# Newbie's Travels To Sandbox

Lee JiHun
wh_pesante@naver.com

# CONTENTS

# Sandbox?

- Derive from sandbox that prevent children getting hurt

- Security mechanism for sepa rating running programs

# Sandbox?

**Sandbox** (controlled environment)


- controlling the resources (for example, fd, memory, file system space, etc.) that a process may use.
- Used for various purposes in different fields

# Sandbox?

## Without Sandbox


Write

Read

## With Sandbox


Write

restricted

MONSTERZ

How to use this in Windows?

# UAC(User Access Control)

- a technology and security infrastructure introduced with Windows Vista and Windows Server 2008

- a feature in Windows that can help you stay in control of your computer by informing you when a program makes a change that requires administrator-level permission

# UAC(User Access Control)

Windows XP

관리자 권한 Access Token


관리자 그룹의 계정

# UAC(User Access Control)

Windows Vista

관리자 권한 Access Token


표준 사용자용 Access Token


관리자 그룹의 계정

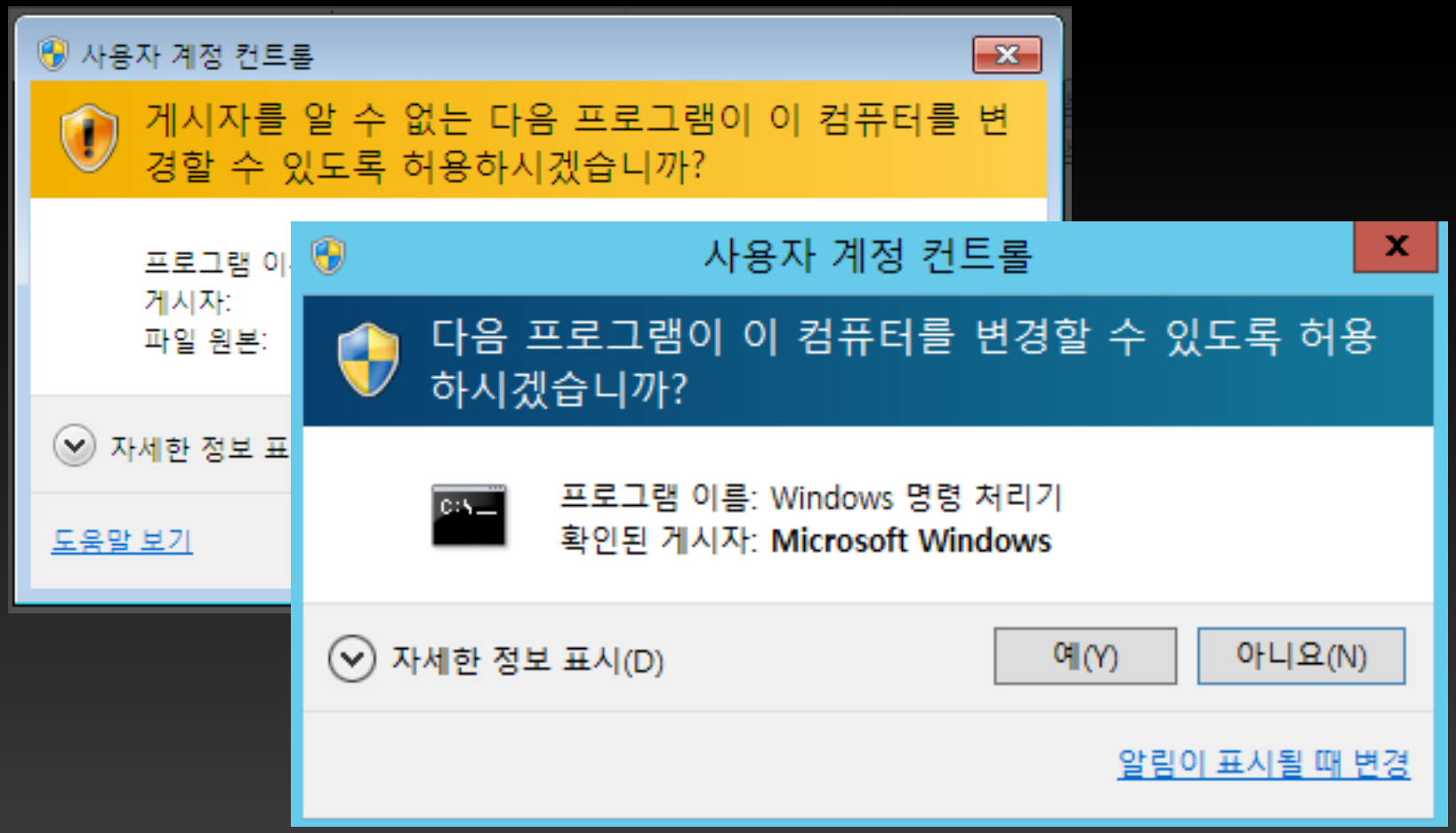
# UAC(User Access Control)


표준 사용자용 Access Token

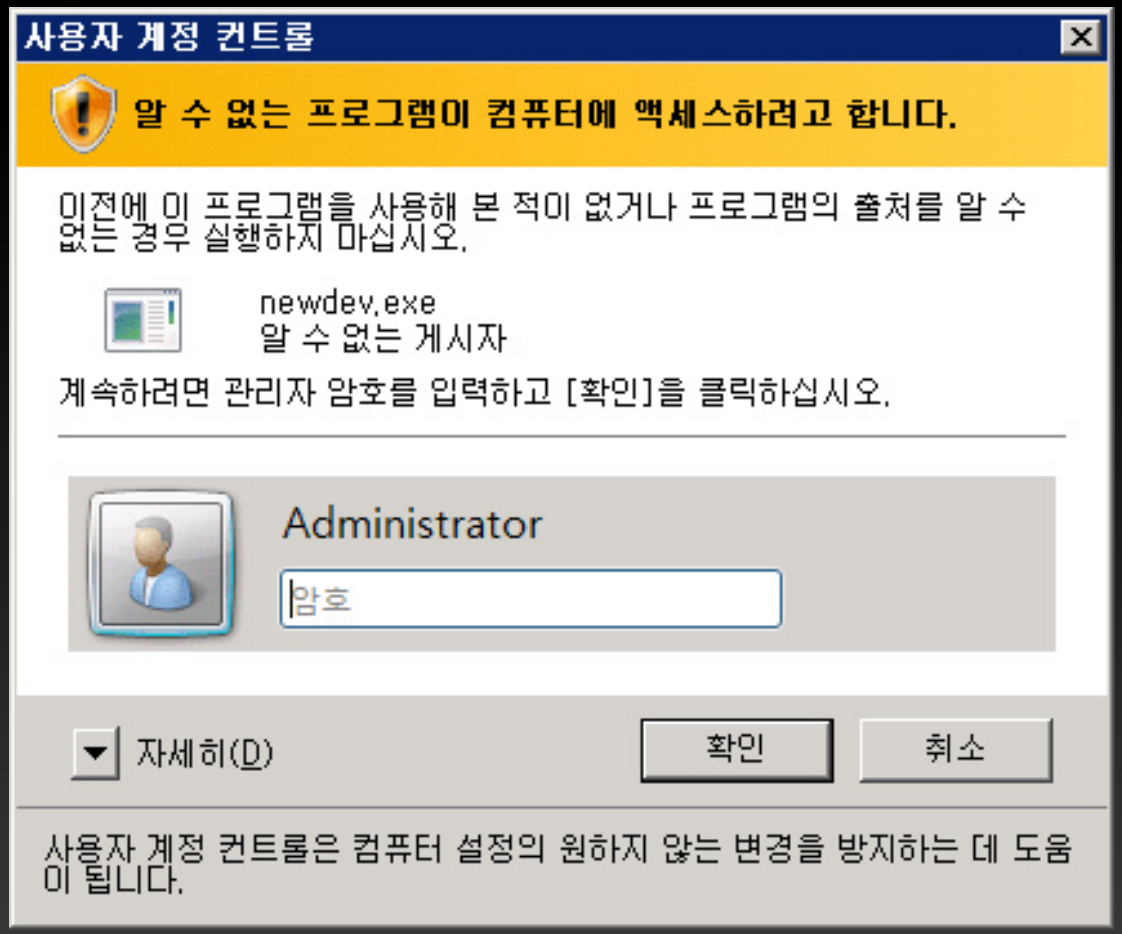


관리자 그룹의 계정

# UAC(User Access Control)



# UAC(User Access Control)



# UAC(User Access Control)


관리자 권한 Access Token


관리자 권한 프로세스 실행

관리자 그룹의 계정

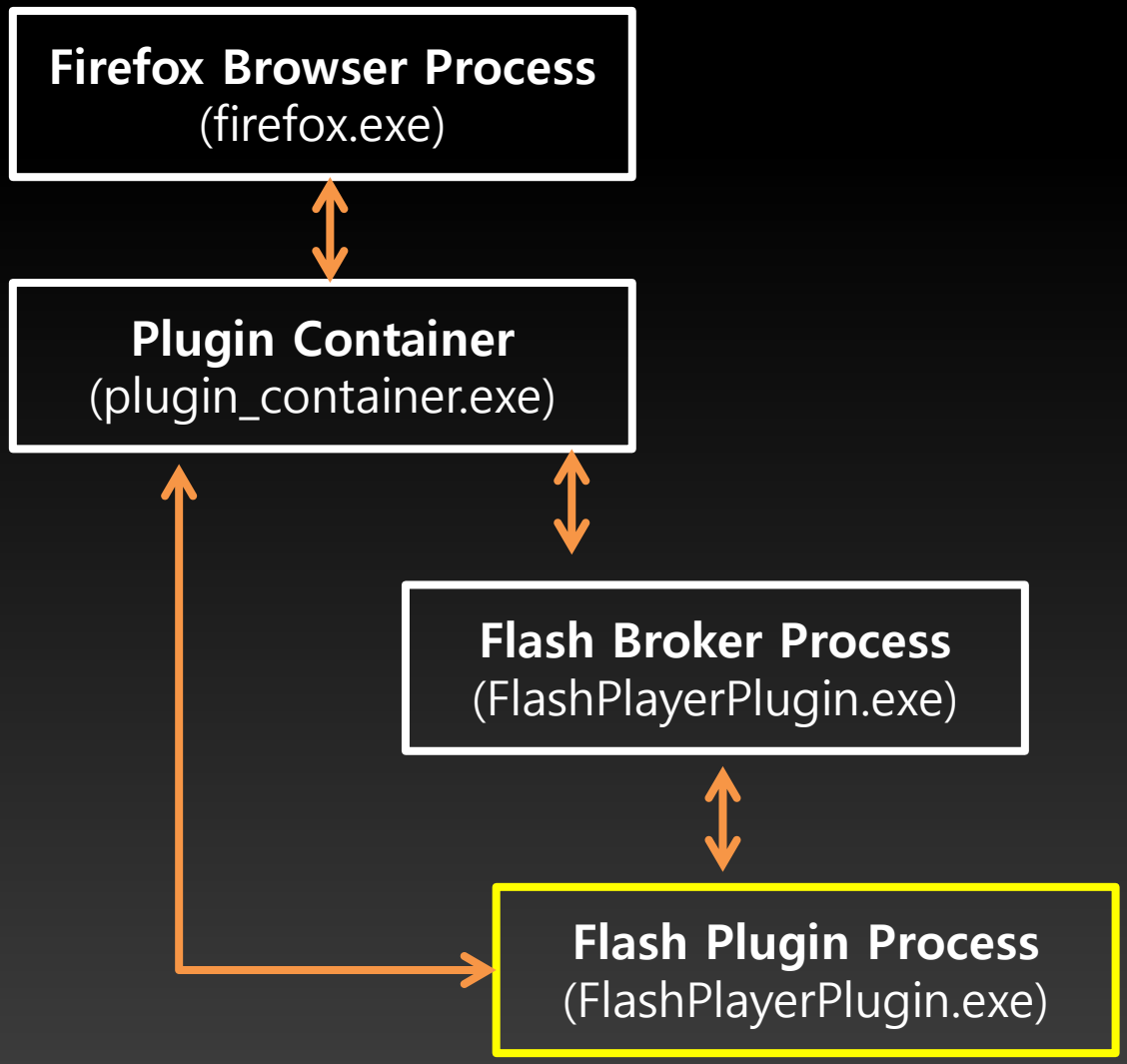
MONSTERZ

How to use this in Flash Player?

# 1. SandBox Architecture

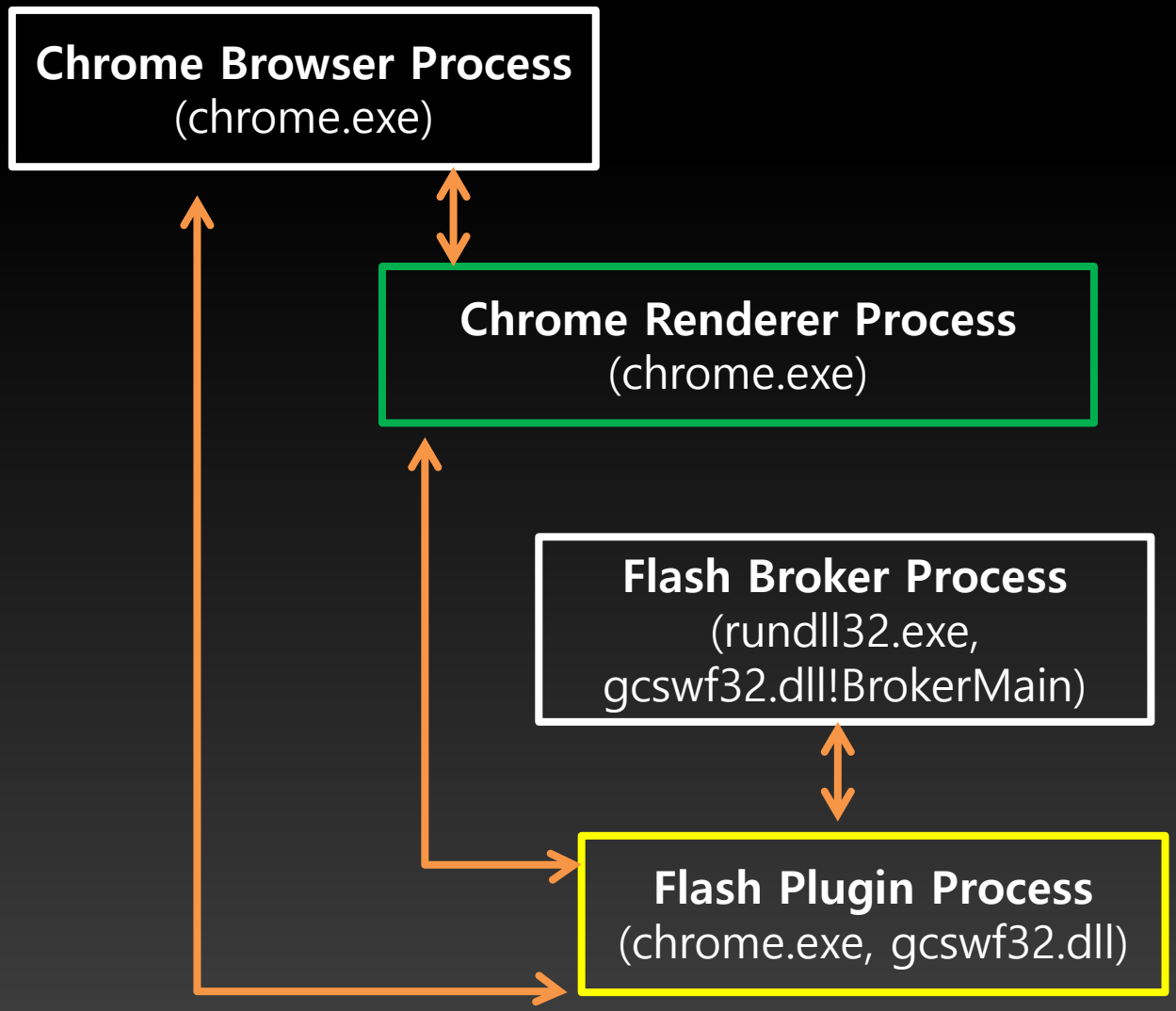
# Sandbox Architecture

## - Flash Player Protected Mode For FireFox



# Sandbox Architecture

- Flash Player Protected Mode For Chrome



# 2. SandBox Mechanisms

# Sandbox Restrictions


1. Restricted Token
2. Intergrity Level
3. Job Objects

# Sandbox Restrictions

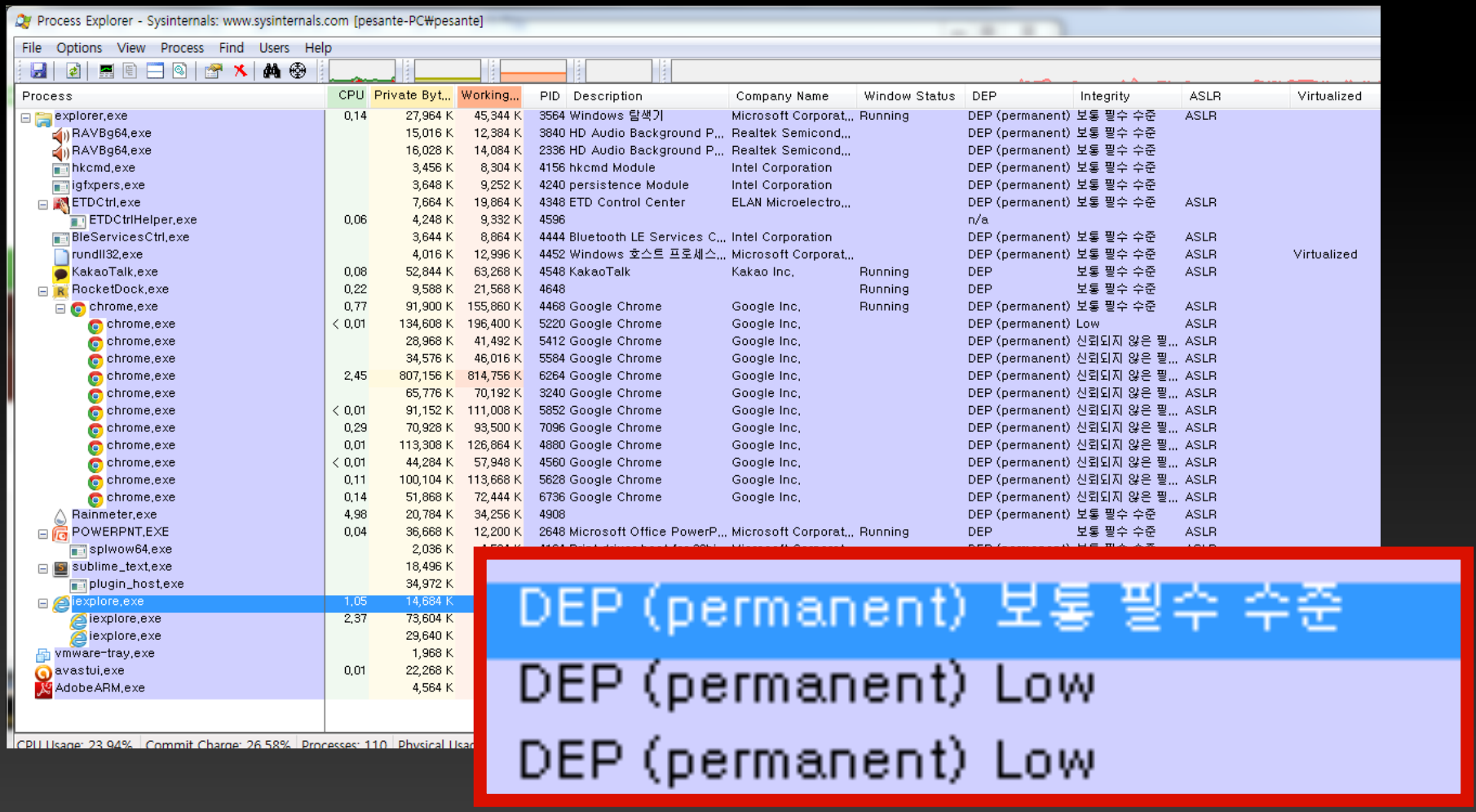
## - Restricted Token

1. Restricted Token

2. Limited Privileges

# Sandbox Restriction

## - Intergrity levels



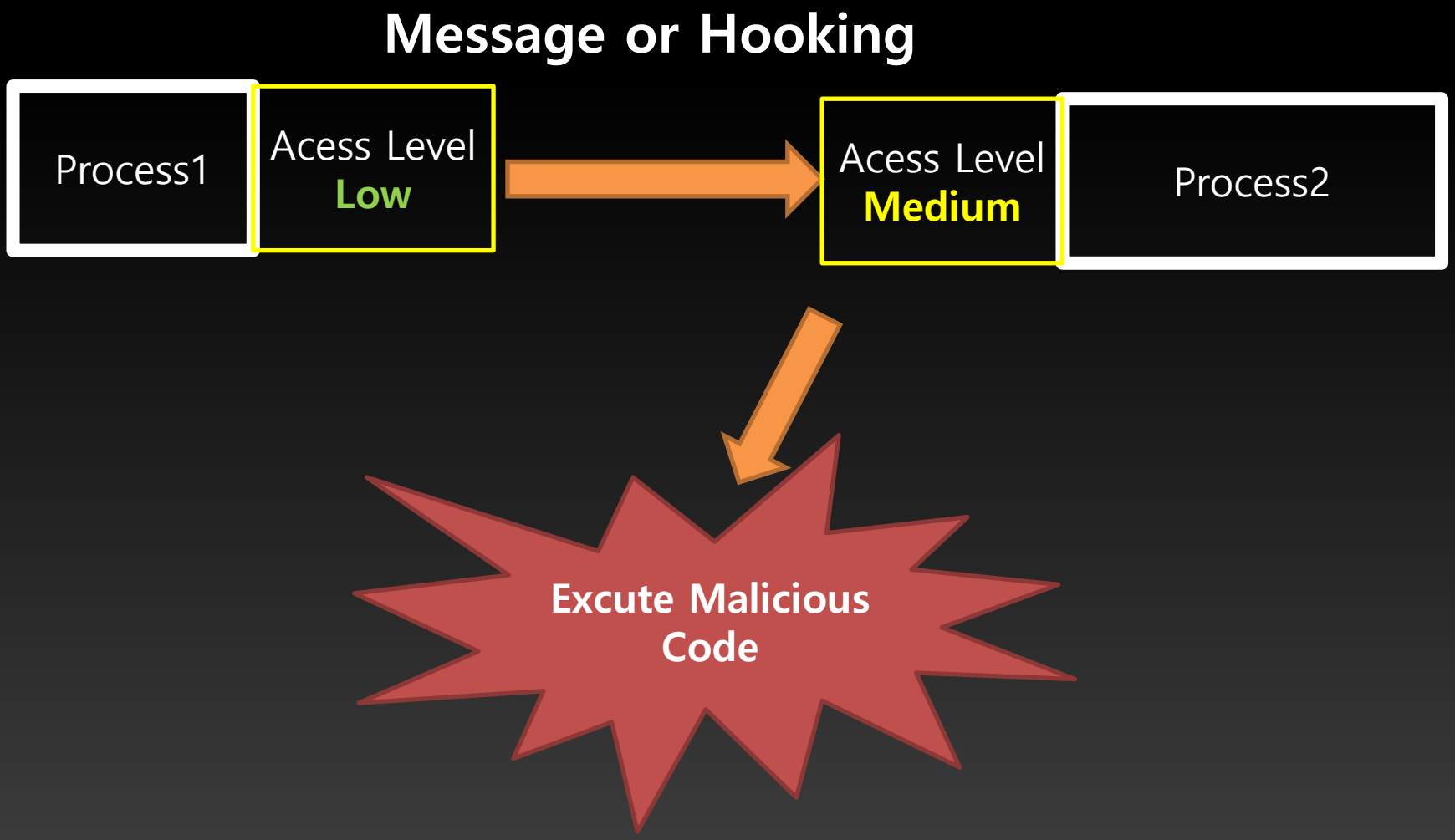
# MIC(Mandatory Integrity Mechanism)

| 무결성 접근 수준 | 시스템 권한 |
| --- | --- |
| 높음 (High IL) | 관리자 (프로세스에서 Program Files 폴더에 파일을 설치하고 HKEY_LOCAL_MACHINE 같은 중요한 레지스트리 영역에 기록) |
| 보통 (Medium IL) | 사용자 (프로세스에서 사용자의 문서 폴더에 파일을 만들고 수정하며 HKEY_CURRENT_USER 같은 레지스트리의 사용자 관련 영역에 기록 |
| 낮음 (Low IL) | 신뢰 안 함 (프로세스에서 Temporary Internet Files₩Low 폴더 또는 HKEY_CURRENT_USER₩Software₩LowRegistry 키처럼 무결성 수준이 낮은 위치에만 기록) |

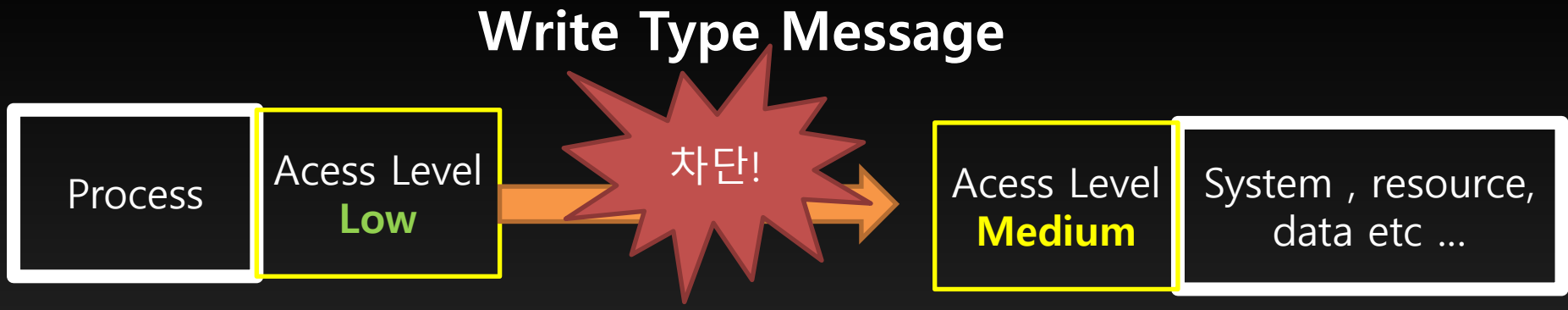
# UIPI(User Interface Privilege Isolation)

- restrictions in the windows subsystem that prevents lower-privilege applications from sending window messages or installing hooks in higher-privilege processes

# UIPI(User Interface Privilege Isolation)

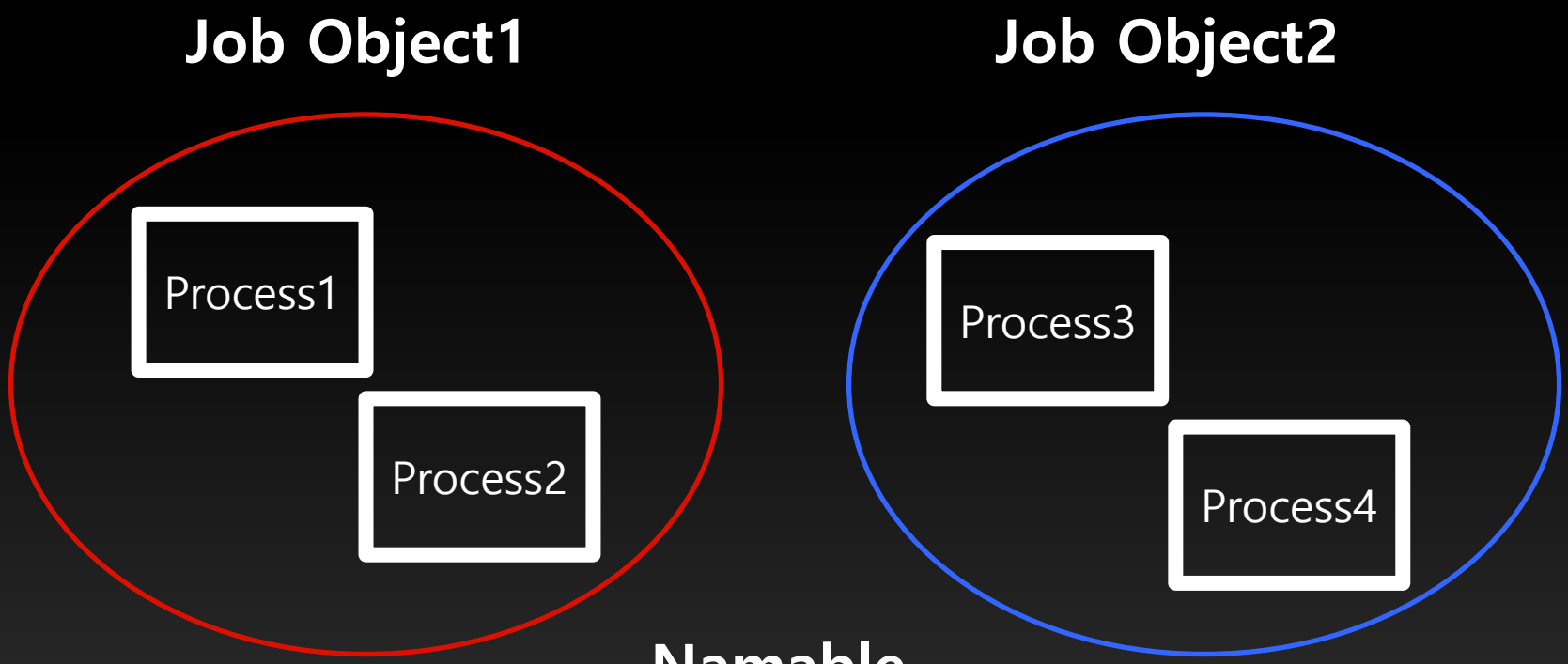


# UIPI(User Interface Privilege Isolation)



# Sandbox Restriction

- Job Objects

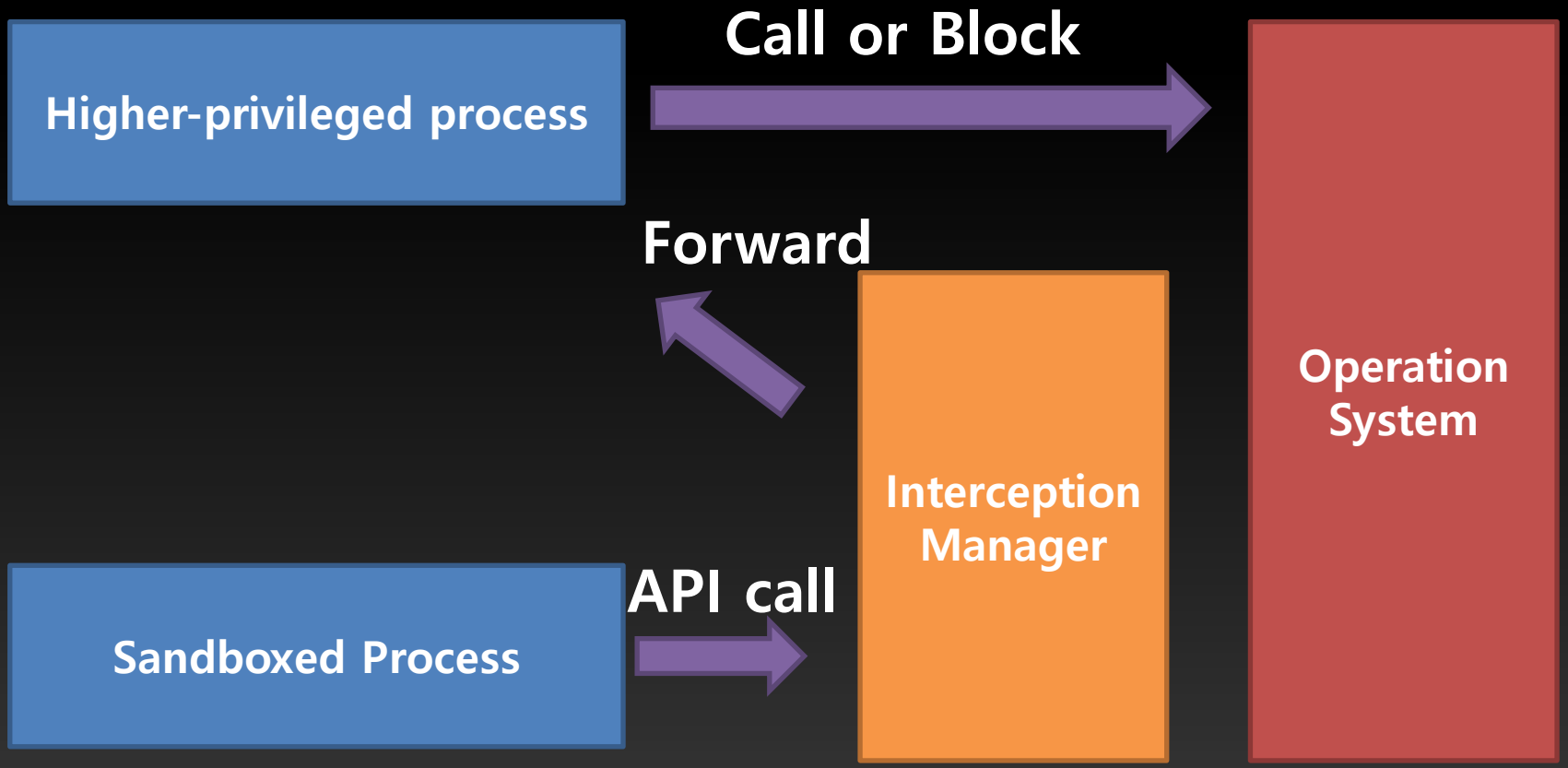



-Namable

-Securable

-Sharable

# Interception Manager

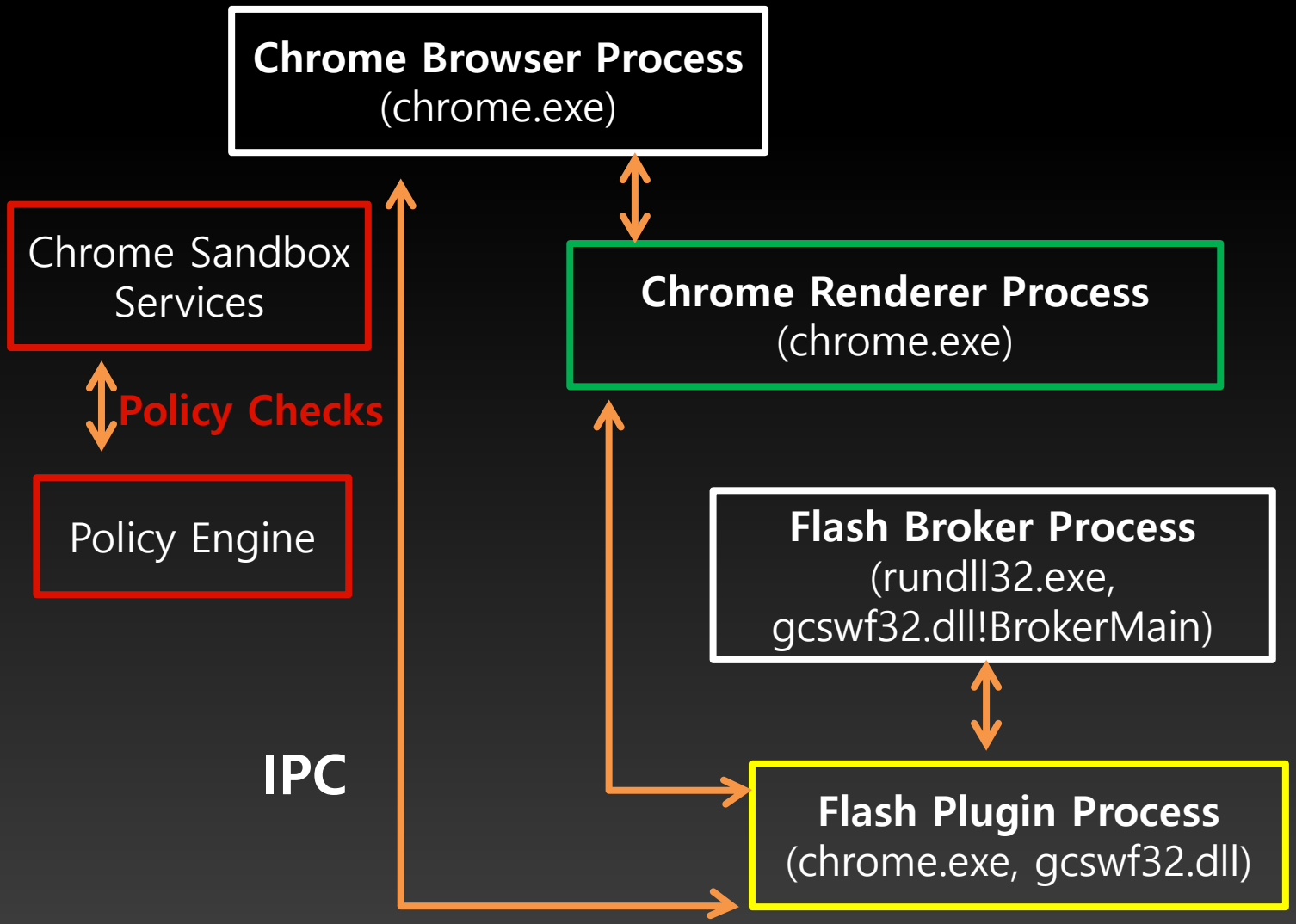


# Services

- we will now take a look at the services exposed by the different processes that are part of the Flash sandbox implementations.

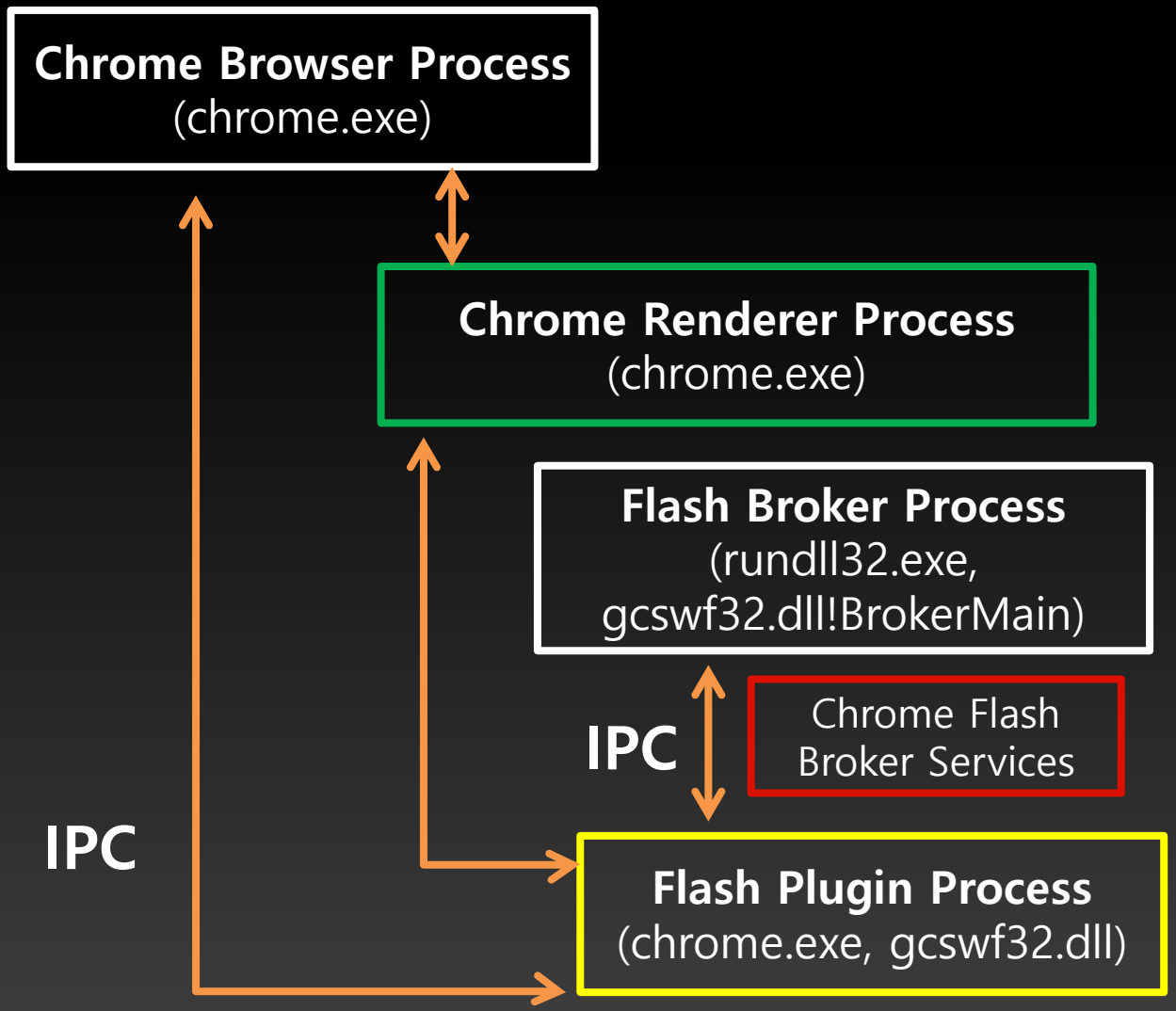
# Service

## - Chrome Sandbox Services



# Service

## - Chrome Flash Broker Services

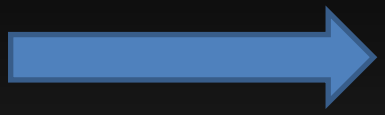


# Service

## - Firefox Flash Broker Services

1. Sandbox Services
2. Flash Services
3. Permission Services

# Policy Engine

접근허용

AddRule(subsystem, semantics, pattern)

# Policy Engine

| Subsystem | Description |
|---|---|
| **SUBSYS_FILES** | Creation and opening of files and pipes. |
| **SUBSYS_NAMED_PIPES** | Creation of named pipes. |
| **SUBSYS_PROCESS** | Creation of child processes. |
| **SUBSYS_REGISTRY** | Creation and opening of registry keys. |
| **SUBSYS_SYNC** | Creation of named sync objects. |
| **SUBSYS_MUTANT** | Creation and opening of mutant objects. |
| **SUBSYS_SECTION** | Creation and opening of section objects. |

# Policy Engine

| Semantics | Description |
|---|---|
| FILES_ALLOW_ANY | Allows open or create for any kind of access that the file system supports. |
| FILES_ALLOW_READONLY | Allows open or create with read access only. |
| FILES_ALLOW_QUERY | Allows access to query the attributes of a file. |
| FILES_ALLOW_DIR_ANY | Allows open or create with directory semantics only. |
| NAMEDPIPES_ALLOW_ANY | Allows creation of a named pipe. |
| PROCESS_MIN_EXEC | Allows to create a process with minimal rights over the resulting process and thread handles. No other parameters besides the command line are passed to the child process. |
| PROCESS_ALL_EXEC | Allows the creation of a process and return fill access on the returned handles. This flag can be used only when the main token of the sandboxed application is at least INTERACTIVE. |
| EVENTS_ALLOW_ANY | Allows the creation of an event with full access. |
| EVENTS_ALLOW_READONLY | Allows opening an event with synchronize access. |
| REG_ALLOW_READONLY | Allows read-only access to a registry key. |
| REG_DENY | Deny all access to a registry key. |
| MUTANT_ALLOW_ANY | Allows creation of a mutant object with full access. |
| SECTION_ALLOW_ANY | Allows read and write access to a section. |
| REG_ALLOW_ANY | Allows read and write access to a registry key. |

# Policy Engine

## - Admin-configurable policies

- %WINDIR%₩System32₩Macromed₩Flash
  for 32-bitWindows

- %WINDIR%₩SysWow64₩Macromed₩Flash
  for 64-bitWindows

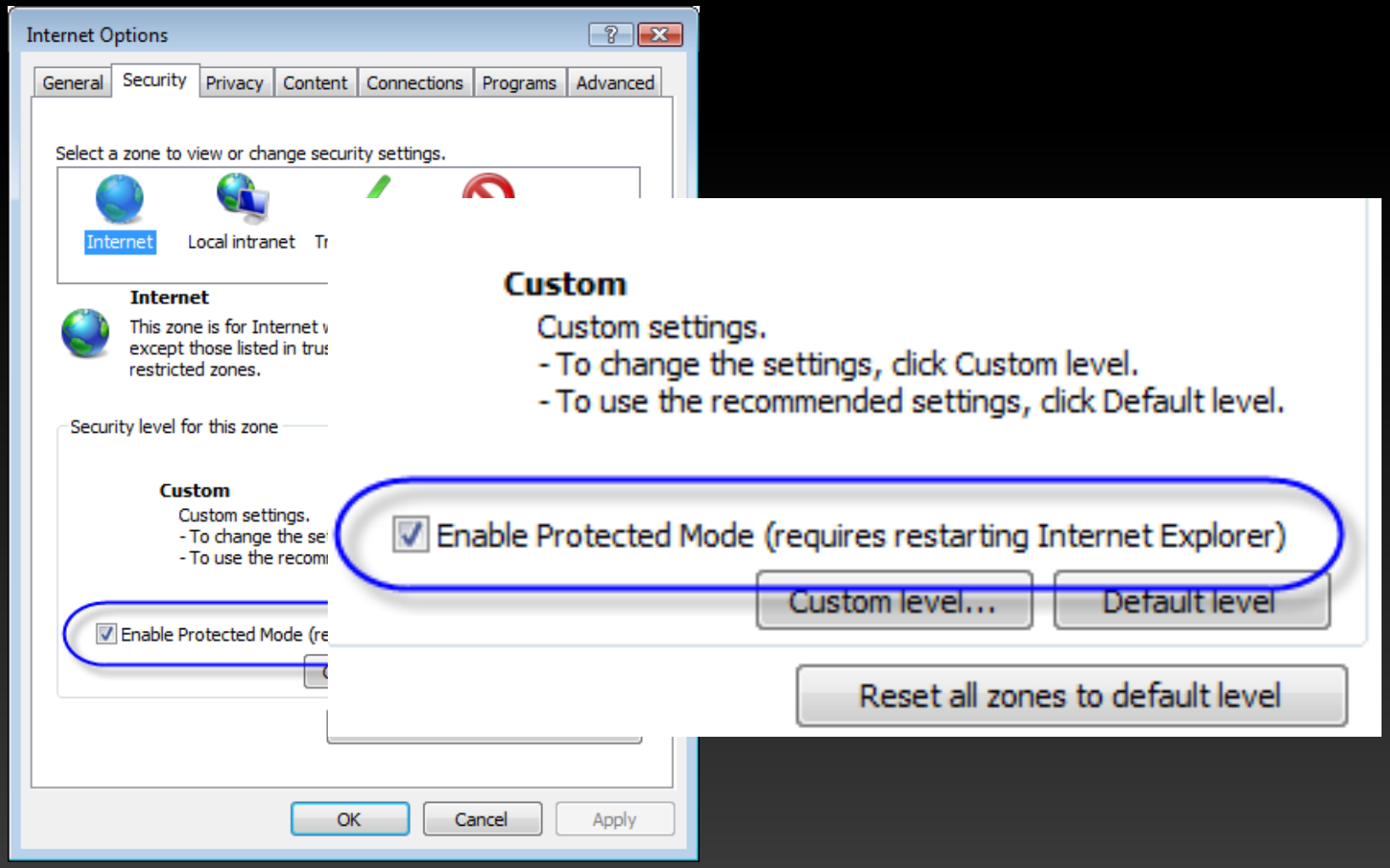
*ProtectedModeWhitelistConfig.txt*

How to use this in IE?

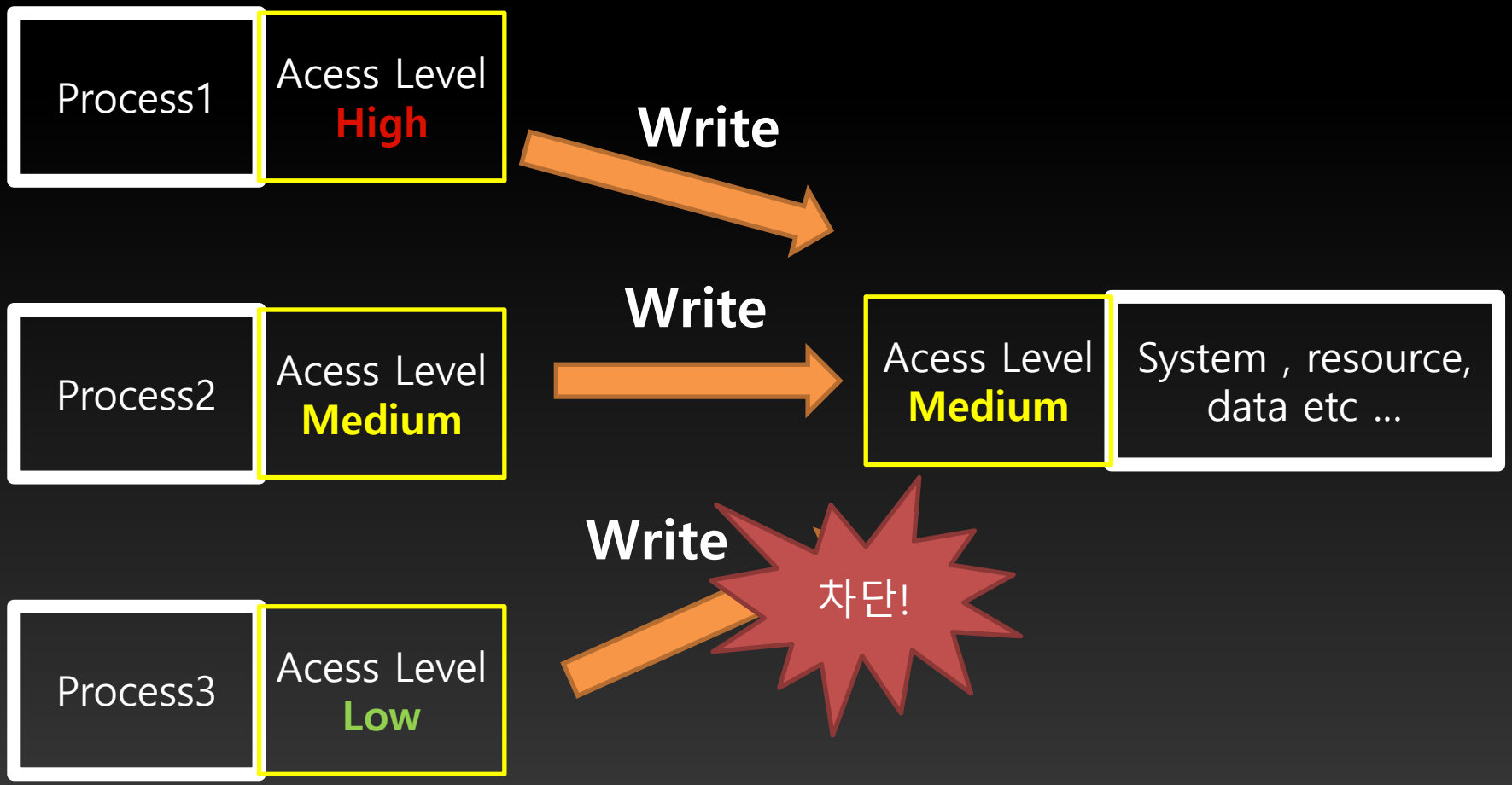
# Protected Mode in IE7

- In Windows Vista, Internet Explorer 7 runs in Protected Mode, which helps protect users from attack by running the Internet Explorer process with greatly restricted privileges. Protected Mode significantly reduces the ability of an attack to write, alter, or destroy data on the user's machine or to install malicious code.

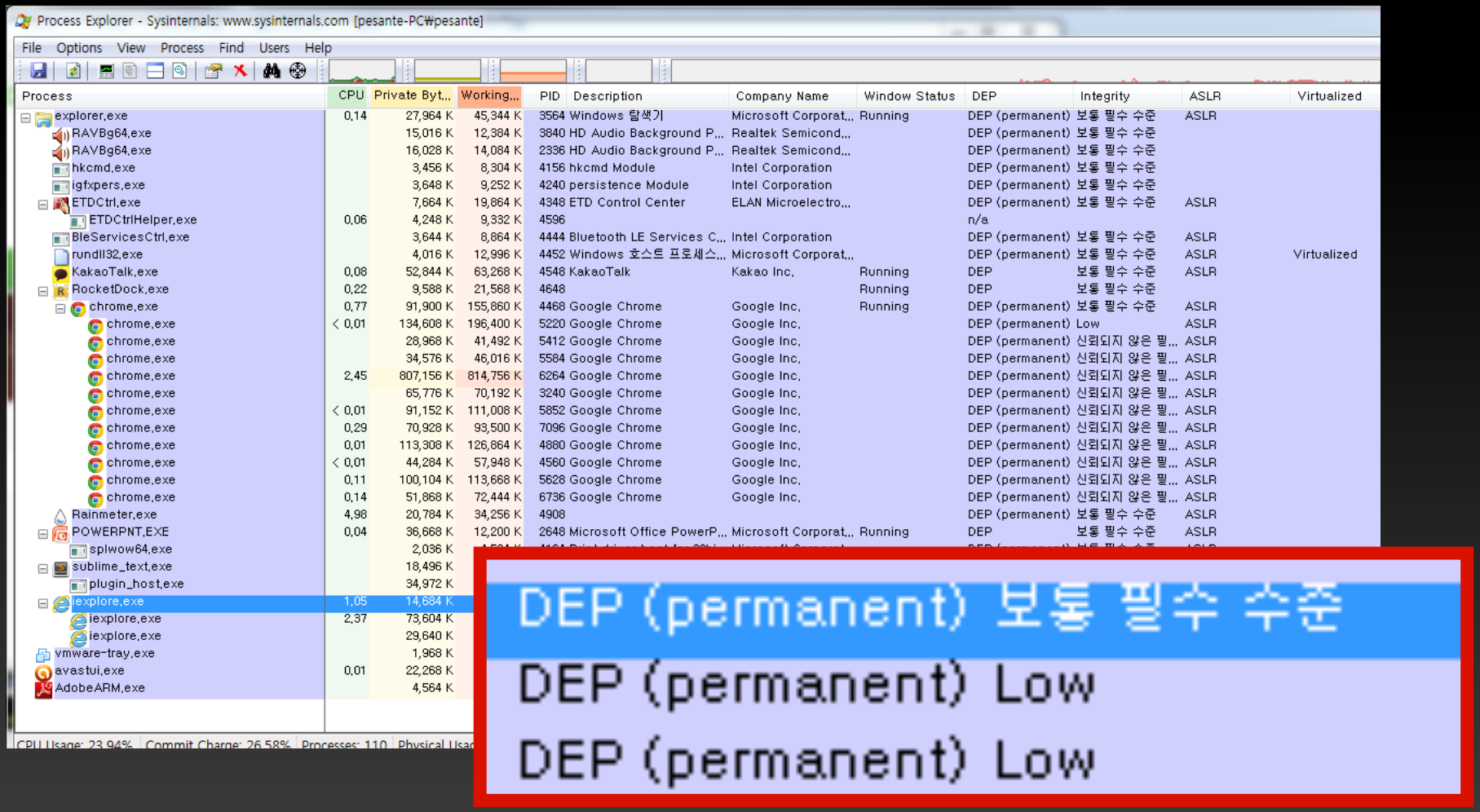
# Protected Mode in IE7



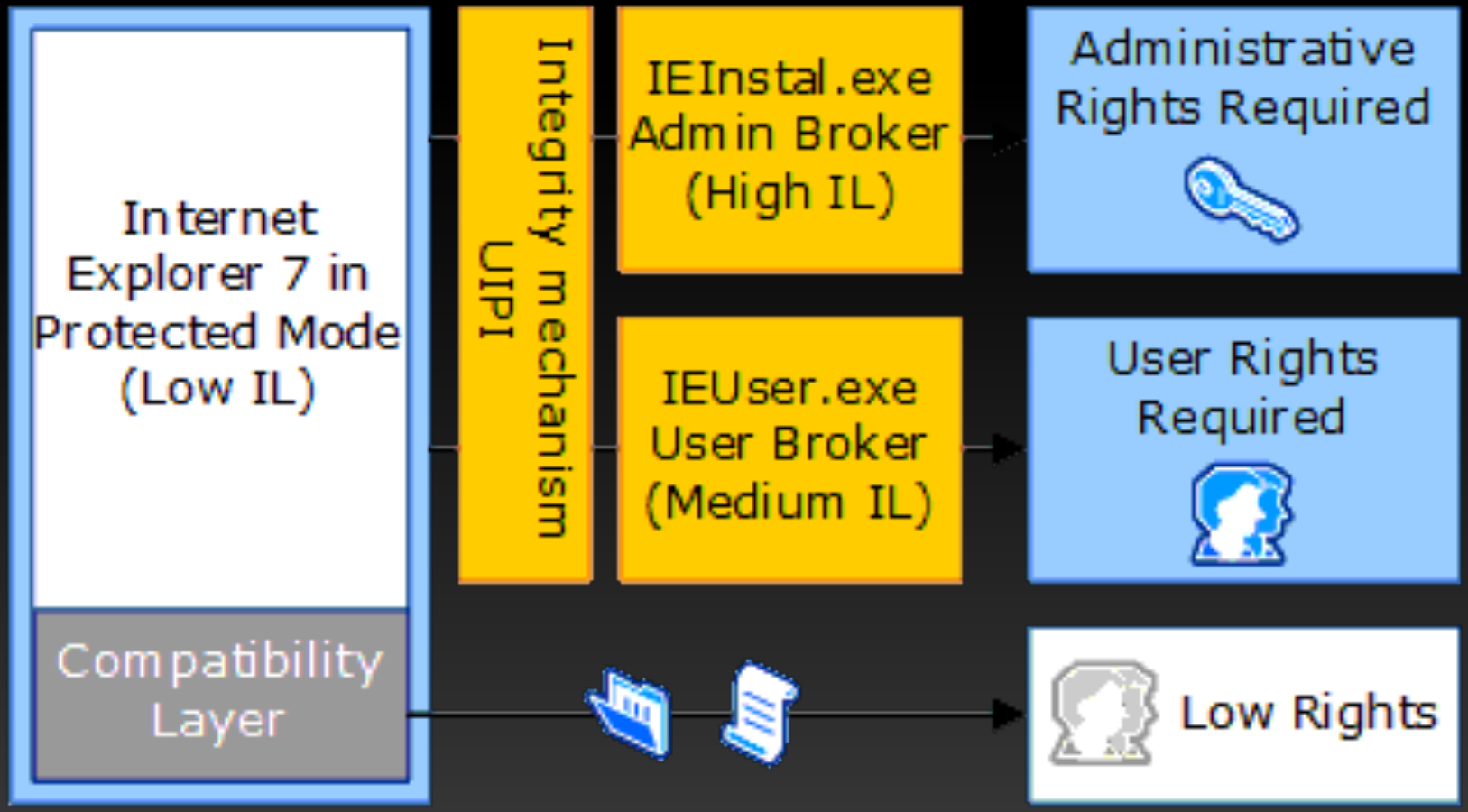
# Protected Mode in IE7



# Protected Mode in IE7



# How to Activate IE7 in PM

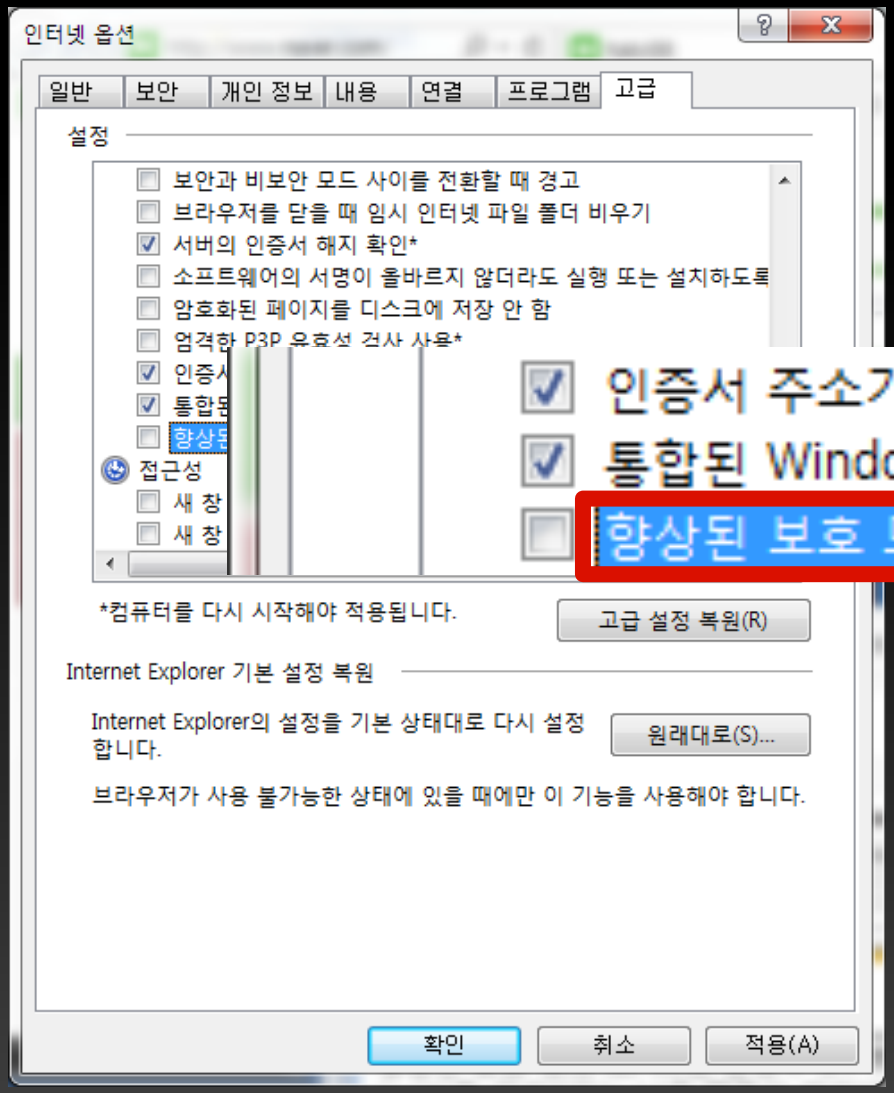


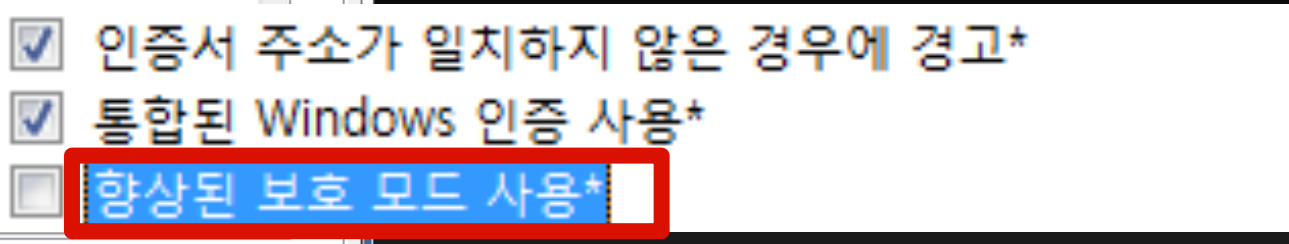
# Enhanced Protected Mode

-“Enhanced” Protected Mode takes this concept further by restricting additional capabilities

-Enhanced Protected Mode (EPM) adds additional security to Protected Mode and includes AppContainer and 64-bit tabs.

# Enhanced Protected Mode



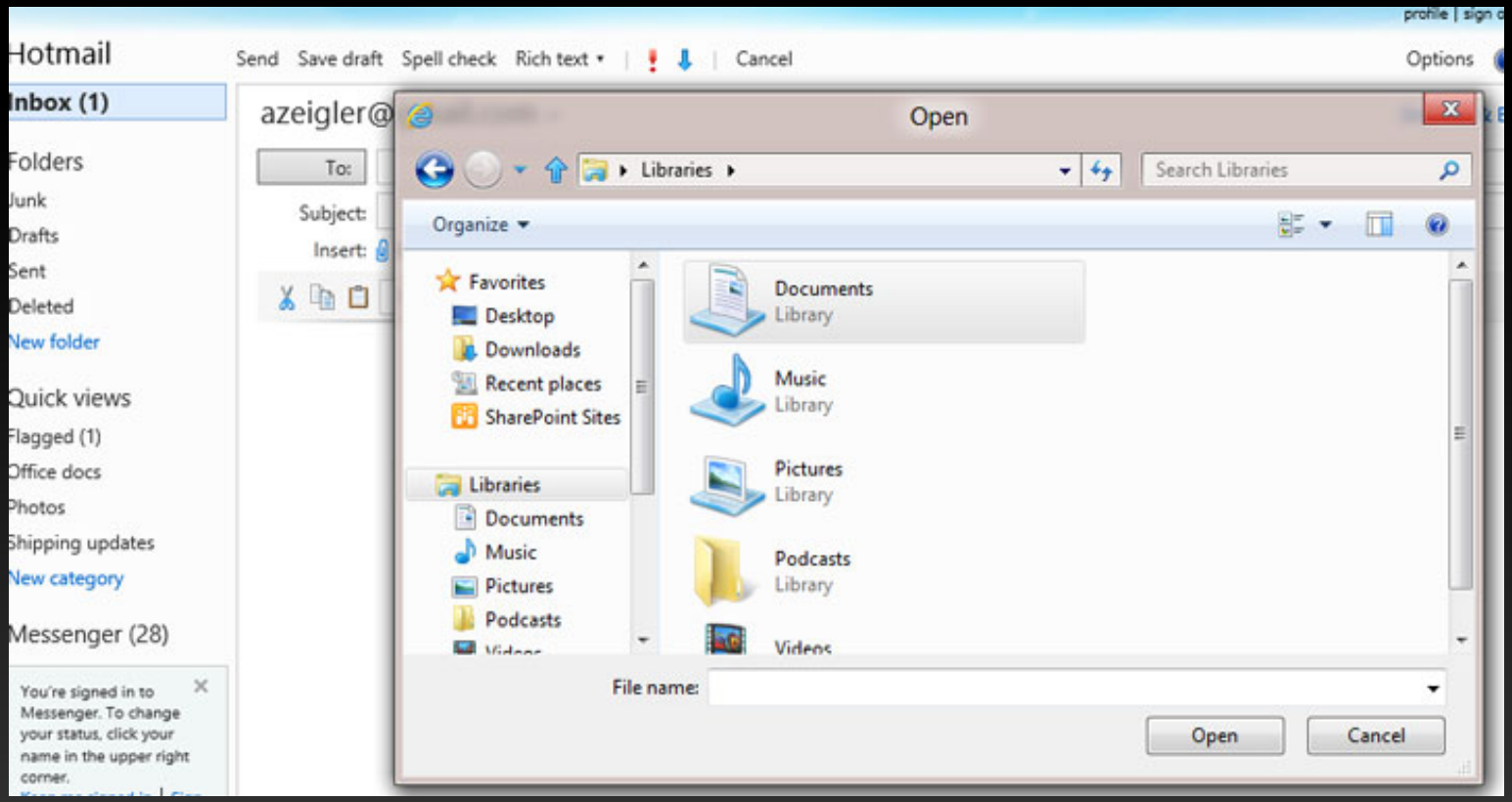



# Enhanced Protected Mode


- 64bit Processes

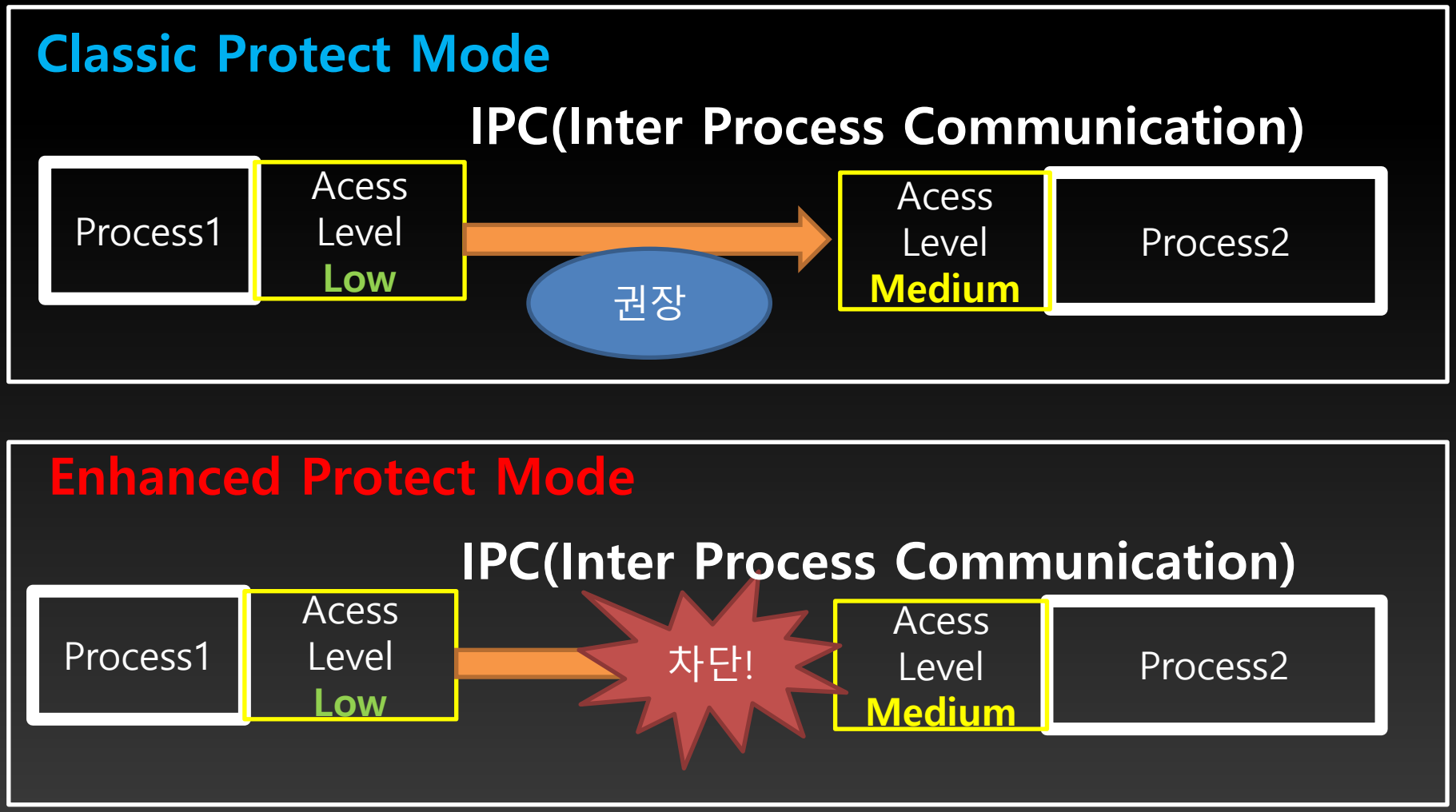
- More Effective in ASLR

# Enhanced Protected Mode

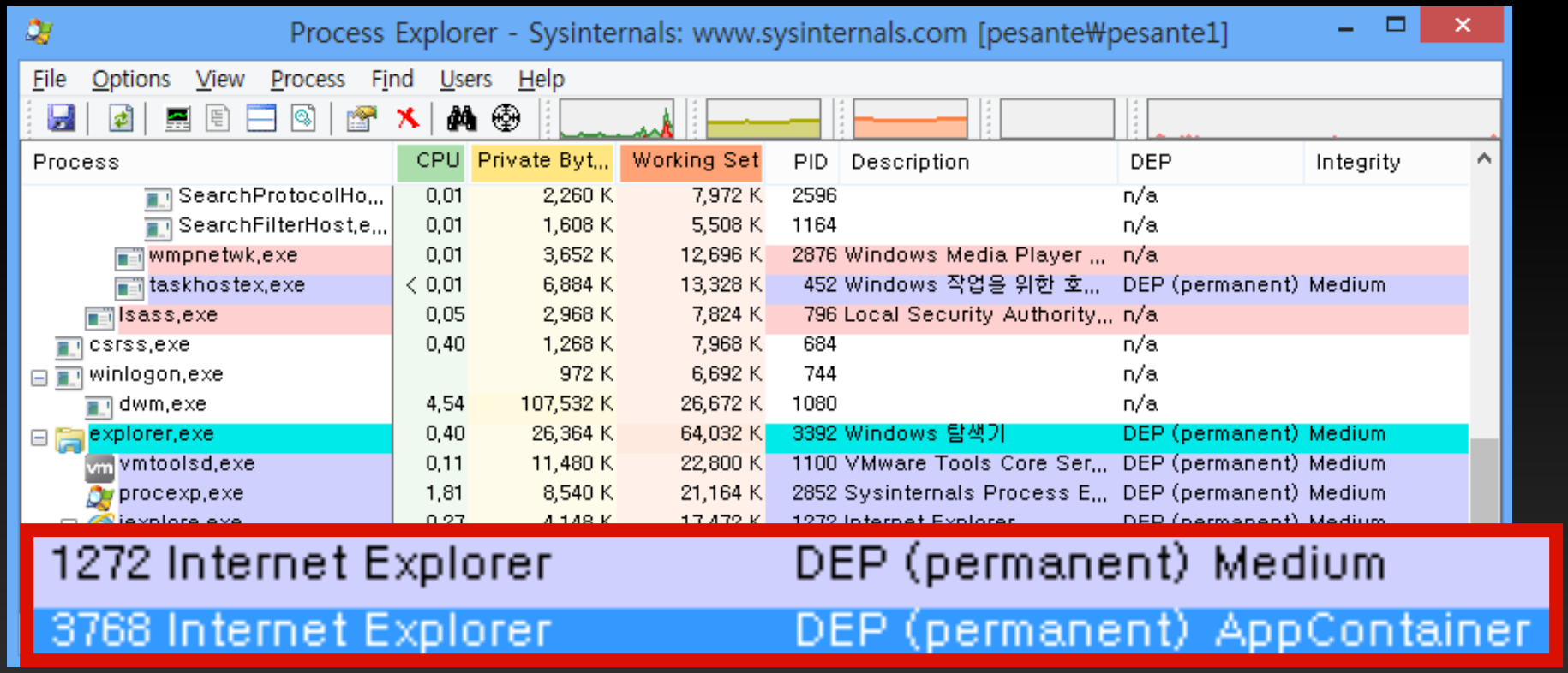



- Read access to the file system (and registry) is blocked

# Enhanced Protected Mode



# Enhanced Protected Mode




- AppContainer와 호환

# What is App Container?

# What is App Container?

- By default, an app can access only its AppData folder (including local, roaming, and temp sub-folders, all of which are deleted when a user uninstalls an app).

# What is App Container?

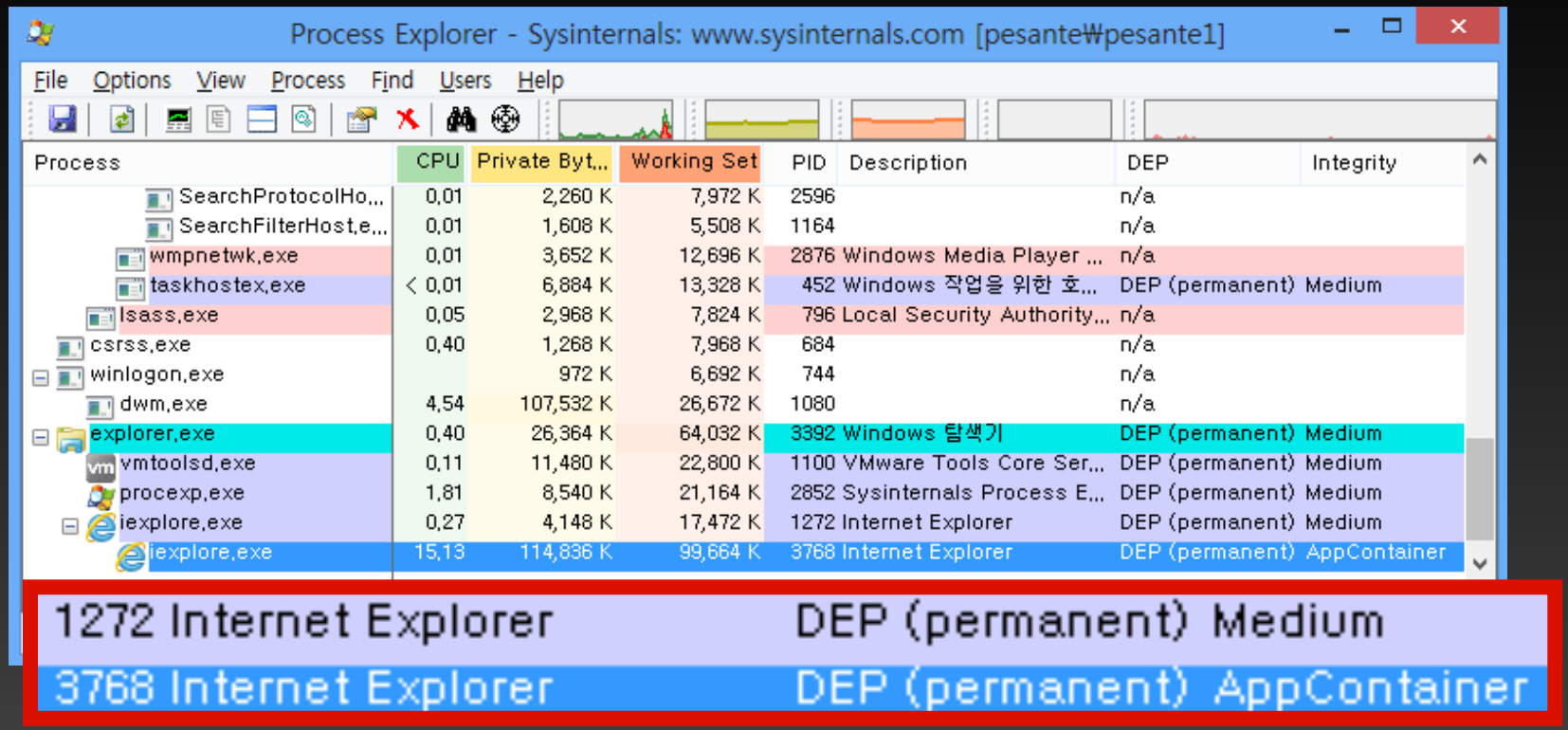
- To directly access anything else through APIs, such as media libraries or documents, an app must declare that intent in its app manifest or a user must grant access by explicit action. Otherwise the APIs used to access the file system will fail

# What is App Container?

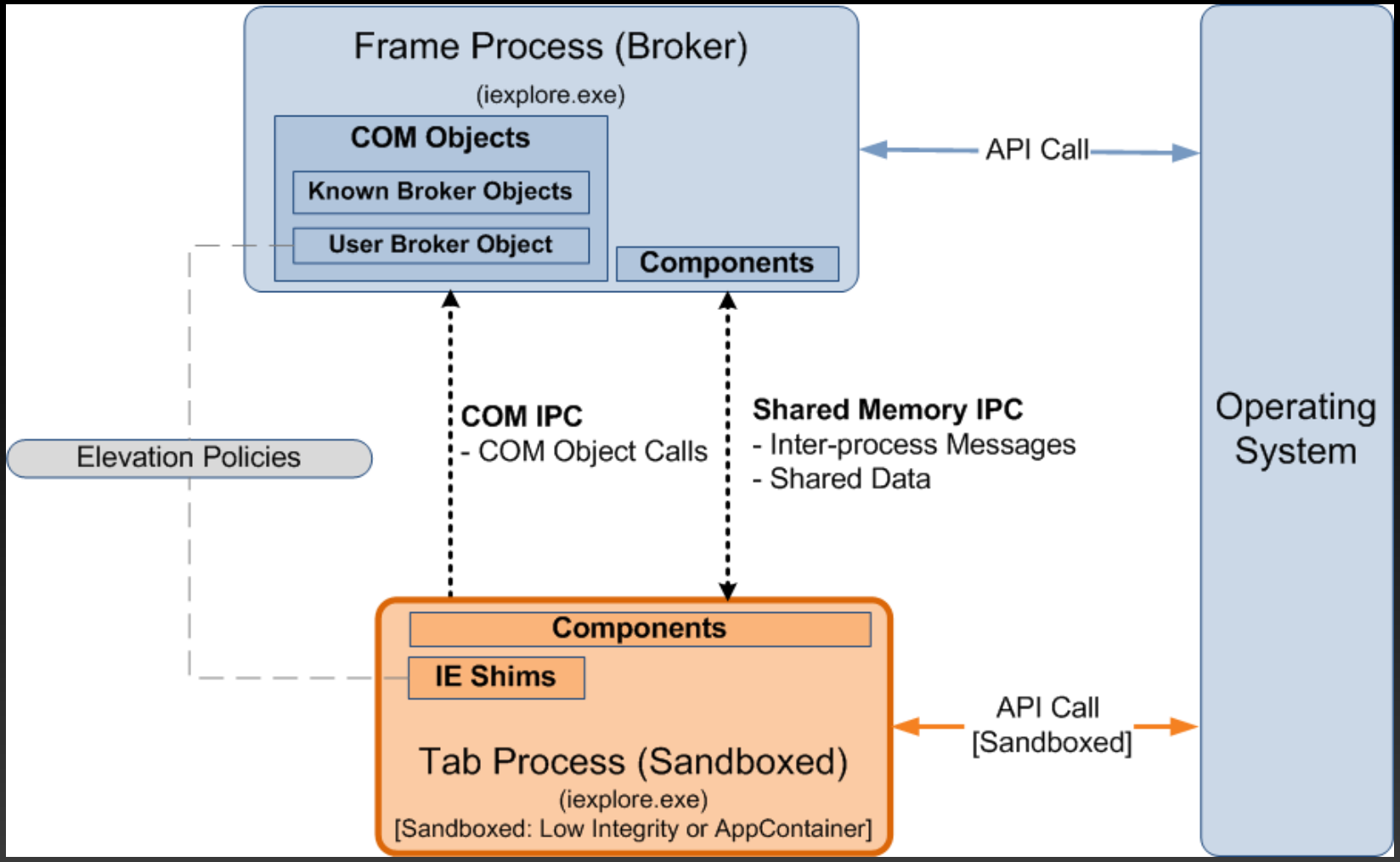
# Integrity Levels and App Container

- App Container is actually its own integrity level.

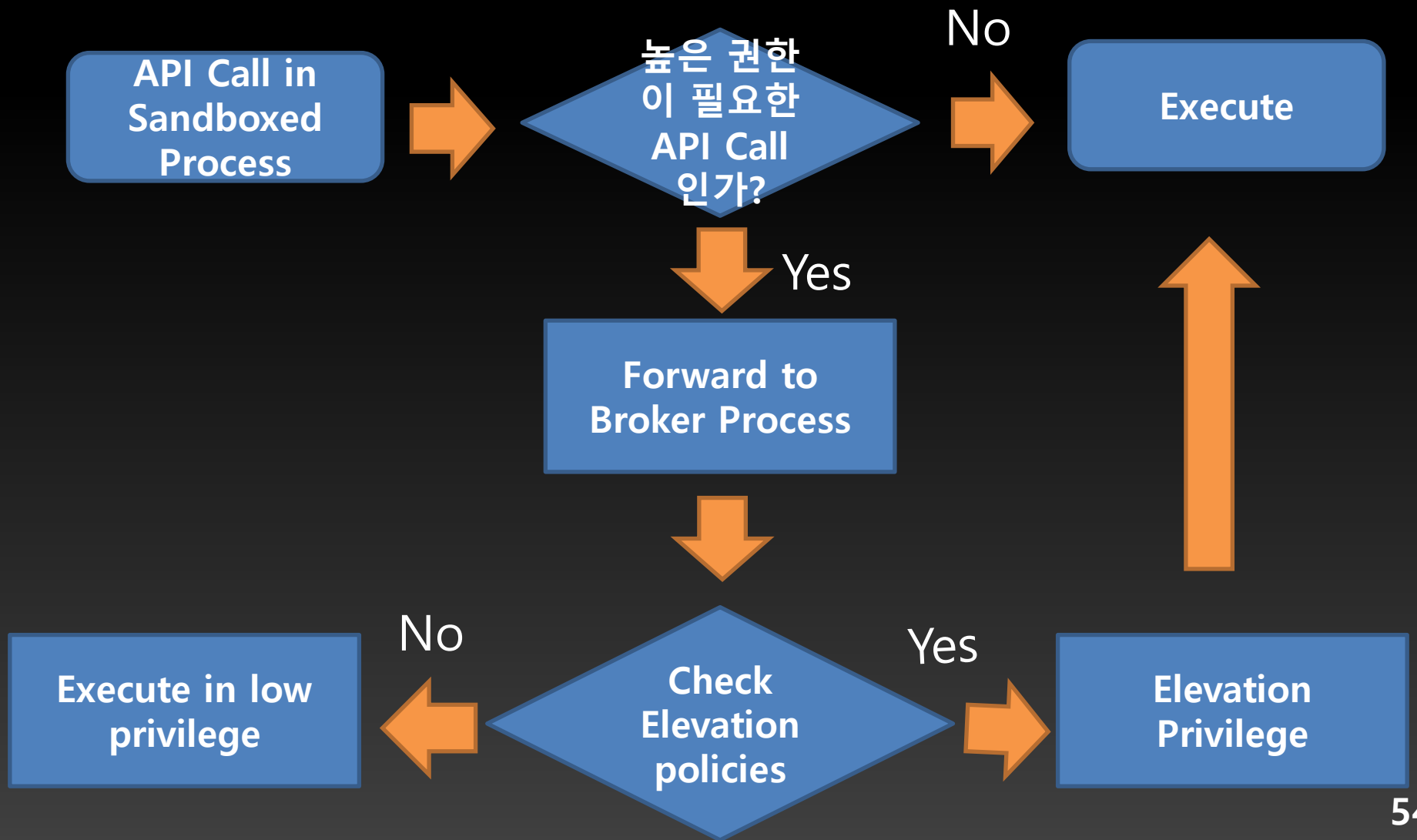
This can be seen in the screen shot below:



# EPM Architecture

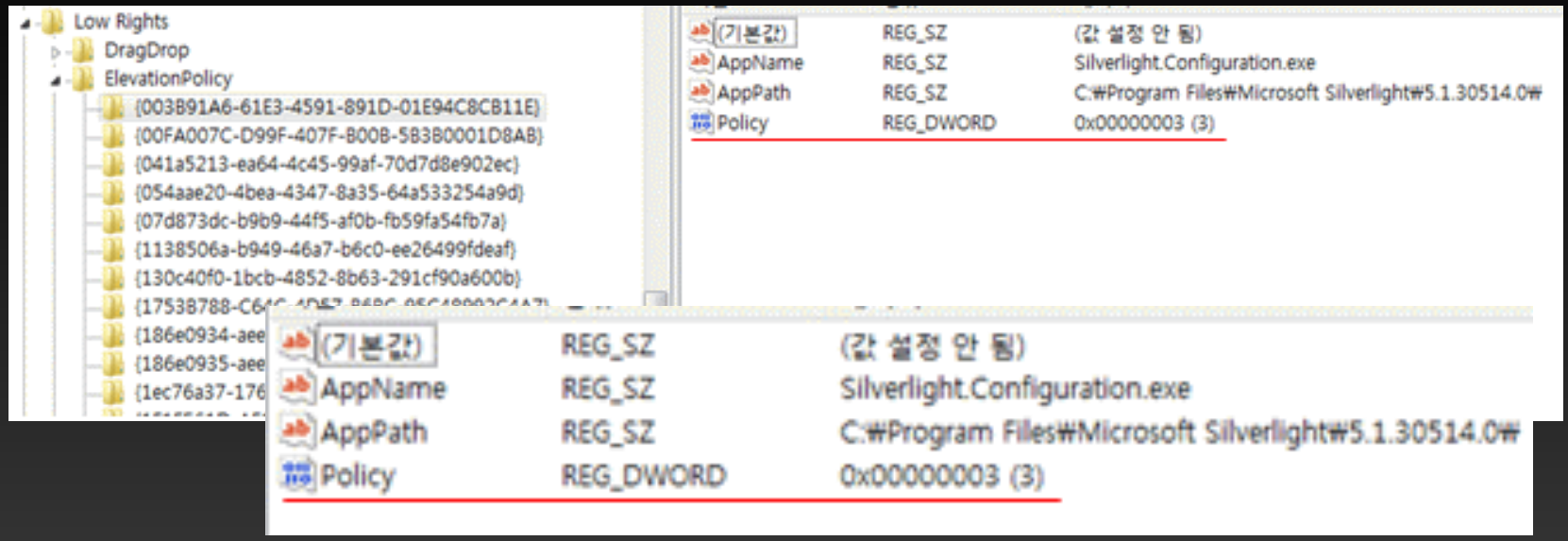


# IE SHIMS (COMPATIBILITY LAYER)



# Elevation Policy

- HKLM₩Software₩Microsoft₩Internet Explorer₩Low Rights₩ElevationPolicy₩<GUID>



# Elevation Policy

| 값 | 결과 |
| --- | --- |
| 3 | 보호 모드에서 브로커를 자동으로 무결성 수준이 보통인 프로세스로 시작합니다. |
| 2 | 보호 모드에서 프로세스를 시작할 수 있는 권한을 사용자에게 확인하도록 요청합니다. 권한이 부여되면 프로세스는 무결성 수준이 보통인 프로세스로 시작됩니다. |
| 1 | 보호 모드에서 브로커를 자동으로 무결성 수준이 낮은 프로세스로 시작합니다. |

# Conclude..

THANK YOU!