**Spoofing System Executables**

**(spoofing system executable to elevate priviledges)**

**Description 1**

Attacker might Spoof system executables to provide a backdoor. [1]

**Concrete Example in windows:**

Windows contains accessibility features that may be launched with a key combination before a user has logged in (for example, when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.

Two of these accessibility programs are C:\Windows\System32\utilman.exe, launched when the Windows + U key combination is pressed, and C:\Windows\System32\sethc.exe, launched when the shift key is pressed five times. The program "sethc.exe" is often referred to as sticky keys, and has been used by adversaries for unauthenticated access through a remote desktop login screen.

Depending on the version of Windows, an adversary may take advantage of these features in different ways:

On Windows XP and Windows Server 2003/R2, the program (e.g., C:\Windows\System32\utilman.exe) may be replaced with "cmd.exe" (or another program that provides backdoor access). Subsequently, pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over Remote Desktop Protocol will cause the replaced file to be executed with SYSTEM privileges.2

On Windows Vista and later as well as Windows Server 2008 and later, a Registry key may be modified that configures "cmd.exe," or another program that provides backdoor access, as a "debugger" for the accessibility program (e.g., "utilman.exe"). After the Registry is modified, pressing the appropriate key combination at the login screen while at the keyboard or when connected with RDP will cause the "debugger" program to be executed with SYSTEM privileges.2

**REFERENCES:**

[1] https://attack.mitre.org/wiki/Privilege\_Escalation