New Options for Securing the NonStop Server

George Haskell
Product Management
Wendy Bartlett
Distinguished Technologist
2 November 2006
Agenda

• NonStop security environment
• Today’s security environment
• Securing data at rest
• Key Management
• New features
• Work in progress
• Questions for you – what do you need to survive audits and improve your security environment?
What do NonStop customers want in security?

- Customers want their IT resources (systems, networks, uptime, data, personnel) protected from external or internal attack and miss-use.
- Customers want their data protected from internal and external unauthorized access.
- Customers want proof - a secure audit trail of all the above.
- Customers want it easy and transparent. Just plug products together and you have it.
HP Security Products for NonStop Servers

• Authentication/authorization/audit
  – Standard security (part of NonStop OS)
  – Safeguard
    • Optional product on S series
    • Bundled on H series
  – OSS security
  – Middleware (SQL/MX, ODBC, JDBC, Java, Tuxedo)

• Encryption
  – Atalla Ax100 Network Security Processors
  – Atalla Key Block key management system
Traditional NonStop security model

- HP supplies basic infrastructure, especially pieces that need to be wired in at a low level in the system.
- Partners supply products built on top that offer enhanced functionality such as:
  - Finer-grained access control to potentially-destructive operations
  - Operational audit, up to keystroke level
  - Network security
  - Intrusion detection
<table>
<thead>
<tr>
<th>Who does what?</th>
<th>HP</th>
<th>Partners</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Basic facilities</td>
<td>Password quality, including dictionary checks; challenge/response</td>
</tr>
<tr>
<td>Authorization</td>
<td>Coarse level of control</td>
<td>Finer-grained control; audit down to keystroke level</td>
</tr>
<tr>
<td>Object security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit</td>
<td>Audit generation</td>
<td>Audit interpretation</td>
</tr>
<tr>
<td>Encryption</td>
<td>Roadmap currently under construction – will be a mix of HP and partners</td>
<td></td>
</tr>
<tr>
<td>Data at rest</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The past two years in NonStop Security

- Significant enhancements to Safeguard
  - ITUG Big 6
  - Longer/Stronger Passwords
- Enhancements to OSS Security
  - Almost full security API implementation
  - OSS ACL support
  - Partners have made significant enhancements to their products
Today’s Market Snapshot

• Privacy and regulatory environment creating visibility and demand for security
  – Many US states have laws requiring disclosure
  – Number of disclosed breaches this year are greater than the last 3 combined
  – US in the forefront today; quickly followed by Europe and then Asia

• Real consequences
  – Cost per incident is $10M – $100M
  – Growing concern by large organizations for lost IP, especially the technology sector
  – Impact to brand image and revenue
  – Jail
# Compliance Drivers in the US

<table>
<thead>
<tr>
<th>Name of Law or Regulation</th>
<th>Potential Penalty</th>
<th>Potential Fines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarbanes-Oxley Act</td>
<td>20 years in prison</td>
<td>$15 million</td>
</tr>
<tr>
<td>Gramm-Leach-Bliley Act (GLBA)</td>
<td>10 years in prison</td>
<td>$1 million</td>
</tr>
<tr>
<td>USA Patriot Act</td>
<td>20 years in prison</td>
<td>$1 million</td>
</tr>
<tr>
<td>Health Insurance Portability and Accountability Act (HIPAA)</td>
<td>10 years in prison</td>
<td>$100 per violation, subject to a calendar year cap of $25k for all violations of an identical requirement or prohibition</td>
</tr>
<tr>
<td>SEC Rule 17a-14</td>
<td>Suspension / Expulsion</td>
<td>$1 million</td>
</tr>
<tr>
<td>PCI DSS - Visa</td>
<td>Fine per Incident and potentially others</td>
<td>$500,000 per incident</td>
</tr>
<tr>
<td>State Privacy Laws (e.g. CA SB1386 + 21 others)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What Does it Mean to our Customers?

• Customers are subject to increased data retention, privacy, protection, and audit/compliance requirements
• Over past 2 years, customers have adopted stronger IT security policies, made sensitive data protection a business imperative, and moved security to top IT budget priority
• Auditors are getting tough
• Last year, auditors gave waivers – now demanding compliance
• Looking to HP for leadership and solutions in information security and compliance
Data-at-Rest Security

- Encryption and key management requirements include:
  - Application/DB layer security services
  - Storage encryption
  - Storage Key Management
The number of public breaches this year is greater than the number of public breaches in the last 3 years.
## Reported lost tapes in the US in 2005

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>User records</th>
<th>Potential Cost @ $25 - $140/record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb. 25, 2005</td>
<td>Bank of America</td>
<td>1,200,000</td>
<td>$30M - $168M</td>
</tr>
<tr>
<td>April 20, 2005</td>
<td>Ameritrade</td>
<td>200,000</td>
<td>$5M - $28M</td>
</tr>
<tr>
<td>May 2, 2005</td>
<td>Time Warner</td>
<td>600,000</td>
<td>$15M - $84M</td>
</tr>
<tr>
<td>June 6, 2005</td>
<td>CitiFinancial</td>
<td>3,900,000</td>
<td>$97M - $546M</td>
</tr>
<tr>
<td>July 6, 2005</td>
<td>City National Bank</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>Sept 19, 2005</td>
<td>Children's Health Council, San Jose</td>
<td>5,000 - 6,000</td>
<td>$0.15M - $0.84M</td>
</tr>
<tr>
<td>Oct 21, 2005</td>
<td>Wilcox Memorial Hospital, Hawaii</td>
<td>130,000</td>
<td>$3M - $18M</td>
</tr>
</tbody>
</table>
Customer requirements

- Meet regulatory requirements
- Not require application code changes
- Have minimal impact on performance
  - Throughput and latency
- Be able to encrypt and rotate keys online
- Be affordable
Approaches to Protecting Data at Rest (1)

• Application level
  – Selective field encryption under application control
  – Supports mandates such as Payment Card Industry (PCI)
  – Encrypted field contents are unusable by DB for sorts, joins, ...
  – Can be done in conjunction with hardware security module (e.g. Atalla)
  – Requires application changes by user
  – Potential for performance issues if number of fields to be encrypted is extensive
Approaches to Protecting Data at Rest (2)

- **Database level**
  - Selective field encryption
  - Selective element (field/row intersection) encryption
  - Must be explicitly supported by the database (e.g. SQL/MX)
  - Potential performance issues depending on amount of data to be encrypted/decrypted
  - Long term hardware assist would be ideal
  - Not practical in short term
Approaches to Protecting Data at Rest (3)

- **Storage level**
  - Entire contents of disk volume or tape
  - Protects against loss of physical media, but not rogue access
  - Done below the database level – contents can be used by DB for sorts, joins, …
  - Meets many regulatory requirements (e.g. PCI, CA1386)
  - Several 3rd party products currently available
  - Likely short-term approach
Tape protection

• We are looking to our partners for tape encryption
  – TSI is now offering an encryption option (TE2000)
    • Supports FC and SCSI connectivity
  – Both TapeLabs (Crossroads) and TSI offer an encryption option for virtual tapes
  – Software-only options are available from security partners
  – Expect to see encryption built into tape drives in the future
Disk Volume-level Encryption: Hardware based

- Likely short-term approach is to insert “bump in the wire” third-party appliance
  - Puts encryption/decryption outboard; data is in the clear everywhere in the host
- Additional requirements for NonStop environment
  - Fault tolerance
  - Online initial encryption and key rotation
- Performing initial device evaluation
Volume-level bump-in-the-wire encryption (simplified)

Data written to storage

Encryption Appliance

Storage Encryption

Network

Volume 1
Volume 2
Volume 3

Data read from storage
Issues

• No hardware-based solution for SCSI connected disks (no place to insert a bump-in-the-wire appliance
  – Users must either convert to Fibre Channel (XP or JBOD) or look at software solutions
  – Host-based encryption done entirely in software is acceptable in many, but not all, environments (ANSI X9 may be an issue)

How big an issue is this for you?
Disk Volume-Level Encryption: Software based

- Also investigating potential for software-based encryption
  - Combination of HP (encryption) and third-party (key management) components
  - Performance may not be acceptable for many customers
    - Throughput
    - Latency
Other Disk Protection Options

• Options under investigation:
  – Combinations of volume-level disk encryption with database activity monitoring and/or compensating controls
  – Improved support for application-level field column/field encryption via Atalla, possibly via third party software partner
  – Column-level database encryption
    • Longer-term solution
Volume-level encryption combined with database activity monitoring

- Gartner recommendation as a way to meet audit requirements, probably for the next few years
- Database activity monitoring:
  - We currently log queries from ODBC and JDBC in EMS
  - Embedded SQL is not logged
  - MXCI queries and DDL are not currently logged
- Keystroke logging and auditing packages from our partners may meet your requirements
- We’re investigating additional options
Volume encryption coupled with dual controls at file system/DB level

- **Enhanced permission scheme with additional permission information kept in an outboard appliance**
  - Sysadmin controls NSK permissions
  - Security officer controls outboard appliance permissions
  - Requires their collusion to circumvent checking
  - Potential to actively terminate offending TCP/IP connections
  - Potential for eventual database plug-ins to protect against rogue DBA

- **This combination may be adequate for some customers for the medium to long term**
Other potential approaches to software-based encryption

- Object file system call interception
- Source code preprocessing to insert encryption/decryption calls
- May be either selective or full file/table encryption

*Does either approach meet your requirements?*
Potential Issues with Software-Based Encryption

• Possible performance issues based on amount of data to be encrypted/decrypted
• Inability to search on encrypted fields, depending on where the encryption is done
• Acceptability in certain regulatory environments
Key Management

• Encrypted data is protected if and only if encryption keys are protected
  – Data protection and compliance
  – Data preservation and recoverability
  – KM is the point of control for policy, enforcement, compliance, audit
  – Data and keys may need to outlast specific products, 5-10 years or more

• Customers want a single, consistent Key Management architecture
  – Seamless, interoperable, automated
    • Point/proprietary KM solutions can create an unmanageable mix
  – Stable, supported, standards-based
  – From a trusted major vendor
Certification

• ISO 15408, otherwise known as Common Criteria, has become an expectation
  – Beginning to see government requirements or benefits for certification (Japan – tax benefits; EU – under discussion)

• Certification comes in 6 levels, EAL1 to EAL6 (higher is stronger)

• What are your certification requirements?
  – Are you getting demands for CC?
  – If so, what level is needed and in what timeframe?
ITUG ‘Big 6’ RFEs are done!

1. Support for wildcard ACLs – G06.25, all H06
2. Warnings enabled at the ACL level – G06.22, all H06
3. Multiple owners of Userids/Aliases – G06.27, H06.07
4. Comment field in Userid/Alias records – G06.27, H06.06
5. Explicit remote system names in ACLs – G06.24, all H06
6. Can create persistent ACLs before the object exists – G06.21, all H06

Technical details on all 6 are in the backup slides of Wendy’s ITUG talk (on ITUG website)
Recently-released features

- OSS (POSIX) security APIs:
  - setregid, setreuid – G06.27, H06.05
  - lchown, lchmod, fchown, fchmod – G06.28, H06.05
  - getsid, setpgrp – G06.29, H06.07

- See backup slides for details
Safeguard V3R1:  
(G06.29, H06.06)

- Optional new password encryption algorithm: HMAC with SHA-256 (HMAC256)
- New USERAX file
  - Stores passwords, password history
  - Passwords also kept in USERID unless using HMAC256
- New config file: $SYSTEM.SAFE.CONFIGP
- Better management of password options in the non-Safeguard environment
  - New program: PWCONFIG
Safeguard V3R1: Changes in default settings

- New default values:
  - PROMPTPASSWORD BLIND
  - PASSWORD-MINIMUM-LENGTH 6
  - PASSWORD-ENCRYPT ON
  - PASSWORD-ALGORITHM DES

- Use SAFECOM to override new values if needed

- Fallback to a prior Safeguard version will revert to using old settings from CONFIG file
Safeguard V3R1: Improved encryption - HMAC256

- Fallback requires care once HMAC256 has been enabled:
  - Older versions of Safeguard do not understand HMAC256, USERAX or CONFIGP
  - Existing users must revert to using the last password they had set under DES/cleartext
  - Users added after switching to HMAC256 will have to establish new passwords
  - Fallback documentation has been published in Hotstuff S06055

- See backup slide for more information on HMAC256
Safeguard V3R1: PWCONFIG options

- PROMPTPASSWORD {BLIND | ECHO | OFF}
  - BLIND – Prompt for the old and new passwords. Passwords are not displayed on the screen
  - ECHO - Prompt for the old and new passwords. Passwords are echoed on the screen
  - OFF – Read new password from command line

- MINPASSWORDLEN { n }
  - n is an integer between 0 and 8
  - Specifies the minimum length allowed when passwords are changed
  - 0 indicates that NULL passwords can be accepted
Safeguard V3R1: PWCONFIG

- **ENCRYPTPASSWORD {ON | OFF}**
  - ON – Indicates passwords will be encrypted, as described by ALGORITHM
  - OFF – Indicates passwords will be stored as clear text, and not encrypted

- **ALGORITHM {DES | HMAC256}**
  - The values for this attribute are only used if ENCRYPTPASSWORD is ON
  - DES – Indicates stored passwords will be encrypted using DES
  - HMAC256 – Indicates stored passwords will be encrypted using HMAC with SHA-256

- **INFO:**
  - Returns the current PASSWORD configuration
OSS ACLs
(G06.29, targeted for H06.08)

- Based on the Posix standard document 1003.1e
  - Posix ACLs do not specify wildcards, therefore wildcards have not been implemented
- OSS ACLs are stored internally in the inode for speed
- For performance reasons, we have chosen an integrated implementation rather than use of a user exit (SEEP)
- We expect that partners will develop management tools for OSS ACLs
OSS ACLs
Commands and system calls

- `acl(2)` Implemented
- `chmod(2)` Enhanced
- `cp(1)` Enhanced
- `getacl(1)` Implemented
- `ls(1)` Enhanced
- `setacl(1)` Implemented
- `stat(2)` Enhanced

1 = command, 2 = system call
Restoring backups of files with OSS ACLs

• Earlier versions of Backup/Restore 2 do not understand the format of tapes containing files with OSS ACLs

• Compatibility SPRs allow the files to be restored on H06.05 and G06.23 and later
  – The files themselves can be restored, but not their ACLs
Security-OSS-Administrator group

• This group has been added as part of OSS ACL support

• In addition to the file owner and super-user, members of this new security group are allowed to change an OSS object’s:
  – File permissions, including its OSS ACL
  – Ownership
What’s in the works

Disclaimer: Future product plans, dates, and functionality are subject to change without notice.
Longer, more flexible passwords and basic password quality checks

• Implementation for the H series is under development
  – S-series support is under consideration
• The new maximum length will be 64
  – Customers will be able to configure a compatibility mode and a maximum length
• Implementation will be staged across multiple releases
  – Length will support for blanks and quality checks
  – HP subsystem support will be phased
• Support will be only via USER_AUTHENTICATE_
  – No VERIFYUSER support
  – Send email to Wendy if you need the details in advance of release
Longer Passwords

- The following subsystems will support longer passwords in the initial release:
  - TACL
  - NetBatch, NetBatch +
  - OSS utilities
  - FTP
  - TELSERV
  - NFS
  - SQL/MX Executor
  - iTP WebServer
  - CORBA
  - iTS/Gateway
  - Visual Inspect server
  - SCA
  - OSM
  - DSM/SCM
  - Web Viewpoint
  - CSG
  - SSG
Longer Passwords

- The following subsystems will support longer passwords in a subsequent release:
  - OSI/MHS/FTAM
Password quality

- Pass phrases (embedded blanks) will be supported in a subsequent release
- We’re also planning on supporting very basic “must include” quality checks in a subsequent release
We need your input

• What do you need in order to pass audits?
• What other security features are required?
  – We’re especially interested in hearing about features that can’t be supplied by partners

• Send email to us
• File RFE cases
Passing audits

• Are you passing now?
• Are you passing with waivers?
  – What is getting waived?
  – How long do you think you’ll continue to get waivers?
• Are you failing?
  – What is causing you to fail?
Working with your auditors

• What confuses them?
  – Terminology?
  – Concepts?

• What can we do to help?
  – White papers?
  – What else?
Prioritization Criteria for Security RFES

• Unable to comply with laws (e.g., SOX, HIPAA) or regulations (e.g., PCI) without this feature
  – Timeframe?

• Unable to pass their internal audits without this feature
  – Timeframe?

• Mightily inconvenienced without this feature, e.g.
  – Drowning in unnecessary audit
  – Having to correlate different pieces of information by hand
  – Not enough granularity

• Can do what we need without this feature, but it performs badly or is very clumsy

• Could do something cool if we had this feature

• It'd be nice to have this because…
Safeguard RFEs under consideration

• Note: the default is to implement only on the H series

• User/alias management:
  – Extensible user attributes
  – Aliases that are not tied to userids
  – Ability for aliases to own objects
  – Reset total failures etc. without deleting/adding user

• Authentication:
  – Single sign-on

• Access:
  – Time-based access control
Safeguard RFEs under consideration

• Note: the default is to implement only on the H series

• Audit generation and management:
  – Include IP address in audit records
  – Audit TACL LOGOFF for non-Safeguard-started TACL

• Safeguard configuration and status display:
  – Optionally constrain use of INFO command (see Barclays RFEs)

• Partner support:
  – More hooks
  – Better performance for functions that access Safeguard files
Safeguard RFEs under consideration

• Alias enhancements
  – Don’t tie aliases to userids
  – Allow aliases to own objects

• Etc.
Other RFEs under consideration

- $CMON hook for OSS
- Port monitoring / intrusion detection for TCP/IP

What else should be on our radar?
Next steps

• For product RFEs, get a case filed
  – Include business case information (e.g., failing audits because this is missing)
  – Send George and me email with the case number

• For suggestions on white papers etc., send us email
  – George.Haskell@hp.com
  – Wendy.Bartlett@hp.com