What are these SIDs of the form S-1-15-3-xxx?

devblogs.microsoft.com/oldnewthing/20220503-00

May 3, 2022

Raymond Chen

Last time, we decoded the mysterious S-1-15-2-xxx SIDs. Another family of SIDs you may run across are the S-1-15-3-xxx SIDs.

SIDs of the form S-1-15-3-xxx are app capability SIDs. These SIDs are present in the token of apps running in an app container, and they encode the app capabilities possessed by the app.

As I noted last time, the rules for Mandatory Integrity Control say that objects default to allowing write access only to medium integrity level (IL) or higher. Granting access to these app capability SIDs permit access from apps running at low IL, provided they possess the matching capability.

SID	Description
Explicitly assigned	
S-1-15-3-1	internetClient
S-1-15-3-2	internetClientServer
S-1-15-3-3	privateNetworkClientServer
S-1-15-3-4	picturesLibrary
S-1-15-3-5	videosLibrary
S-1-15-3-6	musicLibrary
S-1-15-3-7	documentsLibrary
S-1-15-3-8	enterpriseAuthentication
S-1-15-3-9	sharedUserCertificates
S-1-15-3-10	removableStorage
S-1-15-3-11	appointments

S-1-15-3-12	contacts
S-1-15-3-4096	internetExplorer
Autogenerated	
S-1-15-3-x1-x2-x3-x4	device capability
S-1-15-3-1024-x1-x2-x3-x4-x5-x6-x7-x8	app capability

You can sort of see how these assignments evolved. At first, the capability RIDs were assigned by an assigned numbers authority, so anybody who wanted a capability had to apply for a number. After about a dozen of these, the assigned numbers team (probably just one person) realized that this had the potential to become a real bottleneck, so they switched to an autogeneration mechanism, so that people who needed a capability SID could just generate their own.

For device capabilities, the four 32-bit decimal digits represent the 16 bytes of the device interface GUID. Let's decode this one: S-1-15-3-787448254-1207972858-3558633622-1059886964.

787448254				1207972858				3558633622				105988696	
`0x2eef81be`				`0x480033fa`				`0xd41c7096`				`0x3f2c97`	
`be`	`81`	`ef`	`2e`	`fa`	`33`	`00`	`48`	`96`	`70`	`1c`	`d4`	`74`	`97`
`2eef81be`				`33fa`		`4800`		`96`	`70`	`1c`	`d4`	`74`	`97`
`{2eef81be-`				`33fa-`		`4800-`		`96`	`70-`	`1c`	`d4`	`74`	`97`

And we recognize `{2eef81be-33fa-4800-9670-1cd474972c3f}` as `DEVINTERFACE_AUDIO_CAPTURE`, so this is the microphone device capability.

For app capabilities, the eight 32-bit decimal numbers represent the 32 bytes of the SHA256 hash of the capability name. You can programmatically generate these app capability SIDs by calling `DeriveCapabilitySidsFromName`.

Raymond Chen

Follow