

WF – Boot Process



Twitter : @pr0neer

Blog : forensic-proof.com

Email : proneer@gmail.com

Kim Jinkook

Outline

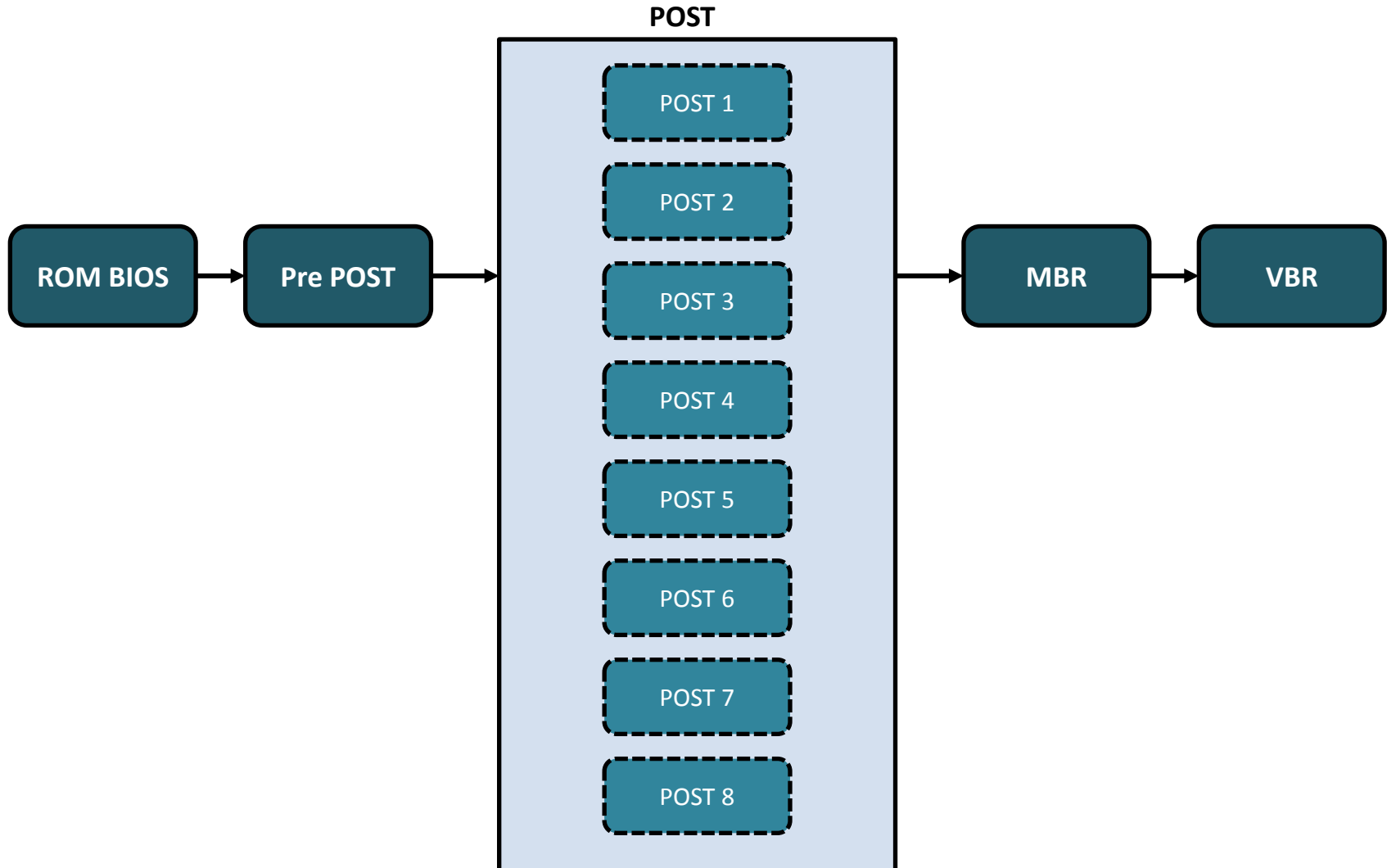
1. 공통된 부팅 절차 (Common Boot Process)
2. DOS 부팅 절차 (DOS Boot Process)
3. 윈도우 NT/2000/XP 부팅 절차 (Windows NT/2000/XP Boot Process)
4. 윈도우 Vista/7 부팅 절차 (Windows Vista/7 Boot Process)

Common Boot Process

Security is a people problem...

Common Boot Process

공통된 부팅 절차



공통된 부팅 절차 (1)

1. ROM BIOS 부트 프로그램(boot program, bootstrap) 로드

- 전원 버튼 클릭
- 전원공급기(Power Supply)는 외부 전압을 시스템에서 사용가능한 전압으로 변환
- 변환된 전기 흐름은 CPU로 전달, CPU의 이전 값들을 지우고 PC(Program Counter) 초기화 (보통 0xF000)
- 초기화 값은 메인보드 ROM BIOS의 부트 프로그램 주소 값

2. POST(Power On Self-Test) 작업 수행을 위한 기본 테스트

- 부트 프로그램은 먼저 CPU 이상 유무 테스트
- POST 작업 수행을 위한 기본 테스트 수행
- 테스트 결과가 ROM BIOS에 저장된 값과 일치하면 POST 작업 수행

3. POST – 1단계 : 시스템 버스 테스트

1. 시스템 버스가 정상적으로 동작하는지 확인하기 위해 시스템 버스에 특정 시그널을 보냄
2. 테스트가 이상 없다면 다음 단계

공통된 부팅 절차 (2)

4. POST – 2단계 : RTC(Real-Time Clock) 테스트

- RTC는 시스템의 전기적 신호를 동기화하기 위한 클럭
- 테스트가 이상 없다면 다음 단계

5. POST – 3단계 : 시스템 비디오 구성 요소(비디오 메모리 등) 테스트

- 과정이 완료되면 비로소 표준 출력을 이용해 부팅 과정 출력 확인 가능

6. POST – 4단계 : RAM 테스트

- RAM이 정상적인지 테스트

7. POST – 5단계 : 키보드 테스트

- 키보드가 정상 연결되었는지 혹은 눌러진 키가 없는지 테스트

8. POST – 6단계 : 드라이브 테스트

- 시스템에 연결된 모든 드라이브(플로피, CD, 하드디스크 등)에 신호를 보내 정상적인지 테스트

공통된 부팅 절차 (3)

9. POST – 7단계 : POST 결과 검사

- POST 결과가 RTC/NVRAM에 저장된 구성 값과 일치하는지 검사

10. POST – 8단계 : 추가적인 BIOS 로드

- 추가적인 BIOS(SCSI BIOS 등)가 있을 경우, 해당 BIOS를 RAM으로 로드

11. MBR 로드 후 부팅 가능한 파티션 검색

- 부트 프로그램은 운영체제 로드를 위해 BIOS에 설정된 첫 번째 부팅 장치에서 첫 번째 섹터(MBR)를 로드
- MBR의 파티션 테이블에서 부팅 가능한 파티션 검색
- 부팅 가능한 파티션의 VBR(Volume Boot Record)로 점프

12. VBR 로드

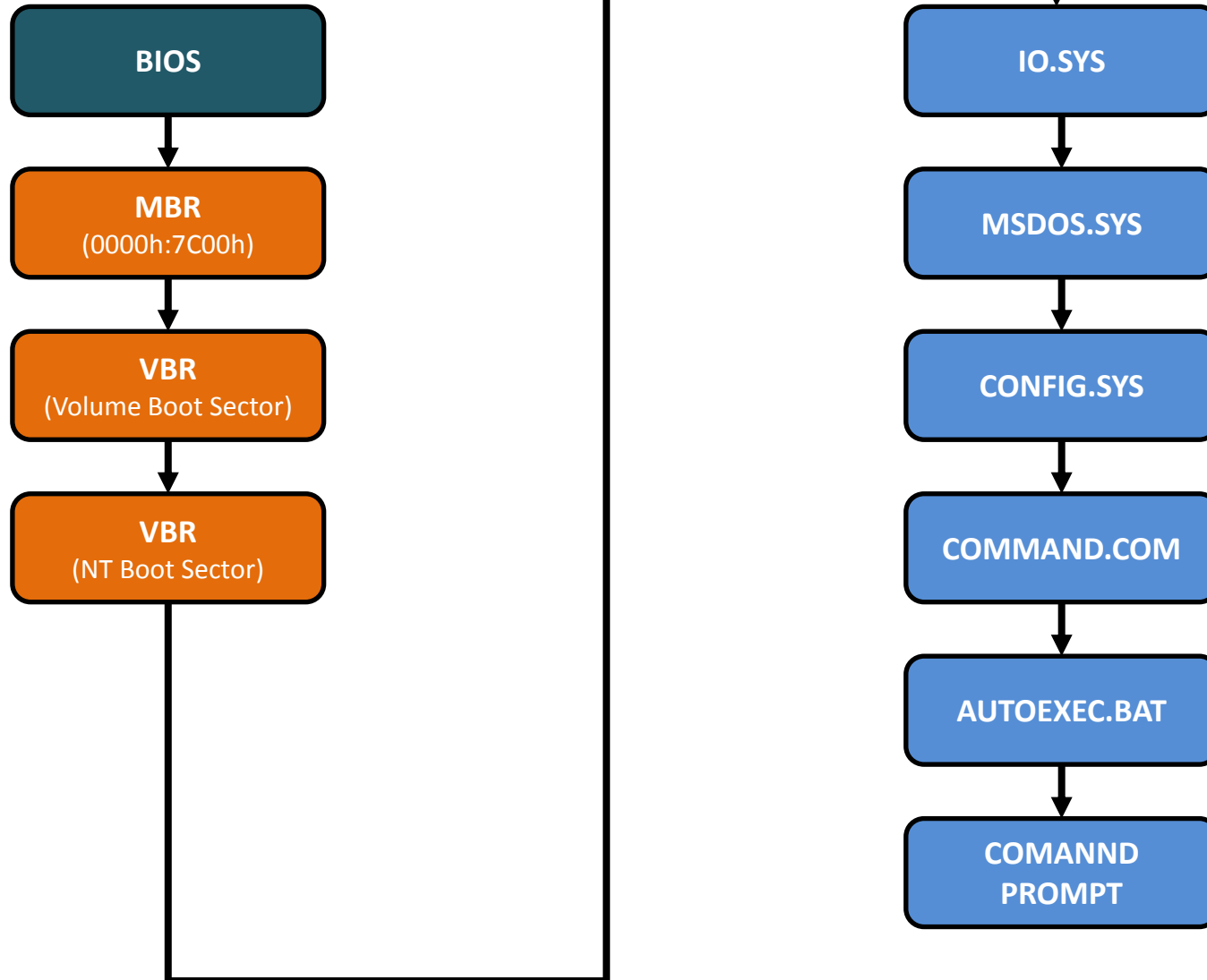
- MBR의 정보를 바탕으로 시스템 파티션(운영체제가 설치된)의 VBR을 메모리에 로드
- VBR에는 각 운영체제의 커널을 메모리에 로드하는 작업을 수행

DOS Boot Process

Security is a people problem...

DOS Boot Process

DOS 부팅 절차



DOS Boot Process

DOS 부팅 절차 (1)

❖ VBR 로드 이후 (VBR 부트 프로그램부터)

1. IO.SYS 실행

- 루트 디렉터리(Root Directory)에 존재하는 IO.SYS를 메모리에 로드 한 후 실행됨
- IO.SYS의 서브루틴인 SYSINIT는 MSDOS.SYS 파일을 읽어 자신과 읽은 내용을 메모리에 복사

2. MSDOS.SYS 실행

- SYSINIT는 MSDOS.SYS를 실행시킴
- MSDOS.SYS는 기본 장치 드라이버를 초기화시키고 시스템 장치들의 상태를 점검
- 기본적인 DOS 실행 환경을 설정 및 DOS 파일시스템 수행

3. COMMAND.COM 실행

1. SYSINIT는 CONFIG.SYS 읽어 관련 내용 수행 (하드웨어 장치 드라이버/확장 메모리 관리자를 메모리에 로딩)
2. SHELL 상태가 이미 존재한다면 수행, 존재하지 않는다면 기본 매개변수를 가지는 기본 셸(COMMAND.COM) 실행
3. COMMAND.COM은 기존 SYSINIT 메모리 영역에 덮어써지므로 SYSINIT는 종료됨

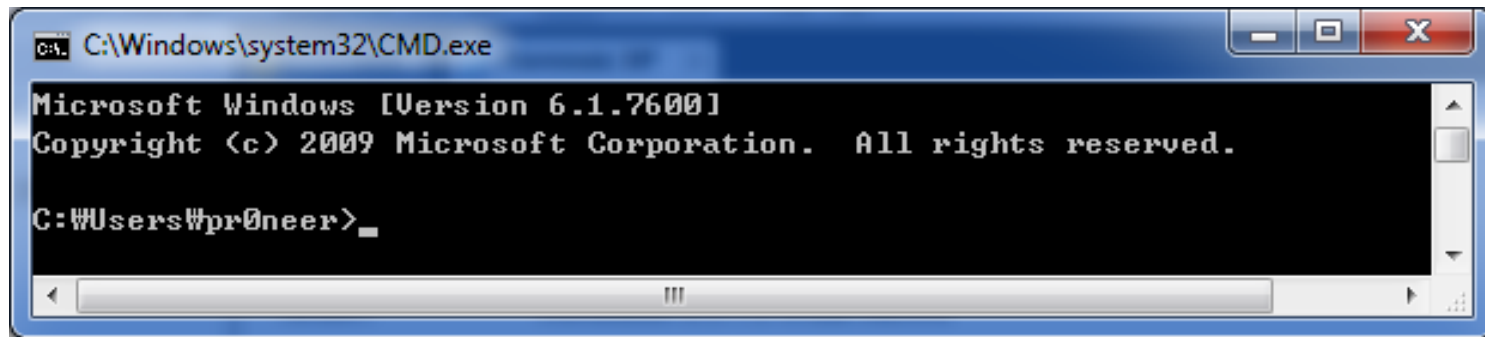
DOS Boot Process

DOS 부팅 절차 (1)

4. AUTOEXEC.BAT 수행

- AUTOEXEC.BAT(배치파일)가 존재한다면 COMMAND.COM에 의해 수행됨
- 경로(path) 설정, 사운드카드 설정, 기타 환경변수 설정 등 추가적인 설정
- 만약, AUTOEXEC.BAT가 없다면, COMMAND.COM은 DATE, TIME 명령어를 실행하고
- 카피라이트 메시지를 출력

5. 이후 깜빡이는 DOS 프롬프트 확인 가능



The image shows a screenshot of a Windows Command Prompt window. The title bar reads "C:\Windows\system32\CMD.exe". The window content displays the following text:

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

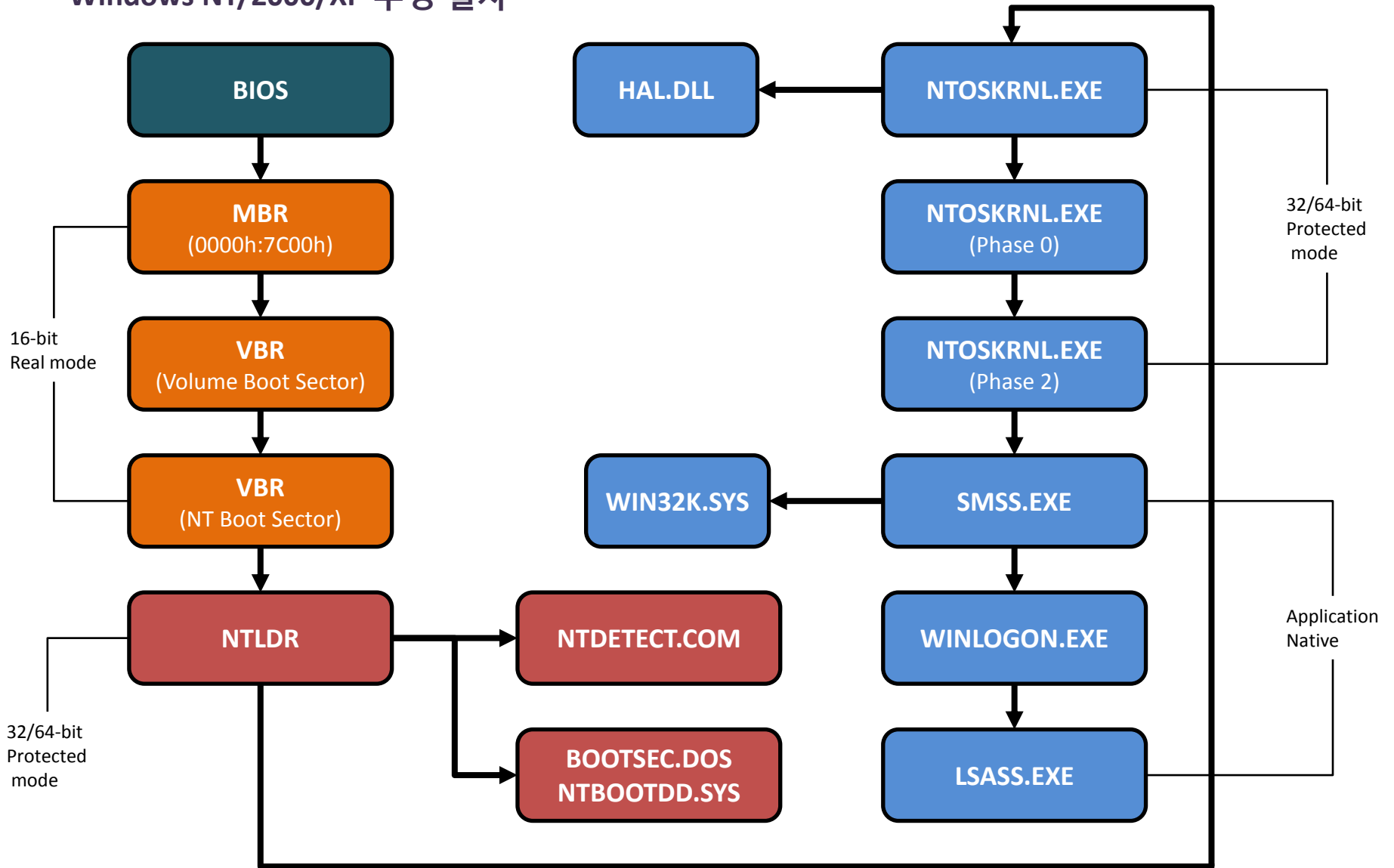
C:\Users\wpr0neer>_
```

Windows NT/2000/XP Boot Process

Security is a people problem...

Windows NT/2000/XP Boot Process

Windows NT/2000/XP 부팅 절차



Windows NT/2000/XP Boot Process

Windows NT/2000/XP 부팅 절차 (1)

❖ VBR 로드 이후 (VBR 부트 프로그램부터)

1. NTLDR

- VBR 2번째 섹터의 NTLDR (NT Loader)의 위치 정보를 읽어 NTLDR 로드
- 파일시스템 초기화
- BOOT.INI 파일을 읽어 부트 초기화 설정 및 부트 메뉴(F8) 설정
- 듀얼 부팅일 경우 BOOTSECT.DOS 수행
- SCSI 드라이버에 추가적인 파일 (NTBOOTDD.SYS)이 있다면 수행

2. NTDETECT

- NTLDR은 하드웨어 탐지를 위해 NTDETECT.COM 로드
- NTDETECT.COM은 현재 설치된 하드웨어 구성요소들 정보를 수집
- 수집된 정보를 HEKY_LOCAL_MACHINE\HARDWARE 에 유지 (메모리에 존재)
- 하나 이상의 하드웨어 프로필이 존재할 경우, 현재 하드웨어와 프로필이 맞는지 확인한 후 프로필 수행 (프로필/구성 복구 메뉴)

Windows NT/2000/XP Boot Process

Windows NT/2000/XP 부팅 절차 (2)

3. NTOSKRNL

- 하드웨어 구성 선택이 완료되면 NTLDR에 의해 NTOSKRNL.EXE (NT OS Kernel) 로드
- 커널, Hardware Abstraction Layer(HAL.DLL), 시스템 레지스트리, 드라이버, TCP/IP 등 로드
- Phase 0
 - Microkernel 자체 초기화, Executive subsystem 초기화
- Phase 1
 - Object Manager, Executive, Microkernel, Security Reference Monitor, Memory Manager, LPCS, I/O Manager, Process Manager 등 초기화
- 이 단계에서 그래픽 모드로 전환, 로딩 상태바 표시

4. SMSS

- 기본적인 초기화가 완료되면 Session Manager (SMSS.EXE) 로드
- 추가적인 레지스트리, Win32 subsystem(WIN32K.SYS)를 수행하기 위한 환경 구성 정보 로드

5. WINLOGON

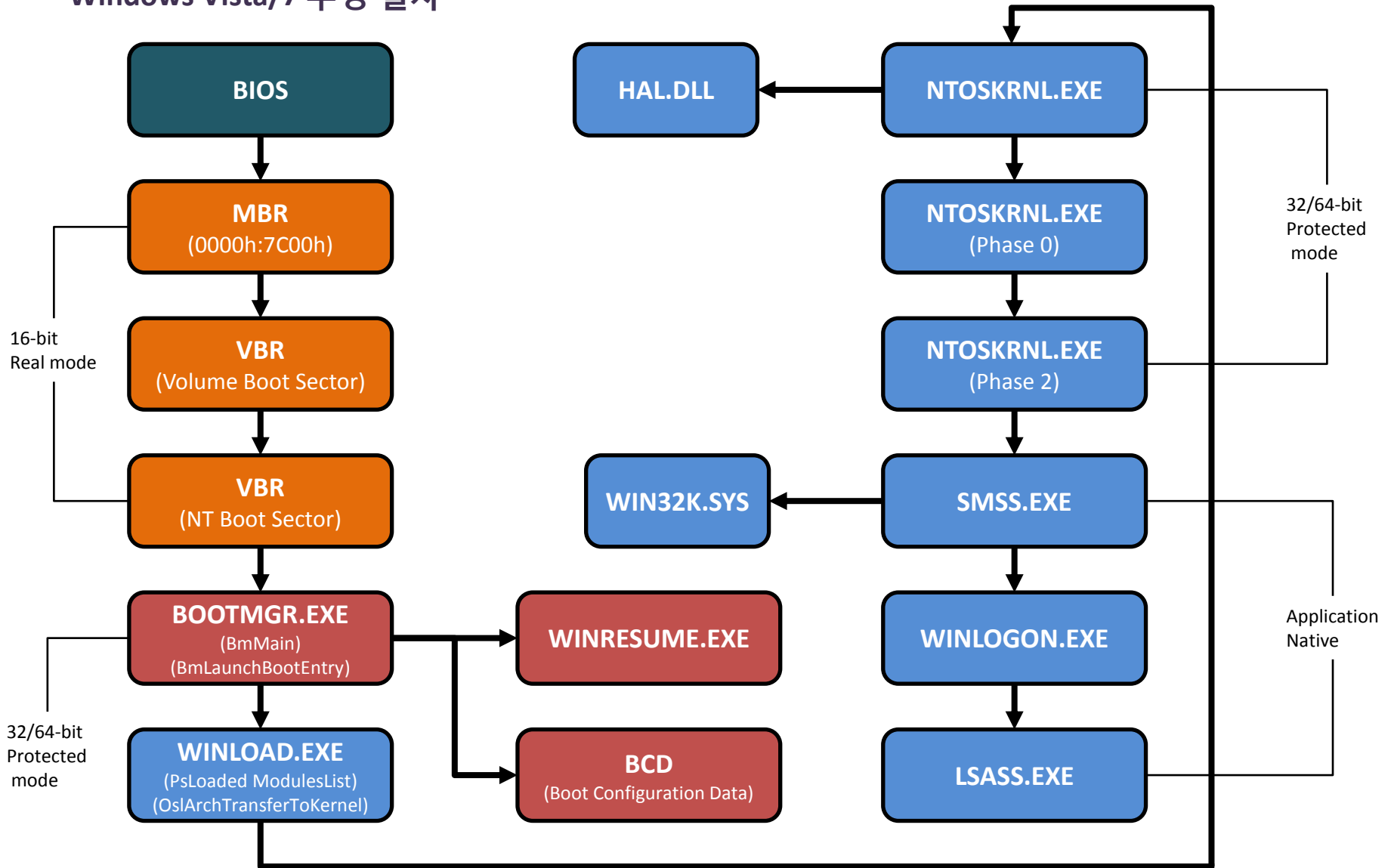
- WINLOGON.EXE 파일을 로드 → Local Security Authority (LSASS.EXE) → 로그인 화면
- 성공적으로 로그인할 경우 현재 상태를 HEKY_LOCAL_MACHINE\SYSTEM\LastKnownGoodRecovery 에 갱신
- 로그인을 수행하면 Plug and Play에 의해 새로운 장치 검사, DRIVER.CAB에서 드라이버 마운트

Windows Vista/7 Boot Process

Security is a people problem...

Windows Vista/7 Boot Process

Windows Vista/7 부팅 절차



Windows Vista/7 Boot Process

Windows Vista/7 부팅 절차 (1)

❖ VBR 로드 이후 (VBR 부트 프로그램부터)

1. BOOT MANAGER

- NT Boot Sector의 BOOTMGR.EXE 위치 정보(system32, system32/boot)를 기반으로 로드
- 자신의 체크섬 계산 후 0x400000에 매핑
- 32비트 BmMain() 함수 수행
- 하이버네이션(Hibernation) 상태일 경우, WINRESUME.EXE 로드
- BCD (Boot Configuration Data, boot.ini를 대신)로 부터 기본적인 부팅 정보 획득
- 64비트 시스템이라면 CPU를 64비트 모드로 전환

2. WINLOAD

- Boot Manager에 의해 부트 로더인 WINLOAD.EXE 로드 (NTLDR과 비슷한 기능)
- 부트 로더에 의해 NTOSKRNL.EXE, HAL.DLL, 부트 드라이버, 시스템 레지스트리 등이 로드

Windows Vista/7 Boot Process

Windows Vista/7 부팅 절차 (2)

3. NTOSKRNL

- OslArchTransferToKernel을 사용하여 커널로 제어를 전환
- NTOSKRNL.EXE를 2단계의 시스템 초기화
- Phase 0
 - 커널 자체를 초기화 → HallInitializeBios 호출 → 디스플레이 드라이버 초기화 → 디버거 시작 → KillInitializeKernel 호출
- Phase 1
 - Phase1InitializationDiscard → HallInitSystem → ObInitSystem → ASLR set → PsInitialiSystemProcess 호출 → StartFirstUserProcess
- 이 단계에서 그래픽 모드로 전환, 로딩 상태바 표시

4. SMSS

- 기본적인 초기화가 완료되면 Session Manager (SMSS.EXE) 로드
- 추가적인 레지스트리, Win32 subsystem(WIN32K.SYS)를 수행하기 위한 환경 구성 정보 로드

5. WINLOGON

- SMSS.EXE에 의해 WINLOGON.EXE 로드
- 사용자 세션 프로세스 생성, 서비스 시작, 장치 드라이버 로드, Local Security Authority Subsystem(LSASS.EXE) 로드

Linux Boot Process

Security is a people problem...

Linux Boot Process

Linux 부팅 절차 (1)

❖ VBR 로드 이후 (VBR 부트 로더부터)

1. BOOT LOADER

- Linux Loader(LILO)와 Grand Unified Bootloader(GRUB) 부트 로더가 존재하지만 현재는 GRUB이 대세
- `/etc/grub.conf` 또는 `/boot/grub/grub.conf`에서 부트 메뉴와 로드 과정 설정
- 초기 부트 메뉴를 보여 준 후 리눅스 커널 로드과 초기 RAM 디스크 로드
- 커널을 로드하는 역할이 주 목적이어서 커널 로드라고도 불림

2. kernel & initrd LOAD

- 부트 로더에 의해 커널 이미지와 initrd 이미지가 로드

3. BSS(Block Started by Symbol) & Decompress

- 커널 이미지 앞 부분의 간단한 하드웨어 검사 루틴 실행
- 기본 환경을 설정하고 BSS를 초기화
- 실제 커널 데이터 압축 해제

Linux 부팅 절차 (2)

4. PID 0 swapper process

- 프로세스 ID 0 번인 swapper 프로세스가 실행되고 페이지 테이블을 초기화하여 메모리 페이징 수행
- CPU 유형과 FPU(Floating-Point Unit) 검사

5. PID 1 init process

- 사용자 공간 프로세스로 기본적인 사용자 환경 구성
- /etc/inittab 의 환경 설정 파일의 부팅 레벨에 따라 사용자 환경 구성

Reference

- EnCE – The Official EnCase Certified Examiner Study Guide
- http://vittoriop77.altervista.org/download/XP_Boot_Process.pdf
- <http://bandwidthco.com/whitepapers/compforensics/volume/boot/The%20Windows%207%20Boot%20Process.pdf>
- <http://www.ibm.com/developerworks/kr/library/l-linuxboot/>

