

본 컬럼에 대한 모든 저작권은 DevGuru에 있습니다.
컬럼을 타 사이트 등에 기재 및 링크 또는 컬럼 내용을 인용 시 반드시
출처를 밝히셔야 합니다.
컬럼 들을 CD나 기타 매체로 배포하고자 할 경우 DevGuru에 동의를
얻으셔야 합니다.

© DevGuru Corporation. All rights reserved

기타 자세한 질문 사항들은 웹 게시판이나 support@devguru.co.kr으로
문의하기 바랍니다.

Device Driver Security에 대한 고찰 I

© 2003 Devguru (Device driver Guru), Inc.

이번 칼럼에서는 Windows 2000/XP에서 Device Driver에 대한 보안 문제를 기술하고자 한다. 앞으로 Windows 2000/XP를 간단히 Windows라고 사용함을 먼저 밝힌다. 본 column을 쓰게 된 동기는 Device Driver에서 IoCreateDevice()함수를 사용하여 Device Object를 만드는데 어떤 security permission이 적용될까 하는 궁금 점에서부터 기인한다.

물론 이 부분에 대한 언급은 DDK나 그 외 M/S 문서를 봐도 전혀 정보가 없다. 그리고 종종 어떤 device에 대해 non-Administrative user가 아니면 접근을 할 수 없는 경우를 만나는데 이러한 경우가 바로 Device Object에 적용된 security때문이다. 따라서 본 칼럼에서는 device object에 적용되는 security에 대해서 알아보하고자 한다.

한 번의 원고로는 모든 것을 기술하기에 본 저자의 시간이 허락하지 않기에 몇 번의 기사로 나누어서 기술하고자 한다.

따라서 이 기사에서는 먼저 Windows security를 논의하기 위해서 필요로 하는 몇 가지 용어 정리부터 하고자 한다.

Principal

- a. Each unique entity that we can securely identify in secure system.
- b. Authenticable entity in the system.
- c. The entity in a system that can be distinguished from one another in a secure fashion.
- d. 예를 들면, Users, Computers, Groups

Authentication

- a. The mechanism by which one principal proves its identity to another principal.
- b. answers the question "Who you are?"
- c. enables the establishment of a secure channel so that the actual data being sent back an forth between the two principals can be verified as being authentic.

Account

A record in the security database for information about principals.

Security identifiers(SIDs)

Machine-readable identifier for a principal is guaranteed to be globally unique.

SID의 구조는 대체로 다음과 같다.

S-R-I-SA-[SA,...]-RID

S : letter S

R : reversion number, 현재는 1

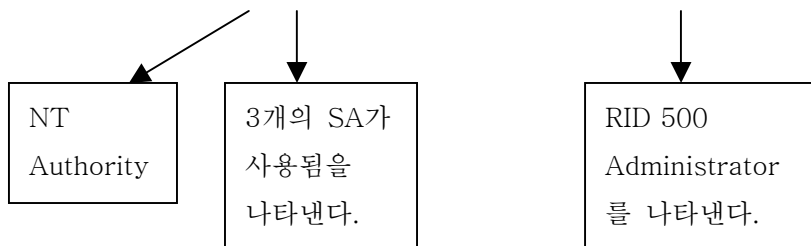
I : 48bit identifier authority

SA: 32bit sub-authority

RID: relative identifier

예를 보면

Administrator : S-1-5-21-XXXX-XXXX-XXXX-500



Local Security Authority(LSA)

The subsystem in Windows that is responsible for performing the core duties of an authority, that is, providing authentication services.

Authorization

- Answers the question "What can you do?"
- 이 질문에 대한 답변 정보는 authorization attributes이다.

Authorization attributes

- a. principal SID
- b. group
- c. privilege

가. help administrators deal with global policy decisions. And provide flexibility to allow certain groups of users to be treated differently than others.

나. the right for a user to perform a system-related operation on the local computer, such as loading a driver, changing the time, or shutting down the system.

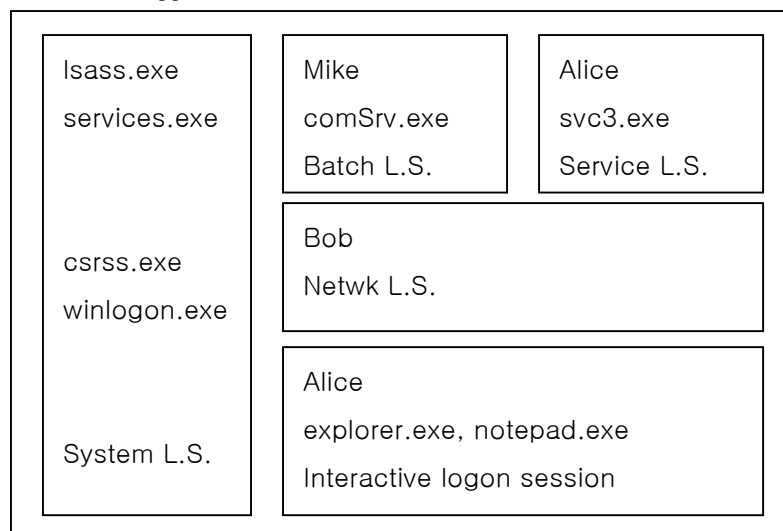
다. The access token for each process contains a list of the Privileges granted to the process.

라. Privilege는 access right와 다르다 왜냐하면 Privilege는 object에 적용되는 것이 아니라 system-related tasks와 resources에 적용되기 때문이다.

마. Privileges는 항상 사용하기 전에 enabled되어져야 한다.

Logon Session

- a. Represents an instance of a particular principal on a machine.
- b. A logon session allows a user to use secured resources on the machine.
- c. logon session consist of a collection of information about a principal who has logged in to a machine.



A typical collection of logon sessions

Tokens

- 어떤 principal이 logon할 때 LSA에 의해서 만들어진다.
- An important level of indirection that allows individual processes to make localized changes to the security attributes for the logon session
- logon session이 만들어질 때 system은 groups, privileges에 대한 authorization attributes를 token에 저장한다.

Identity and Authorization Attributes	
User SID	Group SIDs
User Name*	Privileges
Defaults for New Objects	Miscellaneous Stuff
Owner SID	Logon session ID
Group SID	Token ID
DACL	Token Type
	Expiration time
	Impersonation level

Token 구조체

Process(security관점에서...)

- Is a collection of resources that are being managed by a Particular principal.
- Has its own copy of a token that links back to the logon session

Security Descriptor(SD)

- every named Windows object has a security descriptor
- some unnamed object do, too
- describes the owner and group SIDs for the object along with its ACLs.
- is typically created by the function that creates the object.
- Is data structure that contains all the security settings for an Object

Owner SID
Primary group SID
DACL
SACL

Security descriptor 구조체.

Access Control Lists(ACLs)

- a. enables fine-grained control over access to objects.
- b. Discretionary access control list(DACL)
- c. System access control list(SACL)
- d. Each Access Control Entry(ACE) contains a SID(User, Group, or Computer) and the corresponding rights
- e. each ACE can either Deny or Allow those rights.
- f. Security checks compare ACL's against the caller's token.

DACL

Is basically a list that says who can touch the object and in exactly what way.

SACL

Is a list that says who will be audited if they succeed or fail while attempting to touch the object in a particular way.

여기까지 우리는 몇 가지 용어들을 살펴보고 또한 그 역할과 특징에 대해서도 간략하게 보았다.

다음 번 기고에서는 이러한 기본적인 지식을 바탕으로 device driver에서 어떻게 security가 이루어지는지를 알아보겠다.