Windows Vista

All Staff Breakout Session
June 28, 2006

Windows Vista

Windows Vista Task Force

- Group formed to assess Vista impact on PSU
  - Co-chair: Connie Welch & Al Williams
  - Participants from all ITS Operating Units
  - Meeting monthly since March 1
  - Several Vista Beta subscribers – testing every build
  - Several MSDN subscribers – testing customer technology previews (ctp)
- Logging experiences on a wiki
- Have initiated a communication plan
  - Online updates: http://its.psu.edu/headsup/VistaOS/
  - Will publish in ITS news distributions
  - Will participate in ITS events

Windows Vista

- A replacement for Windows XP
- A long time coming (will be 5 years in October)
- Lacking in many of the promised features
- Not going to be available on a PC you buy in 2006
- Not a replacement for Server 2003
  - Windows Longhorn Server predicted for 2007 or 2008
- Very graphically intense GUI
- Has confusing hardware requirements

A single product with 5 versions

Differentiated Feature	Home Basic	Home Premium	Business	Enterprise	Ultimate
Security & Perf. Enhancements	✓	✓	✓	✓	✓
Search & Organize	✓	✓	✓	✓	✓
P2P Meeting Space	Join Only	✓	✓	✓	✓
Scheduled & Networked Backup		✓	✓	✓	✓
Aero glass, animations and visuals		✓	✓	✓	✓
Media Center (incl. extender)		✓			✓
HD MovieMaker & DVD authoring		✓			✓
Network Projection		✓	✓	✓	✓
Mobility (Tablet, Aux Display)		✓	✓	✓	✓
Encrypted File System			✓	✓	✓
Remote Desktop			✓	✓	✓
Web Server			✓	✓	✓
Fax & scanning utility			✓	✓	✓
Domain Join			✓	✓	✓
Offline folders			✓	✓	✓
Group Policy			✓	✓	✓
SUA (Unix Subsystem)				✓	✓
BitLocker (Full Volume Encryption)				✓	✓
Virtual PC Express				✓*	✓*
MUI -All Languages				✓*	✓*
Windows Ultimate Extras					✓*

***Available separately for free for these SKUs only**

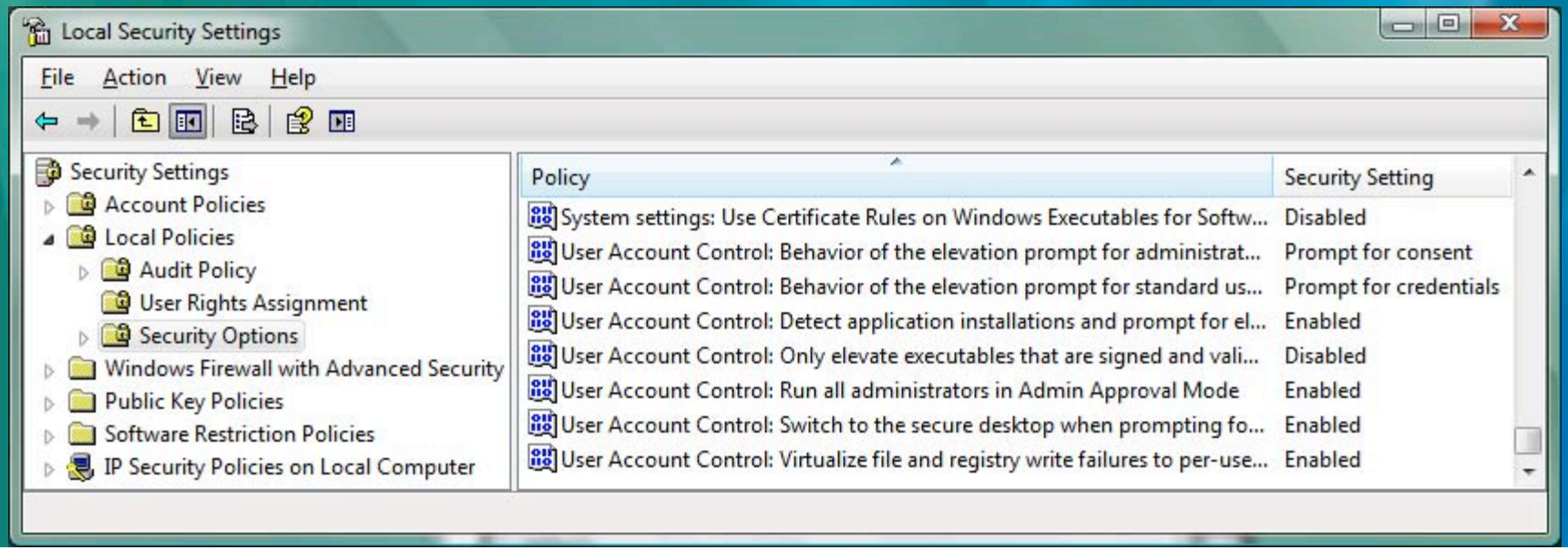
All features are subject to change. Confidential to ITS

New Features

- User Account Control Changes
  - All users run in the context of a standard user
  - Standard users can do more
  - Registry and file system Virtualization
- Bidirectional firewall
- BitLocker™
  - What is it?
  - Who should use it?
  - Recovery/Forensics
  - Secure Decommissioning
- User Interface Changes

User Account Control

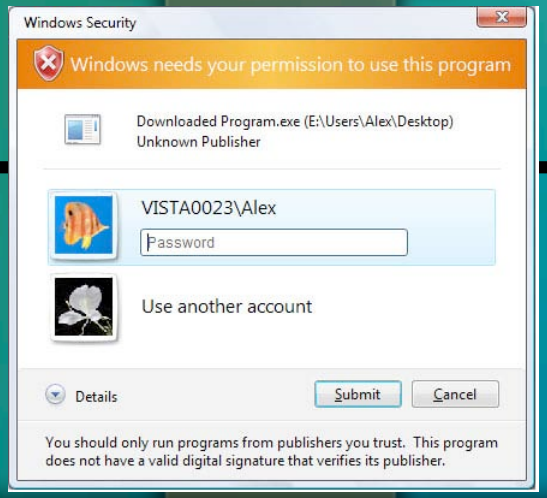
- Many options are configured via Local Security MMC
  - Elevation prompt for admins – consent/credentials/no prompt
  - Elevation prompt for standard users – credentials/no prompt
  - Installer detection on/off
  - Admin approval mode on/off
  - Only allow signed/trusted admin apps on/off
  - File/registry virtualization on/off



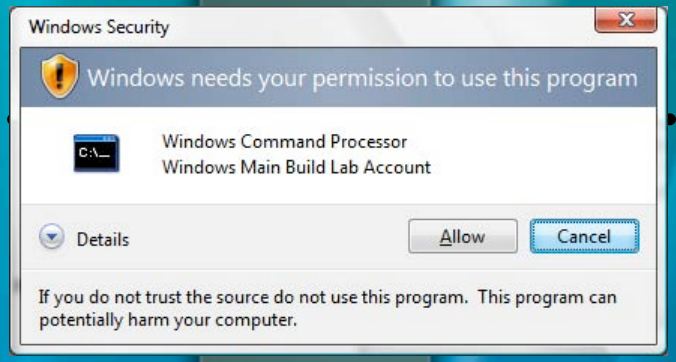
Elevation Model

Windows Vista

Administrator Privileges



Ways to Request Elevation
Application marking
Setup detection
Compatibility fix (shim)
Compatibility assistant
Run as administrator



Standard User Privileges (Default)

Standard User Account

Administrator Account

All features are subject to change. Confidential to ITS

Standard Users Can Do More

- View system clock and calendar
- Change time zone
- Configure secure wireless (WEP/WPA) connection
- Change power management settings
- Create and configure a Virtual Private Network connection
- Add printers and other devices that have the required drivers installed or allowed by group policy
- Disk defragmentation is a scheduled background process

- Shield icons mark what actions require administrative users

Registry and Personal Data Virtualization

- Virtualization defaults to
  On for all standard users
  Off for administrators
- Registry Virtualization
  - Writes: Redirect per-machine file and registry writes to equivalent per-user locations
  - Reads: Try the per-user location first, then the global location
- Data Redirection
  - Legacy applications write to administrator locations
    - HLKM\Software
    - %SystemDrive%\Program Files, etc
  - Redirection removes need for elevation
    - Writes to HKLM go to HKCU redirected store
      - HKU->(user SID)_classes->VirtualStore
    - Writes to system directories redirected to per-user store
      - (%localappdata%\virtualstore)

All features are subject to change. Confidential to ITS

Vista Firewall

	Windows XP SP2	Windows Vista
Direction	Inbound	Inbound, outbound
Default action	Block	Configurable for direction
Packet types	TCP, UDP, some ICMP	All
Rule types	Application, global ports, ICMP types	Multiple conditions from basic five-tuple to IPsec metadata
Rule actions	Block	Block, allow, bypass; with rule merge logic
UI and tools	Control Panel, netsh	C-Panel, more netsh, MMC
APIs	Public COM, private C	More COM to expose rules, more C to expose features
Remote management	none	Via hardened RPC interface
Group policy	ADM file	MMC, netsh
Terminology	Exceptions; profiles	Rules; categories=profiles

All features are subject to change. Confidential to ITS

Trusted Platform Module (TPM)

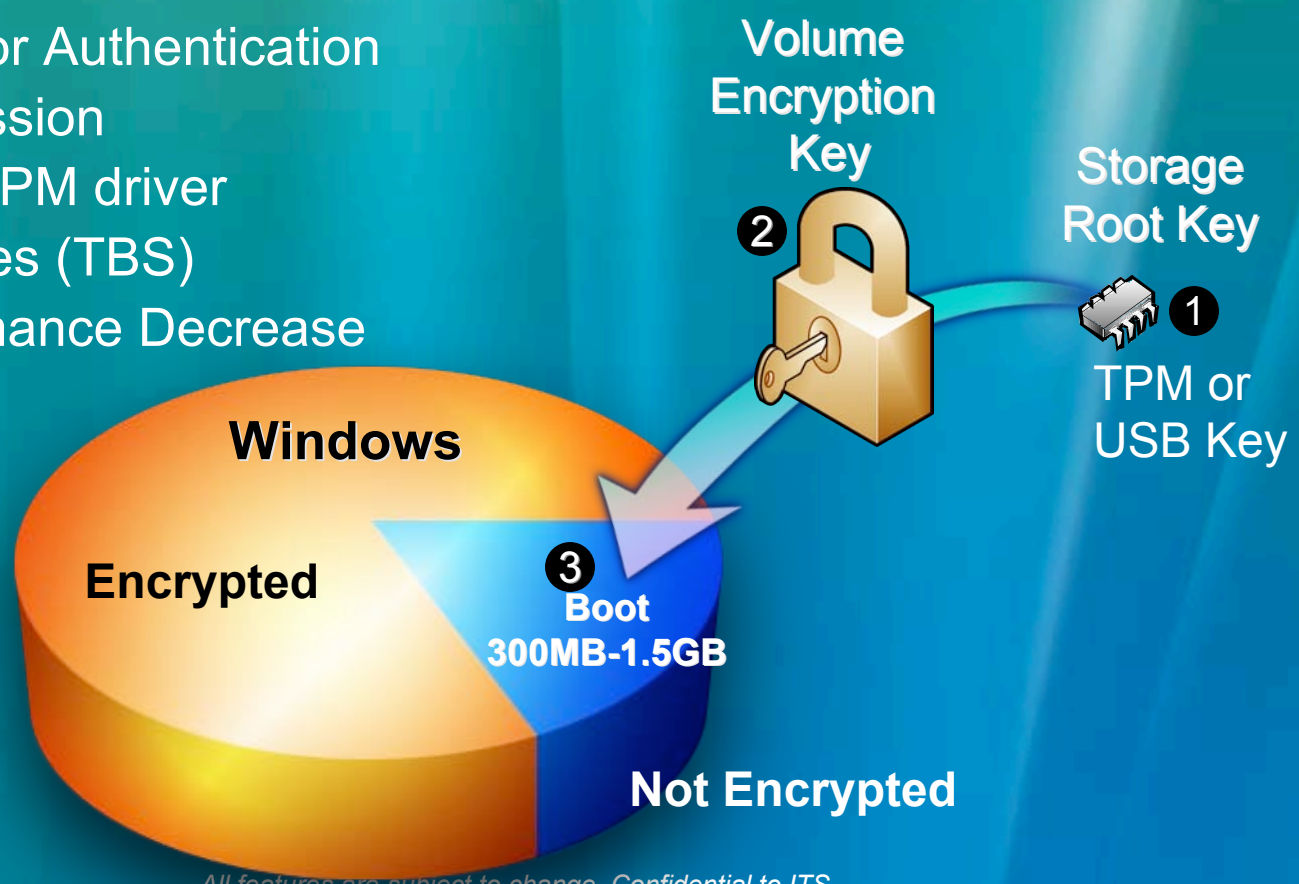
Smartcard-like module on the motherboard

TPM 1.2 offers the following features:

- Performs cryptographic functions
  - RSA, SHA-1, RNG
  - Meets encryption export requirements
- Can create, store and manage keys
- Holds Platform Measurements
- Anchors chain of trust for keys and credentials
- Protects itself against attacks

BitLocker™ Features Overview

- BitLocker Drive Encryption – Windows Volume
  - AES-128 or AES-256
- Integrity Checking of Windows Boot Files
- Pre-OS Multi-factor Authentication
- Secure Decommission
- Single Microsoft TPM driver
- TPM Base Services (TBS)
- 0% - 15% Performance Decrease
- 4 Implementation
  - USB
  - TPM
  - TPM + Pin
  - TPM + USB



Who's BitLocker™ for?

"If I wrote Policy!"

- **REQUIRED:**
  - Anyone with Domain/Enterprise Administrator Rights
  - Anyone who touches Confidential Data
  - Anyone using a machine provided for the purpose of telecommuting
- **STRONGLY RECOMMENDED:**
  - Any workstation storing confidential information
  - Any laptop primarily used by staff who access confidential information
  - Any system (specifically laptops) containing test scores, course rosters or other information that may identify individual students
- **OPTIONAL:**
  - The desktops and laptops of anyone performing an IT function on campus

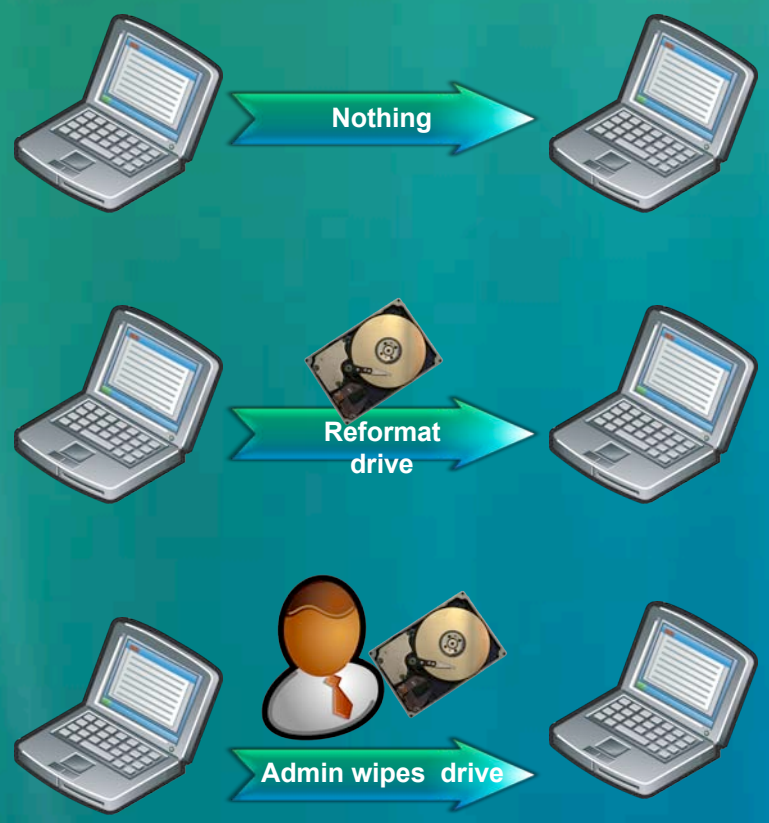
Confidential Data: Student Records, SSN's or PSU-ID, HR / Salary Information, etc.

Recovery/Forensics

- Recovery Keys
  - Can be stored at a specified file locations (USB Key/File Server)
    - Cannot be stored on the same USB key used to start a machine
  - Can be automatically stored in AD (Windows 2003 SP1 or higher AD Schema Required)
  - Group Policies can control all these settings
- Forensics
  - Everything is encrypted with AES-128 or AES-256
  - You'll need the recovery keys
  - Don't implement this technology without having a good recovery key strategy!

Secure Decommissioning

Normal Vs. Secure Decommission



User Interface Changes

- Vista will be confusing because of new GUI
  - Everything looks and feels like you are running Internet Explorer
  - The menu is missing
  - Familiar things like File Explorer, Network Center and Control Panel are sufficiently different to be disconcerting
  - Mouse actions are sometimes not clear as to when mouse-over does something vs mouse hover vs single click vs double click
- How fast the system functions is directly proportional to how glitzy you want the UI to look
  - The more glitz, the more confusing at first
- Glitzy UI features can be turned off for less powerful machines
  - We'll document this in more detail

Some Things Don't Work Yet

- Cisco VPN
- Symantec Anti-Virus
- Wireless 802.**
  - Can access unsecured
  - Some WEP works
  - Does not support 802.1x EAP-TTLS

Remember - it's still Beta Code

Public Beta Available

- Windows Vista Beta 2 has been released.
- The Public Beta is available for everyone to download and use
  - http://www.microsoft.com/windowsvista/getready

Vista Reference Sites

- Microsoft Marketing Site:
  - http://www.microsoft.com/windowsvista/
- Vista Versions :
  - http://www.microsoft.com/windowsvista/versions/
- Interesting Alternate Opinion (Paul Thurrott):
  - http://www.winsupersite.com/reviews/
- Where Vista Fails (Paul Thurrott):
  - http://www.winsupersite.com/reviews/winvista_5308_05.asp

All features are subject to change. Confidential to ITS

Let’s Take a Tour