris)
  - etc.
- Can save/export traces to many different formats:
  - tcpdump
  - netmon (Windows)
  - etc.

Ethereal

- Filter packets during capture or display
- Protocol decoders for many protocols
  - LDAP
  - Kerberos
  - FTP
  - Ethernet
  - ICQ
  - more…

Ethereal Example





SUDO

- Allows the administrator to give users or groups the ability to run commands as root
- Verbose logging provides detailed audit trail
- Elevated privileges are granted on a command by command basis
- Configuration file can be used across multiple systems granting different privileges for each system

SUDO - Example

```
$ grep admin /opt/iexpress/sudo/etc/sudoers
admin1    hpatcux4=/usr/sbin/useradd

$ sudo /usr/sbin/useradd newuser1

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these two things:

    #1) Respect the privacy of others.
    #2) Think before you type.

System Password:
$ id newuser1
uid=125(newuser1) gid=20(users)
```

SUDO - Example

```
$ date
Wed Apr 28 16:50:10 PDT 2004
$ sudo /usr/sbin/useradd newuser2
$ id newuser2
uid=126(newuser2) gid=20(users)
$ date
Wed Apr 28 16:55:20 PDT 2004
$ sudo /usr/sbin/useradd newuser3
System Password:
$ id newuser3
uid=127(newuser3) gid=20(users)
```

No password required

Password required

Stunnel

- Used as an SSL wrapper for applications that do not support SSL
- Supports TCP only
- Can be used when only the server application supports SSL
- Can execute program (inetd style) on connection
- Compiled with OpenSSL

Stunnel Example

- Start 2 Stunnel process, one on the client & one on the server
- Client TCP application connects to the local stunnel port
- Local stunnel process creates an SSL tunnel to the remote stunnel process
- Remote stunnel process connects to the Server TCP application and passes client data

Stunnel Example

Client stunnel configuration:
# cat /tmp/stunnel.conf.client
pid = /tmp/stunnel.pid.client
client = yes
RNDfile = /tmp/rand.file
[example]
accept = stunnel-example-local
connect = hpatcux5.rose.hp.com:stunnel-example-remote

Start stunnel process (it will go into the background)

/opt/iexpress/stunnel/sbin/stunnel /tmp/stunnel.conf.client

ps -ef | grep stunnel
root 23576   1 0 09:16:29 ?   0:00 /opt/iexpress/stunnel/sbin/stunnel
/tmp/stunnel.conf.client

Stunnel Example

Server stunnel configuration:

```
# cat /tmp/stunnel.conf.srv
pid = /tmp/stunnel.pid.srv
CApath = /certs
CAfile = /opt/iexpress/stunnel/etc/stunnel/stunnel.pem
RNDfile = /tmp/rand.file

[example]
accept  = stunnel-example-remote
connect = example
```

Start stunnel process (it will go into the background)

```
# /opt/iexpress/stunnel/sbin/stunnel /tmp/stunnel.conf.srv
# ps -ef | grep stunnel
    root  9569     1  0 09:13:20 ?      0:00 /opt/iexpress/stunnel/sbin/stunnel
/tmp/stunnel.conf.srv
```

Stunnel Example

```
# grep example /etc/services
example                    9876/tcp
stunnel-example-local      9877/tcp
stunnel-example-remote     9878/tcp

# ./client.tcp localhost 9877
Using port: 9877
Connected to localhost on port 64842 at Thu Apr 29 09:32:31 2004
Received result number 1
Received result number 2
Received result number 3
Received result number 4
Received result number 5
All done at Thu Apr 29 09:32:41 2004
```

Server Log's:

Startup from **localhost** port 63336 at Thu Apr 29 09:29:13 2004
Completed **localhost** port 63336, 5 requests, at Thu Apr 29 09:29:23 2004

OpenLDAP

- LDAP Directory Server
- Standard Directory Server on Linux
- Multiple Backend support
- LDAP client applications
- LDAP libraries (C-SDK)
- No Configuration GUI
- No Online Schema updates
- Support for NS-SLAPI plugins
- SASL Authentication (including GSSAPI)
- SSL/TLS Support (OpenSSL)

Nessus

- Open source network scanner
- Used to audit/scan remote systems for known security vulnerabilities
- Client/Server model
- “Plugins” for new vulnerabilities are being developed/contributed on a regular basis: http://www.nessus.org/scripts.php
- Easy to use scripting language NASL *(Nessus Attack Scripting Language)*

More..

Session #3749 (Mon 3:45pm):
Ethereal: Analysis on a Budget

Developing a Security Solution

- Will vary from environment to environment
  - Understand what you want/need to secure
  - Look at what you should secure
- Start with a solid foundation!
- Identity Management
- Authentication
  - What technology should be used for authentication?
- Authorization
  - Do you know who has access to what?
- Verify and Audit it!!!

What do you want?

- Many needs are because of regulation requirements
  - What regulations must you abide by, and what do they mean for HP-UX security?
- Do you have a security policy, if not that's where to start
- What do you want to secure?
  - Network
  - Login's?
  - Audit?
- What should you secure
  - Remember 70% of attacks are from inside

Start with a Solid Base

- A Security policy must be in place
- All Enterprise systems need some level of security
- Any service not needed should be disabled
  - Run Bastille!
  - Use Install Time Security to build a secure system out of the box
- Keep current on security patches
  - Run Security Patch Check on a regular basis
  - READ and ACT on the reports

Start with a Solid Base

- Use SSH
  - Passwords and **data** are sent over the clear with traditional applications like ftp, telnet, etc.
- Use Shadow Password or Trusted Systems to deter “password crackers”

Secure the Network

- Do you consider your internal networks secure. Really?
- IPSec can be used to secure internal traffic between critical systems (i.e. HR and Finance)
- Ipfilter is a good way to restrict access from systems that should not be used to access the secure system (Internal, External or DMZ)
- Ipfilter DCA can be used to protect Internet facing services for DOS attacks
- Consider wireless access as if it were external
  - Use AAA Server to authenticate wireless or open hardwired ports
- Network Switches don't always stop snooping:
  - http://archive.infoworld.com/articles/op/xml/00/05/29/000529opswatch.xml

Identity Management

- How is user provisioning going to be done?
- Do you already have a centralized repository for user's and groups?
- LDAP Directory servers are good place for user repositories
  - Centralized management
  - Centralized password polices
  - More and more applications/OS's are LDAP aware, but not all
- HP's Trulogica/Select Access

Authentication

- What type of authentication should be used for non-local accounts?
  - LDAP
  - Kerberos
  - Standard Unix
- What technologies do existing applications and/or other operating systems support
- Use Shadow Password or Trusted Systems for auditing and stronger local password policy

Authentication

- Kerberos can be used as the basis for a Single Sign On environment, need additional repository for user information
- Kerberos/LDAP combination
  - HP-UX Kerberos Server v3.1 (new)
  - Microsoft Active Directory
- LDAP with SSL for LDAP only environments
- Avoid NIS+
  - Discontinued
  - LDAP-UX 3.3 supports Trusted Systems co-existence
- Enforce password policies

Authorization

- Restrict network access to the system
  - IPFilter
  - TCP Wrappers
  - PAM_AUTHZ
  - LDAP Search filters
  - WUFTP
- Restrict root privileges
  - Restricted SAM
  - SUDO
  - Service Control Manager

Auditing

- HP-UX HIDS to detect system breaches
- Trusted Systems Audit capabilities
- Enable inetd logging
- Snort for NIDS
- Use Nessus to periodically verify your security strength

More..

Session #3626 (Wed 8am):
SIG Security

Session #3809 (Today 4pm):
Meet the Technology Planners

Session #3892 (Mon 3:45pm):
Basic Security for HP-UX System Administrators

More Information

Documentation

HP-UX 11i Security:

http://www.hp.com/products1/unix/operating/security/index.html
http://www.net-security.org/article.php?id=52

http://docs.hp.com/hpux/onlinedocs/os/11i/59807127en.pdf

Internet and Security:

http://www.docs.hp.com/hpux/internet/index.html

HP-UX 11i

http://www.docs.hp.com/hpux/os/11i/index.html

Internet Express

http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXIEXP1123

More…

Session #3180 (Mon 9:30am):

Maintaining HP-UX System Security

Session #3202 (Wed 4pm):

Integrating HP-UX Authentication with Windows 2000 Active Directory

Questions?

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