



Newbie's Travels To Sandbox

Lee JiHun
wh_pesante@naver.com

CONTENTS



- 1. SandBox?**
- 2. Sandbox in Flash Player**
 - Chrome
 - Firefox
- 3. Sandbox in IE**

Sandbox?



- Derive from sandbox that prevent children getting hurt
- Security mechanism for separating 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



With Sandbox



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)

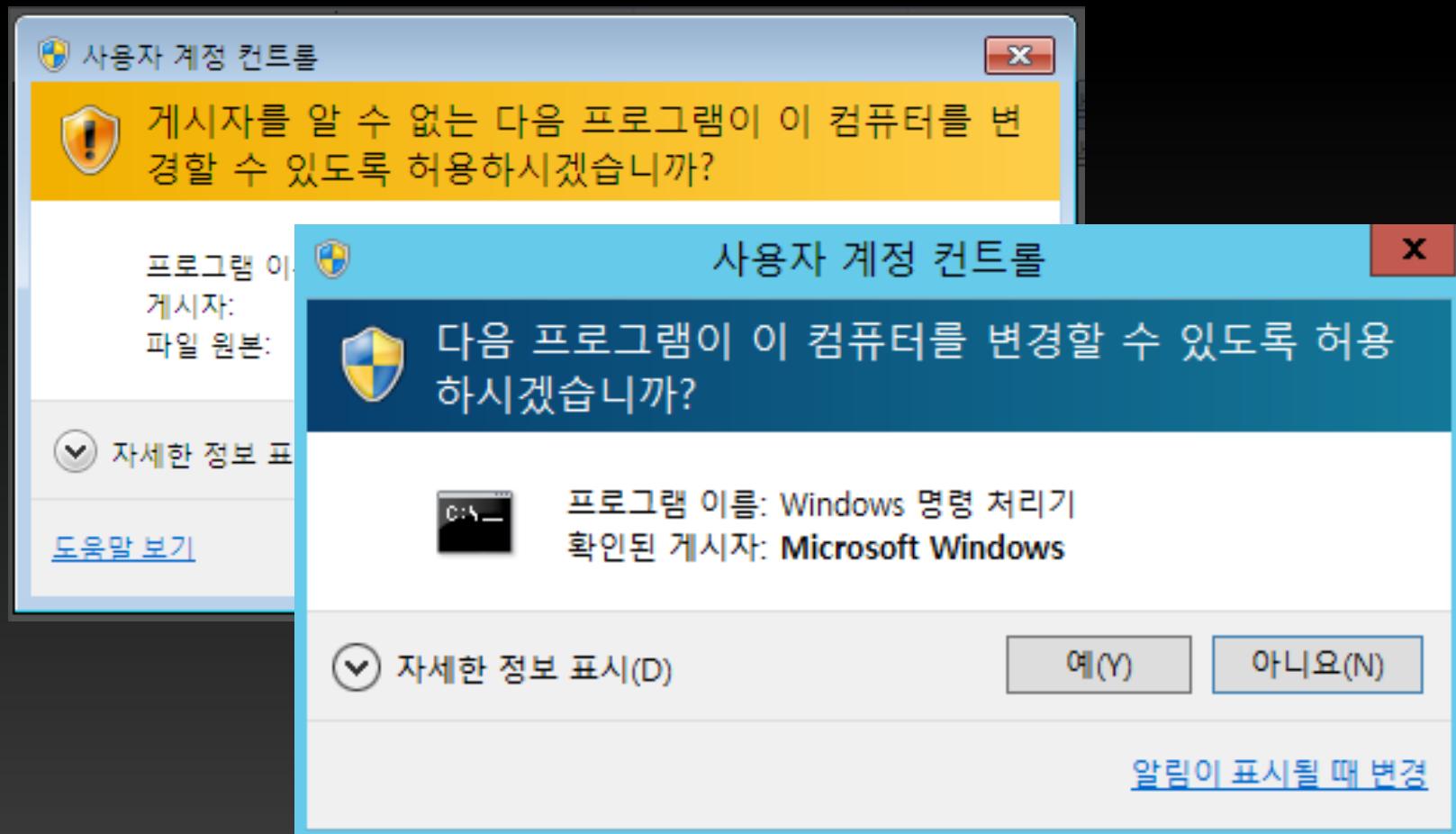


표준 사용자용 Access Token

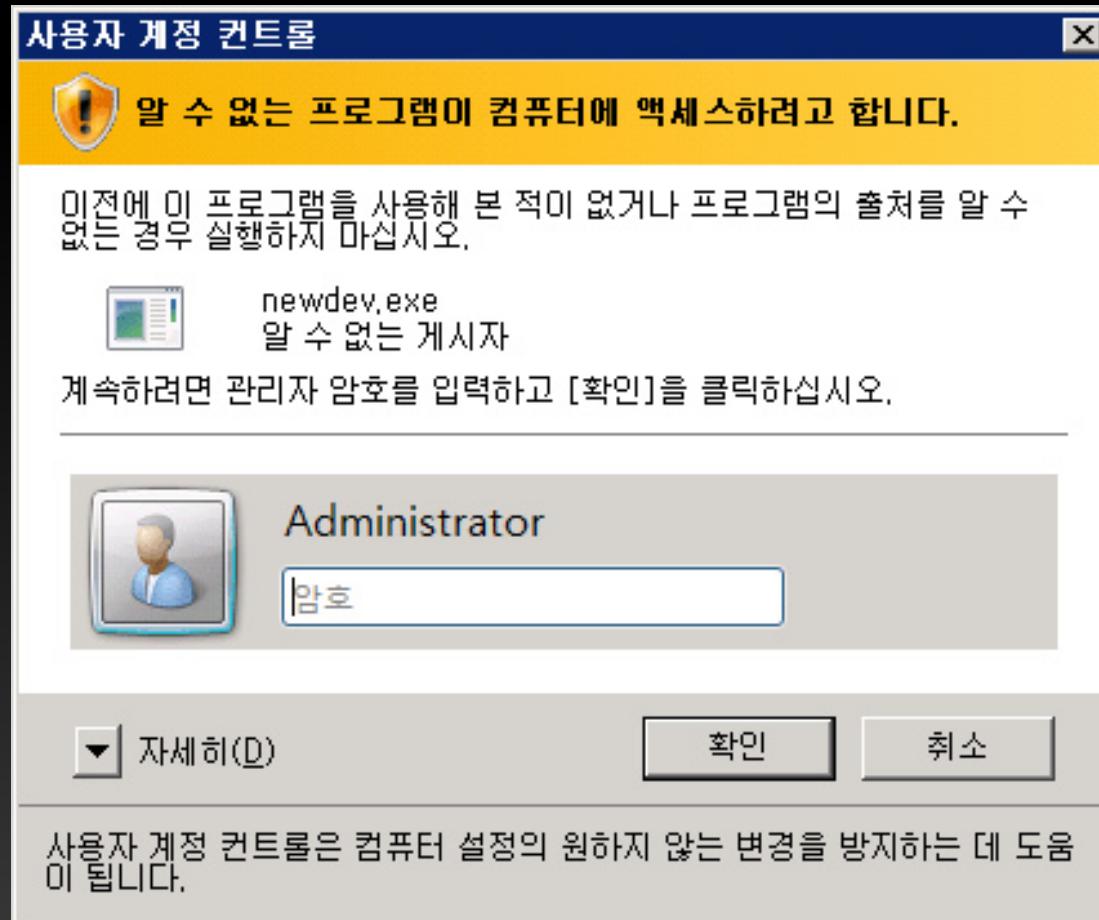


관리자 그룹의 계정

UAC(User Access Control)



UAC(User Access Control)



UAC(User Access Control)



관리자 권한 Access Token



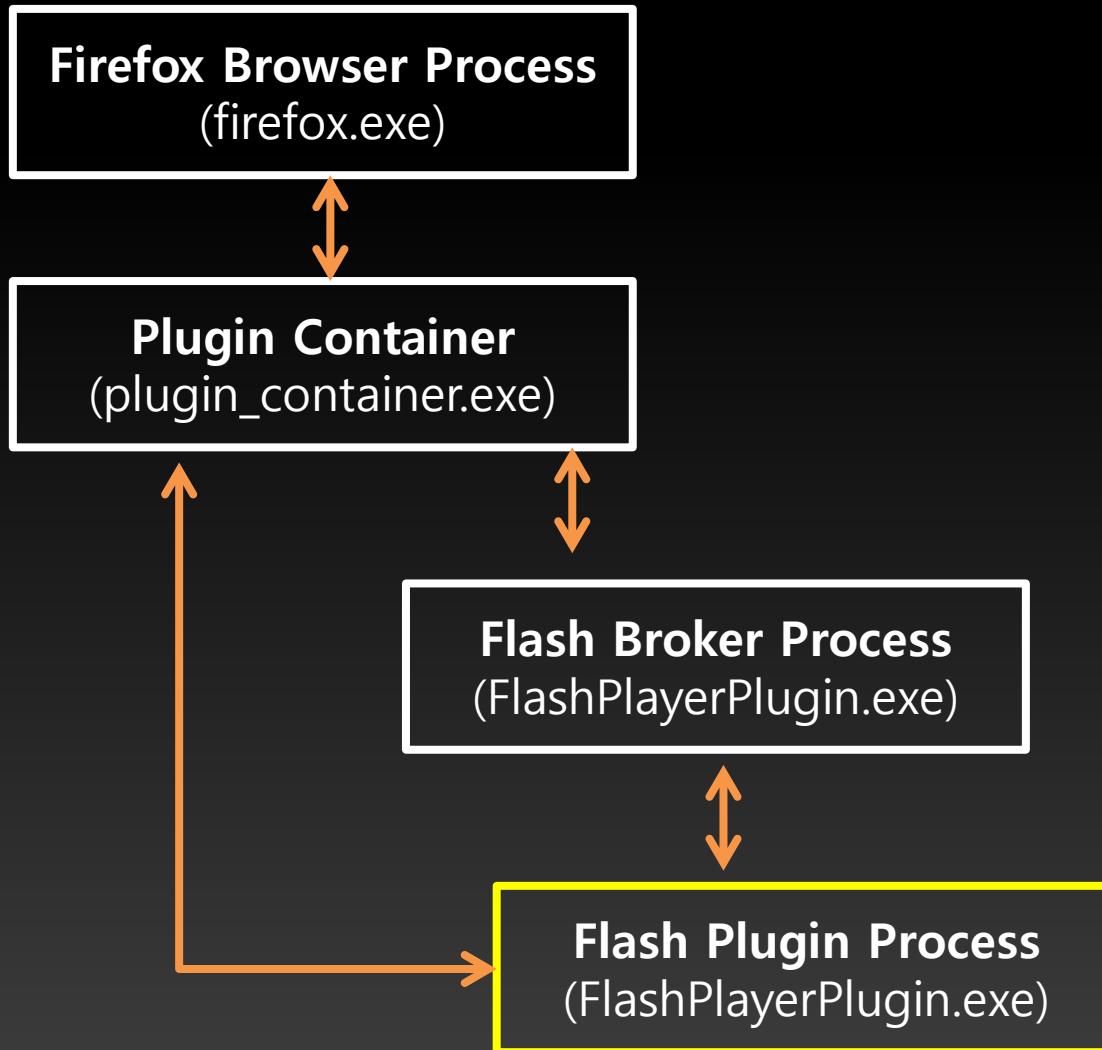
관리자 그룹의 계정

How to use this in Flash Player?

1. SandBox Architecture

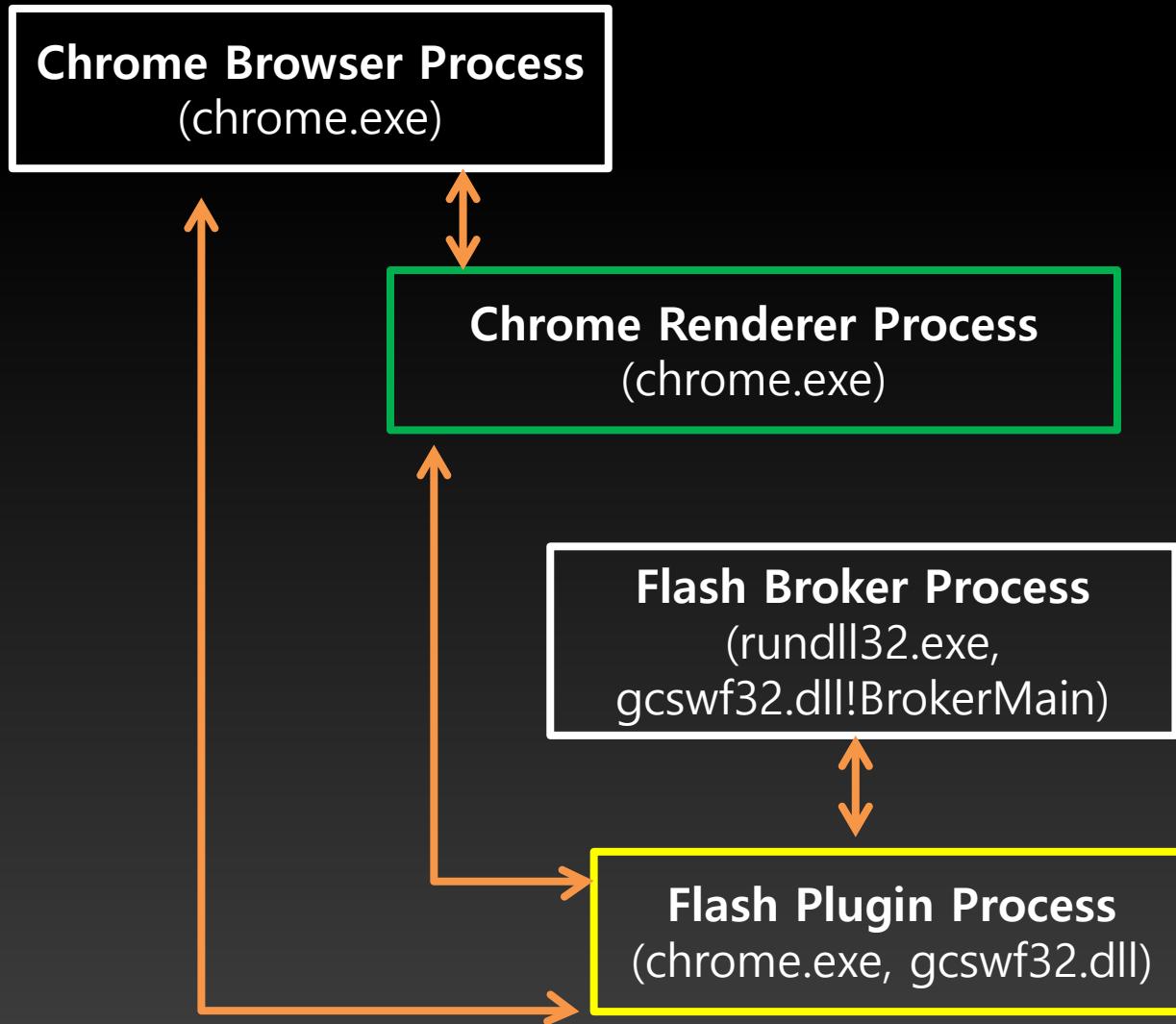
Sandbox Architecture

- Flash Player Protected Mode For FireFox



Sandbox Architecture

- Flash Player Protected Mode For Chrome



2. SandBox Mechanisms

Sandbox Restrictions



restricted

An orange arrow points from the devil icon towards the yellow box, with the word "restricted" written above it.

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

Sandbox Restrictions

- Restricted Token

1. Restricted Token
2. Limited Privileges

Sandbox Restriction

- Integrity levels

Process Explorer - Sysinternals: www.sysinternals.com [pesante-PC\pesante]

Process	CPU	Private Byt...	Working...	PID	Description	Company Name	Window Status	DEP	Integrity	ASLR	Virtualized
explorer.exe	0,14	27,964 K	45,344 K	3564	Windows 탐색기	Microsoft Corporat...	Running	DEP (permanent)	보통 필수 수준	ASLR	
RAVBg64.exe		15,016 K	12,384 K	3840	HD Audio Background P...	Realtek Semicond...		DEP (permanent)	보통 필수 수준		
RAVBg64.exe		16,028 K	14,084 K	2336	HD Audio Background P...	Realtek Semicond...		DEP (permanent)	보통 필수 수준		
hkcmd.exe		3,456 K	8,304 K	4156	hkcmd Module	Intel Corporation		DEP (permanent)	보통 필수 수준		
igfxpers.exe		3,648 K	9,252 K	4240	persistence Module	Intel Corporation		DEP (permanent)	보통 필수 수준		
ETDCtrl.exe		7,664 K	19,864 K	4348	ETD Control Center	ELAN Microelectro...		DEP (permanent)	보통 필수 수준	ASLR	
ETDCtrlHelper.exe	0,06	4,248 K	9,332 K	4596				n/a			
BleServicesCtrl.exe		3,644 K	8,864 K	4444	Bluetooth LE Services C...	Intel Corporation		DEP (permanent)	보통 필수 수준	ASLR	
rundll32.exe		4,016 K	12,996 K	4452	Windows 호스트 프로세스...	Microsoft Corporat...		DEP (permanent)	보통 필수 수준	ASLR	Virtualized
KakaoTalk.exe	0,08	52,844 K	63,268 K	4548	KakaoTalk	Kakao Inc.	Running	DEP	보통 필수 수준	ASLR	
RocketDock.exe	0,22	9,588 K	21,568 K	4648			Running	DEP	보통 필수 수준		
chrome.exe	0,77	91,900 K	155,860 K	4468	Google Chrome	Google Inc.	Running	DEP (permanent)	보통 필수 수준	ASLR	
chrome.exe	< 0,01	134,608 K	196,400 K	5220	Google Chrome	Google Inc.		DEP (permanent)	Low	ASLR	
chrome.exe		28,968 K	41,492 K	5412	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe		34,576 K	46,016 K	5584	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe	2,45	807,156 K	814,756 K	6264	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe		65,776 K	70,192 K	3240	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe	< 0,01	91,152 K	111,008 K	5852	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe		0,29	70,928 K	93,500 K	7096	Google Chrome	Google Inc.	DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe	0,01	113,308 K	126,864 K	4880	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe	< 0,01	44,284 K	57,948 K	4560	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe	0,11	100,104 K	113,668 K	5628	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe	0,14	51,868 K	72,444 K	6736	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
Rainmeter.exe	4,98	20,784 K	34,256 K	4908				DEP (permanent)	보통 필수 수준	ASLR	
POWERPNT.EXE	0,04	36,668 K	12,200 K	2648	Microsoft Office PowerP...	Microsoft Corporat...	Running	DEP	보통 필수 수준	ASLR	
splivw64.exe		2,036 K						DEP (permanent)	보통 필수 수준	ASLR	
sublime_text.exe		18,496 K									
plugin_host.exe		34,972 K									
iexplore.exe	1,05	14,684 K									
iexplore.exe	2,37	73,604 K									
iexplore.exe		29,640 K									
vmware-tray.exe		1,968 K									
avastui.exe	0,01	22,268 K									
AdobeARM.exe		4,564 K									

CPU Usage: 23.94% Commit Charge: 26.58% Processes: 110 Physical Usage:

DEP (permanent) 보통 필수 수준
 DEP (permanent) Low
 DEP (permanent) Low

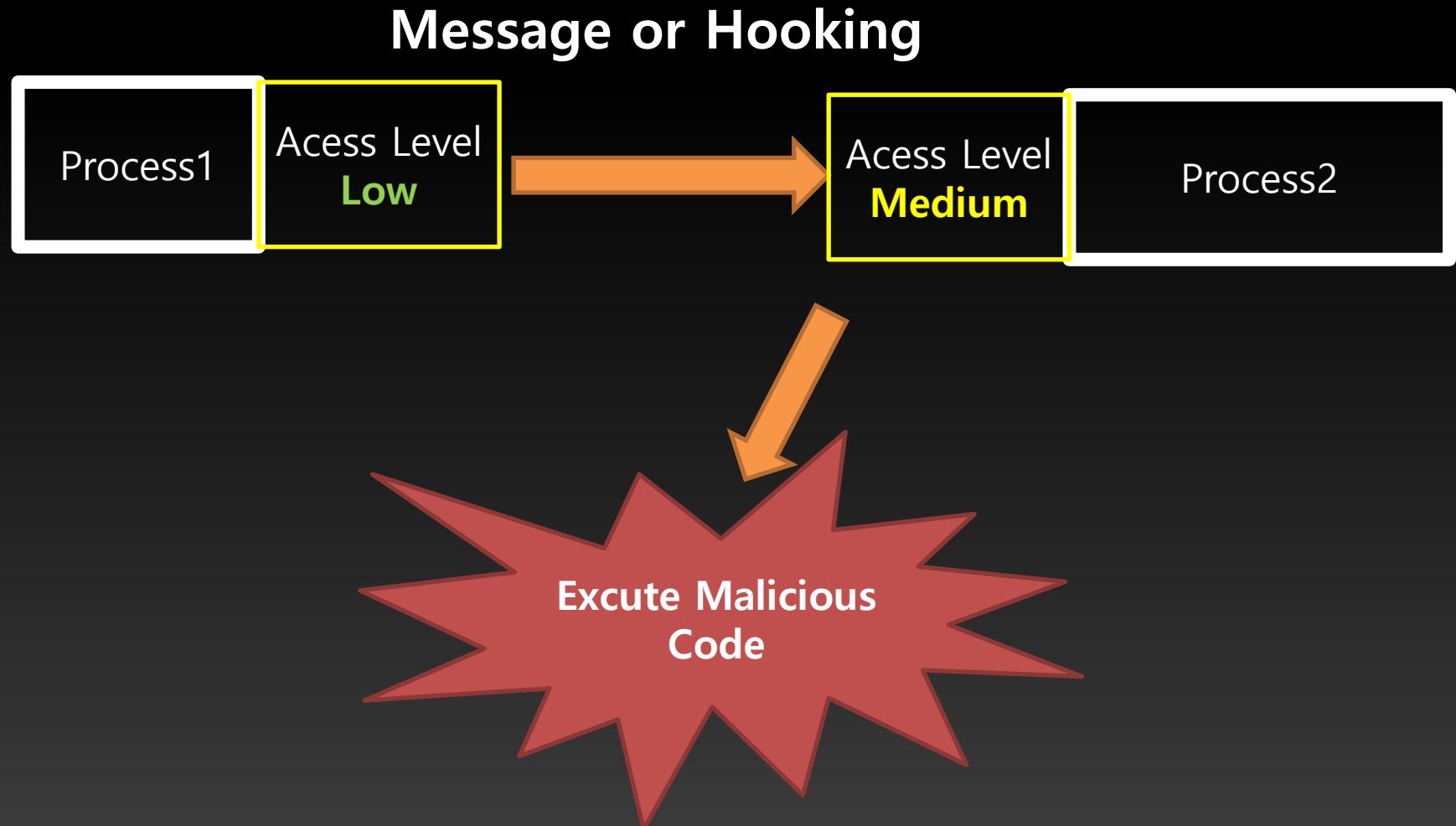
MIC(Mandatory Integrity Mechanism)

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)



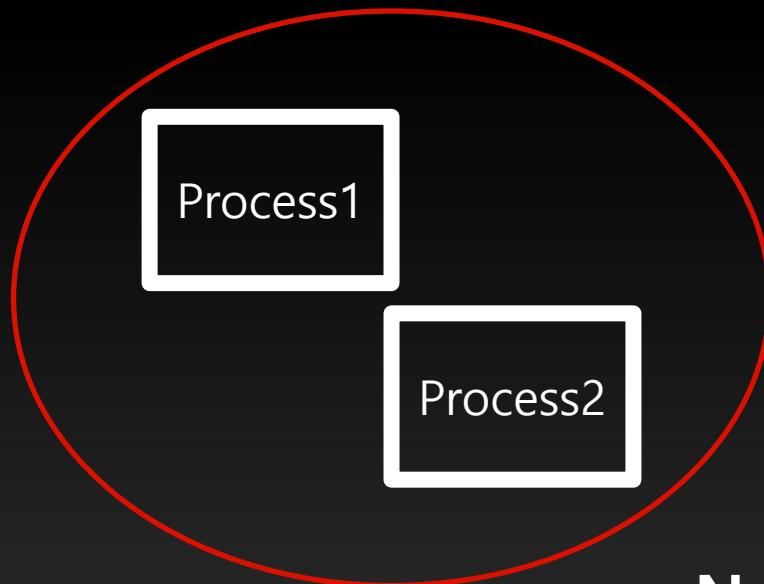
UIPI(User Interface Privilege Isolation)



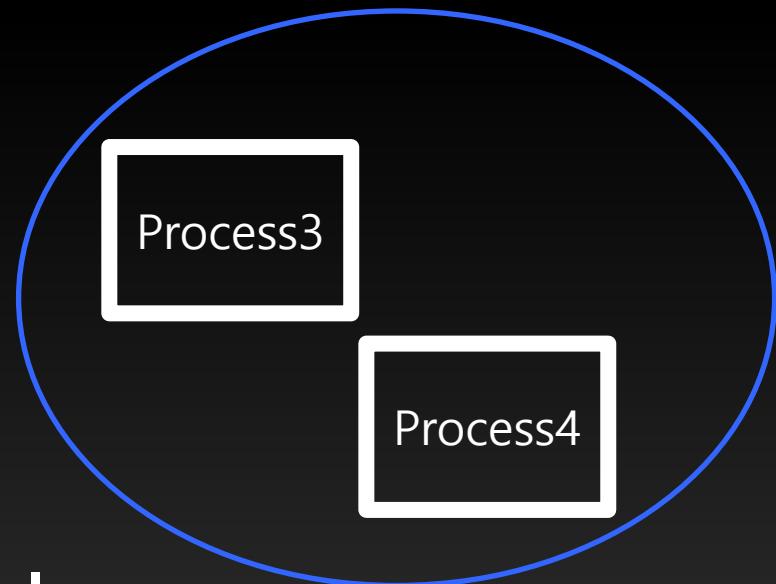
Sandbox Restriction

- Job Objects

Job Object1



Job Object2

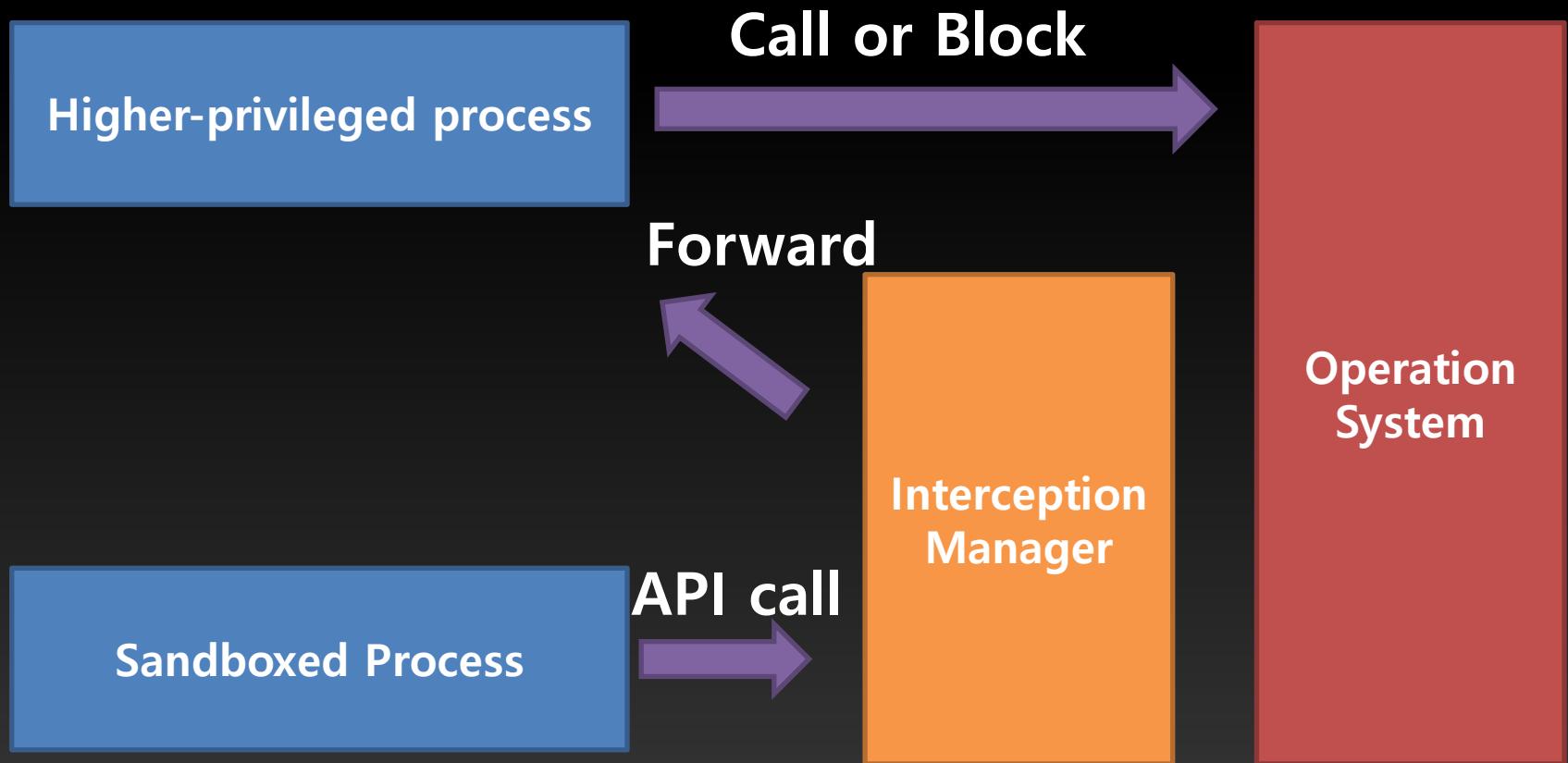


-Namable

-Securable

-Sharable

Interception Manager

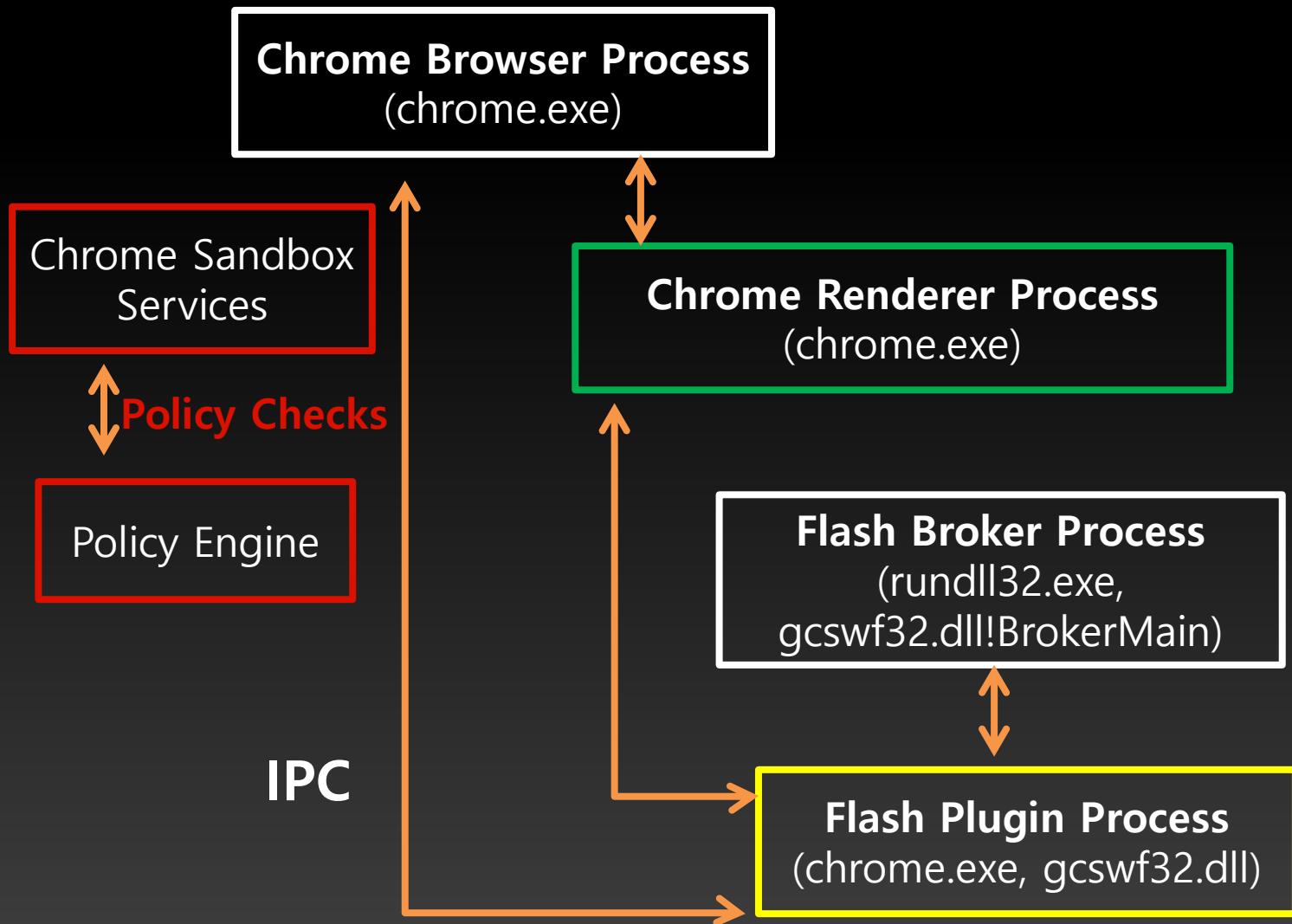


Services

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

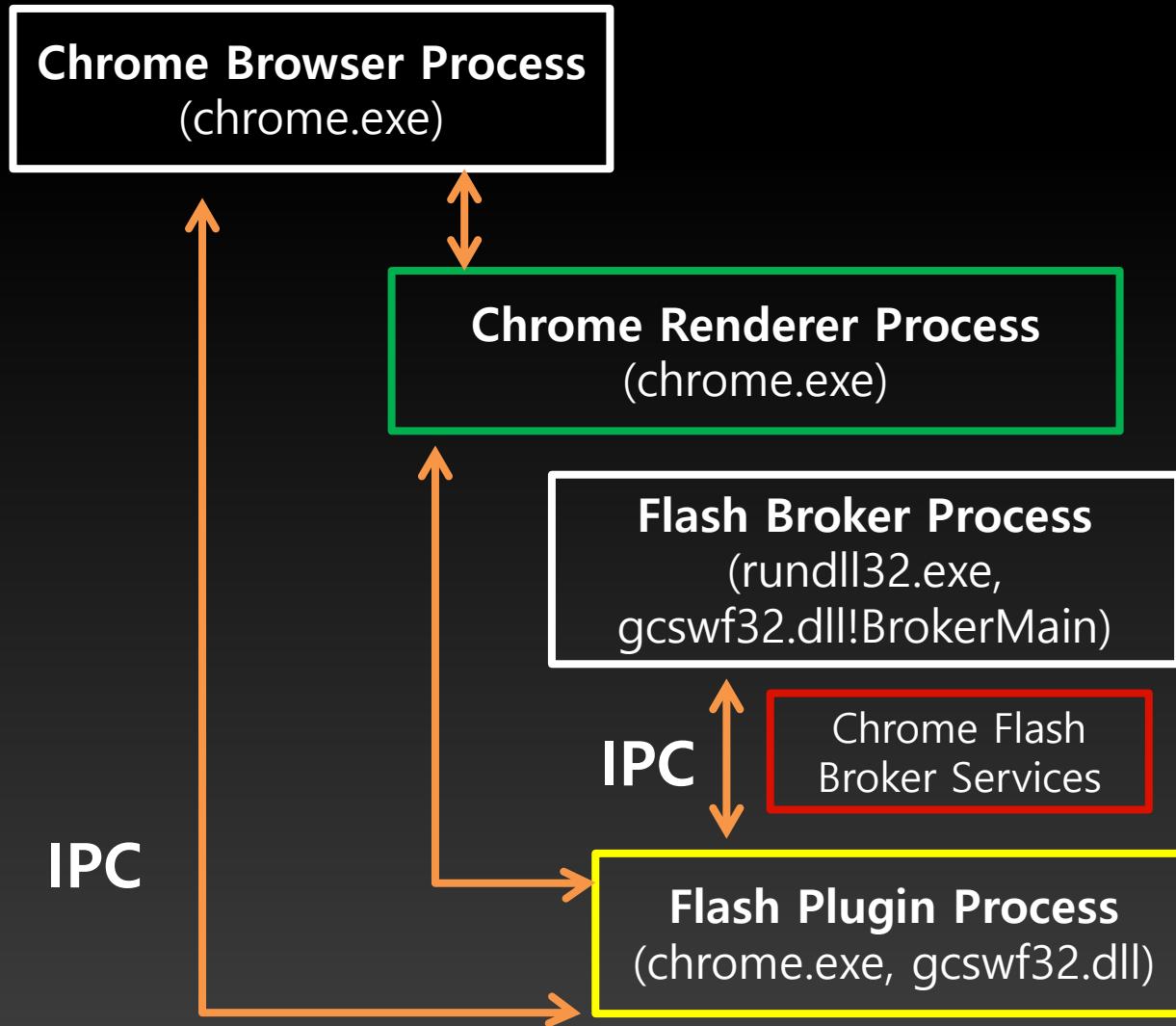
Service

- Chrome Sandbox Services



Service

- Chrome Flash Broker Services



Service

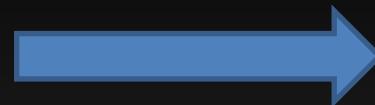
- Firefox Flash Broker Services

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 full 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

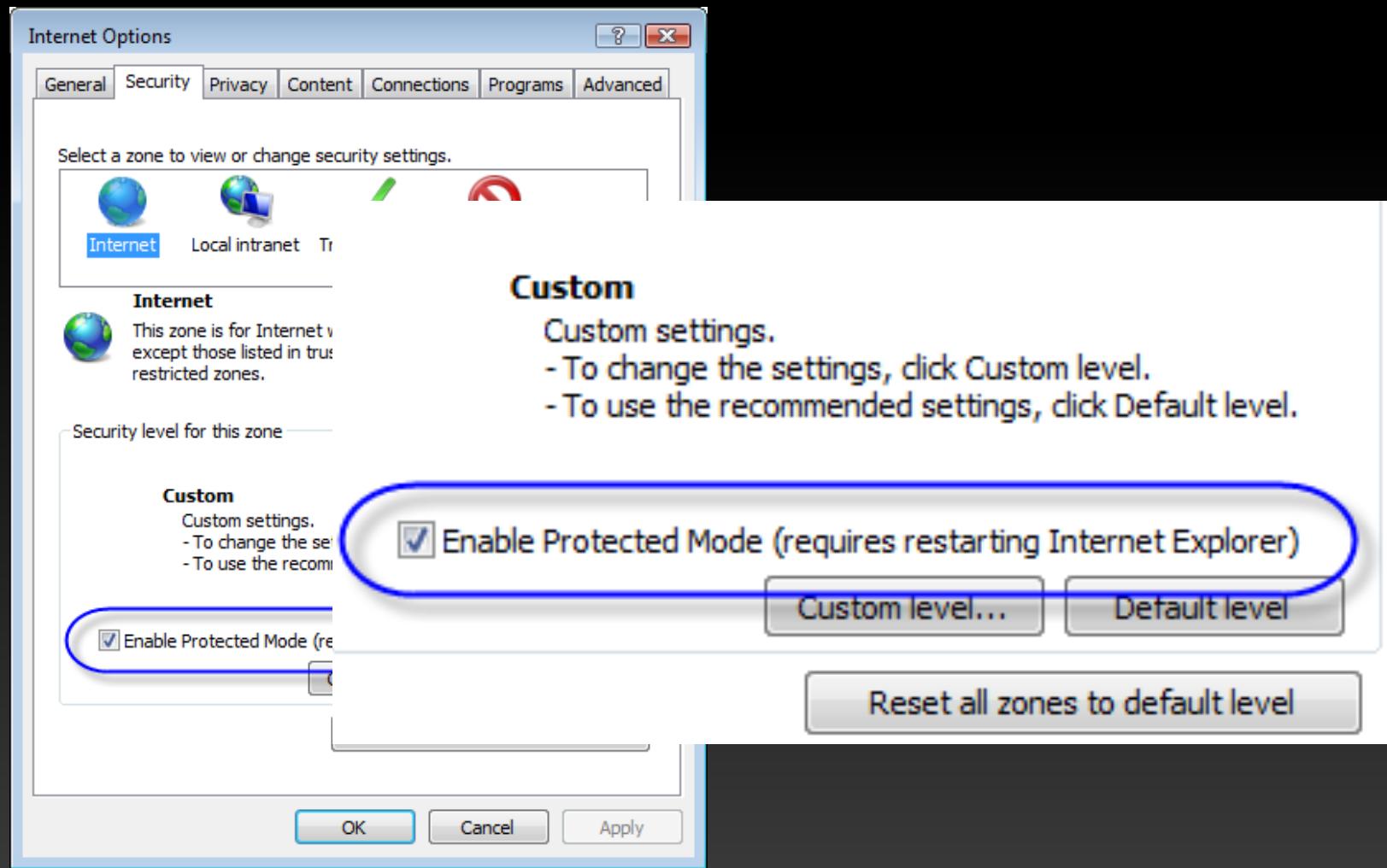
ProtectedModeWhitelistConfig.txt

How to use this in IE?

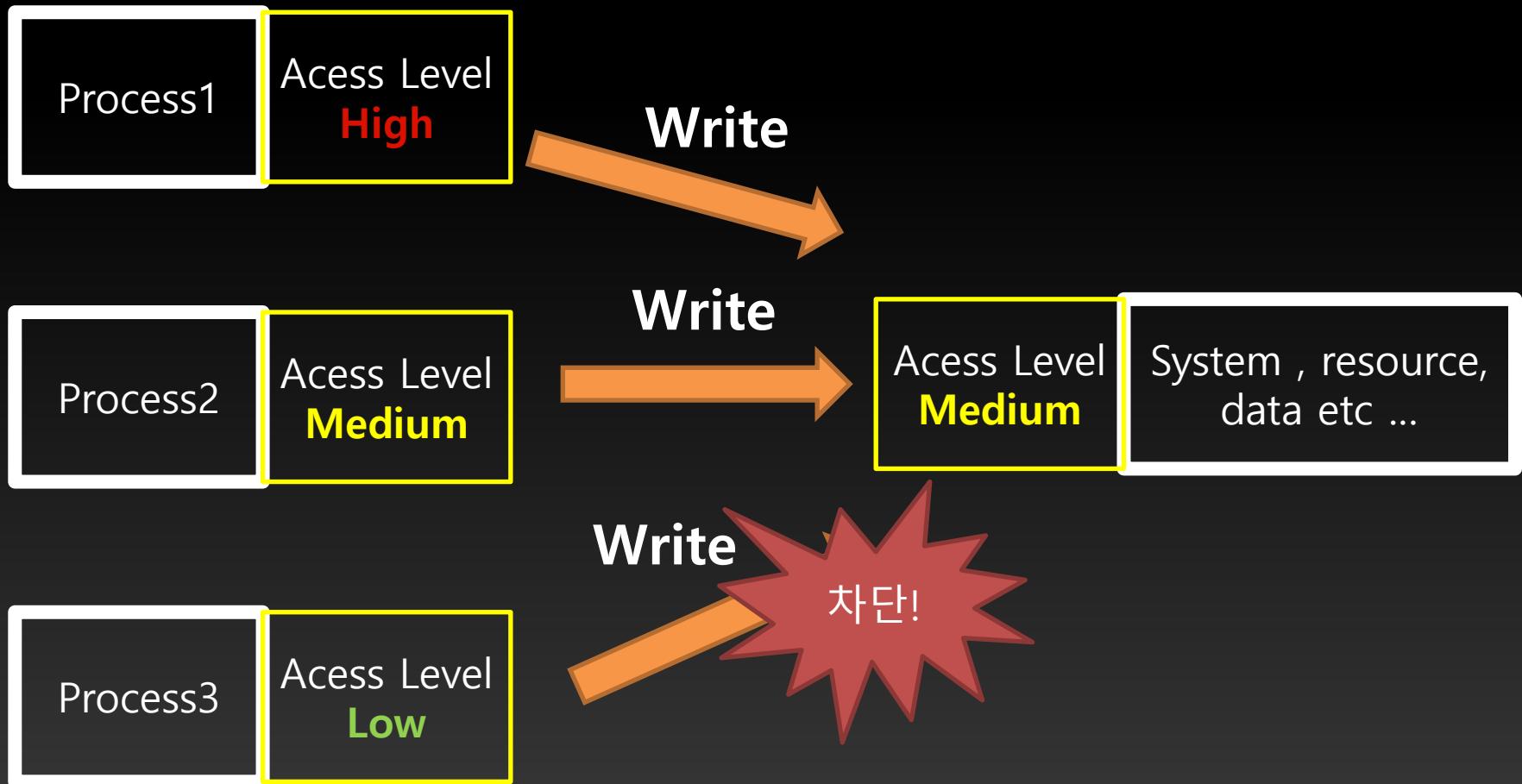
Protected Mode in IE7

- 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

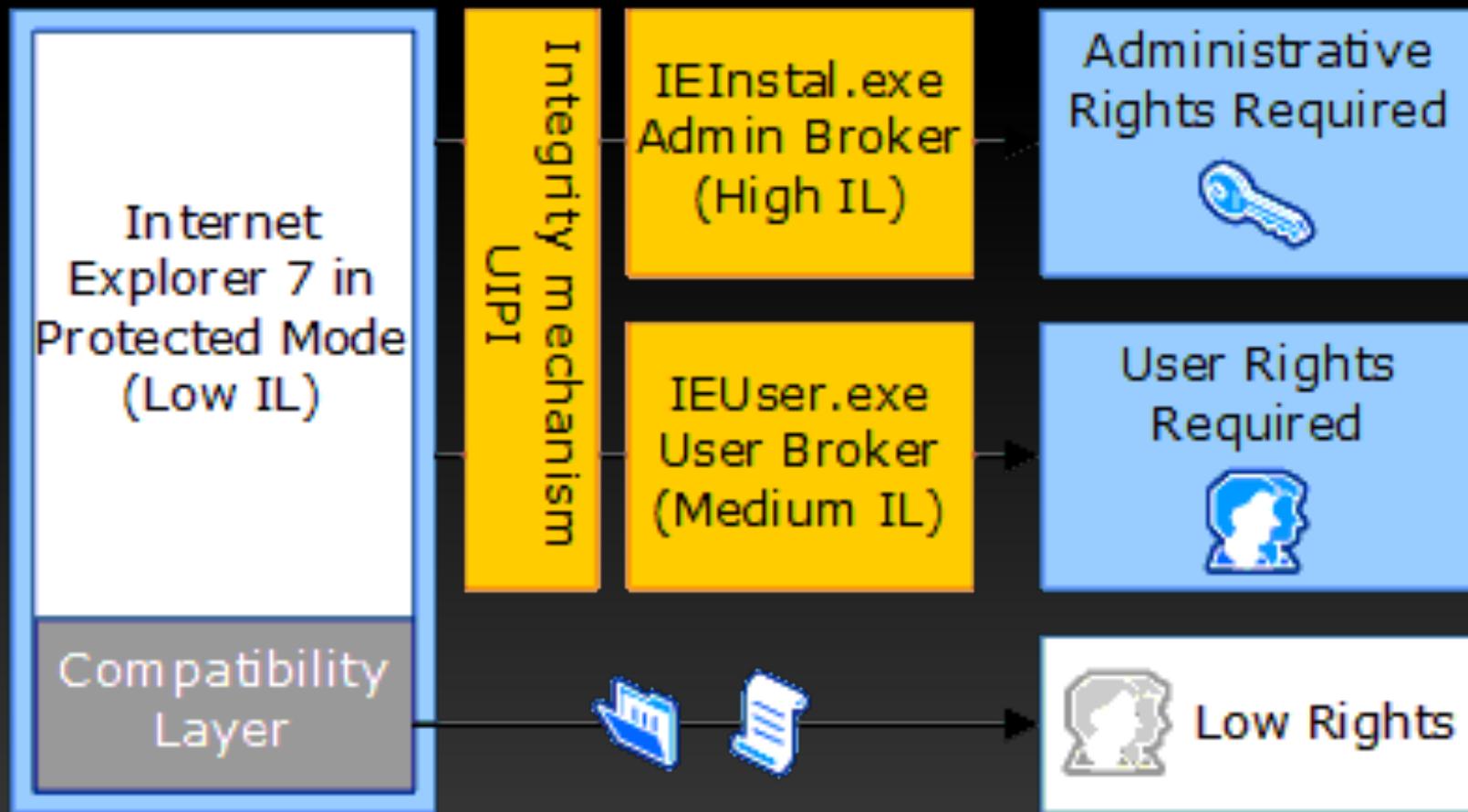
Process Explorer - Sysinternals: www.sysinternals.com [pesante-PC\pesante]

Process	CPU	Private Byt..	Working...	PID	Description	Company Name	Window Status	DEP	Integrity	ASLR	Virtualized
explorer.exe	0,14	27,964 K	45,344 K	3564	Windows 탐색기	Microsoft Corporat...	Running	DEP (permanent)	보통 필수 수준	ASLR	
RAVBg64.exe		15,016 K	12,384 K	3840	HD Audio Background P...	Realtek Semicond...		DEP (permanent)	보통 필수 수준		
RAVBg64.exe		16,028 K	14,084 K	2336	HD Audio Background P...	Realtek Semicond...		DEP (permanent)	보통 필수 수준		
hkcmd.exe		3,456 K	8,304 K	4156	hkcmd Module	Intel Corporation		DEP (permanent)	보통 필수 수준		
igfxpers.exe		3,648 K	9,252 K	4240	persistence Module	Intel Corporation		DEP (permanent)	보통 필수 수준		
ETDCtrl.exe		7,664 K	19,864 K	4348	ETD Control Center	ELAN Microelectro...		DEP (permanent)	보통 필수 수준	ASLR	
ETDCtrlHelper.exe	0,06	4,248 K	9,332 K	4596				n/a			
BleServicesCtrl.exe		3,644 K	8,864 K	4444	Bluetooth LE Services C...	Intel Corporation		DEP (permanent)	보통 필수 수준	ASLR	
rundll32.exe		4,016 K	12,996 K	4452	Windows 호스트 프로세스...	Microsoft Corporat...		DEP (permanent)	보통 필수 수준	ASLR	Virtualized
KakaoTalk.exe	0,08	52,844 K	63,268 K	4548	KakaoTalk	Kakao Inc.	Running	DEP	보통 필수 수준	ASLR	
RocketDock.exe	0,22	9,588 K	21,568 K	4648			Running	DEP	보통 필수 수준		
chrome.exe	0,77	91,900 K	155,860 K	4468	Google Chrome	Google Inc.	Running	DEP (permanent)	보통 필수 수준	ASLR	
chrome.exe	< 0,01	134,608 K	196,400 K	5220	Google Chrome	Google Inc.		DEP (permanent)	Low	ASLR	
chrome.exe		28,968 K	41,492 K	5412	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe		34,576 K	46,016 K	5584	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe	2,45	807,156 K	814,756 K	6264	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe		65,776 K	70,192 K	3240	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe	< 0,01	91,152 K	111,008 K	5852	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe	0,29	70,928 K	93,500 K	7096	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe	0,01	113,308 K	126,864 K	4880	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe	< 0,01	44,284 K	57,948 K	4560	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe	0,11	100,104 K	113,668 K	5628	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
chrome.exe	0,14	51,868 K	72,444 K	6736	Google Chrome	Google Inc.		DEP (permanent)	신뢰되지 않은 필...	ASLR	
Rainmeter.exe	4,98	20,784 K	34,256 K	4908				DEP (permanent)	보통 필수 수준	ASLR	
POWERPNT.EXE	0,04	36,668 K	12,200 K	2648	Microsoft Office PowerP...	Microsoft Corporat...	Running	DEP	보통 필수 수준	ASLR	
splivew64.exe		2,036 K						DEP (permanent)	보통 필수 수준	ASLR	
sublime_text.exe		18,496 K									
plugin_host.exe		34,972 K									
explore.exe	1,05	14,684 K									
iexplore.exe	2,37	73,604 K									
explore.exe		29,640 K									
vmware-tray.exe		1,968 K									
avastui.exe	0,01	22,268 K									
AdobeARM.exe		4,564 K									

CPU Usage: 23.94% Commit Charge: 26.58% Processes: 110 Physical Usage:

DEP (permanent) 보통 필수 수준
DEP (permanent) Low
DEP (permanent) Low

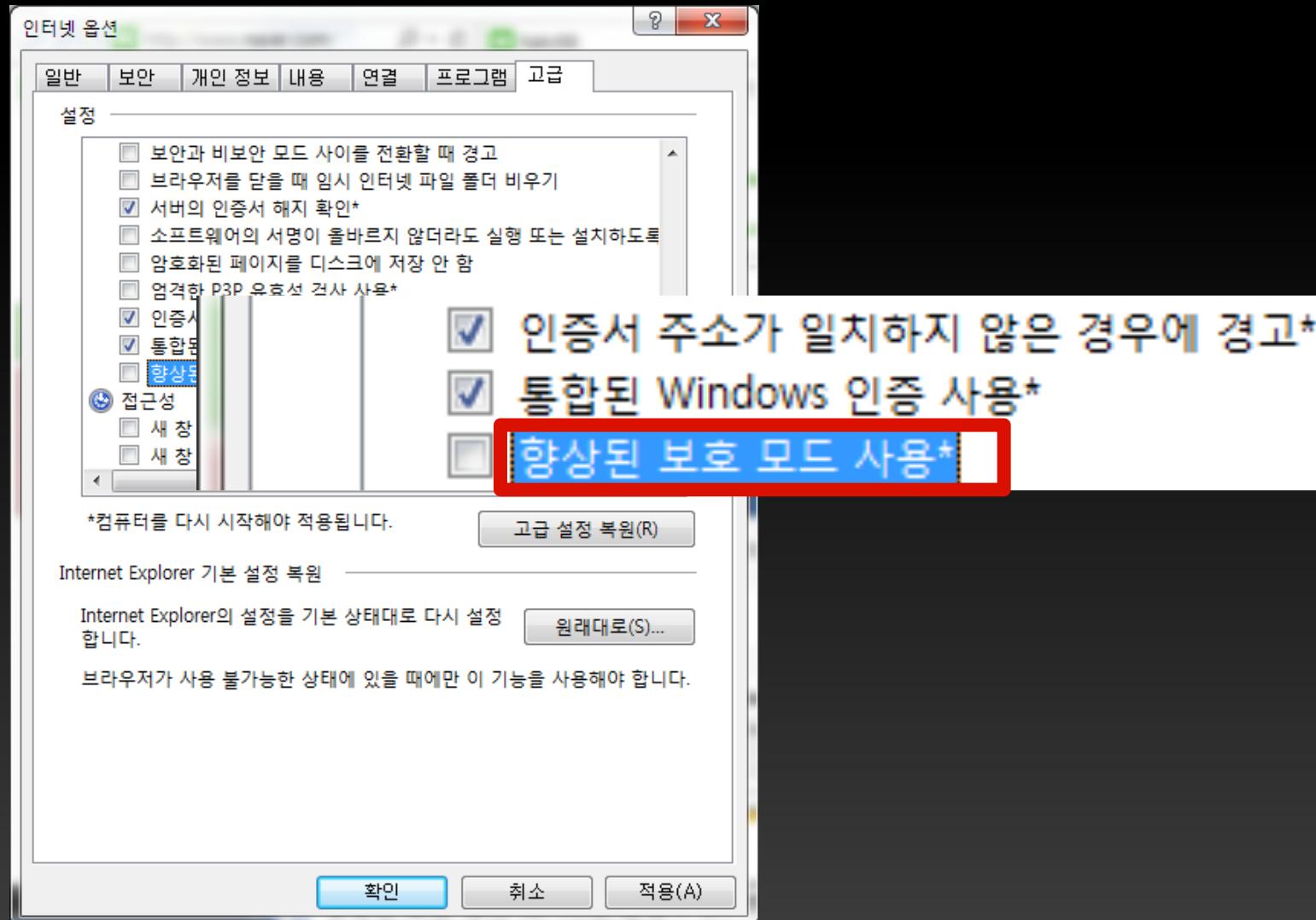
How to Activate IE7 in PM



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

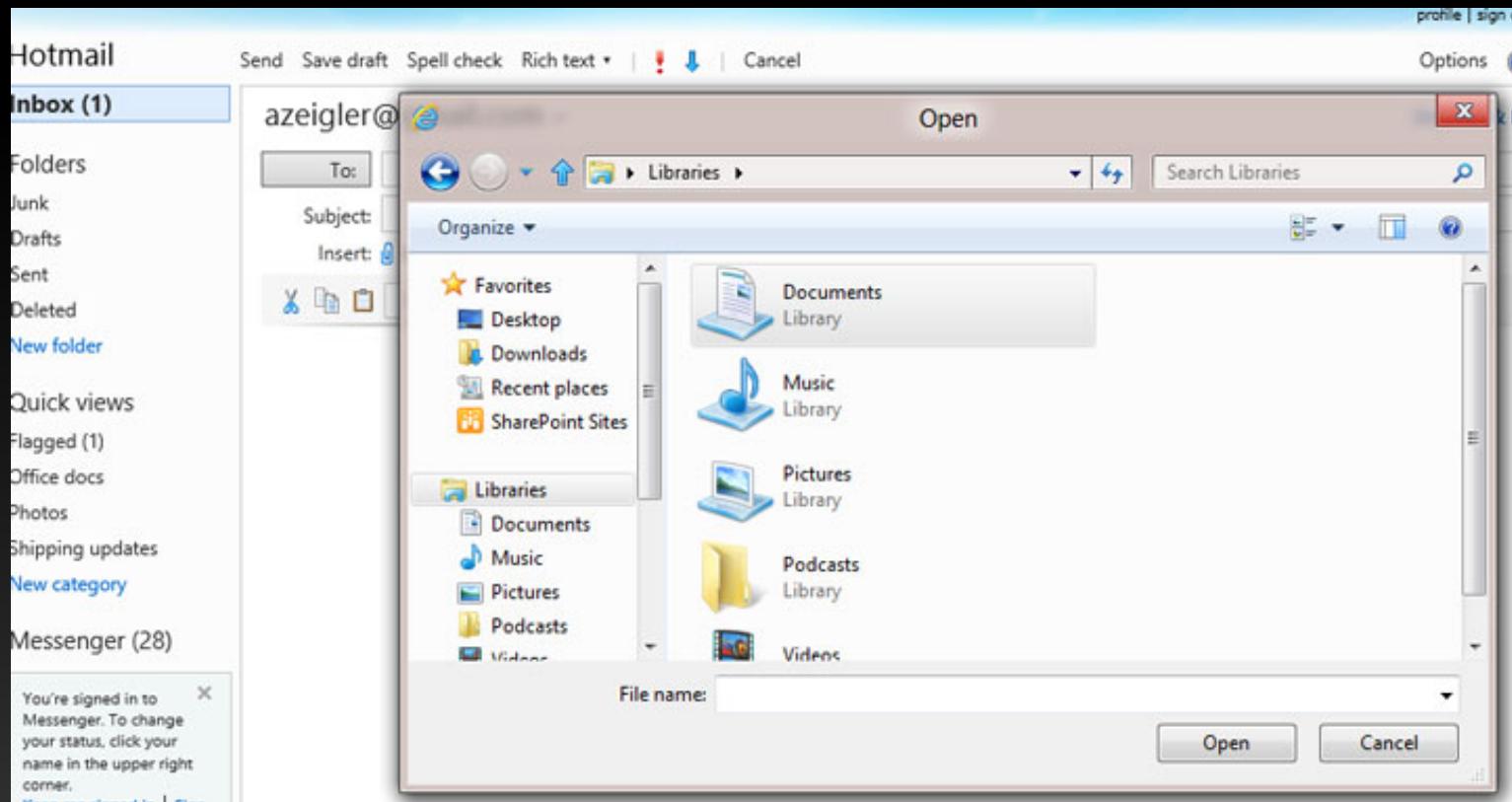


Enhanced Protected Mode



- 64bit Processes
- More Effective in ASLR

Enhanced Protected Mode

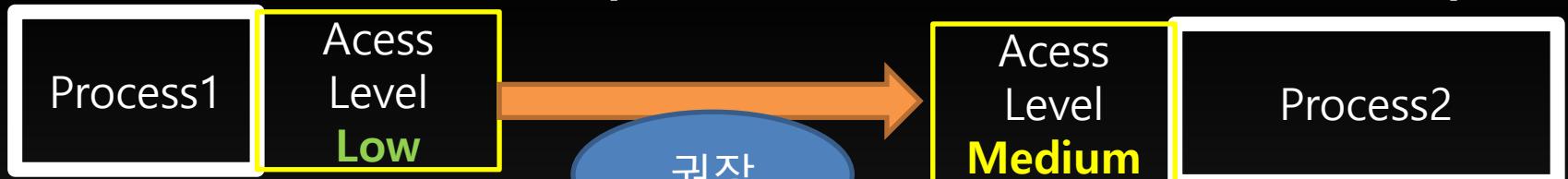


- Read access to the file system (and registry) is blocked

Enhanced Protected Mode

Classic Protect Mode

IPC(Inter Process Communication)



Enhanced Protect Mode

IPC(Inter Process Communication)



Enhanced Protected Mode

The screenshot shows the Process Explorer application from Sysinternals. The window title is "Process Explorer - Sysinternals: www.sysinternals.com [pesante\pesante1]". The main table lists various Windows processes with their CPU usage, private bytes, working set, PID, description, DEP status, and integrity level. Two specific entries for Internet Explorer are highlighted with red boxes:

Process	CPU	Private Byt...	Working Set	PID	Description	DEP	Integrity
SearchProtocolHo...	0,01	2,260 K	7,972 K	2596		n/a	
SearchFilterHost.e...	0,01	1,608 K	5,508 K	1164		n/a	
wmpnetwk.exe	0,01	3,652 K	12,696 K	2876	Windows Media Player ...	n/a	
taskhostex.exe	< 0,01	6,884 K	13,328 K	452	Windows 작업을 위한 호...	DEP (permanent)	Medium
lsass.exe	0,05	2,968 K	7,824 K	796	Local Security Authority...	n/a	
csrss.exe	0,40	1,268 K	7,968 K	684		n/a	
winlogon.exe		972 K	6,692 K	744		n/a	
dwm.exe	4,54	107,532 K	26,672 K	1080		n/a	
explorer.exe	0,40	26,364 K	64,032 K	3392	Windows 탐색기	DEP (permanent)	Medium
vmtoolsd.exe	0,11	11,480 K	22,800 K	1100	VMware Tools Core Ser...	DEP (permanent)	Medium
procexp.exe	1,81	8,540 K	21,164 K	2852	Sysinternals Process E...	DEP (permanent)	Medium
ieexplorer.exe	0,27	4,148 K	17,472 K	1272	Internet Explorer	DEP (permanent)	Medium

Two rows are highlighted with red boxes:

- Row 1: "1272 Internet Explorer" with status "DEP (permanent) Medium".
- Row 2: "3768 Internet Explorer" with status "DEP (permanent) AppContainer".

- 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

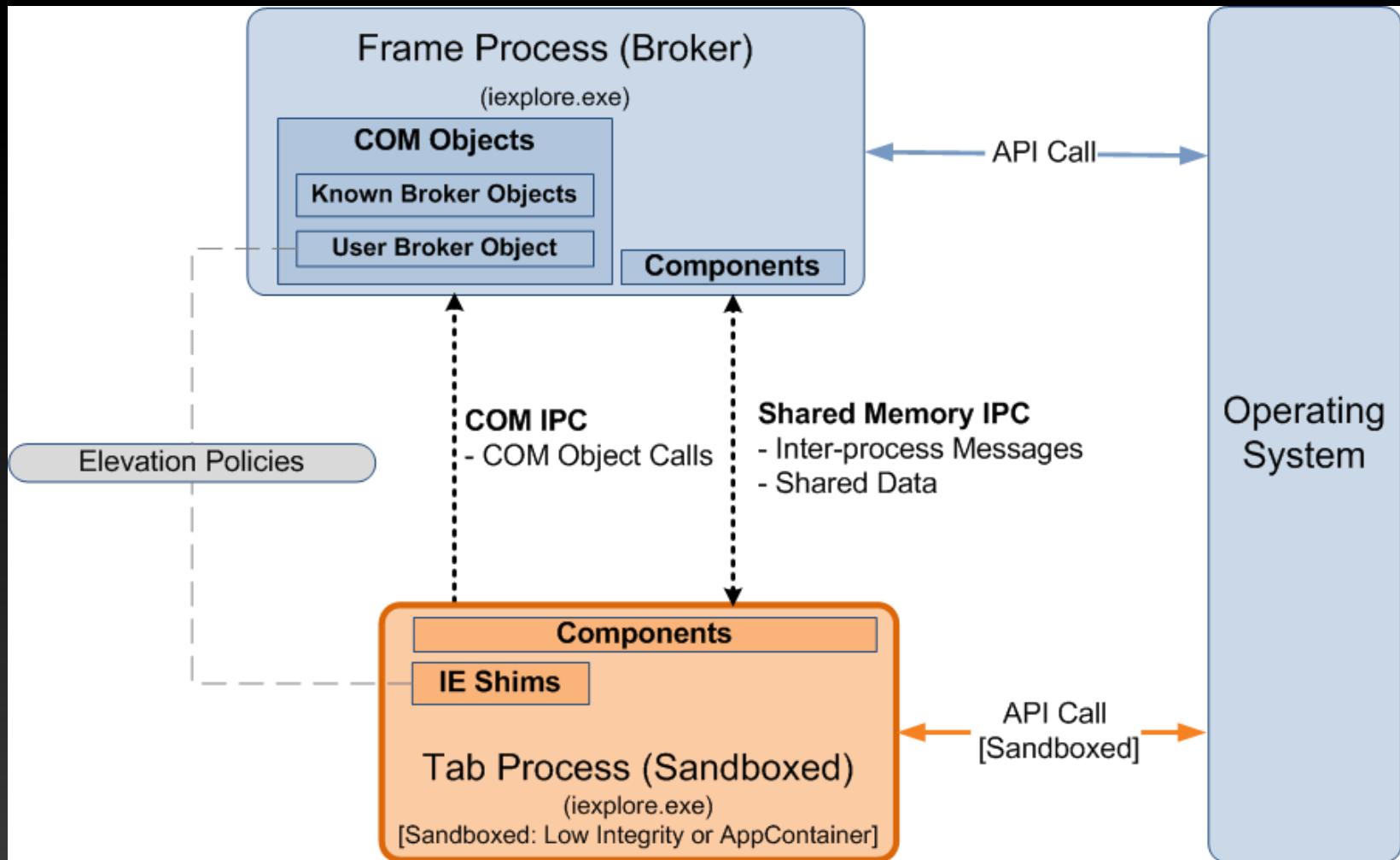
- App Container is actually its own integrity level.
This can be seen in the screen shot below:

The screenshot shows a Process Explorer window with a list of running processes. The columns are CPU, Private Byt..., Working Set, PID, Description, DEP, and Integrity. Two specific rows are highlighted with red boxes and labeled at the bottom.

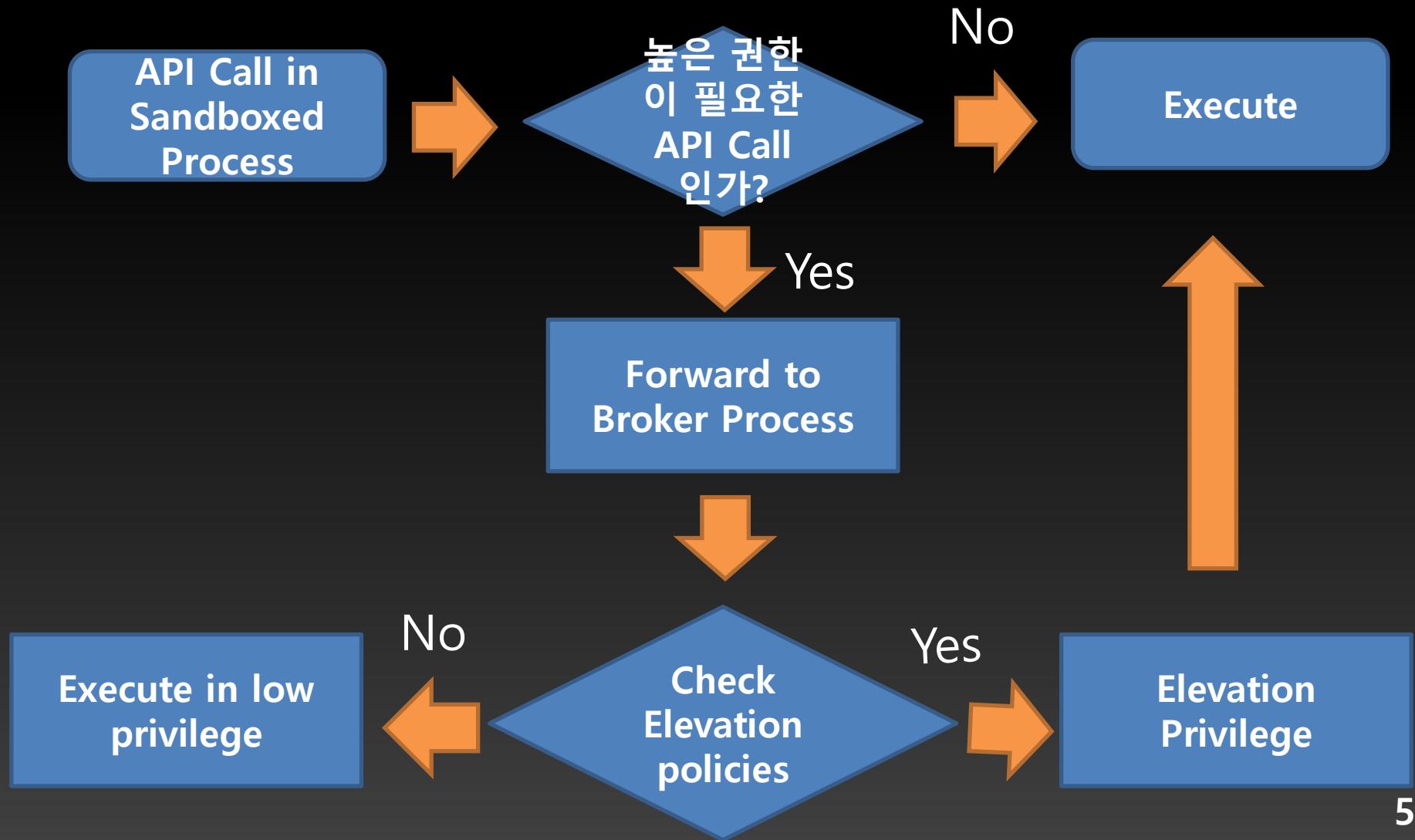
Process	CPU	Private Byt...	Working Set	PID	Description	DEP	Integrity
SearchProtocolHo...	0,01	2,260 K	7,972 K	2596		n/a	
SearchFilterHost,e...	0,01	1,608 K	5,508 K	1164		n/a	
wmpnetwk.exe	0,01	3,652 K	12,696 K	2876	Windows Media Player ...	n/a	
taskhostex.exe	< 0,01	6,884 K	13,328 K	452	Windows 작업을 위한 호...	DEP (permanent)	Medium
lsass.exe	0,05	2,968 K	7,824 K	796	Local Security Authority...	n/a	
csrss.exe	0,40	1,268 K	7,968 K	684		n/a	
winlogon.exe		972 K	6,692 K	744		n/a	
dwm.exe	4,54	107,532 K	26,672 K	1080		n/a	
explorer.exe	0,40	26,364 K	64,032 K	3392	Windows 탐색기	DEP (permanent)	Medium
vmtoolsd.exe	0,11	11,480 K	22,800 K	1100	VMware Tools Core Ser...	DEP (permanent)	Medium
procesp.exe	1,81	8,540 K	21,164 K	2852	Sysinternals Process E...	DEP (permanent)	Medium
iexplore.exe	0,27	4,148 K	17,472 K	1272	Internet Explorer	DEP (permanent)	Medium
iexplore.exe	15,13	114,836 K	99,664 K	3768	Internet Explorer	DEP (permanent)	AppContainer

1272 Internet Explorer DEP (permanent) Medium
3768 Internet Explorer DEP (permanent) AppContainer

EPM Architecture

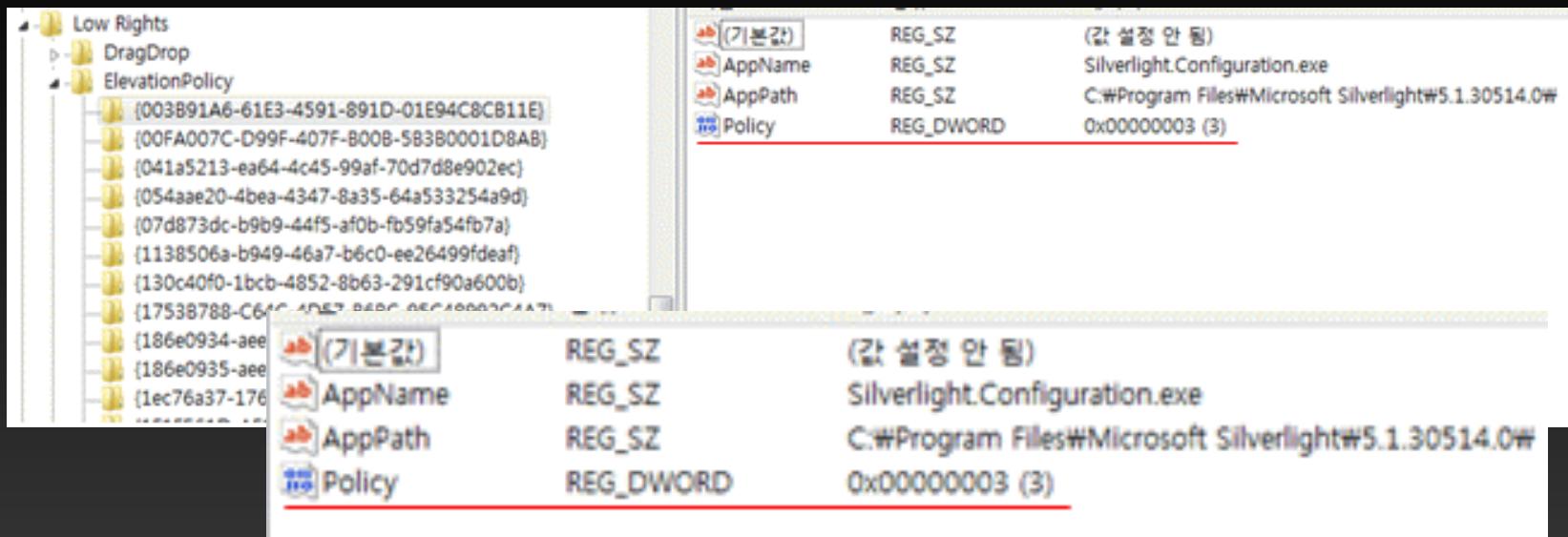


IE SHIMS (COMPATIBILITY LAYER)



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!