Windows Vista Security

Windows Vista introduced numerous security and defense-in-depth features:

- Build based on SDL
- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)
- Protected Processes
- Authentication Infrastructure enhancements (incl. smart cards)
- User Account Control (UAC)
- Full Volume Encryption (BitLocker)
- Secure Boot (BitLocker/TPM)
- Code Integrity, Code Signing, Crypto enhancements
- Software Restriction Policy (SRP)
- Advanced Audit Policies
- and much more.....
Windows 7 Security

Builds upon the proven security lineage of Vista, retaining the multiple layers of defense
Responds to requests from IT professionals to make the security features more usable and manageable
Delivers new security features to help IT professionals more effectively address the continually evolving threat landscape
Engineering Excellence

Windows Development Process

- Security Development Lifecycle (SDL)
  - Periodic mandatory security training
  - Assignment of security advisors for *all* components
  - Threat modeling as part of design phase
  - Security reviews and testing built into the schedule
  - Security metrics for product teams
- Common Criteria (CC) Certification compliance is one of major goals
Data Encryption Enhancements

**Windows Vista BitLocker**
- Full volume encryption for system disks
- Integrity checking of early boot components

**Windows 7 Enhancements**
- BitLocker deployment improvements
- Key Management Improvements (Data Recovery Agent)
- Support for FAT and ExFAT formatted volumes
- BitLocker To Go – policy-enforced data protection for USB and portable drives

**Customer Value**
- Easier to configure and deploy BitLocker
- Roam protected data between work and home
- Share protected data with co-workers, clients, partners, etc.
- Improved compliance and data security
AppLocker™ - Software Lockdown

Software Restriction Policies – XP / Vista
- Hash-based rules for allow-to-run applications
- Hash rules too fragile for IT to manage and keep up to date

Windows 7 Capabilities
- Simple, powerful policies for which applications can run
- Rule sets for executables, scripts, and Windows Installer
- Publisher rules may utilize product name, file name & file version
- Rules can have built-in exceptions, simplifying rule sets
- Policy export/import capabilities allows for easier administration

Improved Legal and Regulatory Compliance
- Enables application standardization within an organization without increasing TCO
- Increase security to safeguard against data and privacy loss
- Support compliance enforcement
AppLocker™ Example Rules

Publisher

• “Allow Art-Dept to run Adobe Photoshop 10.2 or greater”

Publisher w/ Exception

• “Allow Everyone to run Windows OS7 except Regedt32 etc

Hash

• “Allow unsigned per-user app with hash XYZ”

Path

• “Allow Everyone to run scripts from \\scriptserver\share”
UAC Improvements

Windows Vista User Account Control

- Make the system work well for standard users
- Common user tasks redesigned to work for Standard User
- All users run as Standard User by default even when you log on as admin
- Administrators use full privilege only for administrative tasks or applications
- User provides explicit consent before using elevated privilege

Windows 7

- Reduce the number of OS applications and tasks that require elevation
- Refactor applications into elevated/non-elevated pieces
- User control over UAC settings – similar to IE “zones”

Customer Value

- Users can do even more as a standard user
- Administrators will see fewer UAC Elevation Prompts
Advanced Audit Policy Creation & Reporting

**Windows Vista**
- All new in Windows Vista
- Fine grain support for multiple audit categories

**Windows 7 Enhancements**
- Group Policy support for fine grain audit capabilities
- Include why a user has access to an object
  - List of ACE or privileges that resulted in gaining access
- Capture the reason why a user received access denied
  - ACL, integrity level or lack of permission
- Simplified management of “track all changes made by group X”
  - Global System Access Control Lists

**Customer Value**
- Demonstrate why a person has access to specific information
- Easier to manage resulting in lower TCO
Object Access Reason Information

Access Due To Ownership
Access Check Results:
ReadData: Granted by Ownership
Access Due To Multiple Permissions
Access Check Results:
ReadData: Granted by D: (A;;RPWPCCDCLCSWRCWDWO;A;;REDMOND\Everyone)
ReadAttributes: Granted by D: (A;;RPWPCCDCLCSWRCWDWO;A;;REDMOND\john)
Access Due To Privilege
Access Check Results:
ReadData: Granted by Privilege: SeBackupPrivilege.
ReadAttributes: Granted by Privilege: SeBackupPrivilege.
Access Due To Mixed Reasons
Access Check Results:
ReadAttributes: Granted by Privilege: SeBackupPrivilege.
ReadData: Granted by D: (A;;RPWPCCDCLCSWRCWDWO;A;;REDMOND\Everyone)
Access Denied Due To No ACEs
Access Check Results:
ReadData: Denied by No ACEs granting access to this resource
Access Denied Due to Access Check Failure
Access Check Results:
ReadData: Granted by D: (A;;RPWPCCDCLCSWRCWDWO;A;;REDMOND\Everyone)
Denied by D: (D;;RPWPCCDCLCSWRCWDWO;A;;REDMOND\Everyone)
Cryptography

- **Support for NSA Suite B**
  - **Encryption**: AES
    - FIPS 197 (with keys sizes of 128 and 256 bits)
  - **Digital Signature**: Elliptic Curve Digital Signature Algorithm
    - FIPS 186-2 (using the curves with 256 and 384-bit prime moduli)
  - **Key Exchange**: Elliptic Curve Diffie-Hellman or Elliptic Curve MQV
    - Draft NIST Publication 800-56 (curves with 256 and 384-bit prime moduli)
  - **Hashing**: Secure Hash Algorithm
    - FIPS 180-2 (using SHA-256 and SHA-384)

- **Improved Pseudo Random Number Generator (PRNG)**
Smartcards

Windows 7 Focus: Remove deployment blockers, improve usability and performance

- Smart card Plug-and-Play
  - Windows Update and SUS based driver installation
  - Pre-Logon driver installation
  - Non-Admin based driver installation
- Smart card class mini-driver
  - NIST SP800-73-1 (PIV) support
  - INCITS GICS (Butterfly) support
- Windows 7 Smartcard Framework Improvements
  - Improved support for Biometric Based Smart card unlock
  - Improved certification program
  - New APIs enabling Secure Key Injection
- Improved platform support for “Smart card require” scenarios
Public Key Infrastructure

- New web services based protocol for certificate enrollment
- Cross-forest certificate enrollment
- Improved support for NAP scenarios
- Improved user experience for certificate selection
- Support for Transport Layer Security (TLS) 1.2
- General architectural and performance improvements
- Improved support for certificate and smart card logon scenarios
Biometrics

Windows Vista

- No common biometrics framework
- Varied management and user experience with OEM/ISV bio components

Windows 7 Enhancements

- New platform/framework for Biometric Devices Drivers
- Partners bringing additional enterprise scenarios
- New driver model and basis for future certification program
- Integrated User Experience - Windows Logon, Local and Domain, UAC
- Enterprise Management: Disable Biometric via Group Policy, Allow use for applications but not domain logon
Kerberos

- ECC-based Smartcard domain logon
- Authentication mechanism (i.e. Smart card) addition to the token
- Access policy based on authentication mechanism
- Channel-binding token (CBT) – integration with the policy
- Forest search with short names
- Configurable selection of the encryption algorithm
- New account mapping for S4U