



Everything you've always wanted to know about NonStop Security

Presented to CTUG, November 2003

Ron LaPedis, CBCP, CISSP
Product Manager, Continuity and Security

Parts of this presentation from Steven
Moriarty, NonStop Security Program Office



Agenda



- NonStop Enterprise Division security view, vision & directions
- What's hot in NonStop security?
- Security best practices
- Safeguard Security for OSS



NonStop Enterprise Division Security View, Vision & Directions



- View: what is enterprise security?
 - A customer view
 - NonStop Enterprise Division's view (HP's, too)
- Vision: where do we need to get
 - A logical model for enterprise security
- Direction: how we're going to get there
 - NED components
 - HP components
 - Partner components

***This is not a best-practices presentation!
This is also not a product pitch!***

A Suggested View of Enterprise Security



Environments

- Network
- Platform
- Application
- Data



Process

- Identity Management
- Security Management
- Secure Software Process
- Software vulnerability response
- Secure software delivery

Infrastructure

- Crypto services
- Authorizations Services
- Authentication Services
- Audit

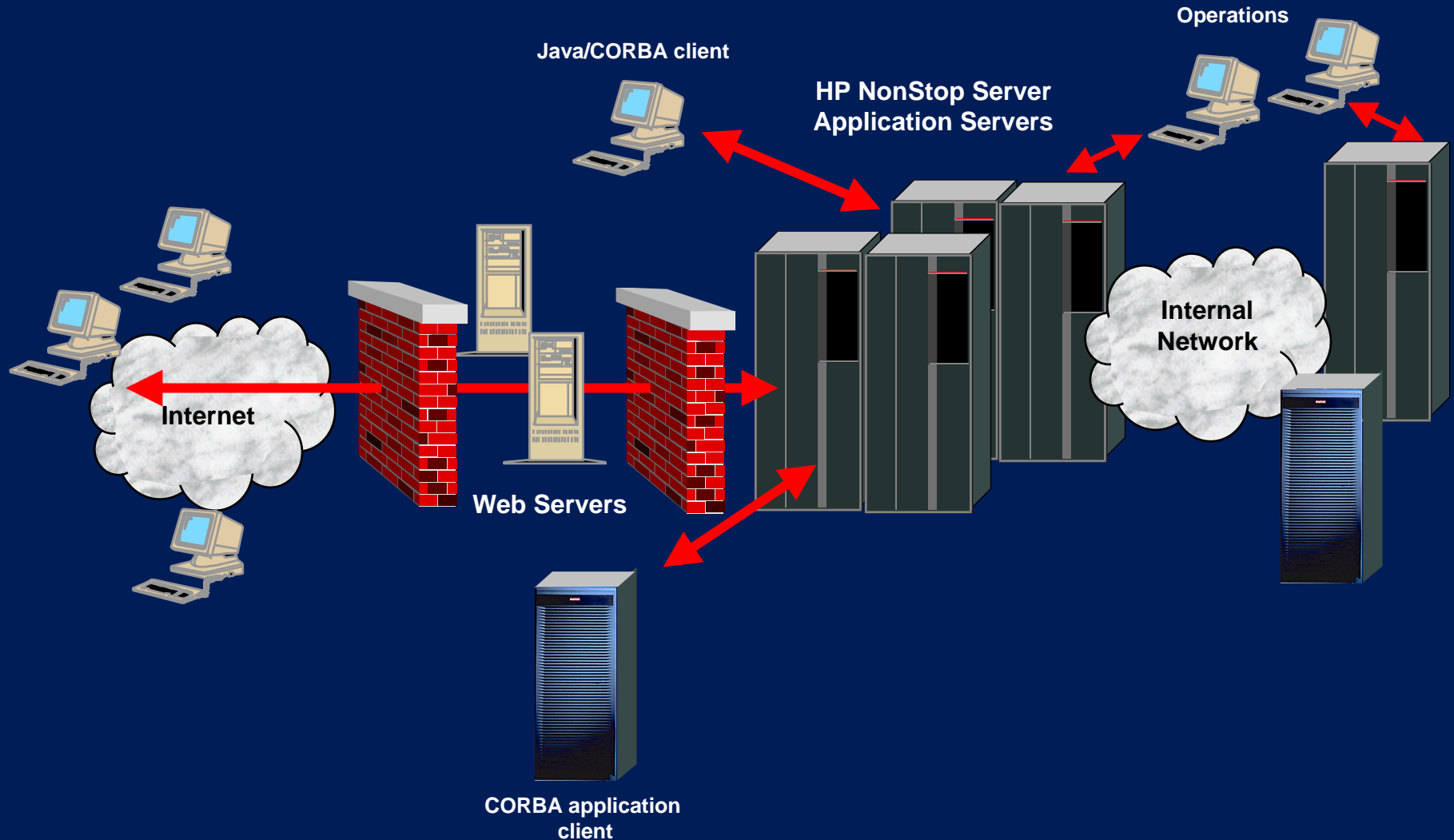
50,000 Foot View of Security



- Terms “Management” hears associated with security
 - network/perimeter security
 - identity management
 - federation/delegation
 - application security
 - single sign-on

Network, Operations, Application Security

Network Security - many access points to secure



Operations Security Environments



- Local,
- Remote,
- Enterprise,
 - Multi-tier (delegation)
 - Multi-owner (federation)

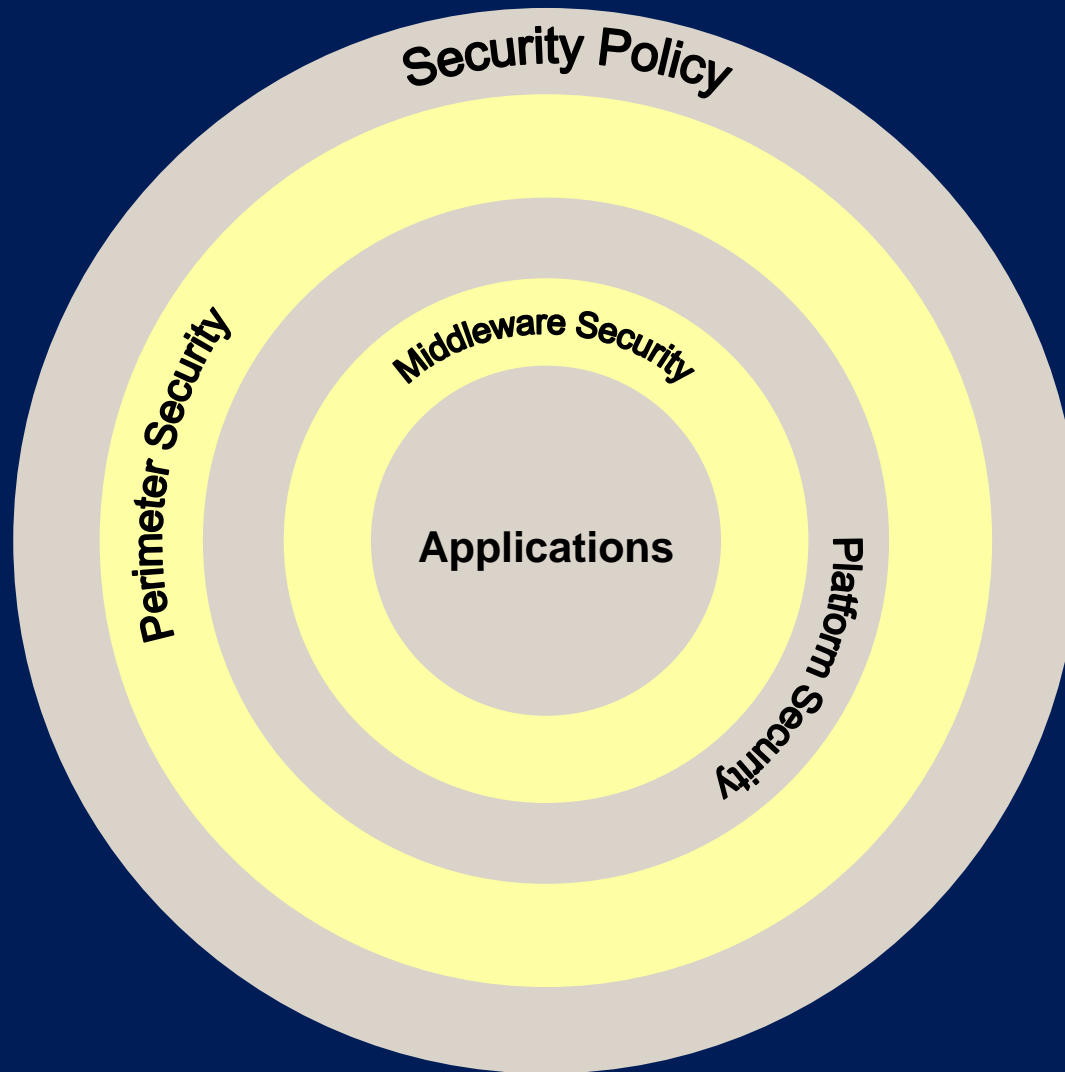
- As environments get more complicated, the interdependency of the components get more complex
 - For example: where and when does your LDAP server run?
 - Answers aren't always obvious

Application Environments

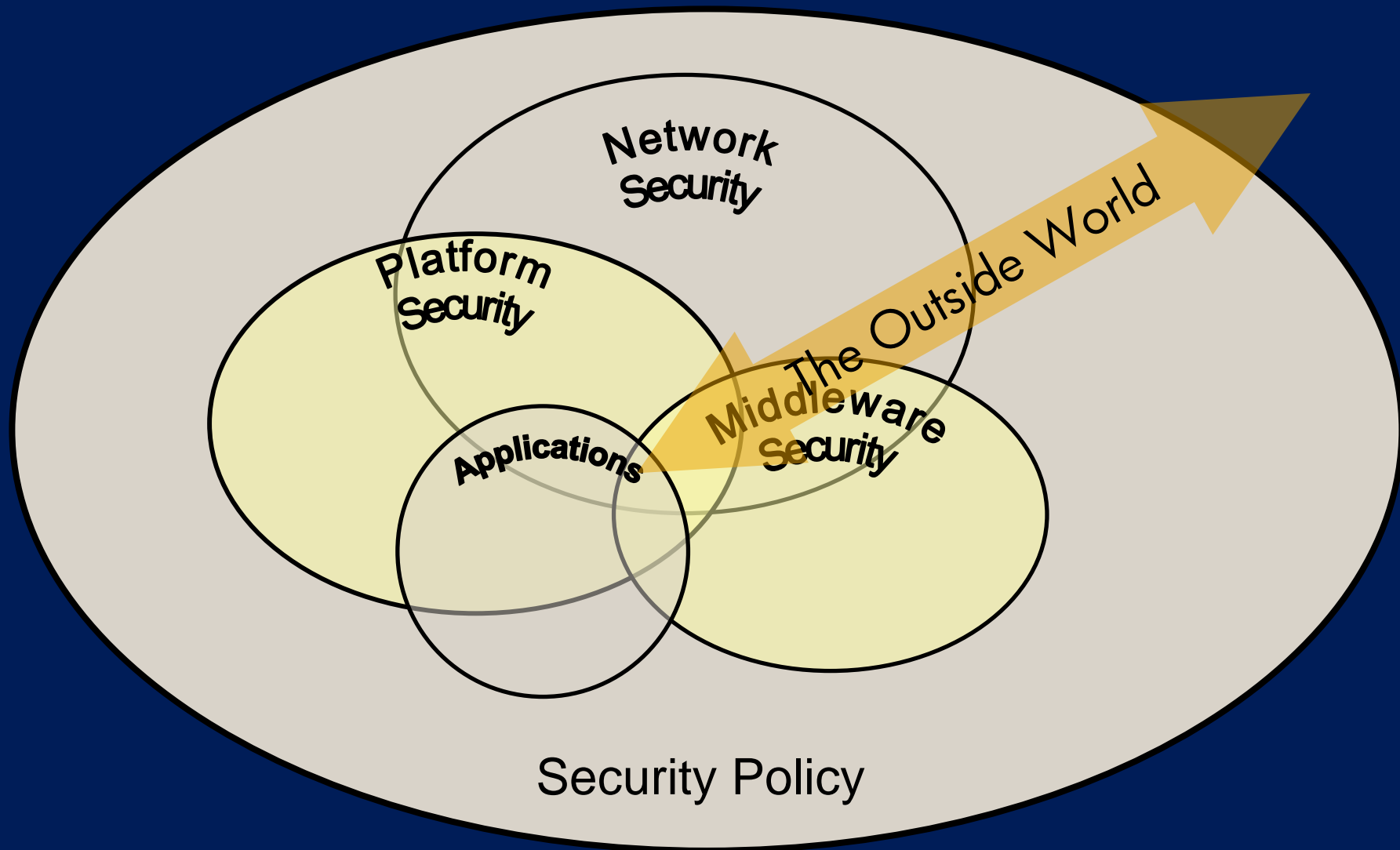


- Major Application Environments have their own requirements/approaches & need to share some common infrastructure
- Web-services apps
- B-2-B
- Distributed legacy apps
 - e.g., Pathway, C/C++, TAL
- Middleware-based apps
 - Tuxedo, CORBA, J2EE, MOM (e.g.. MQSeries, Tibco, SeeBeyond ...)

Conceptual Model of Security



The Real World



Vision – Where we want to go



- Customer security evaluation service
- Enhanced communications security
- Comprehensive Identity Management solution
- Integrated Application Services security
- Integrated security management
- Secure software distribution
- Enhanced data security
- Certification

Customer Security Evaluation Service



- Have to understand the business needs for security in your enterprise
- Like any other project, you can't succeed unless you can measure – need formal security evaluation
 - HP currently offers NonStop-related security evaluation service
 - http://www.hp.com/hps/security/sc_readiness.htmlSecurity
 - Partners also offer security evaluation services
 - <http://hp.com/go/nonstopsecurity> -> select Safeguard
- The “missing ingredient” is people.

Enhanced Communications Security



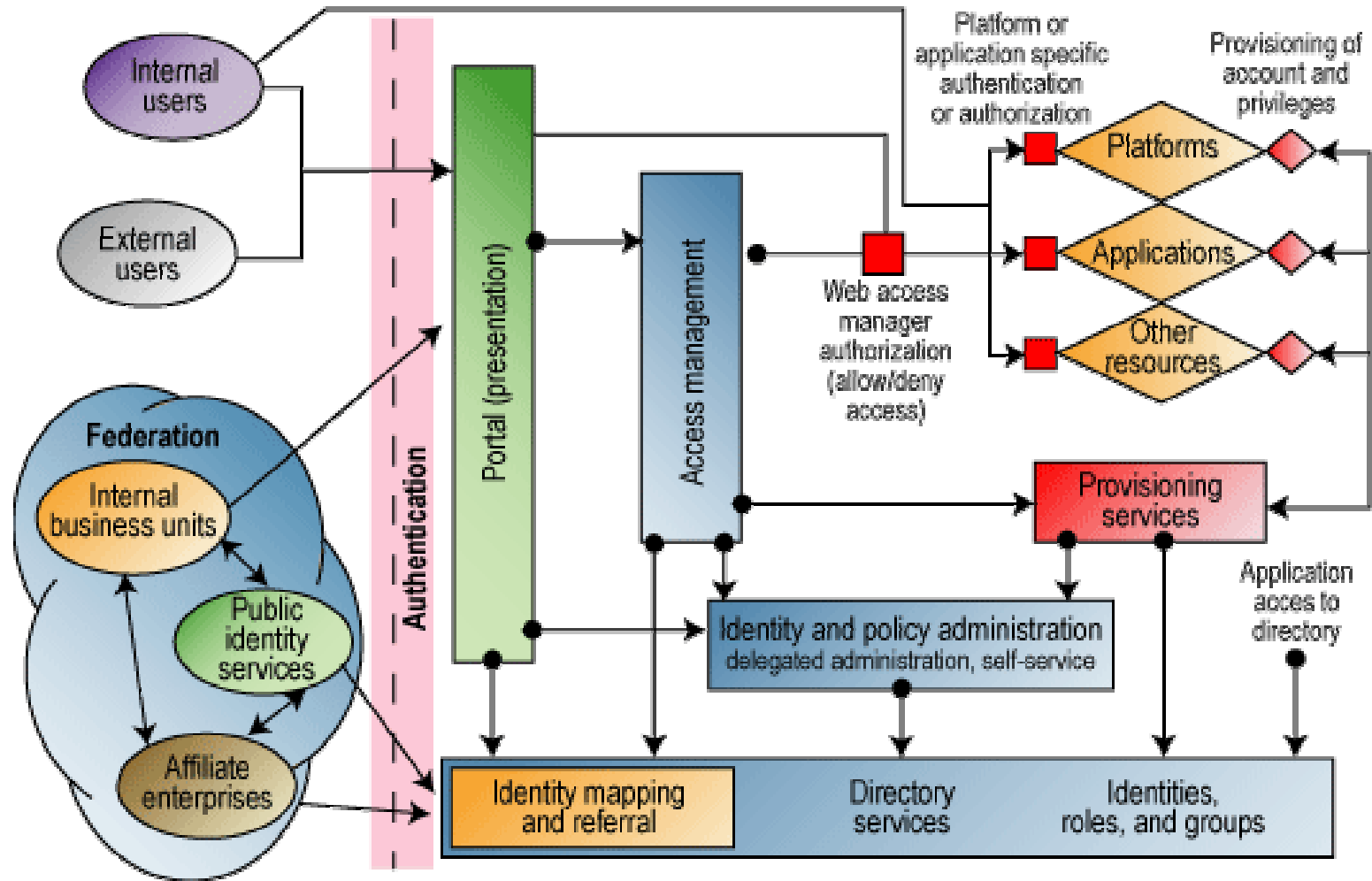
- Includes network security, authentication of participants and privacy
- Network security (perimeter security) generally implemented in routers, firewalls, etc.
- SSL provides authentication and link-level privacy
- IPSec provides transparent end-to-end application level security

Identity Management



- Managing secure access to information and applications scattered across a wide range of internal and external computing systems.
- Providing access to a growing number of users, both inside and outside the corporation, without diminishing security or exposing sensitive information.
- The management of multiple versions of user identities across multiple applications makes the task even more daunting
- Major components
 - Password reset
 - Password synchronization
 - Single sign-on
 - Access management

Identity Management: Burton Group Reference Template



Application Services Security



- Major Application Environments have their own characteristics and need to share some common infrastructure
 - Span multiple platforms and technologies
 - Middleware
 - WLS, Tuxedo, CORBA, ACS, etc.
 - Web Services (emerging)
 - Security must be integrated
 - Component distribution must be secure

We are looking at vehicles for management integration

Integrated Security Management



- Managing the security of your components is complex
 - Application environments have their own security management pieces
 - Perimeter security environments have their own management pieces
 - Different individuals (or groups) manage different parts of the environments
- Our vision says that it will be necessary to integrate the management of security
 - To insure that policy is enforced
 - To insure that there is a consistent record

Secure Software Distribution



- How do you know you're running the right software
 - In the operating system?
 - In your middleware?
 - In your applications?
- Software configuration management
- Software Updates
 - How do you know when to update?
 - How do you know you got the right thing?

Enhanced data security



- Enhanced data access controls
- Encryption of fields, files, drives
 - Will be driven by legislation
 - HIPAA, CA SB1386, etc.

We are evaluating hardware crypto support for future platforms

- Certification ties together many issues mentioned in previous slides
- We need to be able to assure customers that all components work together as advertised
 - Generally involves independent evaluation against standards
- Harder than it looks
 - Which standard?
 - Likely to be Common Criteria
 - How important is it to you?
 - Near term – long term?
 - How often?
 - What's it worth to you? What's it worth to us?

What's going on?

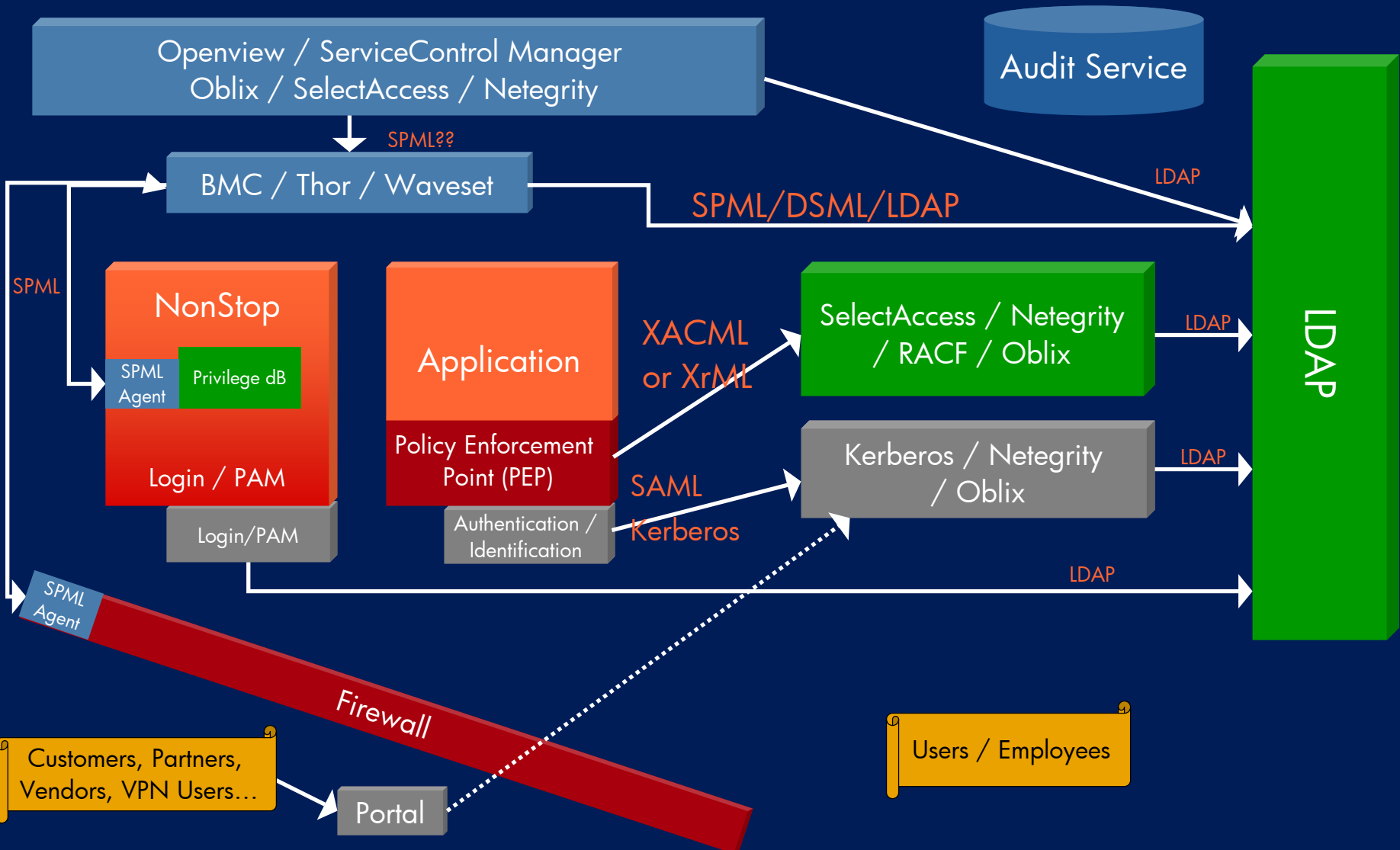
- SSL
 - Partners supply software solutions
 - Off-platform hardware solutions can enhance performance and provide key management capabilities
 - Project to evaluate some alternatives and publish results under consideration
- IPSec
 - Integral component of IPv6 standard
 - Hardware approach for higher performance
- Hardware support
 - HP makes routers, firewalls . . .

Operations Security



- Continuing to enhance Safeguard
 - ITUG RFEs
 - Infrastructure changes including support for ISC
- Continuing to enhance security for OSS
 - ACLs
 - Better conformance to UNIX security commands
- OpenView
- OSM

Identity Management: Possible HP Enterprise Architecture



Middleware security functionality



- Tuxedo
 - Access Control Lists for apps, queues & events, user-level or group-level authorization, Link Level Encryption, Tuxedo domains mutual authentication, single sign-on with WebLogic Server
- WLS
 - Release 8.1 includes JAAS, JCE, JSEE
- CORBA
 - Rel 2.6 (interceptors, IIOP/SSL - due 12/03)
 - C20 (CSIv2 - distributed authorization & authentication, 3rd party interfaces)
- MQSeries
 - Release 5.3 implements SSL (negotiating for implementation)

Secure Software Distribution



- Tripwire
- Fingerprints
- Reporting
- NED end-to-end software distribution
 - Currently holding focus groups, showing prototypes

NonStop Security partners

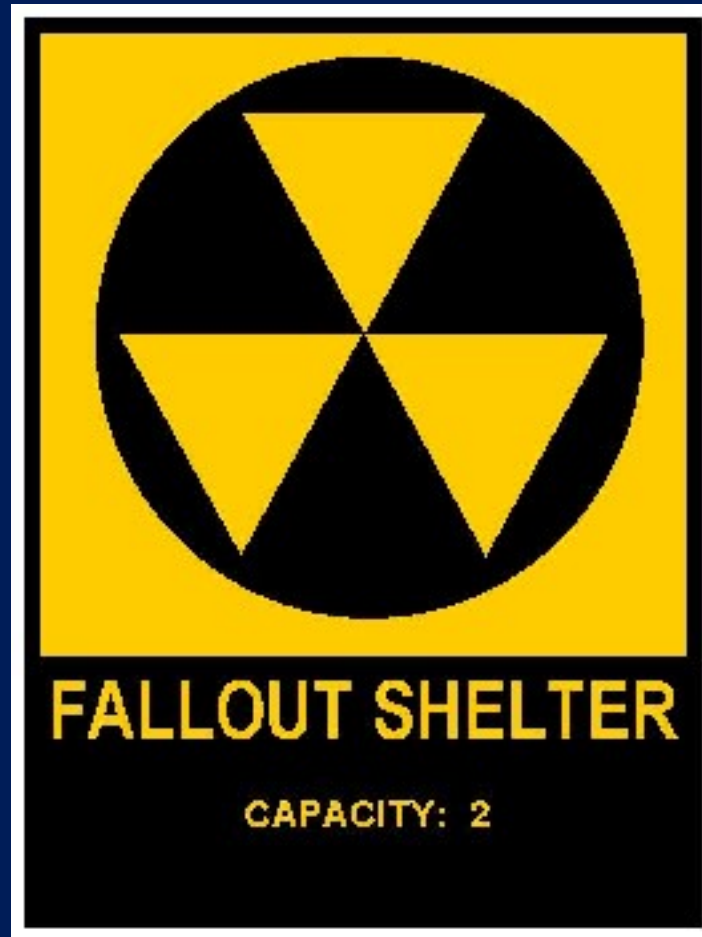
- Baker Street Software www.bakerstreetsoftware.com
- Bowden Systems www.bsi2.com
- CAIL www.cail.com
- Computer Associates www.ca.com
- comForte www.comforte.com
- CSP www.CSPsecurity.com
- Cross-EL www.crossel.com
- GreenHouse www.greenhouse.de
- Gresham Enterprise Software www.gresham-software.com
- Insession Technologies www.insession.com
- SIONET International www.sionet-intl.com
- Unlimited Software Assoc. www.usahero.com
- XYPRO www.xypro.com

To sum up...



- Security is way more complicated than any of us tend to think it is – and it is getting more so every day
- Security policy has to support your business goals
- It isn't all hardware and software: PEOPLE MAKE SECURITY WORK (or fail)
- NED is actively working with the rest of HP to insure that at least everyone knows what everyone else is doing

What's hot in NonStop security?



Standalone Security Event Exit Process (SEEP)



- A reminder – The standalone SEEP (product ID T8949) is no longer present on the SUT as of NonStop Kernel operating system Release Version Update (RVU) G06.19 (March 2003).
- Any customer using features included in T8949 must license Safeguard software (product T9750) which has all of the functionality and more that was in T8949.

- Major thrust will be responding to ITUG Security SIG 6 RFEs regarding Safeguard functionality. Current work is for:
 - support for wild card ACLs
 - warnings enabled at ACL level
 - allow ACLs to use EXPAND node names
 - allow creation of disk file ACL for non-existent files if “persistent” option used
- Working on infrastructure improvements:
 - to allow 3rd parties to create integrated functionality
 - to improve the scalability and performance of Safeguard

- Audit & Security SIG Safeguard requests will be delivered in a series of releases
 - release 1 contains **persistence for non-existent files**
 - release 2 will contain **warning mode**
 - release 3 will contain **allow node names**
 - Release 4 will contain **patterns functionality**
- Version 2, release 1 was shipped with G06.21
- Version 2, release 2 is planned for G06.22
- No dates for remaining releases at this time



Best Practices

Information security



- Key concepts
 - Encryption isn't only SSL
 - Authentication, authorization, and privacy
- What does the Internet look like?
- Where do hackers come from?
- Priorities

Encryption

- SSL—only protects business information from PC to Web server
 - Sometimes not even then
- Record/file encryption—protects business information on the servers
- Communications encryption
 - End-to-end encryption
 - Line encryption
 - VPN/tunneling



Identification, authentication, authorization, and privacy



- Identification—who you are not
- Authentication—who you are
- Authorization—what are you allowed to access?
- Privacy—should you be allowed in the first place?



Identification, authentication, authorization, and privacy



- Proper user verification
- What business information goes online and who can access it?
- Interception of business information
- Hacking of business information—extortion (CD universe)
- Liability

Authentication



- Multiple-use passwords are not secure
 - Can be given away or stolen
- Single-use passwords
 - Challenge/response
- System-assigned passwords are often written down
 - Password quality check is better
- What you are, what you have, what you know
 - Biometrics
 - Token
 - PIN

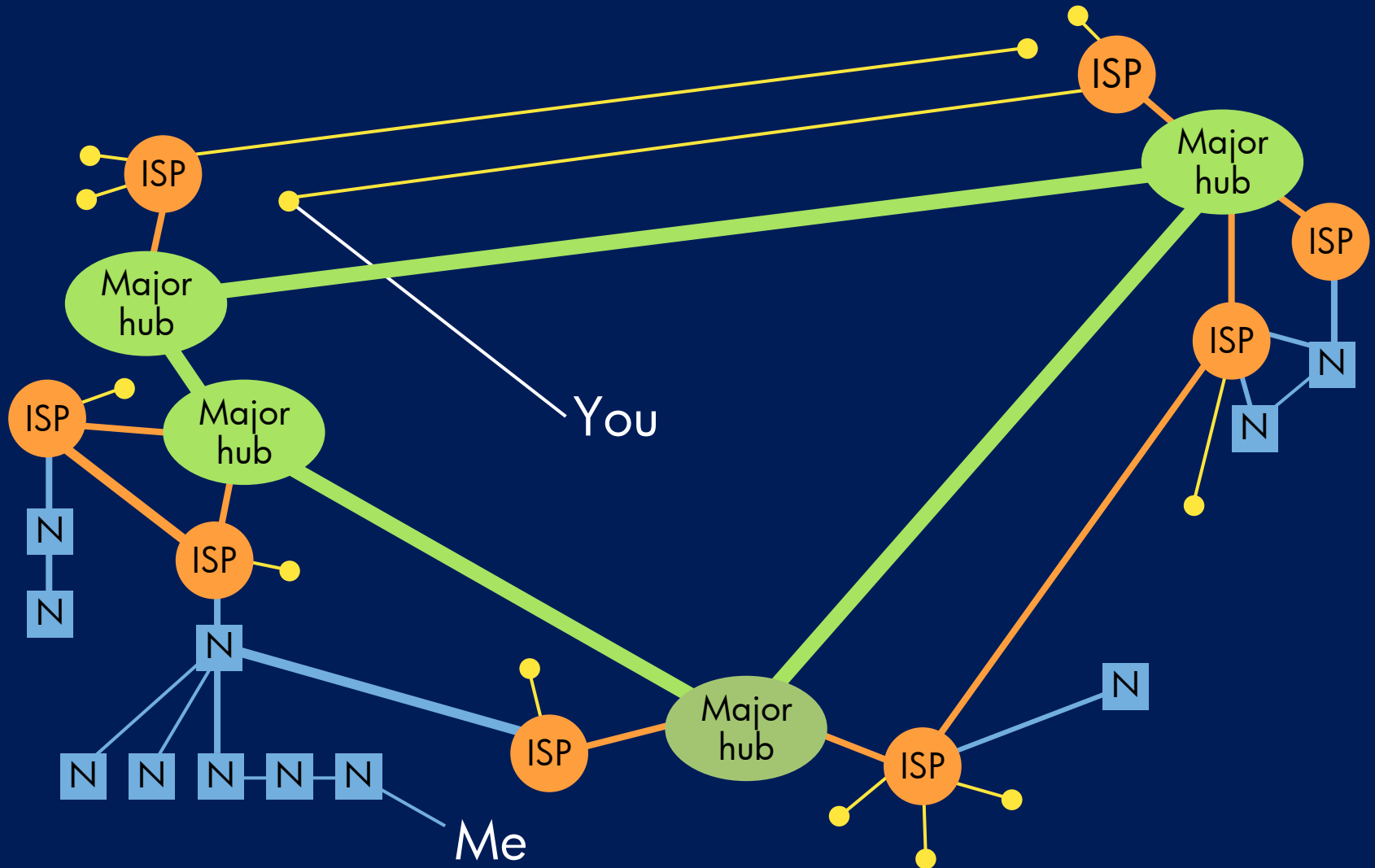
Authorization



- Least privilege
- Role-based security
- Subject/object access control model

- Hot topic on the Internet
- Must flow from corporate policy
- Should be stated
- Your company's reputation relies on it
- Cookies
 - <http://www.junkbusters.com/ht/en/cookies.html>
- Web bugs
 - <http://profiles.yahoo.com/webbug2000>
- Classification of business information and least privilege

What does the Internet look like?

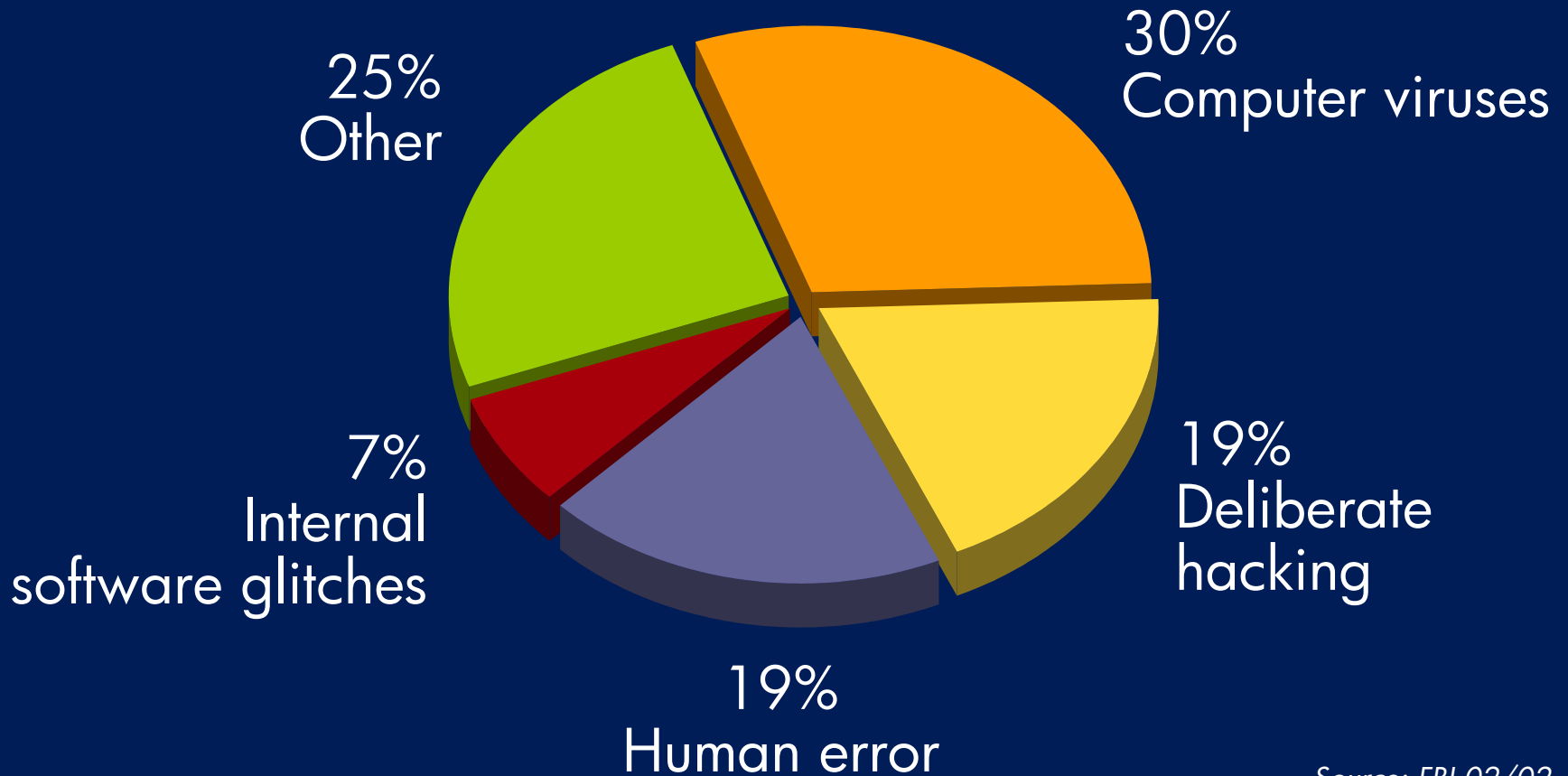


Where do hackers come from?

- Most information security breaches come from insiders.
- Companies usually keep quiet about breaches.



Banking and financial institution security breaches



Source: FBI 02/02

Where do I start?

- Protect your systems from insiders first, then from the outside
 - Least privilege
 - Separation of duties
 - Quick deletion of terminated employee access
- Firewalls
- Encrypted databases, if necessary
- Multi-tier architecture
- Hardware key management

Where do I start?



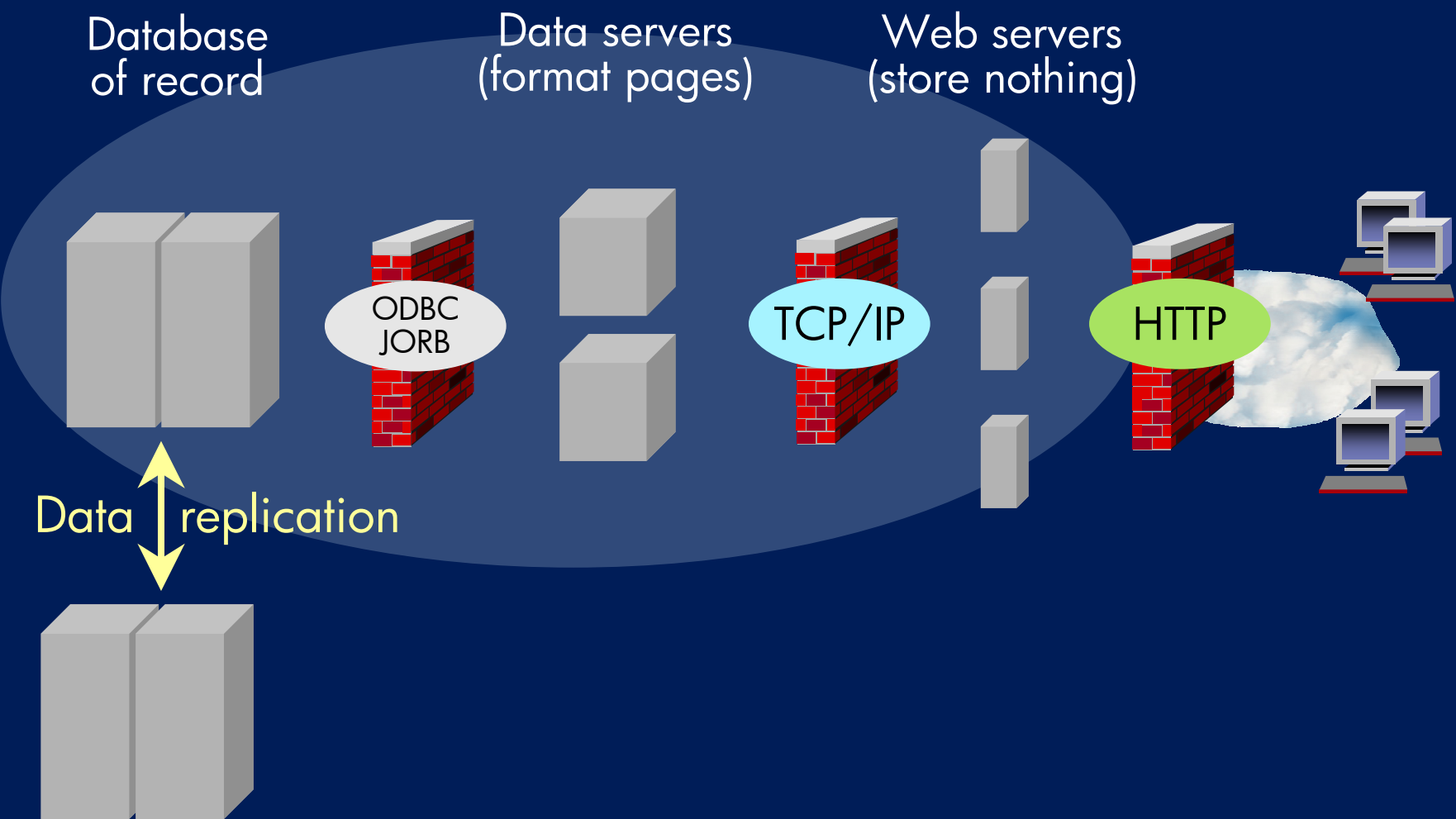
- Don't store anything on Web servers because they can be hacked.
- Subscribe to patch lists like bugtraq.
 - www.securityfocus.com
- Carefully evaluate the hardware and software you are using for inherent security.

Multi-tier architecture



- Multi-tier infrastructure can help provide security.
- At each stage, use different ports or protocols to connect the systems.
 - The front end serves the pages (HTTP).
 - The middle serves the data (TCP/IP).
 - The database server protects the data (ODBC/CORBA/JORB).

Multi-tier architecture



Hardware key management



- Don't tempt even loyal employees.
 - 82 percent of bank computer fraud committed by insiders (Ernst and Young, 2000).
- Overriding goal: there are never any keys "in the clear."
- No one sees or holds the complete "master" key.
 - Choose two (preferably more) trusted employees to hold key parts.
 - Choose from different departments to lessen possibility of collusion.
 - Combine key parts in a secure key injection device to create master.

Hardware key management



- Encrypt all keys to be stored outside hardware security module (disk, cache, etc.).
 - Use a strong master key and a strong algorithm (like Triple-DES).
- Disable commands you don't use.
 - Weakest link is “common denominator” standards for interoperability with other systems.
- Work closely with product vendors.
 - Key management is an evolving science.

- If you cannot detect intrusions, how do you know your security program is working?
 - Intrusion detection system (IDS)
 - Timely review of security logs (batch or real time)
 - Third-party IDS services

If you are hacked



- Get the system off your network as soon as possible.
 - Possibly leave it connected to the Internet.
- Don't touch the computer unless you are skilled in forensic analysis.
- Do not power down the computer—what appears on the screen or in random access memory can be important.
- Get help if you need it.
- Get a bit-by-bit backup of the hard drives and archive the original drives for evidence.

Why HP NonStop systems provide better protection



- Modular operating system
 - Except for a small kernel, most operating system functionality is handled by specialized system processes.
- Processes run in their own virtual address space
 - Communication is by messages; therefore, they cannot overwrite each other's memory.

No system is hack-proof, especially from insiders—
always follow best practices.

Safeguard security for OSS



Please read along with me:

Disclaimer:

The information herein and future product plans, dates, and functionality are subject to change without notice.

OSS Security Futures



- OSS currently implements basic UNIX security (POSIX.1 / FIPS 151-2/P1003.1) for files (read, write, and execute settings for user, group, and others).
- Safeguard currently supports access control lists (ACLs) only on Guardian files, processes, and devices. Therefore, only Guardian file, process, and device access requests are sent to Safeguard which can then forward them to an authorization Security Event Exit Process (SEEP), if one is configured.
- There is only one authorization SEEP permitted on a system.

OSS Security program:

- The OSS ACL Infrastructure Project will allow OSS file authorization rulings similar to Guardian file authorization rulings. The exact mechanism is not yet known at this time. Maybe within Safeguard, maybe by sending to a SEEP.
- This feature will be dynamically enabled and disabled on each fileset using the Subsystem Control Facility (SCF).

What new functionality?

- Allow customers to make authorization rulings on named OSS files, similar to the Guardian SEEP implementation.
- Allow customers to make authorization rulings on OSS accesses into the Guardian (/G) namespace.
- Allow customers to make authorization rulings on OSS accesses into the Expand (/E) namespace.
- Authorization rulings will be audited via new security audit records.

Current Safeguard Security for OSS



- Uses existing Safeguard Audit Service for audit trail management (integrated OSS/Guardian audit trail)
- Audit of access control decisions regarding objects in the OSS name space
 - Object access
 - Object creation and deletion
 - Change of object attribute values

Current Safeguard Security for OSS



- Provides an audit trail of actions regarding OSS processes:
 - Process creation
 - Process modification
 - Process termination (kill)
 - New operation types for OSS-specific process control operations

Current Safeguard Security for OSS



- OSS file system auditing is controlled at the fileset level
 - New AUDITENABLED fileset attribute
- Process auditing continues to be controlled by Safeguard Global configuration
 - AUDIT-PROCESS-ACCESS-PASS
 - AUDIT-PROCESS-ACCESS-FAIL

The OSS Security Audit Trail



- Reflects the outcome of the access control decisions that are made while performing audited operations and do not necessarily reflect the outcome of the operations themselves
 - Operations might fail before an access control decision is made; in these cases, no audit records are created by the operation
 - The absence of an audit record about process X creating directory Y does not mean that process X did not try to create directory Y.

The OSS Security Audit Trail



- Operations might fail after an audit record showing “outcome = granted” is created
 - An audit record saying that process X was allowed to create directory Y does **not** necessarily mean that process X was actually successful in creating directory Y
 - These cases are rarer and usually involve some type of hardware or software failure

Audited File System Operations* (1 of 2)



- access()
 - bind (AF_UNIX only)
 - chown()
 - chmod()
 - link()
 - mkdir()
 - mkfifo()
 - mknod()
 - open()
 - opendir()
 - rename()
 - rmdir()
 - symlink()
 - unlink()
 - utime()
 - FILE_OPEN_() when options.<10> = 1**.
- * Audit of these operations is controlled by the AUDITENABLED fileset setting
 - ** This option bit indicates that the name passed is an OSS path name rather than a Guardian filename

Audited File System Operations (2 of 2)



- During path-name resolution, if directory search access is denied in a directory whose fileset is audit-enabled, an audit record is created
 - This record is created even if the operation being performed is not normally audited
 - Example: `ls -l /a/b/c/d`
 - Suppose that the user entering this command does not have search permission to directory `/a/b`
 - An audit record with `ObjectName = "/a/b"`, `Operation = DirSearch` and `Outcome = Denied` will be generated
- Note that an audit record is not generated when search access is granted; to do so would generate excessive audit and would result in unacceptable performance

Audited Process Operations*



- exec() family
- fork()
- kill()
- setgid()
- setpgid()
- setsid()
- setuid()
- tdm_exec() family
- tdm_fork()
- tdm_spawn() family
- PROCESS_SPAWN_()

*Auditing is controlled by Safeguard global settings

Audited OSS SCF Operations



- ADD FILESET when AUDITENABLED ON
- DELETE FILESET when AUDITENABLED ON
- START FILESET when AUDITENABLED ON
- STOP FILESET when AUDITENABLED ON
- ALTER FILESET when AUDITENABLED is included

Identification of Objects (1 of 6)



- New object types
 - Directory
 - FIFO
 - Socket
 - OSSDiskFile
 - OSSFileset
 - ProcessGroup
 - Symlink
 - TTY

Identification of Objects (2 of 6)



- Most OSS objects have one or more external names and a unique internal name
- For objects in the OSS Name Space, the external names are absolute OSS path names normalized as follows:
 - Symbolic link references are resolved
 - “.” and “..” references are resolved
 - Redundant slashes (“/”) are removed
 - If longer than 1023 characters, truncated on the left with the truncated portion replaced by “...” (should never happen as OSS pathnames have a max. length of 1023)
- For OSS filesets, the external name is the name used in SCF (for example, ROOT)

Identification of Objects (3 of 6)



- The internal name is dependent on the type of object
 - Because internal names are reused, they include a qualifier to distinguish between instances
 - Each time that a given internal name is reused, it will be assigned a new qualifier
 - For regular files:
 - The internal name is the corresponding “ZYQ” file name
 - The qualifier is the file’s Creation Version Sequence Number (CRVSN), which is a unique 48-bit number assigned by DP2 when the file is created
 - In audit records, the CRVSN appears with leading zeros suppressed, for example:
 - \$OSS.ZYQ00000.Z000004G:34569

Identification of Objects (4 of 6)



- Internal names (continued)
 - For other files (directories, FIFOs, and so forth):
 - The internal name is \$ZPNS.Znnnnn.Ziiiiiii where:
 - nnnnn is the fileset number (DEVICELABEL shown by SCF INFO FILESET, DETAIL) and is displayed in base 32 (e.g., 00011 is fileset 33).
 - iiiiii is the inode number (number returned by “ls -li” converted to base 32)
 - The qualifier is a 48-bit timestamp representing the time when the file was created. In audit records, it appears as a simple integer with leading zeros suppressed
 - Example:
 - \$ZPNS.Z00000.Z000004G:345678980

Identification of Objects (5 of 6)



- Internal names (5 of 6)
 - For OSS filesets:
 - The internal name is \$ZPMON.Znnnnn where nnnnn is the fileset number
 - The qualifier is the date and time when the fileset was created expressed in LCT
 - Example (ROOT fileset created 6/28/1998 at 2:53:22pm):
 - \$ZPMON.Z00000:19980628145322
- In the ObjectName field of most audit records, both the external and internal name are given separated by "=".
 - Examples:
 - Regular file:
 - /bin/lS=\$OSS1.ZYQ00000.Z000006G:95678
 - Other file:
 - /etc=\$ZPNS.Z00000.Z00000F5:345677895
 - Fileset:
 - HOME=\$ZPMON.Z00005:19991022073918

Identification of Objects (6 of 6)



- In some cases (open() of an existing file, for example), only the internal name appears in the ObjectName field
- Such audit records are preceded by an audit record with OPERATION = OSSResolve. That record gives both the external and internal names
- Operations that follow this convention are:
 - All process creation APIs that accept a path name
 - open() and FILE_OPEN_() where options.<10> = 1
- Example: open("/etc/profile", O_RDONLY, 0);
 - OSSResolve record with ObjectName =
/etc/profile=\$OSS1.ZYQ00000.Z000001F:23456
 - OPEN record with Object Name =
\$OSS1.ZYQ00000.Z000001F:23456

SAFEART Enhancements (1 of 2)



- To be able to relate records by both external and internal names, SAFEART now supports wildcards in object names
- Example: Who opened "/a/b"?
 - SET WHERE OBJECTNAME = "/a/b=*" and OPERATION = OSSRESOLVE OR OPERATION = OPEN
 - OPERATION = OPEN is included to handle the case where the /a/b was created and opened in the same operation
 - START
 - Returns OSSRESOLVE record with object name = /a/b=\$OSS.ZYQ00000.Z00003D3:22456
 - SET WHERE OBJECTNAME = "\$OSS.ZYQ00000.Z00003D3:22456 and OPERATION = OPEN
 - START

SAFEART Enhancements (2 of 2)



- Continue example: Find all records pertaining to this instance of /a/b:
 - RESET WHERE
 - SET WHERE OBJECTNAME =
"\$*OSS.ZYQ00000.Z00003D3:22456*"
 - START
- SAFEART has also been enhanced to support the new object types, operations and text area formats added for OSS security auditing

For more information...



- **Useful URL**

- <http://www.hp.com/go/nonstopsecurity>

- **Product manager for continuity and security products**

- Ron LaPedis, +1 (408) 285 5987

- ron.lapedis@hp.com

Thank you



i n v e n t