How can I tell whether my process is running as SYSTEM?

devblogs.microsoft.com/oldnewthing/20210106-00

January 6, 2021

Raymond Chen

A customer wanted to know how to check whether the current process is running as the SYSTEM account. They proposed this algorithm:

```
// Code in italics is wrong
bool IsCurrentProcessRunningAsSystem()
{
 DWORD session_id;
 return ProcessIdToSessionId(GetCurrentProcessId(), &session_id) &&
        session_id == 0;
}
```

This algorithm is flawed both for the possibility of false positives as well as false negatives.

You can see this for yourself by opening Task Manager:

Name	User name	Session ID
LogonUI.exe	SYSTEM	3
winlogon.exe	SYSTEM	3
fontdrvhost.exe	UMFD-0	0

We have some processes running as SYSTEM which aren't in session zero. And we have a process in session zero that is not running as SYSTEM.

If you want to know whether you are running as SYSTEM, check your token to see whether it represents the SYSTEM user.

I'm going to use wil as my RAII library.

```
#include <wil/token_helpers.h>

bool DoesTokenRepresentSid(HANDLE token, WELL_KNOWN_SID_TYPE type)
{
 // maps to GetTokenInformation(token, TokenUser, ...);
 auto user = wil::get_token_information<TOKEN_USER>(token);
 return !!IsWellKnownSid(user->User.Sid, type);
}

bool IsCurrentProcessRunningAsSystem()
{
 return DoesTokenRepresentSid(GetCurrentProcessToken(),
                              WinLocalSystemSid);
}

bool IsCurrentThreadRunningAsSystem()
{
 return DoesTokenRepresentSid(GetCurrentThreadEffectiveToken(),
                              WinLocalSystemSid);
}
```

Raymond Chen

Follow