Refs: Nghiên cứu, tìm hiểu cấu trúc dữ liệu & cách thức Windows

sử dụng để quản lý Process, Thread.

Windows->Process,

->Thread

1.Process là gì?

2.Thread là gì?

3.Cách mà Window tổ chức các process và thread

4.

**1.Process là gì?**

Process đơn giản là một chương trình đang được chạy hay còn gọi là tiến trình. Các tiến trình đều có một ID riêng để phân biệt với các tiến trình khác. Trong 1 tiến trình có thể có một hoặc nhiều Thread được chạy.

**2.Thread là gì?**

Thread được hiểu là một đơn vị cơ bản mà hđh cấp phát thời gian chiếm dụng bộ xử lý hay còn được gọi là luồng. Một luồng có thể chạy một vài phần của code đang xử lý, bao gồm các phần cũng được chạy bởi một luồn khác. Mỗi luồng đều có một ID riêng để phân biệt với các luồng khác.

**3.Cấu trúc dữ liệu mà Windows dùng để quản lý Process và Thread:**

Trong Windows có một nơi lưu trữ các thông số kỹ thuật của hệ điều hành gọi là Registry. Cơ sở dữ liệu này chứac các thông tin về sự thay đổi, lựa chọn cũng như những thiết lập từ người dùng. Registry sử dụng cấu trúc dạng Tree với nhiều nhánh chứa các thông tin riêng biệt. Trong đó, nhánh **HKEY\_CURRENT\_USER** sẽ chứa các thông tin liên quan đến phần cứng, phần mềm cũng như là quản lý các Process và Thread.

Trong mỗi nhánh sẽ có các nhánh con chứa các dữ liệu có liên quan đến nhánh chính.

Mỗi tiến trình trong Windows được biểu diễn dưới dạng một khối tiến trình thực thi  
(EPROCESS). Mỗi khối EPROCESS trỏ đến một số các cấu trúc dữ liệu liên quan khác  
như khối các luồng (ETHREAD – Chi tiết ở mục 2.3). Khối EPROCESS tồn tại trong không gian địa chỉ hệ thống, EPROCESS liên kết với khối Môi trường tiến trình (PEB)  
nằm trong không gian địa chỉ tiến trỡnh(Vỡ nó chứa các thông tin mà được thay đổi bởi ứng dụng ở user-mode). Ngoài ra một khối EPROCESS còn trỏ đến Khối tiến trình của  
Windows và Bảng điều khiển handle.

4. Cách thức mà Windows dùng để quản lý các Process và Thread:

Quá trình tạo một tiến trình  
Một tiến trình Windows được tạo khi mà ứng dụng gọi hàm tạo tiến trình, như là hàm  
Create Process, Create Process As User, Create Process With Token Who hoặc Create  
Process With LogonW. Để tạo một tiến trình thì cần những thông tin trong thư viện clientserver Kernel32.dll, trình thực thi của Windows và tiến trình hệ thống con của Windows.  
Các bước tạo một tiến trình mới:  
Để tạo một tiến trình với hàm API CreateProcess thì phải qua 6 bước cơ bản sau:  
B1: Mở tệp tin thực thi (.exe)  
B2: Tạo đối tượng thực thi tiến trình  
B3: Tạo luồng khởi tạo và stack, ngữ cảnh của nó.  
B4: Thông báo cho hệ thống con của Windows về tiến trình mới được tạo.  
B5: Bắt đầu thực thi luồng khởi tạo  
B6: Trong ngữ cảnh của luồng và tiến trình mới, hoàn thành việc khởi tạo của không gian  
địa chỉ(mục đích để nạp những thư viện liên kết động DLL) và bắt đầu thực thi chương  
trình.  
Trước khi gọi image, hàm CreateProcess thực hiện những bước sau:  
- Trong hàm CreateProcess,mỗi thứ tự ưu tiên cho các tiến trình mới là - một bít độc lập  
trong cờ CreationFlags, do đó có thể tạo một tiến trình - có nhiều mức ưu tiên, Windows  
sẽ xem xét và chọn thứ tự ưu tiên từ thấp đến cao để gán cho tiến trình mới tạo.  
- Nếu không có một thứ tự ưu tiên nào thì mặc định sẽ được đặt là Nornal.  
- Nếu ứng dụng có mức ưu tiên là Real-time và tiến trình gọi không có khả năng Nâng  
quyền ưu tiên, thì tiến trình mới tạo ra sẽ được gán mức ưu tiên là mức Cao.  
- Tất cả các tiến trình tạo ra đều được gắn với 1 desktop nào đó.