**VIETNAM NATIONAL UNIVERSITY - HO CHI MINH CITY**

**UNIVERSITY OF INFORMATION TECHNOLOGY**

**FACULTY OF COMPUTER NETWORK AND COMMUNICATION**

**LÊ THANH BÌNH**

**CHÂU THIỆN HƯNG**

**THESIS REPORT**

**STUDY MALICIOUS BEHAVIOR ANALYSIS METHODS TO DETECT SECURITY RISKS ON WINDOWS**

**BACHELOR OF ENGINEERING INFORMATION SECURITY**

**Instructor**

**PhD. NGUYỄN ANH TUẤN**

**HỒ CHÍ MINH CITY, 2017**

**VIETNAM NATIONAL UNIVERSITY - HO CHI MINH CITY**

**UNIVERSITY OF INFORMATION TECHNOLOGY**

**FACULTY OF COMPUTER NETWORK AND COMMUNICATION**

**LÊ THANH BÌNH**

**CHÂU THIỆN HƯNG**

**THESIS REPORT**

**STUDY** **MALICIOUS BEHAVIOR ANALYSIS METHODS TO DETECT SECURITY RISKS ON WINDOWS**

**BACHELOR OF ENGINEERING INFORMATION SECURITY**

**Instructor**

**PhD. NGUYỄN ANH TUẤN**

**HỒ CHÍ MINH CITY, 2017**

# **DANH SÁCH HỘI ĐỒNG BẢO VỆ KHÓA LUẬN**

Hội đồng chấm khóa luận tốt nghiệp, thành lập theo Quyết định số

…………………… ngày ………………….. của Hiệu trưởng Trường Đại học Công nghệ Thông tin.

1. …………………………………………… - Chủ tịch
2. …………………………………………… - Thư ký
3. …………………………………………… - Ủy viên
4. …………………………………………… - Ủy viên

# **COMMENT OF INSTRUCTOR**

# **COMMENT OF REVIEWER**

# **ACKNOWLEDGEMENT**

With supports and helps of many individuals, this thesis has become reality. We would like to express our appreciation to all of them. First of all, we would like to thank not only teachers in faculty of computer network and communications but also teachers in University of Information Technology who have taught us very useful lectures with all of their passion, which provide necessary knowledge for us to finish this thesis. Especially, we would like to express our appreciation to professor Nguyen Anh Tuan, our instructor, who has inspired and guided us to dive deeply into information security with this thesis. Secondly, we would like to thank our friends who has helped, supported and exchanged knowledge with us since we started studying at University of Information Technology. Finally, we would like to thank our family for supporting us during the time we develop this project.

**TABLE OF CONTENTS**

[Chapter 1. INTRODUCTION 1](#_Toc483676762)

[1.1 Motivation 1](#_Toc483676763)

[1.2 Thesis’ statement 1](#_Toc483676764)

[1.3 Subject 1](#_Toc483676765)

[1.4 Scope 2](#_Toc483676766)

[1.5 The needs of Registry monitoring module 2](#_Toc483676767)

[1.6 The needs of service monitoring module 2](#_Toc483676768)

[1.7 The needs of distributed log collector hardware 2](#_Toc483676769)

[1.8 The needs of centralized cloud log storage 2](#_Toc483676770)

[Chapter 2. BACKGROUND AND RELATED WORKS 3](#_Toc483676771)

[2.1 Related works 3](#_Toc483676772)

[2.1.1 OSSEC 3](#_Toc483676773)

[2.1.2 Samhain 5](#_Toc483676774)

[2.2 Background 6](#_Toc483676775)

[2.2.1 Windows Registry 6](#_Toc483676776)

[2.2.2 Windows Service 14](#_Toc483676777)

[2.2.3 Graylog 23](#_Toc483676778)

**TABLE OF FIGURES**

[Figure 2.1: OSSEC Processes in a “Server-Agent” Installation 4](#_Toc483575769)

**TABLE OF TABLES**

[Table 2.1 Service Registry values and description 12](#_Toc483646848)

**TABLE OF ABBREVIATIONS**

|  |  |
| --- | --- |
| **Abbreviation** | **Expansion** |
| IDS | Intrusion Detection System |
| HIDS | Host-based Intrusion Detection System |
| SCM | Service Control Manager |
| APT | Advanced Persistent Threat |
| APTIDS | Advanced Persistent Threat Inspection Detection System |
| SIEM |  |
| LAN | Local Area Network |
| RPC | Remote Procedure Call |

**ABSTRACT**

We have developed a malicious behavior analysis solution for Windows Operation System called Advanced Persistent Threat Inspection Detection System (APTIDS), which is an open source solution combined of a System Monitoring Software, a Distributed Log Collector Hardware and a Centralized Log Storage on Cloud. Just like others well know open source host IDS, the software agent of APTIDS has abilities to monitor some common sectors of Windows OS like Registry, Service. Furthermore, we have developed an ability to allow APTIDS to send collected logs to the Collector Hardware, which is a Log Collector built on a Raspberry Pi, and from that hardware another collector will push all the collected log to the centralized log storage on cloud. APTIDS can monitor and alert on its runtime, that means if any malicious activity takes place at where APTIDS is monitoring, APTIDS will capture that activity, write log, and alert to the log storage.

# INTRODUCTION

## Motivation

Nowadays, with the rapid advance and wide spread of modern threats, computer users are facing threats from everywhere. From the most complicated malwares those can transform themselves to create many variants, to those that encrypt the whole computer and keep our information as hostage. For fighting back those advanced threats that are terrorizing the Internet, many company have developed antivirus softwares. To protect the innocent Internet civilians from the cyberwar that are taking place, antivirus softwares come from a free price for basic protection, to some hundred dollars for full protection against most modern attack vectors. Personal Antivirus software is very powerful for protecting a normal user from many security threats. But their shortcoming is that they can only protect a single user at one, and if there are more than one user who want to be protected, they have to buy more than one AV software, install them separately and there is no way to monitor and manage logs from all those softwares simultaneously.

Enterprise Antivirus System come as a full qualified protection for big enterprises, campuses or companies. They support for monitoring and protecting hundreds of users, and manage their logs of activities in some central cloud storage systems. However, the price for such a platinum protection is very expensive, and it is sophisticated for maintaining and operating and especially for protecting small companies or households.

From all those shortcomings of modern Antivirus Softwares amd Security Protection Systems, we want to develop a solution for helping small companies and households to protect themselves against advance threats.

## Thesis’ statement

Successfully develop and run APTIDS for monitoring malicious behaviors of software on Windows Operating Systems. APTIDS monitor Registry and service for detecting softwares that are trying to write the path of their executable files.

Testing APTIDS by using some common malwares running in a controllable environment.

## Subject

Research on how malwares store themselves on Windows System for running on start up. In addition, research on how Graylog works, the method for collector logs and push them to SIEM for storage and analyzing.

## Scope

APTIDS can monitor activities in some factions of Windows Registry and the creation and deletion of Windows Services. Since it has been developed in a limited time, it does not have full features like others well-known antivirus softwares.

## The needs of Registry monitoring module

Malwares usually store the path lead to their executable applications in Registry (1) in case the system has to be restarted, they can run with the start up. Monitoring the Registry allows us to capture any malicious activity and know what is happening in the Registry Hive.

## The needs of service monitoring module

Windows Service allows us to create a so call long-running executable application, which can start automatically at system boot (2). Knowing that, malicious programs write entries in the Service Control Manager which help them to run their executables when system boot up.

## The needs of distributed log collector hardware

The concept of this thesis is aimed to develop a solution for distributed monitoring malicious activities in a big scale network architecture. A distributed log collector hardware plays a role as a local centralize server for a single LAN network which receive the logs from agents those run in the LAN. Those agents, when capture any malicious activity, they send back their log to the log collector hardware. Each collector hardware stores log for a LAN network which can has up to hundreds of agents.

## The needs of centralized cloud log storage

When a single log collector hardware can store logs for hundreds of agents, a centralized cloud log storage can store and manage logs for hundreds of log collector hardware. Each hardware is managed by an input stream, and can be monitor using a single dashboard. A centralized cloud log storage a low us to monitor hundreds of thousands machine in a large network.

# BACKGROUND AND RELATED WORKS

In this chapter, we study some similar projects those have been developed recently. This study does not aim to compare the advantages and disadvantages of those projects, but we would like to know how other people around the world have handled nowadays sophisticated APT threats. This approach has helped us much in developing APTIDS.

## Related works

### OSSEC

OSSEC is a host-based instruction detection system (HIDS) (3). A HIDS can work as a software that monitors events from inside the system rather than monitor the and inspect the network behaviors. Since from a viewpoint of the network, traffics that travel through network link might be encrypted and hard to be inspect. However, to OSSEC, any network traffics always be seen as plaintext in the system viewpoint. Furthermore, OSSEC has a very sophisticated engine that can monitor system activities for recognize and alert upon any file system change, rootkit or malware infection. OSSEC also monitors log file, capture suspicious activities happening in special parts of the system and alert immediately for respond team to interrupt and prevent the attack on time.

OSSEC comes in a deployment with two main parts: a client agent part and a command and control server part. After has been deployed in the client machine, OSSEC agent does the monitor task. OSSEC agent can work on multiplatform, which means we can expand its protection to any host in our network. The agent communicates with its server at UDP protocol using port 1514. When an event is detected for which an alert to a system or security administrator needs to be sent, OSSEC can use one of several methods, including emails, SMS messages, pagers, etc… (3). OSSEC agent can also takes actions for preventing the attack. For example, within an DDOS attack, OSSEC can insert rule into firewall that can be used to prevent the attack immediately. OSSEC server plays a role as a distributed log collector, it store log received from the agents and alert upon those received logs.

A single OSSEC server can monitor many OSSEC agents. In case we want to connect many OSSCE server together, we can configure an agent inside the server. (see Figure 2-1)



Figure 2.1: OSSEC Processes in a “Server-Agent” Installation

From: http://www.ossec.net/ossec-docs/ossec-hids\_oahmet\_eng.pdf

OSSEC Open Source Security has become and high quality Opensource Host IDS software that is trusted and used in protecting many large campuses and enterprises. Although there are few drawbacks, OSSEC has been trusted to be improved and upgrade their abilities.

### Samhain

Samhain is a multi-platform, opensource host-based HIDS for POSIX (4)

## Background

### Windows Registry

#### Introduction

Windows Registry is a hierarchical database that contains critical data for the operation of Windows systems (5). The data stored in Registry follows a tree format. Each node is called a “key”, and each key can store many subordinate keys (sub-keys) and each sub-key stores many data entries called “Values”. Some applications only require the presence of a key, other applications read into the keys and query the values stored in them. A key can store any value and a value can be in any type.

#### Inside the Registry

**Registry Hive**

The Registry is not a large file that is stored in disk, but it is a group of separated files called “hives”. A hive is a tree format data structure which has a key serving as the tree root, and each sub-key is a node of that tree (6). We might think that each key is completely isolated with other key, however, there are correlations between Registry keys in the system. Table 2.1 shows the Registry keys and their correlations.

|  |  |
| --- | --- |
| **Key** | **Description** |
| HKEY\_CLASSES\_ROOT | Symbolic link to HKEY\_LOCAL\_MACHINE \SOFTWARE \Classes. |
| HKEY\_CURRENT\_USER | Symbolic link to a key under HKEY\_USERS representing a user's profile hive. |
| HKEY\_LOCAL\_MACHINE | Placeholder with no corresponding physical hive. This key contains other keys that are hives. |
| HKEY\_USERS | Placeholder that contains the user-profile hives of logged-on accounts. |
| HKEY\_CURRENT\_CONFIG | Symbolic link to the key of the current hardware profile under HKEY\_LOCAL\_MACHINE \SYSTEM CurrentControlSet\ Control\IDConfigDB\Hardware Profiles. |
| HKEY\_DYN\_DATA | Placeholder for performance data lookups. This key has no corresponding physical hive. |

Table 2.1 Registry keys and their correlations.

From: <https://technet.microsoft.com/en-us/library/cc750583.aspx>

Root keys can correlate to each other, but none of them correlate to their hives. Table 2.2 shows the list of Registry hives and their filenames on system disk.

|  |  |
| --- | --- |
| **Hive Registry Path** | **Hive File Path** |
| HKEY\_LOCAL\_MACHINE \SYSTEM | \%windir%\system32\config\system |
| HKEY\_LOCAL\_MACHINE \SAM | \%windir%\system32\config\sam |
| HKEY\_LOCAL\_MACHINE \SECURITY | \%windir%\system32\config\security |
| HKEY\_LOCAL\_MACHINE \SOFTWARE | \%windir%\system32\config\software |
| HKEY\_LOCAL\_MACHINE \HARDWARE | Volatile hive |
| HKEY\_LOCAL\_MACHINE \SYSTEM \Clone | Volatile hive |
| HKEY\_USERS \UserProfile | Profile; usually under \%windir%\profiles\usere |
| HKEY\_USERS.DEFAULT | \%windir%\system32\config\default |

Table 2.2 List of Registry hives and their filenames on system disk.

From: <https://technet.microsoft.com/en-us/library/cc750583.aspx>

The system path variable “%windir%” links to the path “C:\Windows” in the Windows version other than NT, and it links to “C:\WinNT\” in Windows NT 4 and Windows 2000. Registry filename does not have extension, and they cannot be read or write by normal computer user (without administrator rights). The Registry path that says “Volatile hive” does not have any file stored on the system disk, it is just an image that will be loaded to system memory when the system boots, and it contents might be changed every time there is any change made by the system. For example, the hive HKEY\_LOCAL\_MACHINE \HARDWARD, which stores information about physical devices and the devices’ resources, is a volatile hive. The resource assignment to the device and the hardware detection occur every time the system boots, so storing this data on disk is not necessary, and this data might be changed every time there is an installation or uninstallation of hardware devices.

The heart of the Registry is the HKEY\_LOCAL\_MACHINE \SYSTEM hive. The subkey \CurrentControlSet\Control which is a node in HKEY\_LOCAL\_MACHINE \SYSTEM, contains settings that Configuration Manager uses to initialize the Registry. The Configuration Manager is a kernel subsystem which is responsible for implementing, initializing, managing and organizing the Registry (7). To initialize the Registry, the Configuration Manger locates the hives’ files, creates the root keys then link the hives together for building the Registry structure. To locate the hives’ files, Configuration Manger refers to the value HKEY\_LOCAL\_MACHINE \SYSTEM \CurrentControlSet \Control \hivelist. A special type of key call “symbolic link” makes it possible for the Configuration Manager to link hives together as well as organize the Registry. A symbolic link is a key that redirects Configuration Manager to another key. For example, HKEY\_LOCAL\_MACHINE \SAM is a symbolic link to the key at the root of SAM hive.

**Hive Structure**

Configuration Manager divides a hive into allocation units called “blocks” in much the same way that system divides a disk into clusters. A Registry block has a size of 4096 bytes (4KB). When a hive has to expand its size, it will expand the size in block-granular increments. The first block of a hive is called “base block”. In many ways similar to the PE header, the first hive first block contains a magic signature call “regf”, which stands for “Registry File”, for identifying the file as a Registry hive file. The base block also stores information about the timestamp showing the last time a write operation has been initiated on the hive, a hive format version number, a checksum, a file’s full name (e.g., SystemRoot\CONFIG\SAM), an update sequence numbers, … The hive format version number indicates the data format within the hive. Hive formats has changed from NT 3.51 to NT 4.0 since the presence of Windows NT 4.0. Whether we want to load an old NT 3.51 type hive file under a windows operation system which version is higher than Windows NT 4.0, the system will return an error.

Since Windows NT, Microsoft has organized the Registry hive in small containers called “cells”. A cell holds a key, a value, a security descriptor, a list of subkeys or a list of key values. The first field of the cell contains the data’s type. Table 2.3 describes each cell data types in a clear detail.

|  |  |
| --- | --- |
| **Cell** | **Data Type** |
| Key cell | A cell that contains a Registry key, also called a “key node”. A key cell contains a signature (known as “kn” for a key, “kl” for a symbolic link), the timestamp of the most recent update to the key, the cell index of the key's parent key cell, the cell index of the sub- key-list cell that identifies the key's subkeys, a cell index for the key's security descriptor cell, a cell index for a string key that specifies the class name of the key, and the name of the key (e.g., CurrentControlSet). |
| Value cell | A cell that contains information about a key's value. This cell includes a signature (kv), the value's type (e.g., REG\_DWORD, REG\_BINARY), and the value's name (e.g., Boot-Execute). A value cell also contains the cell index of the cell that contains the value's data. |
| Subkey-list cell | A cell composed of a list of cell indexes for key cells that are all subkeys of a common parent key. |
| Value-list cell | A cell composed of a list of cell indexes for value cells that are all values of a common parent key. |
| Security-descriptor cell | A cell that contains a security descriptor. Security-descriptor cells include a signature (ks) at the head of the cell and a reference count that records the number of key nodes that share the security descriptor. Multiple key cells can share security-descriptor cells. |

Table 2.3 Registry hive cells and their data types.

From: <https://technet.microsoft.com/en-us/library/cc750583.aspx>

Figure 2.2 shows cell data types segments that are contained in the hive.

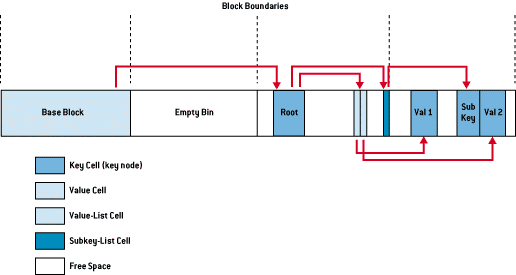


Figure 2.2 Cell data type segments in Registry hive.

From: <https://technet.microsoft.com/en-us/library/cc750583.aspx>

A cell’s header is a cell field that specifies the cell’s size. When a cell joins a hive, in case a hive needs more space to store that cell, the system will create an allocation unit call “bin”. A bin is the size of the new cell rounded up to the next block boundary. The system considers any space between the end of the cell and the end of the bin free space that it can allocate to other cells. Bins also have headers that contain a signature called “hbin” and a field that records the offset into the hive file of the bin and the bin's size.

Using bin instead of cells to track active parts of the Registry, system can reduce the management overheads. The question is why using bins makes system run smoother than cells? For answering that question, we have to identify that cell is a build in unit in Registry hive, but bin is an addon unit in case the hive wants to expand its size then cells are contained in the hive, but bins are not. When Configuration Manager allocates or deallocates bins, nothing changes in the hive. However, when Configuration Manager empties a cell in registry hive, it creates an empty bin in the hive, the hive is now fragmented and leads to the fragmentation of the registry. Fragmentation can slow down read and write processes and makes the system run slower. When a bin becomes empty, the Configuration Manager adjacent that bin and other empty bins to a large empty bin, and make it as contiguous as possible. Configuration Manager also joins empty cells to become larger empty cells.

The links that create the structure of a hive are cell indexes. A cell index is the offset into the hive file of a cell. Thus, a cell index is like a pointer from one cell to another cell that the Configuration Manager interprets relative to the start of a hive. For example, a cell that describes a key contains a field specifying the cell index of its parent key; a cell index for a subkey specifies the cell that describes the subkeys that are subordinate to the specified subkey. A subkey-list cell contains a list of cell indexes that refer to the subkey's key cells. When we want to locate a key that is a subkey belongs to a particular key, we have to locate the cell containing that key’s subkey lists using the subkey-list cell. For each subkey cell, we check the subkey’s name to fine the one we want to locate. Let’s take a look at figure 2.3 default for an example.

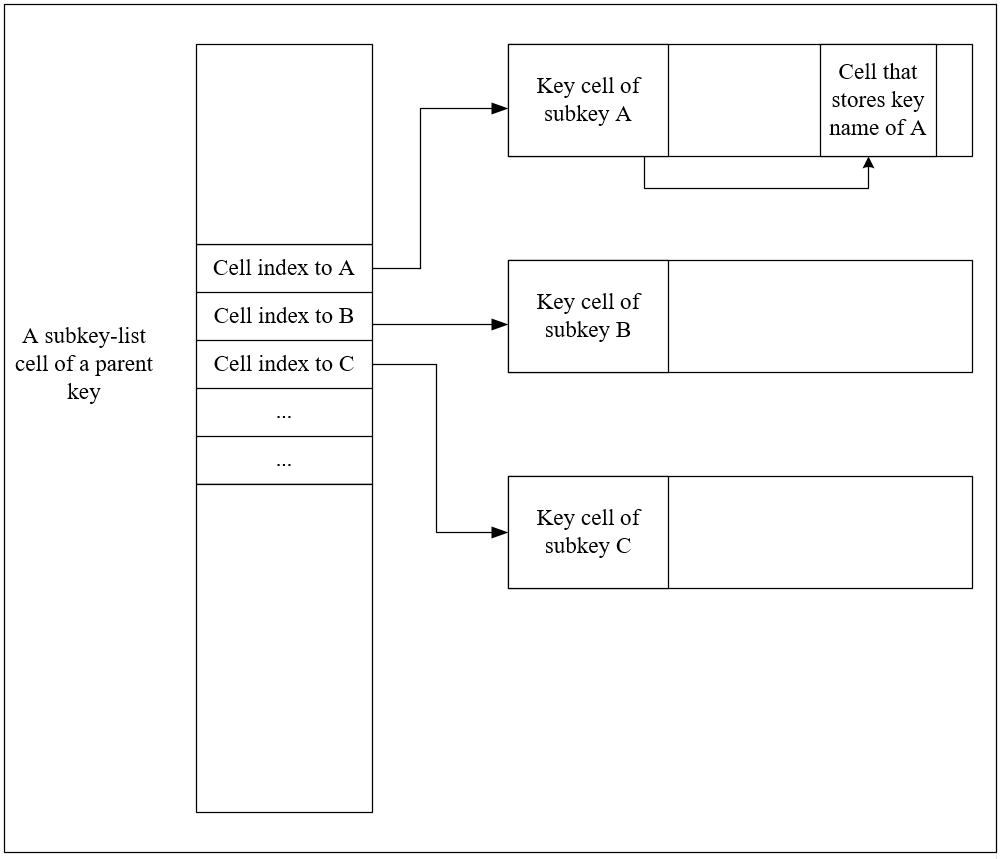


Figure 2.3 Example of cell indexes

Consider that we have a parent key and we want to allocate its subkey. First, we find the parent key’s subkey-list cell which is a cell contained in the hive of the parent key. The subkey-list cell could contain many cell-indexes those point to other *key-cell* cell of other keys, those are subkey of the current parent key. Suppose that we would like to find subkey A, we locate the cell-index that point to the key-cell cell of a subkey, then check the cell-index that point to a cell containing its name. If the name is A, we have located our subkey correctly, if it is not, we do these steps repeatedly for other cell indexes again we find our subkey.

The concept of hive, block, cell and bin might be complicated and undistinguishable. Take a look at figure 2.2 above, we see an entire long square that contains main smaller square. This long square is a registry hive. A hive contains some blocks inside it. A square that is defined by two contiguous dash lines is a block with a fix length of 4096 bytes. The first block of a hive is call a base block, which stores global information for that hive. The free space which is the block next to the base block is an empty bin. The next second blocks compose a bin, that bin consists of many cells. A free space within that bin is an empty cell (or a smaller empty bin). Bin is just a concept, a bin in general is not an object with a specific location and fix length. From a hive perspective, a bin is an allocation unit that stores cells, and those cells can be allocated or free (which can also be called an empty bin).

**Cell Maps**

Since when the system accesses the disk, the overhead for that process is much expensive compare to the outcome speed of these tasks. Configuration Manager decides not to access a hive’s image on disk every time it want to access the Registry. To finish this object, system stores a version of every hive in the kernel’s address space. When initializing a hive, Configuration Manager calculates the size of the hive and allocates enough memory from the kernel’s paged pool to store the hive file, and reads the hive file into memory. “The paged pool is a portion of the kernel's address map that NT reserves for device drivers and the kernel to use. NT can move any memory the system allocates from the paged pool to a paging file when the memory isn't in use. If hives never grew, the Configuration Manager could perform all its Registry management on the in-memory version of a hive as if the hive were a file.” (6)

With a cell index, Configuration Manager can calculate the location of a cell by adding the cell index to the base of the in-memory hive image. This is the task of “Ntldr” (Abbreviation for “NT Loader”) does with the SYSTEM hive when the system boots. When the system boots, Ntldr reads entire SYSTEM hive and load it into memory as a read-only hive, then adds the cell index to the base of the in-memory hive image to locate the cells. However, hives growth by size when they have more subkeys and values added to them, that leads to the system has to allocate paged pool memory to store the new bins. Therefore, the paged pool that keeps the Registry data is not necessary to be contiguous.

For handling the problem of noncontiguous memory buffers those store the hive data, Configuration Manager applies the strategies that Memory Manager does for mapping virtual address space to physical memory addresses (8). The Configuration Manager employs a two-level scheme that takes as input a cell index and returns both the address in memory of the block the cell index resides in and the address in memory of the bin the cell resides in.

Figure 2. describes the process that Configuration Manager handling the noncontiguous memory buffer problems.

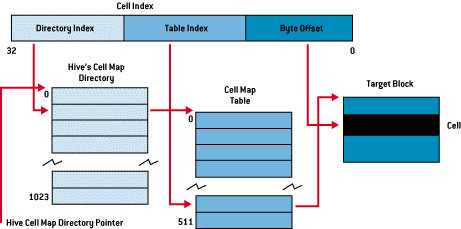


Figure 2.4 Configuration Manager implements a strategy for handling noncontiguous memory buffer problems.

From: <https://technet.microsoft.com/en-us/library/cc750583.aspx>

To implement the mapping, the Configuration Manager divides a cell index logically into fields, in the same way that the Memory Manager divides a virtual address into fields. NT interprets a cell index's first field as an index into a hive's cell map directory. The cell map directory contains 1024 entries, each of which refers to a cell map table that contains 512 map entries. The second field in the cell index specifies the entry in the cell map table that the first index field identified. That entry locates the bin and block memory addresses of the cell. In the final step of the translation process, the Configuration Manager interprets the last field of the cell as an offset into the identified block to precisely locate a cell in memory. When a hive initializes, the Configuration Manager dynamically creates the mapping tables, designating a map entry for each block in the hive, and adds and deletes tables from the cell directory as the changing size of the hive requires.

**Registry Namespace and Operation**

**Registry Root Keys**

A registry key that lying at the top level of a hive is called a root key, all root keys have a prefix of “HKEY” (9). Each root key points to a specific hive that have an essential job to the system operation. Root keys and their descriptions are shown in the table below.

|  |  |
| --- | --- |
| **Root key** | **Description** |
| HKEY\_LOCAL\_USER | Contains the root of the configuration information for the user who is currently logged on. The user's folders, screen colors, and Control Panel settings are stored here. This information is associated with the user's profile. This key is sometimes abbreviated as "HKCU." |
| HKEY\_USERS | Contains all the actively loaded user profiles on the computer. HKEY\_CURRENT\_USER is a subkey of HKEY\_USERS. HKEY\_USERS is sometimes abbreviated as "HKU." |
| HKEY\_LOCAL\_MACHINE | Contains configuration information particular to the computer (for any user). This key is sometimes abbreviated as "HKLM." |
| HEKY\_CLASSES\_ROOT | Is a subkey of HKEY\_LOCAL\_MACHINE\ Software. The information that is stored here makes sure that the correct program opens when you open a file by using Windows Explorer. This key is sometimes abbreviated as "HKCR." Starting with Windows 2000, this information is stored under both the HKEY\_LOCAL \_MACHINE and HKEY\_CURRENT\_USER keys. The HKEY\_LOCAL\_MACHINE\Software \Classes key contains default settings that can apply to all users on the local computer. The HKEY\_CURRENT\_USER\Software\Classes key contains settings that override the default settings and apply only to the interactive user. The HKEY\_CLASSES\_ROOT key provides a view of the registry that merges the information from these two sources. HKEY\_CLASSES\_ROOT also provides this merged view for programs that are designed for earlier versions of Windows. To change the settings for the interactive user, changes must be made under HKEY\_CURRENT \_USER\Software\Classes instead of under HKEY\_CLASSES\_ROOT. To change the default settings, changes must be made under HKEY \_LOCAL\_MACHINE\Software\Classes. If you write keys to a key under HKEY\_CLASSES\_ ROOT, the system stores the information under HKEY\_LOCAL\_MACHINE\Software\Classes. If you write values to a key under HKEY \_CLASSES\_ROOT, and the key already exists under HKEY\_CURRENT\_USER\Software \Classes, the system will store the information there instead of under HKEY\_LOCAL \_MACHINE\Software\Classes. |
| HKEY\_CURRENT\_CONFIG | Contains information about the hardware profile that is used by the local computer at system startup. |

**Registry Data Type**

A registry hive also contains values specify the information that system can use for its operation. A hive can store as many value as it wants and a value can be anything, but its type has to obey the predefined system registry value type. The table below describes the registry types and their descriptions.

|  |  |  |
| --- | --- | --- |
| **Name** | **Data type** | **Description** |
| Binary Value | REG\_BINARY | Raw binary data. Most hardware component information is stored as binary data and is displayed in Registry Editor in hexadecimal format. |
| DWORD Value | REG\_DWORD | Data represented by a number that is 4 bytes long (a 32-bit integer). Many parameters for device drivers and services are this type and are displayed in Registry Editor in binary, hexadecimal, or decimal format. Related values are DWORD\_LITTLE\_ENDIAN (least significant byte is at the lowest address) and REG\_DWORD\_BIG\_ENDIAN (least significant byte is at the highest address). |
| Expandable String Value | REG\_EXPAND\_SZ | A variable-length data string. This data type includes variables that are resolved when a program or service uses the data. |
| Multi-String Value | REG\_MULTI\_SZ | A multiple string. Values that contain lists or multiple values in a form that people can read are generally this type. Entries are separated by spaces, commas, or other marks. |
| String Value | REG\_SZ | A fixed-length text string. |
| Binary Value | REG\_RESOURCE\_LIST | A series of nested arrays that is designed to store a resource list that is used by a hardware device driver or one of the physical devices it controls. This data is detected and written in the \ResourceMap tree by the system and is displayed in Registry Editor in hexadecimal format as a Binary Value. |
| Binary Value | REG\_RESOURCE\_  REQUIREMENTS\_LIST | A series of nested arrays that is designed to store a device driver's list of possible hardware resources the driver or one of the physical devices it controls can use. The system writes a subset of this list in the \ResourceMap tree. This data is detected by the system and is displayed in Registry Editor in hexadecimal format as a Binary Value. |
| Binary Value | REG\_FULL\_  RESOURCE\_DESCRIPTOR | A series of nested arrays that is designed to store a resource list that is used by a physical hardware device. This data is detected and written in the \HardwareDescription tree by the system and is displayed in Registry Editor in hexadecimal format as a Binary Value. |
| None | REG\_NONE | Data without any particular type. This data is written to the registry by the system or applications and is displayed in Registry Editor in hexadecimal format as a Binary Value |
| Link | REG\_LINK | A Unicode string naming a symbolic link. |
| QWORD Value | REG\_QWORD | Data represented by a number that is a 64-bit integer. This data is displayed in Registry Editor as a Binary Value and was introduced in Windows 2000. |

### Windows Service

#### Introduction

Microsoft Windows Service (2) is a computer program which operates silently in the background of the Microsoft Windows Operation System. Window Service program offers an ability for user to create a persistent and auto-running executable applications. Windows services can be started automatically when system boots, or can be stopped, paused and change without interfering any concurrent working users on that local system.

A service application in the window service program is an entity that must conform to the rules, protocols and policy of the Service Control Manager (SCM). Besides that, Windows also support for driver service, which conforms to the device driver protocols for working with system devices.

#### Service Control Manager

**Windows Services and Service Control Manager**

Windows Services (6) are application that run on Windows computers regardless of whether a user is logged in. A Windows services is an entity that comprise a executable file, a directory for storing application components, and Registry settings that define the parameters used for that service. A Windows service can be started automatically when the system is boot, or manually by a software that control the service. Services can be controlled by any program that integrated a service control method, which is a Remote Procedure Call (RPC) (7) (8)to SCM functions.

Service Control Manager (SCM) is a Windows process for managing and controlling application services and driver services (9). SCM maintains a database of installed services and driver services, and provides a unified and secured means of controlling them. SCM database comprise information about each service and how it has to be handled by the system. The information is mainly about how each service could be started when system boots, which information they could need to run their executable applications and what are the security requirements for each service. SCM database is stored in a Registry location: *HKLM\SYSTEM\CurrentControlSet\Services.*

In that location, each installed service is stored as an entry key, which name corresponds to the name of the service (see figure 2.4).



Figure 2.5 Each Windows service is stored as an entry key in the SCM database Registry location

The name of an entry in this location is called a service name. However, when we work with a service, the name that display by a service management tool (such as sc.exe) is called a display name. The display name can be different to the service name, and is stored in the service entry key. For example, a service named “AxInstSV” which has its entry key stored at “HKLM\SYSTEM\CurrentControlSet \Services\AxInstSv” has a display name called “ActiveX Installer”

Opening a service entry key in Registry Editor, we can see that there are so many Registry values for that service. Those Registry values are used to specified the information set to the service (see figure 2.5).



Figure 2.6 Each service entry key stores many Registry values that specify its information

The following table describe those values and their abilities:

|  |  |  |
| --- | --- | --- |
| **Value** | **Type** | **Description** |
| DependOnGroup | REG\_MULTI\_SZ | Lists load-ordering groups on which Windows services depend. Services that depend on a group can run if, after attempting to install all members of a group, at least one member of the group is running. |
| DependOnService | REG\_MULTI\_SZ | Lists the names of Windows services on which this service depends. SCM must start these services before it starts this service. This value can be an empty string if the service has no dependencies. |
| Description | REG\_SZ | Describes the service. The description is simply a comment that explains the purpose of the service. |
| DiagnosticsMessageFile | REG\_SZ | Contains the name of the resource DLL that contains the event description strings for those events that the service writes into the application event log. Resource DLLs are located in the \Program Files\Exchsrvr\Res directory. |
| DisplayName | REG\_SZ | Contains the display name that is used to identify the service. This string has a maximum length of 256 characters. The name is case-preserved in SCM. Display name comparisons are always case-insensitive. |
| ErrorControl | REG\_DWORD | Specifies error severity and the action taken if this service fails to start. This parameter determines one of the following:   * The startup program logs the error but continues the startup operation. * The startup program logs the error and displays a message but continues the startup operation. * The startup program logs the error. If the "last known good" configuration is started, the startup operation continues. Otherwise, the system is restarted with the "last known good" configuration. * The startup program logs the error, if possible. If the "last known good" configuration is started, the system startup is cancelled. Otherwise, the system is restarted with the "last known good" configuration. |
| FailureActions | REG\_BINARY | Cites the action SCM should take for each failure of a service. A service is considered failed when it stops without reporting a status to the service controller (for example, when a service fails). |
| Group | REG\_SZ | Names the load-ordering group of which this service is a member. Note that setting this value can override the setting of the DependOnService value. |
| ImagePath | REG\_EXPAND\_SZ | Contains the fully qualified path to the service binary file. If the path contains a space, it must be quoted, so that it is correctly interpreted. For example, "d:\\Program Files\\Exchsvr\\Bin\\mad.exe".  The path can also include program arguments. |
| ObjectName | REG\_SZ | Specifies the name of the account under which the service should run. If the service uses the LocalService account, this parameter is set to NT AUTHORITY\LocalService. It is also possible to specify an account name in the form DomainName\UserName. |
| Start | REG\_DWORD | Specifies when to start the service. SCM can start a service automatically during system startup, or when a process requests the service start. This value can also specify that a service cannot be started and that attempts to start the service should result in the error code ERROR\_SERVICE\_DISABLED. |
| Tag | REG\_DWORD | Determines the service startup order within a load-ordering group. Tags are only evaluated for driver services. |
| Type | REG\_DWORD | Specifies the service type as file system driver, device driver, a service that runs its own process, or a service that shares a process with one or more other services. MSExchangeSA is an example of a service that runs its own process. EXIFS is an example of an Exchange-specific file system driver. |

Table 2.4 Service Registry values and descriptions

From:<https://technet.microsoft.com/en-us/library/881d8b23-d274-4313-a666-88f80c2cfd92.aspx>

**Service Control Manager manages Windows Services**

Enumerating services by reads each Registry key at one from the services database, SCM can create a record for each service. A service record is a set of a service name, startup type, the service status (the current state, acceptable control codes, …) and a pointer to the dependency list of that service. SCM uses these records to determine which actions are valid for the services, according to their current statuses and dependencies.

To start or stop a service, SCM communicate with the service it controls via a RPC. SCM can start services automatically at system boot, or the service can be started manually by any service control program. However, if an auto-start service demand on a demand-start service, that demand-service is also started automatically. The startup type can be set to “disable”, which tells SCM not to start the service at startup, the service also cannot be started by any mean as well. The dependencies between services are important that we should take a look at them before enabling or disabling a service. Neither an auto-start service nor a demand-start can be started if the service they depend on is disabled. Some services must not be disabled, otherwise, Windows will be failed to boot because the disabled service may be an essential service or a service that essential ones depend on. When starting a service, SCM performs the following steps:

1. **Retrieves the account information stored in the services database**

The username and password of the service account are specified at the time the service is installed. SCM stores the user name in a REG\_SZ Registry value named “ObjectName” within the Registry key of the individual service (HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\<servicename>). The password is in a secure portion of Local Security Authority (LSA).

1. **Logs on the service account**

Any process that runs in Windows has to be run under an authorization of a specific account. For starting a service, SCM query the account information of that service from the services databases and logs on to Windows. The account that SCM uses to log on a local computer must have the user right called “Log on as a service”

1. **Creates the service in suspended state**

SCM starts new services in a suspended state, because the service is useful only after SCM adds the required security information to the new process.

1. **Assigns the access token to the process**

When an account logs on to Windows, the operation system calls winlogon.exe for getting the username and password of that account. When the log process successful, winlogon.exe calls wininit.exe to generate an access token, and any process which runs under that account need that access token to verify themselves (10).

1. **Allow the process to execute**

After SCM completes the logon procedure and assigns the access token, SCM can allow the service to run and perform its functions.

When a service is running, it sends status notifications to the SCM process. SCM maintains this status information in the service record for each service. SCM follow this information so that it does not mistakenly send control requests that violate the current service’s state. The service status sent includes:

* **Service Type:** A service type can be a device driver, a system driver or a Windows service, and can run its own process or share a process with other services.
* **Current State:** Indicates the state of the service as starting, running, paused or not running.
* **Acceptable control codes:** Control code that the service can accept and process in its handler function, according to the state.
* **Windows exit code:** If an error occurs when a service is starting or stopping, it uses this code to reports to the system. To return an error code specific to the service, the service must set this value to ERROR\_SERVICE\_SPECIFIC\_

ERROR to indicate that additional information can be found in the service exit code. The service sets this value to NO\_ERROR when it is running or stopping properly.

* **Service exit code:** The service uses this code to report an error when it is starting or stopping. The value is ignored unless the Windows exit code is set to ERROR\_SERVICE\_SPECIFIC\_ERROR.
* **Wait hint:** The service uses this code to report the estimated time, in milliseconds, required for a pending start, stop, pause, or continue operation.
* **Checkpoint:** The service uses this value to periodically report its progress during a lengthy start, stop, pause, or continue operation. For example, the Services tool uses this value to track the progress of the service during start and stop operations.

When stopping a service, SCM performs the following steps:

1. **SCM receives a stop request for a service**

A service control program which wants to stop a service will send a SERVICE\_CONTROL\_STOP request to the service through SCM.

1. **SCM examines the service dependencies**

If SCM finds any running service that are dependent on the service requested to be stopped, SCM will return an error code to the service control program. Before triggering the stop procedure, the service control program has to enumerate and stop all services that are dependent on the service requested.

1. **SCM forwards the stop request to the service**

If SCM detects that no dependent active services, SCM instructs the specified service to stop by forwarding the stop code to the service. The service must now free its allocated resources and shut down.

### Graylog