HP NonStop Educational Talks

System Security Update for the NonStop Server

Wendy Bartlett
Karen Copeland

10 January 2008

Technology for better business outcomes

© 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice
Your speakers

Karen Copeland
HP Product Manager - NonStop Security

Wendy Bartlett
HP Distinguished Technologist
Agenda

• Security requirements and strategy
• What’s new and what’s coming
• Network security
• Data at rest encryption
• Safeguard
NonStop Customers & Security

• Customers need security capabilities to manage risk appropriately, avoid penalties, remain competitive and in business
  – Example: PCI Compliance requires sensitive cardholder data to be encrypted or otherwise made obscure

• Customers have told us that they want:
  – NonStop Security to be an integrated, inherent part of the system
  – Adding Security options to their system to be as painless as possible
    • Require no or minimal application changes
    • Be easy to plug in for integration
    • Be possible to deploy quickly
  – Security options to be reasonable in terms of costs, including ongoing manageability
  – Security products to be available now
Compliance…it is everywhere

- SEC 17a-4 (USA)
- HIPAA (USA)
- Canadian Electronic Evidence Act
- Basel II Capital Accord
- GDPdU & GoBS (Germany)
- ISO 18501/18509
- FDA 21 CRF Part 11
- Sarbanes-Oxley Act (USA)
- Electronic Ledger Storage Law (Japan)
- 11MEDIS-DC (Japan)
- NF Z 42-013 (France)
- AIPA (Italy)
- Financial Services Authority (UK)
- Public Records Office (UK)
- BSI PD0008 (UK)
- Basel II Capital Accord
- Financial Services Authority (UK)
- Public Records Office (UK)
- BSI PD0008 (UK)
Customer needs and industry trends

- Customers need:
  - Systems, networks, data and personnel protected from external or internal attack and misuse
  - Proof—a secure audit trail of all the above to meet their respective compliance requirements
  - Easy and transparent—just plug HP products together and have them work securely
  - Choices that reflect the value of products and services, and provide a cost-effective solution

86% of enterprises plan significant security upgrades in 2007

Source: Business Technographics November 2006 North American and European Enterprise IT Budgets and Spending
Security and Audit SIG Feedback
Top 3 ITUG Summit 2007 list

• Maintain security functionality for G & H Guardian versions in close synchronization in order for customers to meet audit requirements

• OSM Console Security enhancements – with OSM now being network enabled and with more tools – it is important the HP creates a security policy and tools to enhance and manage the console security in a networked environment

• Forensics information on User/Group profiles in Guardian/Safeguard as well as ACLs, and in audit records
  – Comment field(s) where name, address, phone number, and other miscellaneous information can be recorded with each object type/attribute deployed
  – Creation/change timestamps, etc.
What we heard from ITUG Security SIG Survey

1) Increase Safeguard capabilities in support of compliance requirements and improved manageability

2) Provide a single view of security, or make it possible for third parties to do so (Guardian, Safeguard, OSS, OSS ACLs, SQL/MX grant/revoke, ODBC setup)

3) Improve auditing capabilities

4) Improve HP reporting tools

5) Provide disk and tape encryption
Security Initiative Vision/Strategy

Ensure that customers have the tools available to

- Protect their data
- Pass both internal and external audits
- Manage their security infrastructure at a reasonable ROI
  - Have the capability to integrate their NonStop servers into their enterprise security environment

Short Term:
- Enhance basic platform security options as quickly as possible

Long Term:
- Develop and sustain comprehensive security capabilities that match enterprise customer requirements
The Approach

• Improve NonStop security capabilities offered by HP
  – Correct existing product shortcomings
  – Improve auditing/forensic information

• Leverage expertise within HP
  – Participate in the Secure Advantage program to the degree that our technology allows (Under investigation)

• Leverage Partner products
  – Examine opportunities to leverage existing partner technologies
  – Look for opportunities to engage with partners on new technology projects
Agenda

- Security requirements and strategy
- What’s new and what’s coming
- Network security
- Data at rest encryption
- Safeguard
Current Security Offerings

Available from HP Directly:

• **NonStop SSH** (For both G-series & H-series) – **Available now**!
  – Provides secure data transmission when using terminal emulation, SFTP, etc.
  – **NonStop SSH – Secure FTP** only option at a lower cost.

• **Safeguard Enhancements (H06.12)**
  – AUDITCLEANONPURGE ON/OFF feature
  – Audit Enhancements

• **Atalla Encryption on NonStop**
  – Atalla Ax150 Network Security Processors
Current Security Offerings

Available through HP NonStop Partner Relationships:

• **Decru: DataFort™ on NonStop**
  - Provides volume level encryption on NonStop
  - Supports Fiber Channel only
  - Qualified on NonStop with help from HP

• **TSI: Tape encryption**
  - **Tape Encryption (TE2000)**
    - Supports both SCSI and FC
New Security Offerings

Available from HP directly:

- **Safeguard Enhancements** *(H06.14, H06.15, H06.16, G06.32)*
  - Key features requested by customers

- **NonStop System Console Security** *(G-series and H-series)*
  - Security policy and new defaults to improve NSC access control and auditing
  - Customer choice of several popular security packages to protect against viruses and intrusion

- **SecureVTS - Software Encryption for VTS**
  - Provides embedded Software Encryption layer for Virtual Tape

- **IPSec support in new generation of NonStop comm controllers**

- **Data Sanitization for NonStop**
  - A DoD compliant data sanitization product for NonStop

Note: Future product plans, dates, and functionality are subject to change without notice.
<table>
<thead>
<tr>
<th>In design</th>
<th>Under investigation</th>
</tr>
</thead>
</table>
| • Volume Level Encryption in new Comm controller  
  – SAS and XP drives | • LTO4 Tape with bulk encryption capability  
• Security improvements to Manageability products  
• Integration with HP’s Secure Advantage Program  
  – Compliance Log Warehouse for auditing reporting on the NonStop System  
  – Unified Secure Key Management system for key management across the enterprise  
• Ongoing enhancements to Safeguard and other on-platform security functionality  
• SQL DB Encryption |

Note: Future product plans, dates, and functionality are subject to change without notice.
# NonStop Security Offerings
Partner Offerings - At a Glance

## Product Area

**On Platform Security**  
(includes auditing)

**Data in Motion**

**Data At Rest**  
- SQL DB Column Encryption  
- Application Encryption Libraries

**- Volume Level Encryption**

**- Tape Encryption**

## Partners

- Baker Street Software
- CSP (Computer Security Products)
- Greenhouse
- XYPRO

- ACI (SSL)
- CAIL/Bowden (SSL & SSH-OSS)
- comForte (SSL & SSH)
- XYPRO (SSL & SSH-OSS only)

- XYPRO – SQL/MP Encryption
- comForte
- Greenhouse
- Opsol
- RSA
- XYPRO

- NETAPP/Decru (DataFort) (Hardware)
- comForte – Secure Tape (SW)
- Crossroads – VTS (SW & Hardware)
- TSI – NeoScale (Hardware)
Agenda

- Security requirements and strategy
- What’s new and what’s coming
- Network security
- Data at rest encryption
- Safeguard
HP NonStop SSH

Features

The HP NonStop SSH product is designed to help your organization effectively manage security risks and comply with external and internal security policies.

- Fully compliant to the SSH Protocol
- Strong authentication and multiple cipher suites
- Supports full screen terminal access for TACL and OSS
- Built-in user base
- Central key store
- Secure SFTP transfer
- TCP and FTP Port forwarding
- Advanced Auditing capabilities
- No SYSGEN required to install

A customer talk on NonStop SSH is scheduled for later this month on Thursday, January 24th, 2008.
NonStop Data in Motion without NonStop SSH Installed

HP NonStop Server – Security Encryption without HP NonStop SSH

- TACL
- OSS
- Other Applications
- FTPSERV
- FTP

- TELSERV

- MR-Win6530 emulator on the NonStop System Console
- Any 6530 emulation Client
- OSS emulation client
- FTP client
- FTP server
NonStop Data in Motion
with NonStop SSH Installed

HP NonStop Server – Security Encryption including HP NonStop SSH

- TACL
- OSS
- Other Applications
- Filesystem

HP NonStop SSH

- MR-Win6530 emulator on the NonStop System Console
- Any SSH enabled 6530 emulation Client
- SSH OSS emulation Client (MR-Win6530, PuTTY)
- SFTP client
- SFTP daemon
NonStop SSH
Availability and Licensing

For H-series
• Provided as part of the H06.11 RVU.
• The individual SPR may be applied back to H06.06.

For G-series
• Provided as an Independent Product today.
• Will be resident on the next G-series RVU (probably G06.32).

• SSH capability is free from the NonStop System Console for terminal emulation or Secure FTP when using MR-Win6530 or any SSH capable emulator.
• To get full function SSH capability for applications, emulation and Secure FTP across the system purchase a license.
  – Order SSH01V1 for G-series, Order HSSH01V1 for H-series
• A “Secure FTP only” license is also available.
  – Order SSH02V1 for G-series, Order HSSH02V1 for H-series
A new TCP/IP SCF, ICMP-FILTER-PKTS, causes packets that match the specified filter to be dropped

- The attribute takes a 32 bit hexadecimal value
- Its bits correspond to the ICMP message types for which a filter needs to be applied

SCF command format:
- ALTER MON *, ICMP-FILTER-PKTS <value>

Example usage: disable XDMCPReconfigure from a remote host

- This is done by setting up filters that deny ICMP packets of type 17 (ICMP_MASKREQ)
IPsec (IP Security)

- A suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream
  - Also includes protocols for cryptographic key establishment
- IPsec protocols operate at the network layer, layer 3 of the OSI model
  - Other Internet security protocols such as SSL and TLS operate from the transport layer up (OSI layers 4 - 7)
  - This makes IPsec more flexible, as it can be used for protecting both TCP- and UDP-based protocols
  - It also increases its complexity and processing overhead
    - it cannot rely on TCP (OSI layer 4) to manage reliability and fragmentation

Disclaimer: Future product plans, dates, and functionality are subject to change without notice.
IPsec support for NonStop servers

- IPsec will be supported by a new generation of comm controllers
  - Not available for the S series

Disclaimer: Future product plans, dates, and functionality are subject to change without notice.
New comm controller architecture

Diagram:
- App
  - Socket Calls
  - New SW
- Linux System
  - New SW
  - Linux TCP/IP Stack
- Existing Ethernet Controllers
- ServerNet Link
- Older TCP Stacks
Agenda

- Security requirements and strategy
- What’s new and what’s coming
- Network security
- Data at rest encryption
- Safeguard
Application-based:
Selective field encryption

- Requires customer application changes to encrypt/decrypt sensitive data at appropriate places
- Has the potential for performance issues if the number of fields to be encrypted is large
- Encrypted field contents cannot be used at the database level for sorts, joins, ...

Some customers are encrypting sensitive data in an earlier tier so it is always encrypted on the NonStop server
Application-based encryption: Software

- Multiple partners offer encryption libraries:
  - comForte
  - Greenhouse
  - Opsol
  - RSA
  - XYPRO

- Hardware key management may be an option
- May be able to integrate with existing enterprise key management system
Application-based encryption: Hardware

- Improved crypto performance must be traded off against performance cost of TCP/IP access
  - Overall performance will depend on amount of data to be encrypted/decrypted
  - Your mileage may vary
Database level: selective column encryption

- Must be implemented in the database itself
- Has potential performance issues depending on amount of data to be encrypted/decrypted and frequency of reading/writing it

This is under investigation for SQL/MX but not currently in plan
“Bump-in-the-Wire” Volume Encryption

- Most readily-available short-term approach
- Transparent to OS and application
- Works with disk and tape
- Some potential latency/performance impact
- Appliances exist for FibreChannel
  - No SCSI support

- Request a Key
- Key Database
- "Bump-in-the-Wire" Encryption Device
- Encrypted Data
- Data in Clear

Optional Key Management Device
Disk volume-level encryption – new!

- HP has qualified the DataFort™ encryption appliance from NetApp/Decru
- The NetApp/Decru platform combines wire-speed encryption, access controls, authentication, and automated key management
  - Solution is deployed with no disruption to applications
  - Encryption is done in-line between the NonStop host and drives
  - Validation includes requirements for NonStop environment
    - Fault tolerance
    - Online initial encryption and key rotation
  - Qualification was done for Integrity NonStop servers
  - This is a reference sale by NetApp/Decru
- Visit www.decru.com for more information
NetApp/Decru key management

- DataFort includes built-in key management
  - Satisfactory for smaller configurations
- NetApp offers a product called Lifetime Key Management (LKM)
  - An appliance for key repository for larger configurations
  - Needed for large configurations
  - Contact NetApp’s Decru Division for more information
NetApp/Decru configuration: XPs
NetApp/Decru configuration: FCDMs
NetApp/Decru support model

- Support contracts are with NetApp/Decru
- First-level customer support is done by NetApp/Decru
  - The two companies will work cooperatively to solve problems in cases where it is unclear where the problem resides
- The intention is to make use of the TSANet support process
  - Common industry model for handing off cases between companies to ensure that customer problems are resolved in a timely manner
Other disk protection options

• File-level encryption
  – HP has nothing in plan for file-level encryption at this point

• Compensating controls
  – Convince your auditors that the combination of appropriate policies and procedures and appropriate Safeguard controls is adequate
    • This is currently working for some customers

• Does the current roadmap (volume-level encryption plus database column-level encryption) meet your requirements?
Tape protection

- Our partners are providing tape encryption for current-generation tapes
  - TSI offers an encryption option (TE2000)
    - Supports FC and SCSI connectivity
  - Both HP VTS and TSI offer an encryption option for virtual tape servers
  - Software-only options are available from some of our security partners
- Next generation LTO4 tapes have bulk encryption capabilities
- HP will offer LTO4 tape support
  - The roadmap is under construction
HP Virtual Tape Server

- Strong Encryption
  - Embedded encryption module
    - Compression prior to Encryption
    - AES-256 encryption algorithm
  - Configured from within HP VTS GUI
    - Role-based access supported
  - Auditable log of encrypted operations
    - Can save or print log files for review

- Robust Key Management
  - Embedded key management module
    - Public-key encryption and authentication
  - Complete Key Lifecycle Management
    - Generation, distribution, storage & recovery
    - Random symmetric key generation
  - Complete Key Security
    - Separation of encrypted data from keys
    - Individual authorization per symmetric key

- Available soon
Key management

• Encrypted data is protected if and only if encryption keys are protected
  – The keys themselves must be adequately secured
  – Data and keys must outlast specific products, 5-10 years or more
• Customers want a single, consistent key management architecture
  – Seamless, interoperable, automated
    • Point/proprietary key management solutions without interoperability create an unmanageable mix
  – Stable, supported, standards-based
  – From a trusted vendor

*HP is working with industry partners through its Secure Advantage initiative to make this vision a reality*
Agenda

• Security requirements and strategy
• What’s new and what’s coming
• Network security
• Data at rest encryption
• Safeguard
Safeguard Version 3 New Features

• V3R1: Improved password encryption
  – H06.06, G06.29
• V3R2: Support for 64 character passwords
  – H06.08, G06.31
• V3R3: Support for pass phrases and password quality attributes
  – H06.09, G06.31
V3R1: Improved password encryption
G06.29, H06.06

- User/Alias passwords can be encrypted using HMAC with SHA256 algorithm
  - Check fallback considerations before enabling HMAC
- Existing Safeguard configuration defaults modified:
  - PASSWORD-ENCRYPT ON
  - PASSWORD-MINIMUM-LENGTH 6
  - PROMPTPASSWORD BLIND
  - PASSWORD-ALGORITHM DES
- New utility, PWCONFIG, available for altering password configuration when Safeguard is not up
V3R2: Longer Passwords
H06.08, G06.31

• Safeguard supports user/alias passwords of up to 64 characters
  – Available only when HMAC256 algorithm is enabled
  – Maximum password length is still 8 if using CLEAR or DES
• Longer passwords are a configuration option
  – Default remains at 8
  – Can set a maximum length of less than 64
  – Can set a minimum length > 8 when long passwords are enabled
• USER_AUTHENTICATE_ supports longer passwords, but VERIFYUSER does not
• There are fallback considerations
V3R3: Password Quality
G06.31, H06.09

- Supports optional quality attributes when creating new passwords:
  - PASSWORD-UPPERCASE-REQUIRED
    ON - Specifies that at least one uppercase character is required
  - PASSWORD-LOWERCASE-REQUIRED
    ON - Specifies that at least one lowercase character is required
  - PASSWORD-NUMERIC-REQUIRED
    ON - Specifies that at least one numeric character is required
  - PASSWORD-SPECIALCHAR-REQUIRED
    ON - Specifies that at least one special character is required
- Configurable through either Safeguard or PWCONFIG
V3R3: Password Quality

G06.31, H06.09

- Supports an “M of N required” optional quality governing attribute
  - Example: to require at least 2 of upper case, lower case, and numeric, specify:
    
    | Configuration | Value |
    |---------------|-------|
    | PASSWORD-UPPERCASE-REQUIRED | ON    |
    | PASSWORD-LOWERCASE-REQUIRED  | ON    |
    | PASSWORD-NUMERIC-REQUIRED   | ON    |
    | PASSWORD-MIN-QUALITY-REQUIRED | 2    |

- Supports embedded blank spaces in passwords (pass phrases)
  - Configuration option

- Password quality attributes and embedded blank spaces can be enabled only when HMAC256 and long passwords are enabled
V3R3: Password Quality
G06.31, H06.09

- USER_AUTHENTICATE_ accepts embedded spaces in the password provided in the inputtext parameter
- A new option bit needs to be set if supplying a new password that contains embedded blanks
- VERIFYUSER does not accept embedded spaces
V3R3: GROUP information access policy

• Problem
  – Group record information was visible to any user on the system
  – Perceived by customers as a security hole, and causing them issues in compliance audits

• Solution
  – The INFO command on GROUPs can now be issued only by the group owner, owner’s group manager and SUPER.SUPER
Safeguard Version 4 released new features

- V4R1: Reset failed logon counts
  - H06.10
- V4R2: Sanctioned privileged logon
  - H06.11
- V4R3: TACL logoff/exit audit, audit pool CLEARONPURGE option

- There will be a Version 4 release for G06.32
  - Exact content TBD but at least through V4R3
V4R1: Reset Failed Logon Statistics
H06.10

- The values of user attributes STATIC FAILED LOGON COUNT and LAST-UNSUCCESSFUL-ATTEMPT can now be reset
  - Value of STATIC FAILED LOGON COUNT reset to 0
  - Value of LAST-UNSUCCESSFUL-ATTEMPT reset to *NONE*
- New command attribute for ALTER USER:
  - alter user <User/Alias name>,RESET-STATIC-FAILED-LOGON-COUNT

- INFO USER command displays the timestamp when the RESET-STATIC-FAILED-LOGON-COUNT was performed.
V4R1: Performance Improvement
H06.10

• About 8% performance improvement for SAFECOM user management commands that include wild card characters:
  – INFO USER
  – ALTER USER
  – DELETE USER

• Improvement in performance was observed to be more than 8% when SPI is directly used instead of SAFECOM
V4R2: Sanctioned Privileged Logon
H06.11

• Ability to authenticate any user or alias in the system through Safeguard using USER_AUTHENTICATE() Guardian Procedure call without password checks or delays on authentication failures but with appropriate audit generation
  • Only supported if SUPER.SUPER has set the Safeguard PRIV-LOGON disk attribute for the process’s object file
• If set, this attribute is in effect even when
  • The SAFECOM global attribute PASSWORD-REQUIRED is set to ON, or
  • The USER_AUTHENTICATE_() PASSWORD_REQUIRED bit is set to ON
V4R3: Audit enhancements
H06.12

- Generation of LOGOFF audit records for TACL (not optional)
  - Applies also to TACL EXIT command
- Configurable AUDITCLEARONPURGE attribute for audit files
  - SAFECOM ADD/ALTER/INFO AUDIT POOL commands to set/reset/display the AUDITCLEARONPURGE attribute for the newly-created audit files
Safeguard and standard security further enhancements

- Planning for releases beyond H06.12 and G06.31 is underway
- We have a long list of candidate RFEs
  - See the next slide for RFEs currently prioritized relatively high
Accepted Safeguard RFEs for 2008: audit/forensics

- More granular control over auditing in the OSS environment
- File system error information
- Variable-length audit records for free-text fields
- Object record description fields for volume, subvolume, diskfile, process
- User creation timestamp
- Include LAST-LOGON and LAST-MODIFIED for INFO ALIAS
- IP address in LOGON records (tentative)

Disclaimer: Future product plans, dates, and functionality are subject to change without notice.
Accepted Safeguard RFEs for 2008: other

- USER_GETINFO_ performance improvement
- Ability to reprimary $ZSMP
- No display of passwords on the screen for ADD USER and ALTER USER
- Include object file name in process creation message to SEEP
- PASSWORD program enhancements

Disclaimer: Future product plans, dates, and functionality are subject to change without notice.
Please send us your feedback

• Karen Copeland – security product manager
  – Karen.Copeland@hp.com
• Wendy Bartlett – security technical lead
  – Wendy.Bartlett@hp.com
End of main presentation