PPLSASSRSC

Start

18.07.26 # pinebudweiser

INTRO

What is LSASS?

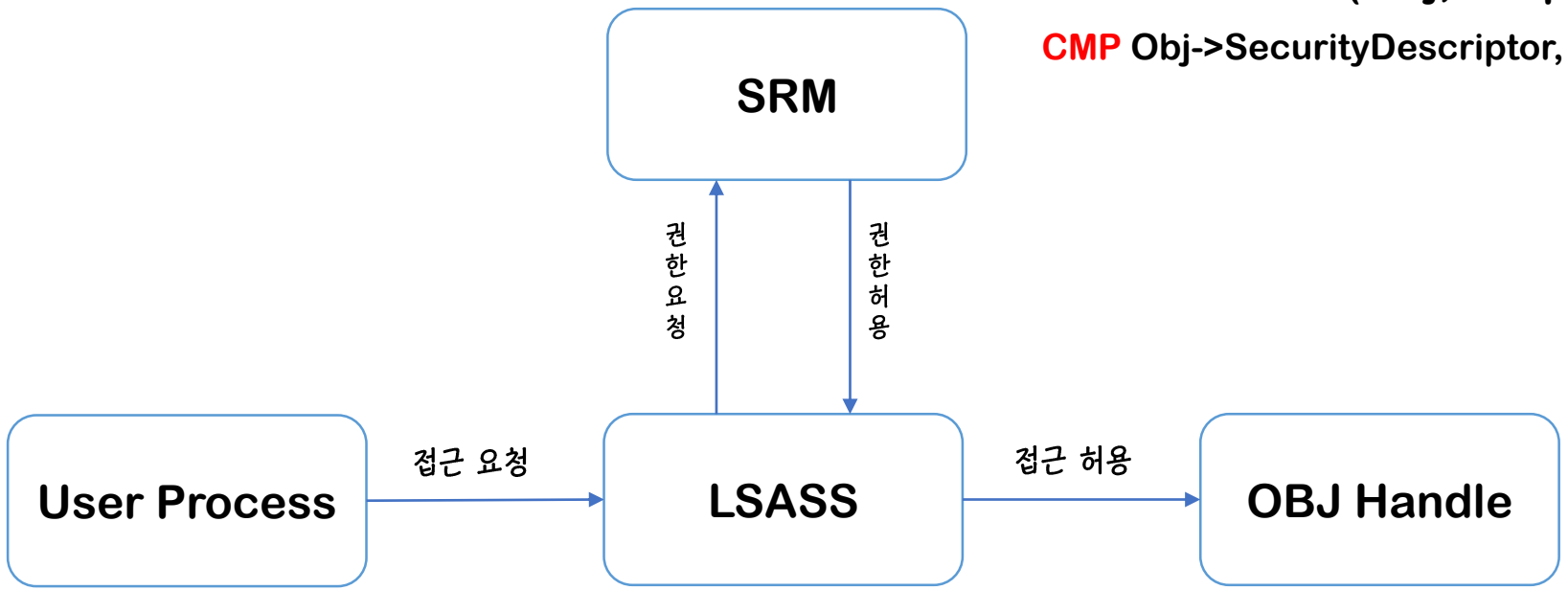
- Lsass 프로세스는 Windows 2000 부터 윈도우 보안 모델에 적용된 기술
- 로컬 시스템 보안 정책, 사용자인증, 비밀번호 변경, 로그인 검사, 이벤트 로그 기록같은 윈도우의 전반적인 보안 담당
- LPC(Local procedure calls)로 유저<->유저, 유저<->커널 통신을 한다.

INTRO

What is LSASS?

SeAccessCheck(Obj, ReqProcessToken)

CMP Obj->SecurityDescriptor, ReqProcessToken



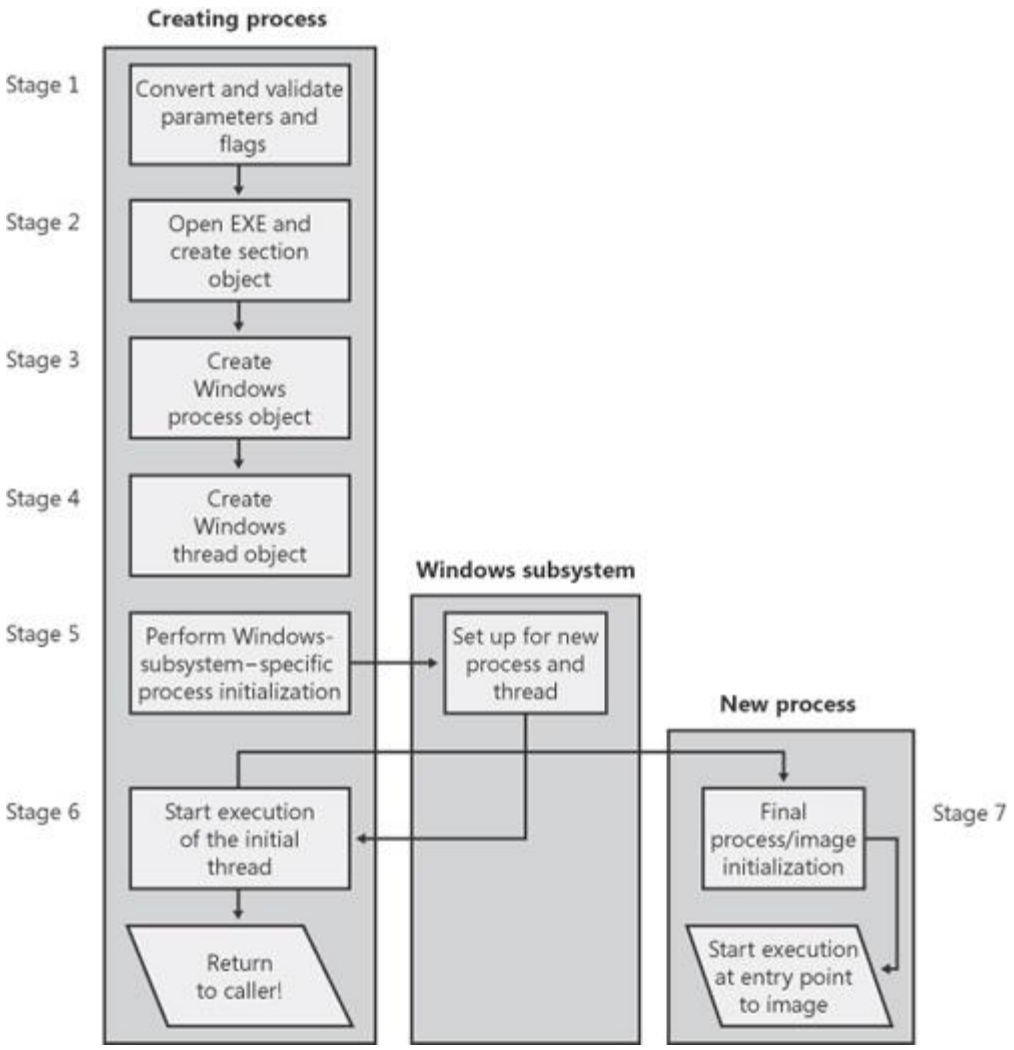
INTRO

What is CSRSS?

- CSRSS 프로세스는 **Windows** 2000 이후로 제공
- 콘솔 윈도우 처리, 프로세스 스레드 생성과 삭제, 16Bit 호환
- LPC(Local procedure calls) 사용

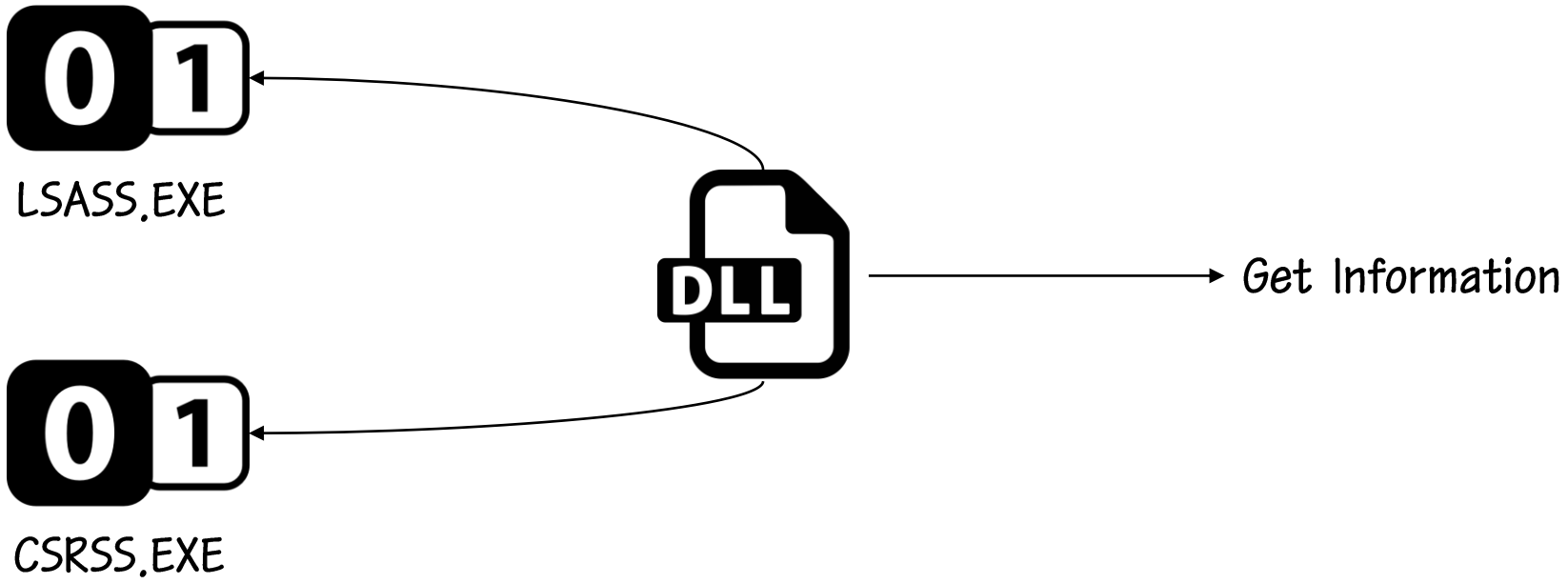
INTRO

What is CSRSS?



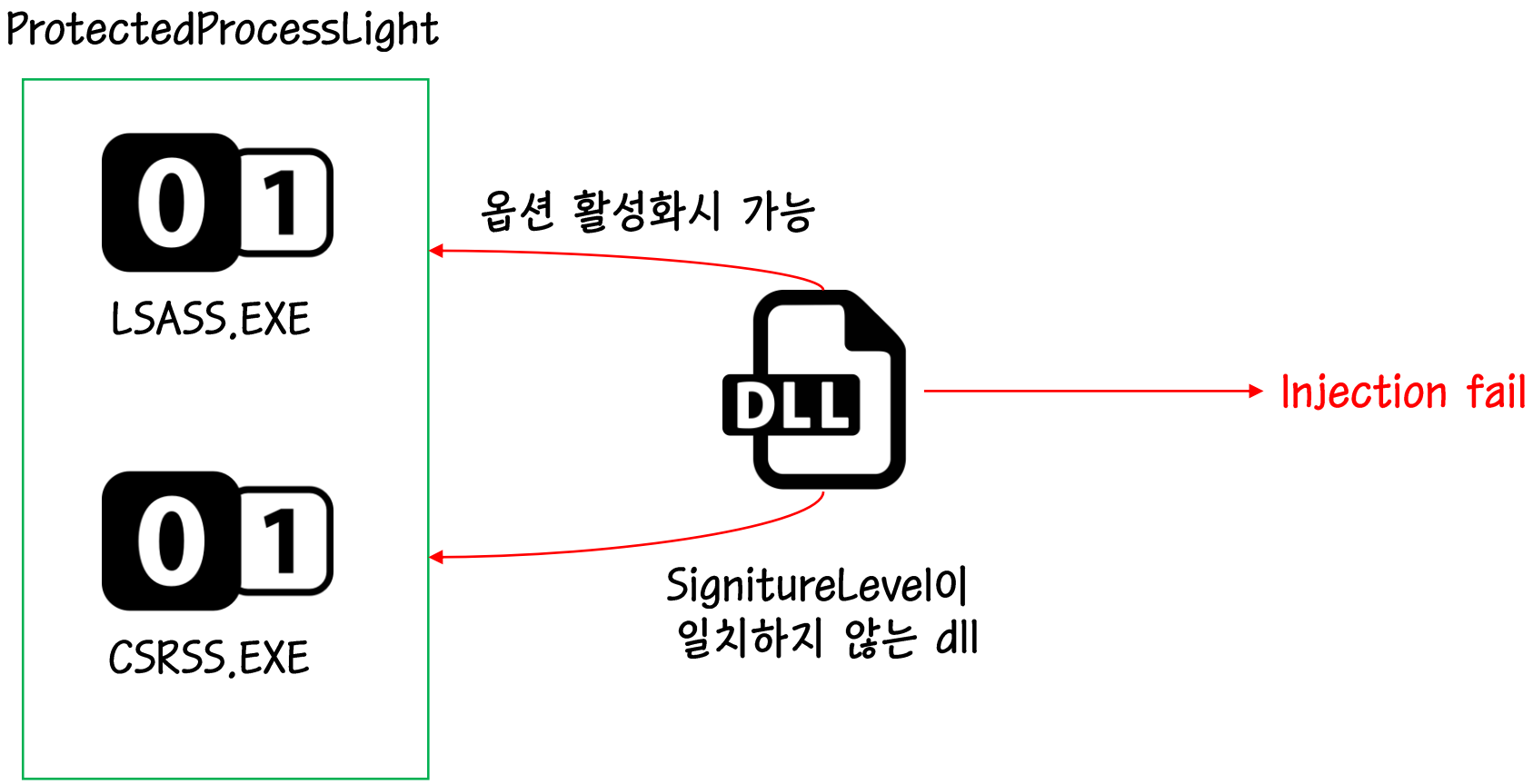
QUEST

What is PPL?



QUEST

What is PPL?



QUEST

Where is PPL?

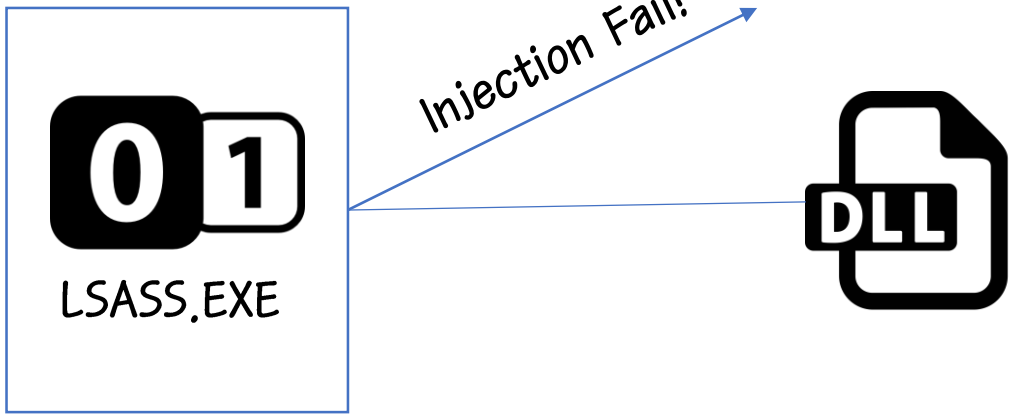
```
EPROCESS → _PS_PROTECTION(1Byte){
        Type    : Pos 0, 3 bits
        Audit   : Pos 3, 1 bit
        Signer  : Pos 4, 4 bits
}
```

```
1 _PS_PROTECTED_TYPE
2         PsProtectedTypeNone = 0n0
3         PsProtectedTypeProtectedLight = 0n1
4         PsProtectedTypeProtected = 0n2
5         PsProtectedTypeMax = 0n3
```

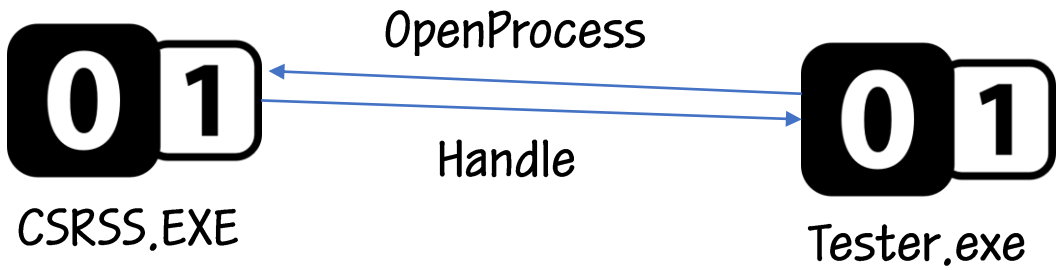
```
1 _PS_PROTECTED_SIGNER
2         PsProtectedSignerNone = 0n0
3         PsProtectedSignerAuthenticode = 0n1
4         PsProtectedSignerCodeGen = 0n2
5         PsProtectedSignerAntimalware = 0n3
6         PsProtectedSignerLsa = 0n4
7         PsProtectedSignerWindows = 0n5
8         PsProtectedSignerWinTcb = 0n6
9         PsProtectedSignerMax = 0n7
```

QUEST How to find PPL?

WinDbg



ProcessProtectedLight bit ON



ProcessProtectedLight bit OFF

Any Question?

Q/A Time