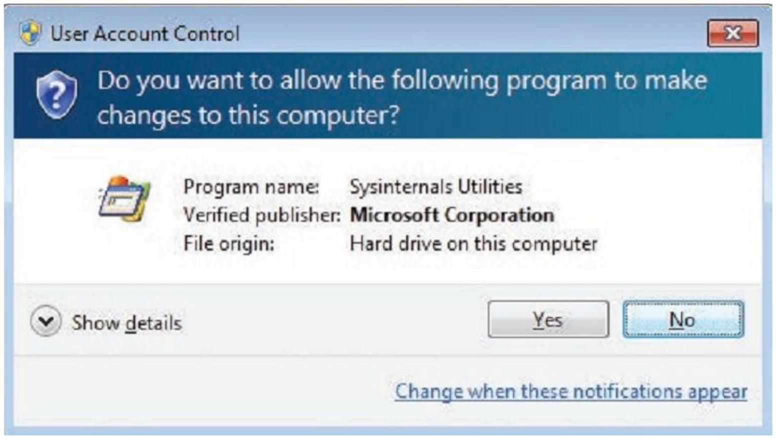
WINDOWS CORE CONCEPTS

ADMINISTRATIVE RIGHTS

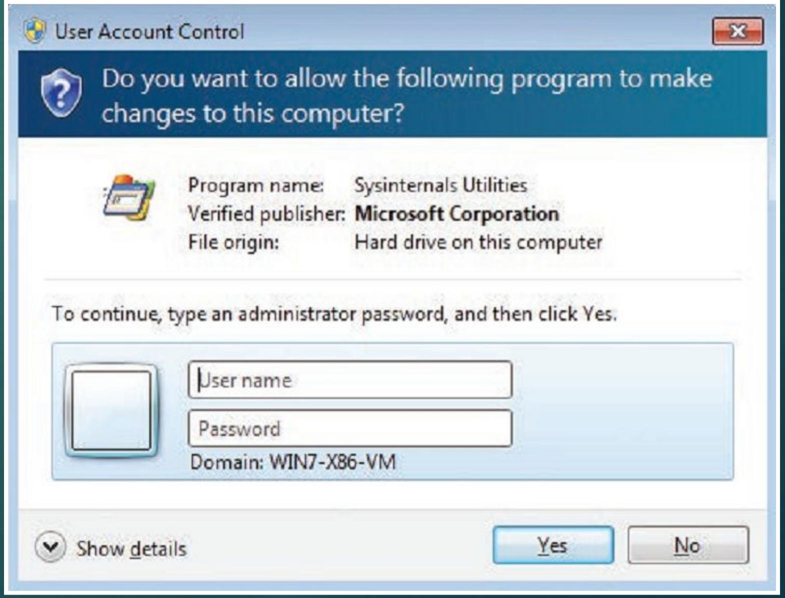
L1
P1

- Administrative rights
- User rights
- Effective administrative control
- User Account Control (UAC)
  - Silently
  - Prompt for Consent
  - Prompt for Credentials
- Access tokens for logon sessions


User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Sysinternals Utilities
Verified publisher: **Microsoft Corporation**
File origin: Hard drive on this computer


User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Sysinternals Utilities
Verified publisher: **Microsoft Corporation**
File origin: Hard drive on this computer

To continue, type an administrator password, and then click Yes.

User name
Password
Domain: WIN7-X86-VM

PROCESSES, JOBS & THREADS

L1
P2

Each **process** contains:

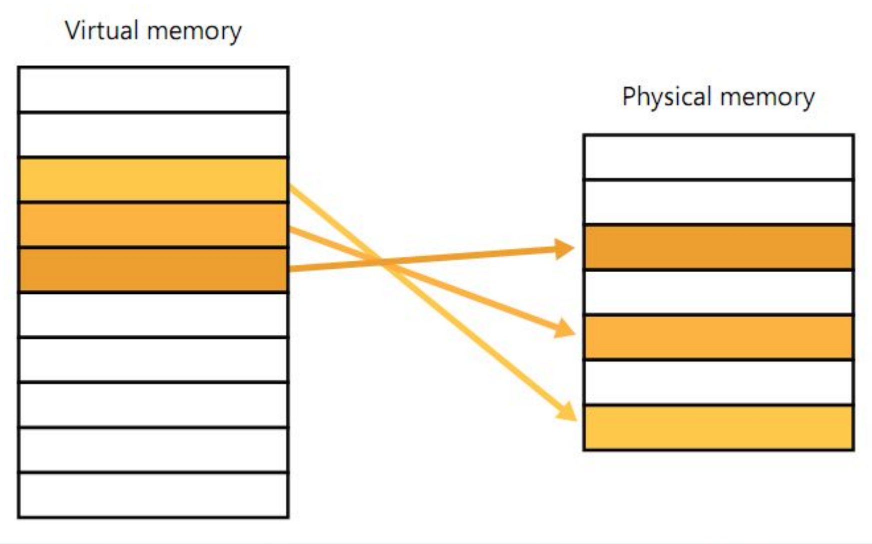
- ❑ PID
- ❑ At least one thread
- ❑ Private Virtual address space
- ❑ An executable program
- ❑ Handles
- ❑ Access token

Each **thread** contains:

- ❑ TID
- ❑ The contents of a set of CPU registers
- ❑ Kernel mode stack
- ❑ User mode stack
- ❑ Thread-local storage (TLS)
- ❑ Access token [*optional*]

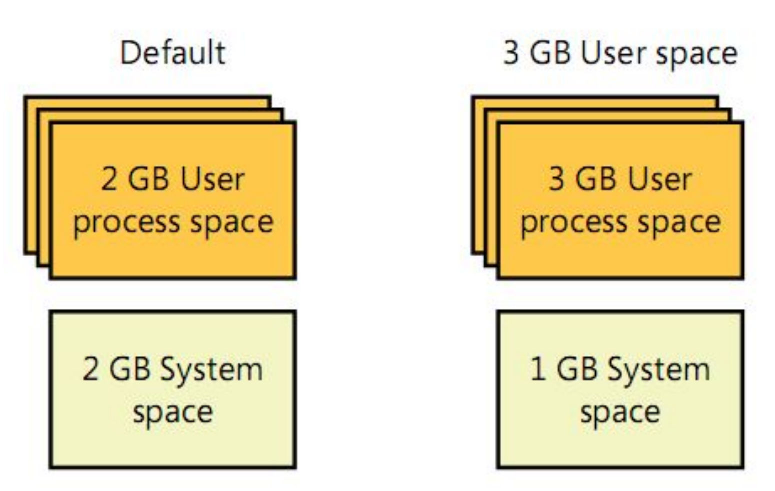
VIRTUAL MEMORY

- ❑ Mapping
- ❑ Paging
- ❑ *Increaseuserva* boot option
- ❑ Address Windowing Extension (AWE)



Typical address space for 32-bit – 2 GB + 2 GB

Typical address space for 64-bit – 8 TB + 8 TB



KERNEL MODE & USER MODE

L1
P4

Kernel mode highlights:

- ❑ Designated for OS code (system services & device drivers)
- ❑ Access to all system memory and all CPU instructions
- ❑ Single virtual address space
- ❑ Driver-signing mechanism
- ❑ Kernel mode code signing (KMCS)

User mode highlights:

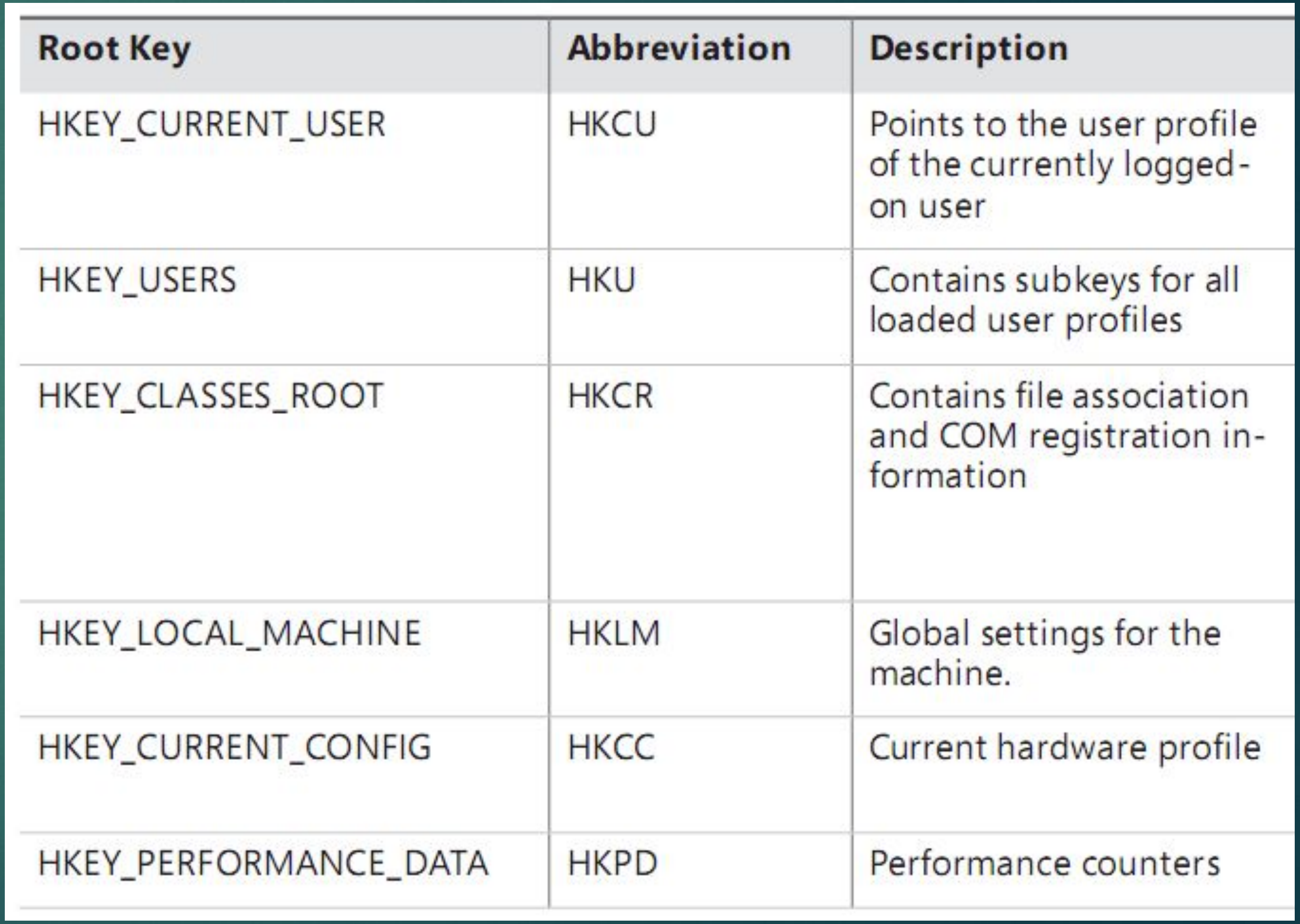
- ❑ designated for user applications
- ❑ Indirect access to resources through system service calls
- ❑ Virtual private address space
- ❑ Isolated execution for each process

WINDOWS CORE CONCEPTS

REGISTRY

L1
P5

- ❑ Viewing and changing Registry
- ❑ Registry Usage
- ❑ Registry Data Types
  - ❑ REG_DWORD
  - ❑ REG_BINARY
  - ❑ REG_SZ
- ❑ Registry Logical Structure



Root Key	**Abbreviation**	**Description**
HKEY_CURRENT_USER	HKCU	Points to the user profile of the currently logged-on user
HKEY_USERS	HKU	Contains subkeys for all loaded user profiles
HKEY_CLASSES_ROOT	HKCR	Contains file association and COM registration information
HKEY_LOCAL_MACHINE	HKLM	Global settings for the machine.
HKEY_CURRENT_CONFIG	HKCC	Current hardware profile
HKEY_PERFORMANCE_DATA	HKPD	Performance counters

OBJECTS & HANDLES

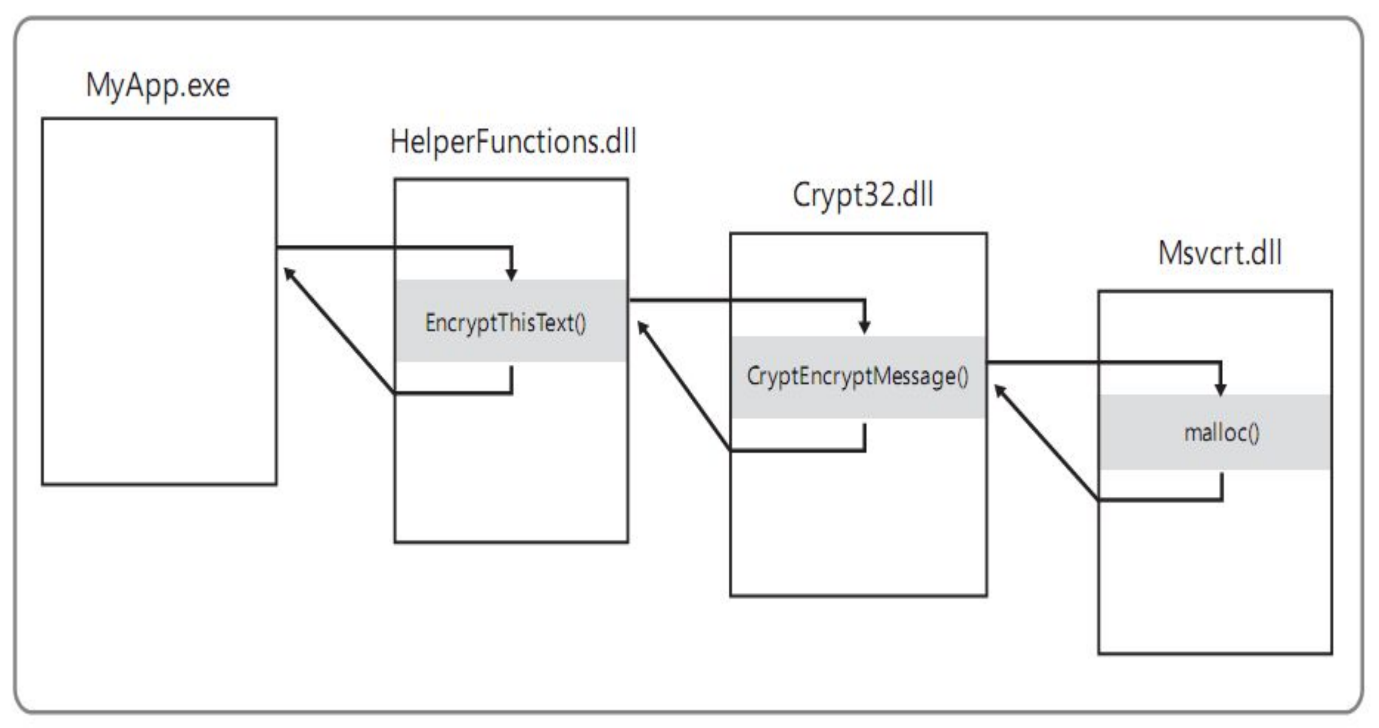
- Objects
    - Providing human-readable names for system resources
    - Sharing resources and data among processes
    - Protecting resources from unauthorized access
    - Reference tracking
- Difference between objects and ordinary data
- Handles

WINDOWS CORE CONCEPTS

CALL STACKS & SYMBOLS

L1
P7

- What is a call stack?
  - module!function+offset e.g.
    crypt32!CryptEncryptMessage+0x9f
- What are symbols?
  - Full (Private) symbol files
  - Public symbol files
- Configuring symbols
  - DBGHelp.dll path
  - Symbols path
  - srv*c:\symbols*https://msdl.microsoft.com/download/symbols

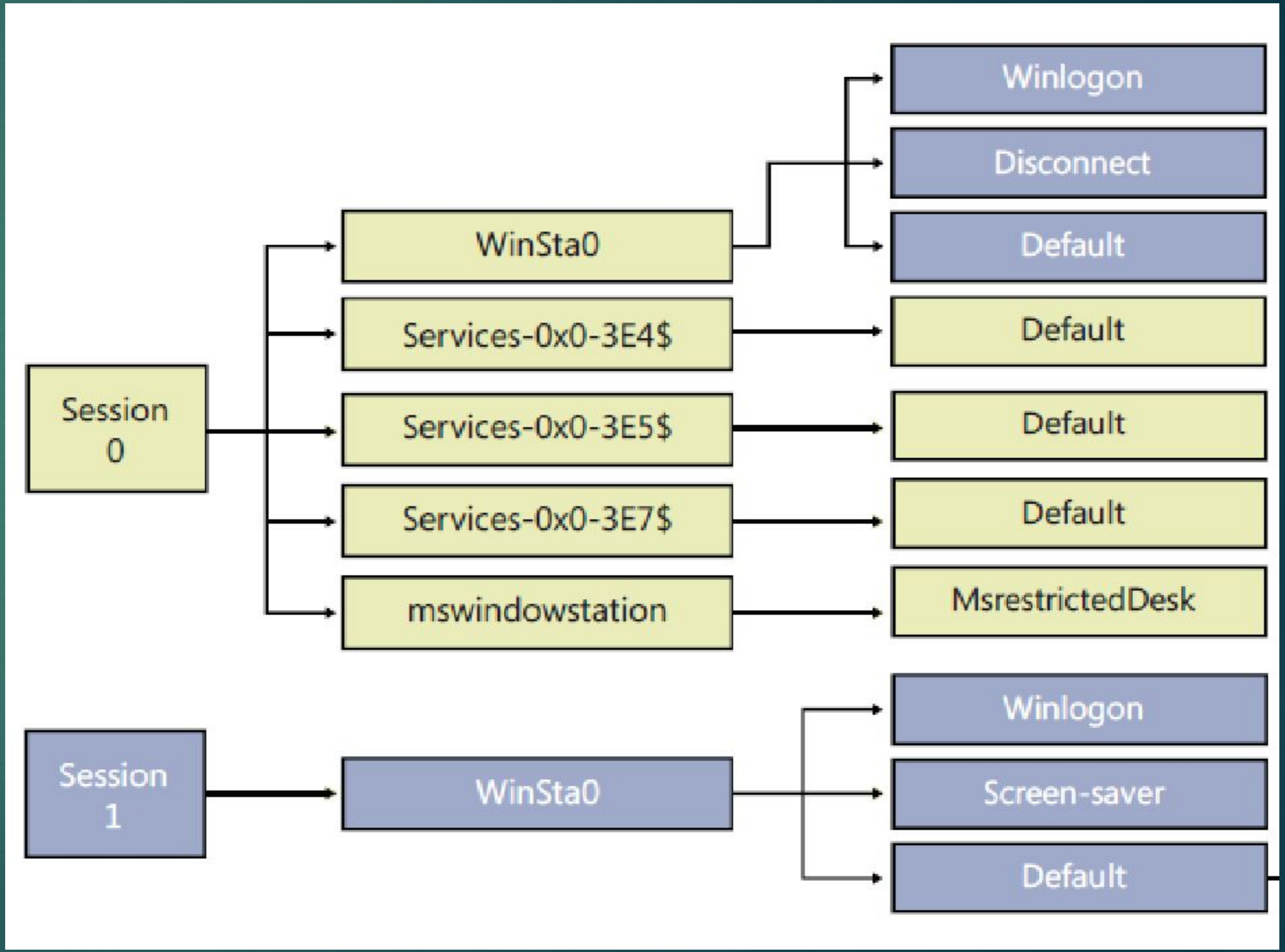


WINDOWS CORE CONCEPTS

WINDOWS SESSIONS, STATIONS & DESKTOPS

L1
P8

- ❑ Overview of Sessions, Window stations and Desktops hierarchy
- ❑ Remote desktop services sessions
  - ❑ RDS session = TS session
  - ❑ Session0 != Console session
- ❑ Fast user switching
- ❑ Windows stations
- ❑ Desktops


Session 0
WinSta0
Winlogon
Disconnect
Default
Services-0x0-3E4$
Default
Services-0x0-3E5$
Default
Services-0x0-3E7$
Default
mswindowstation
MsrestrictedDesk
Session 1
WinSta0
Winlogon
Screen-saver
Default