Yegor Hanov
EECS710, Fall 2012
Homework Assignment 10/23/12

Assignment 2: Core Windows 7 Services

I reviewed the list of active services running on my laptop during normal operation. The list [1] contains 94 services covering a wide variety of functionality for core OS operation, networking functions, security, and a number of services installed by various applications and are not part of the default Windows set. For example, the following services all belong to different third party applications that I installed - Apple Mobile Device, Bonjour Service, Cam Monitor, iPod Service, Office Software Protection Platform, VAIO Care Performance Service, VAIO Event Service, etc.

According to articles [2,3,4] that I used to research the functionality of these services, I can get the list trimmed down to 38 services without sacrificing wireless connection services, security services or the firewall. Considering that I use a laptop computer and majority of my activities require Internet access, I would consider network and security services essential to my needs.

The author of article [2] goes on to suggest trimming the list down to 28 services by shutting down wireless and security services, which would work for a computer that is a standalone machine and does not require access to a network or the Internet.

Windows 7 Core Services:

Application Experience	This service checks a Microsoft maintained database for known problems with popular programs and automatically enables workarounds, either at first installation (using UAC) or at application launch.
Application Information	This new service for Windows Vista works in conjunction with User Account Control and the User Profile Service to limit access to applications desiring full administrator rights.
Background Intelligent Transfer	This service is used to transfer asynchronous data via HTTP 1.1 servers. BITS “continues” a download when you log back in after you log off or shutdown the system during a download. You may require this service for some, Windows Live Messenger, Windows Media Player or future .NET or Live functions.
Base Filtering Engine	The Base Filtering Engine (BFE) is a service that manages firewall and Internet Protocol security (IPsec) policies and implements user mode filtering. Stopping or disabling the BFE service will significantly reduce the security of the system. It will also result in unpredictable behavior in IPsec management and firewall applications.
CNG Key Isolation	The CNG key isolation service is hosted in the LSA process. The service provides key process

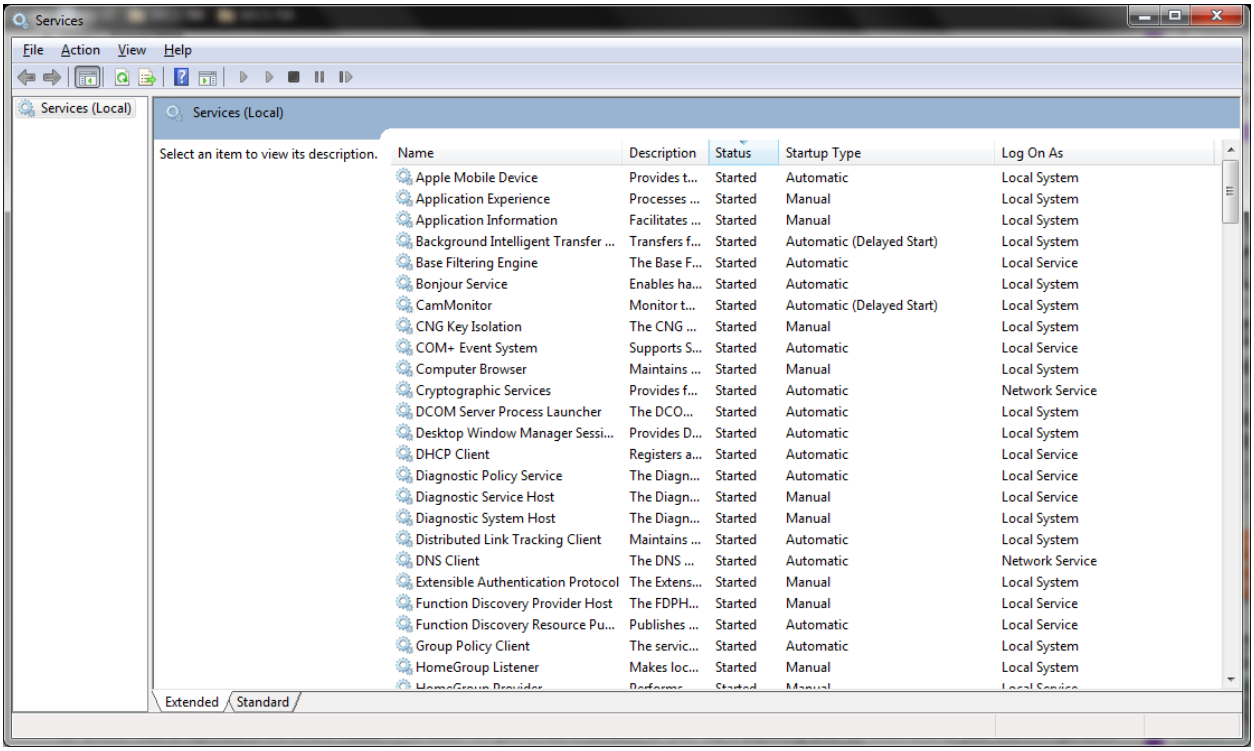
	isolation to private keys and associated cryptographic operations as required by the Common Criteria. The service stores and uses long-lived keys in a secure process complying with Common Criteria requirements.
COM+ Event System	Supports System Event Notification Service (SENS), which provides automatic distribution of events to subscribing Component Object Model (COM) components. If the service is stopped, SENS will close and will not be able to provide logon and logoff notifications. If this service is disabled, any services that explicitly depend on it will fail to start.
Computer Browser	Maintains an updated list of computers on the network and supplies this list to computers designated as browsers. If this service is stopped, this list will not be updated or maintained. If this service is disabled, any services that explicitly depend on it will fail to start.
Cryptographic Services	Provides three management services: Catalog Database Service, which confirms the signatures of Windows files and allows new programs to be installed; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from this computer; and Automatic Root Certificate Update Service, which retrieves root certificates from Windows Update and enable scenarios such as SSL. If this service is stopped, these management services will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.
DCOM Server Process Launcher	The DCOMLAUNCH service launches COM and DCOM servers in response to object activation requests. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the DCOMLAUNCH service running.
DHCP Client	Registers and updates IP addresses and DNS records for this computer. If this service is stopped, this computer will not receive dynamic IP addresses and DNS updates. If this service is disabled, any services that explicitly depend on it will fail to start.
DNS Client	The DNS Client service (dnscache) caches Domain Name System (DNS) names and registers the full computer name for this computer. If the service is stopped, DNS names will continue to be resolved. However, the results of DNS name queries will not be cached and the computer's name will not be registered. If the service is disabled, any services that explicitly

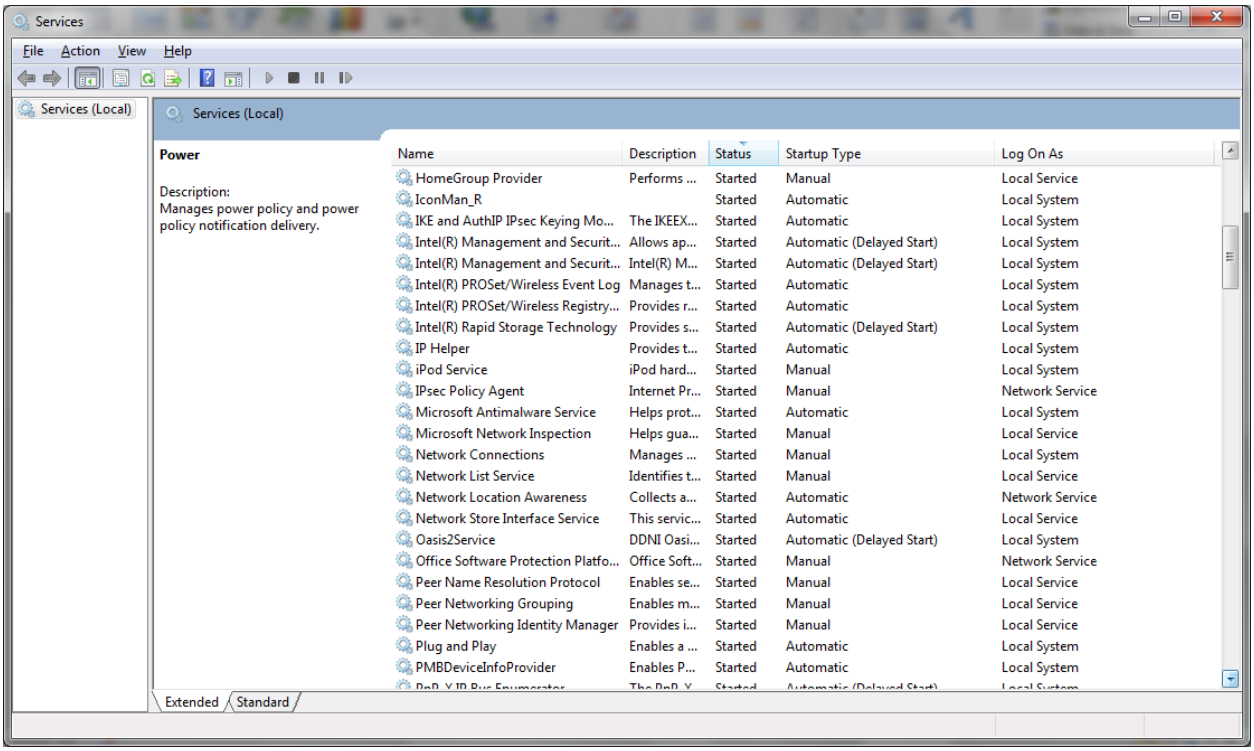
	depend on it will fail to start.
Group Policy Client	The service is responsible for applying settings configured by administrators for the computer and users through the Group Policy component. If the service is stopped or disabled, the settings will not be applied and applications and components will not be manageable through Group Policy. Any components or applications that depend on the Group Policy component might not be functional if the service is stopped or disabled.
Multimedia Class Scheduler	Enables relative prioritization of work based on system-wide task priorities. This is intended mainly for multimedia applications. If this service is stopped, individual tasks resort to their default priority.
Network Location Awareness	Collects and stores configuration information for the network and notifies programs when this information is modified. If this service is stopped, configuration information might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Network Store Interface Service	This service delivers network notifications (e.g. interface addition/deleting etc) to user mode clients. Stopping this service will cause loss of network connectivity. If this service is disabled, any other services that explicitly depend on this service will fail to start.
Plug and Play	Enables a computer to recognize and adapt to hardware changes with little or no user input. Stopping or disabling this service will result in system instability.
Power	New to Windows 7. Manages power policy and power policy notification delivery.
Remote Procedure Call	The RPCSS service is the Service Control Manager for COM and DCOM servers. It performs object activations requests, object exporter resolutions and distributed garbage collection for COM and DCOM servers. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the RPCSS service running.
RPC Endpoint Mapper	Resolves RPC interfaces identifiers to transport endpoints. If this service is stopped or disabled, programs using Remote Procedure Call (RPC) services will not function properly.
Security Accounts Manager	The startup of this service signals other services that the Security Accounts Manager (SAM) is ready to accept requests. Disabling this service will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to fail to start

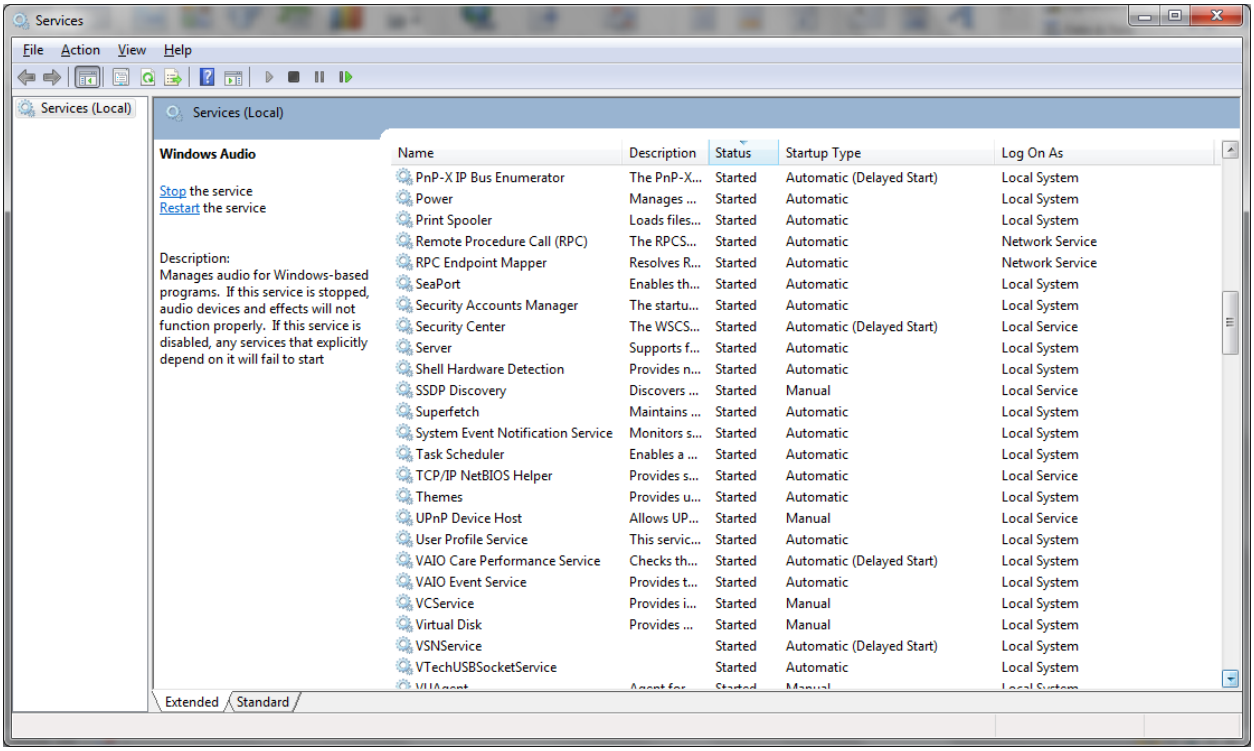
	correctly. This service should not be disabled.
Security Center	The WSCSVC (Windows Security Center) service monitors and reports security health settings on the computer. The health settings include firewall (on/off), antivirus (on/off/out of date), antispyware (on/off/out of date), Windows Update (automatically/manually download and install updates), User Account Control (on/off), and Internet settings (recommended/not recommended). The service provides COM APIs for independent software vendors to register and record the state of their products to the Security Center service.
Shell Hardware Detection	Provides notifications for AutoPlay hardware events.
Software Protection	Enables the download, installation and enforcement of digital licenses for Windows and Windows applications. If the service is disabled, the operating system and licensed applications may run in a notification mode. It is strongly recommended that you not disable the Software Protection service.
SSDP Discovery	Discovers networked devices and services that use the SSDP discovery protocol, such as UPnP devices. Also announces SSDP devices and services running on the local computer. If this service is stopped, SSDP-based devices will not be discovered. If this service is disabled, any services that explicitly depend on it will fail to start.
System Event Notification Service	Monitors system events and notifies subscribers to COM+ Event System of these events.
Task Scheduler	Enables a user to configure and schedule automated tasks on this computer. The service also hosts multiple Windows system-critical tasks. If this service is stopped or disabled, these tasks will not be run at their scheduled times. If this service is disabled, any services that explicitly depend on it will fail to start.
TCP/IP NetBIOS Helper	Provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution for clients on the network, therefore enabling users to share files, print, and log on to the network. If this service is stopped, these functions might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
User Profile Service	This service is responsible for loading and unloading user profiles. If this service is stopped or disabled, users will no longer be able to successfully logon or logoff, applications may have problems getting to users' data, and components registered to receive profile event

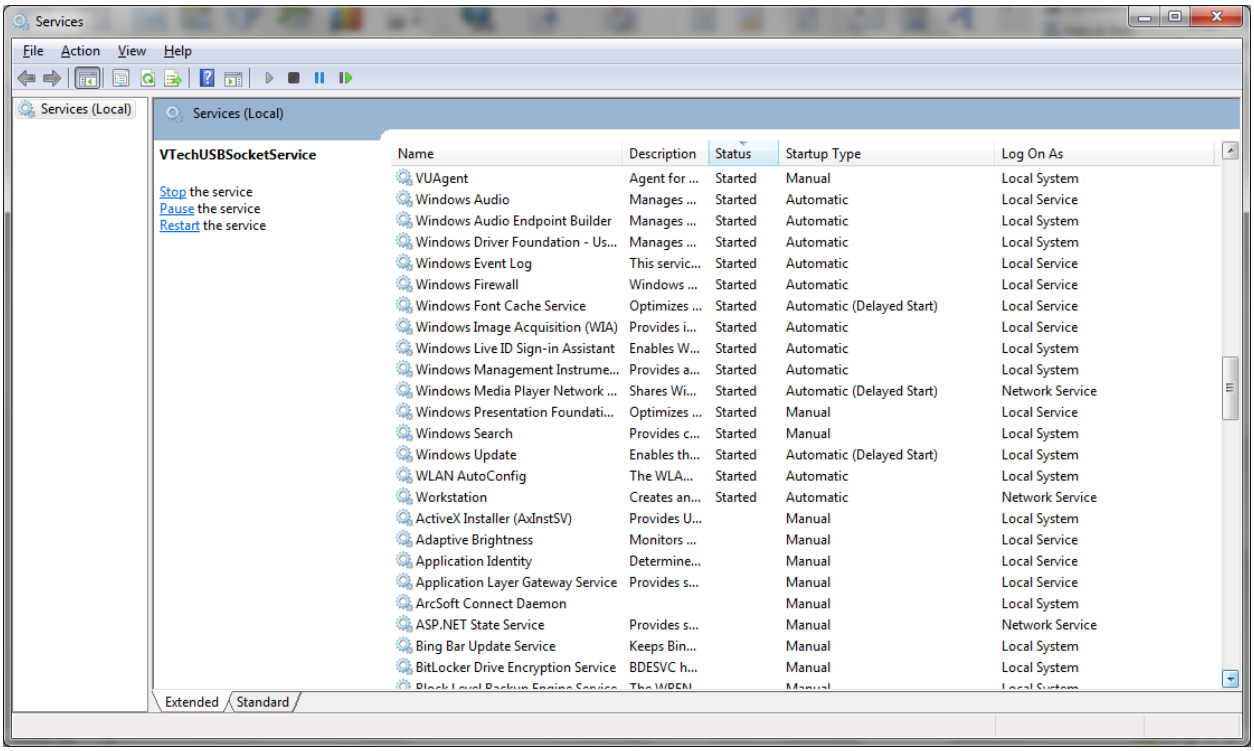
	notifications will not receive them.
Windows Defender	Protection against spyware and potentially unwanted software.
Windows Event Collector	This service manages persistent subscriptions to events from remote sources that support WS-Management protocol. This includes Windows Vista event logs, hardware and IPMI-enabled event sources. The service stores forwarded events in a local Event Log. If this service is stopped or disabled event subscriptions cannot be created and forwarded events cannot be accepted.
Windows Event Log	This service manages events and event logs. It supports logging events, querying events, subscribing to events, archiving event logs, and managing event metadata. It can display events in both XML and plain text format. Stopping this service may compromise security and reliability of the system.
Windows Firewall	Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.
Windows Management Instrumentation	Provides a common interface and object model to access management information about operating system, devices, applications and services. If this service is stopped, most Windows-based software will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.
Windows Update	Enables the detection, download, and installation of updates for Windows and other programs. If this service is disabled, users of this computer will not be able to use Windows Update or its automatic updating feature, and programs will not be able to use the Windows Update Agent (WUA) API.
Workstation	Creates and maintains client network connections to remote servers using the SMB protocol. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

[1]


Services
File Action View Help
Services (Local)
Services (Local)
Select an item to view its description.
Name Description Status Startup Type Log On As
Apple Mobile Device Provides t... Started Automatic Local System
Application Experience Processes ... Started Manual Local System
Application Information Facilitates ... Started Manual Local System
Background Intelligent Transfer ... Transfers f... Started Automatic (Delayed Start) Local System
Base Filtering Engine The Base F... Started Automatic Local Service
Bonjour Service Enables ha... Started Automatic Local System
CamMonitor Monitor t... Started Automatic (Delayed Start) Local System
CNG Key Isolation The CNG ... Started Manual Local System
COM+ Event System Supports S... Started Automatic Local Service
Computer Browser Maintains ... Started Manual Local System
Cryptographic Services Provides f... Started Automatic Network Service
DCOM Server Process Launcher The DCO... Started Automatic Local System
Desktop Window Manager Sessi... Provides D... Started Automatic Local System
DHCP Client Registers a... Started Automatic Local Service
Diagnostic Policy Service The Diagn... Started Automatic Local Service
Diagnostic Service Host The Diagn... Started Manual Local Service
Diagnostic System Host The Diagn... Started Manual Local System
Distributed Link Tracking Client Maintains ... Started Automatic Local System
DNS Client The DNS ... Started Automatic Network Service
Extensible Authentication Protocol The Extens... Started Manual Local System
Function Discovery Provider Host The FDPH... Started Manual Local Service
Function Discovery Resource Pu... Publishes ... Started Automatic Local Service
Group Policy Client The servic... Started Automatic Local System
HomeGroup Listener Makes loc... Started Manual Local System
Extended Standard


Services
File Action View Help
Services (Local)
Services (Local)
Power
Description:
Manages power policy and power policy notification delivery.
Name Description Status Startup Type Log On As
HomeGroup Provider Performs ... Started Manual Local Service
IconMan_R Started Automatic Local System
IKE and AuthIP IPsec Keying Mo... The IKEEX... Started Automatic Local System
Intel(R) Management and Securit... Allows ap... Started Automatic (Delayed Start) Local System
Intel(R) Management and Securit... Intel(R) M... Started Automatic (Delayed Start) Local System
Intel(R) PROSet/Wireless Event Log Manages t... Started Automatic Local System
Intel(R) PROSet/Wireless Registry... Provides r... Started Automatic Local System
Intel(R) Rapid Storage Technology Provides s... Started Automatic (Delayed Start) Local System
IP Helper Provides t... Started Automatic Local System
iPod Service iPod hard... Started Manual Local System
IPsec Policy Agent Internet Pr... Started Manual Network Service
Microsoft Antimalware Service Helps prot... Started Automatic Local System
Microsoft Network Inspection Helps gua... Started Manual Local Service
Network Connections Manages ... Started Manual Local System
Network List Service Identifies t... Started Manual Local Service
Network Location Awareness Collects a... Started Automatic Network Service
Network Store Interface Service This servic... Started Automatic Local Service
Oasis2Service DDNI Oasi... Started Automatic (Delayed Start) Local System
Office Software Protection Platfo... Office Soft... Started Manual Network Service
Peer Name Resolution Protocol Enables se... Started Manual Local Service
Peer Networking Grouping Enables m... Started Manual Local Service
Peer Networking Identity Manager Provides i... Started Manual Local Service
Plug and Play Enables a ... Started Automatic Local System
PMBDeviceInfoProvider Enables P... Started Automatic Local System
Extended Standard





[2] http://www.blackviper.com/service-configurations/black-vipers-windows-7-service-pack-1-service-configurations/

[3] http://www.blackviper.com/windows-default-services/windows-7-default-services/

[4] http://social.technet.microsoft.com/wiki/contents/articles/4484.windows-7-default-services.aspx