Live-CD를 이용한 해킹 방지 Bios 메커니즘의 제안

이종민° 이상인 강흥식
인제대학교 컴퓨터공학부
jm lee@ cs.inje.ac.kr° delpai@ delpai.com hskang@ cs.inje.ac.kr

Bios Mechanism Suggestion to Prevent "Hacking Using Live-CD"

JongMin Lee° SangIn Lee HeungSeek Kang
Dept. of Computer Engineering, Inje University

요 약

Live-CD는 리눅스 설치 과정의 번거로움을 없애기 위한 노력의 일환으로써 시작되었다. CD 한 장에 리눅스 커널과 어플리케이션을 모두 넣고 어디서나 간단하게 부팅 가능하도록 한 CD를 말한다. 하지만 Live-CD가 악용될 경우 CD안에 공격을 위한 exploit 코드와 어플리케이션을 넣고 공공기관이나 PC방등에서 CD 한 장으로 해킹이 가능할 수 있다는 문제점이 발생할 수 있다. Live-CD는 Ramdisk상에서만 동작하며 전원을 끄는 것과 동시에 모든 데이터가 소멸되므로 공격자 추적 또한 불가능하다. 따라서 본 논문에서는 하드디스크를 제외한 모든 저장 장치로 부팅을 할 시에는 관리자 인증 과정을 통해서만 부팅할 수 있는 Bios 메커니즘을 제안하여 Live-CD를 이용한 해킹을 근본적으로 방지할 수 있도록 한다.

1. 서 론

현재 컴퓨터가 널리 보급됨에 따라 언제, 어디에서나 컴퓨터를 할 수 있는 여건이 갖추어져 있다. 장소에 구애 받지 않고 컴퓨터를 통해 E-Mail, 정보검색 등을 할 수 있는 순기능이 있지만 어디에서나 컴퓨터를 이용한 해킹이 가능하다는 역기능 또한 존재한다. 공공기관이나 PC방등 쉽게 컴퓨터를 접할 수 있는 곳에는 빠른 네트워크와 고사양의 PC가 갖추어져 있고 사용자는 불특정 다수를 대상으로 하기 때문에 신분 노출의 위험이 적어 공격자들에게는 최적의 환경이라고 할 수 있다. 여기에 하드디스크 없이 Ramdisk상에서만 동작하는 Live-CD라는 기술이 최근 대두되면서 CD 안에 리눅스 커널, exploit 코드와 공격에 필요한 어플리케이션을 넣어 공개된 PC 환경 하에서 자신의 흔적을 남기지 않고 공격이 가능하게 되었다. 5분 이하의 부팅 시간을 거쳐 Ramdisk의 휘발성이라는 특성 때문에 컴퓨터 포렌식을 우회하는 공격이 가능하게 된다. 아직 Live-CD에 대한 연구가 초기단계이기 때문에 이를 이용한 공격 사례가 적으나 잠재적으로 큰 위험요소를 가지고 있다.

따라서 본 논문에서 이러한 위험요소를 최소화 할 수 있는 Bios 메커니즘을 제안한다. 즉, CD나 기타 장치로 부팅을 위해서는 반드시 관리자 인증을 통해서만 가능하도록 하는 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 Live-CD, Bios, 컴퓨터 포렌식 절차에 대해 알아보며 3장에서는 Live-CD를 이용한 컴퓨터 포렌식 우회 기법에 대하여 알아보고 4장에서는 Bios Password 메커니즘의 설계에 대하여 서술한다. 마지막으로 5장에서 결론을 맺는다.

2. 관련 연구

2.1 Live-CD

리눅스 설치 과정의 번거로움을 없애기 위한 노력의 일환으로써 시작된 것이 Live CD라고 할 수 있다. 즉, 어떤 운영체제가 설치 되어있는 컴퓨터라도 CD 한 장만 넣으면 하드웨어에 변화를 주지 않으면서 리눅스 환경을 제공하고, 사용할 수 있게 만들어 주는 CD를 말한다. 이는 Install CD가 아닌 Ramdisk에 상주하는 Linux로서 그냥 전원을 끈 경우라도 커널의 깨짐을 걱정 하지 않아도 되는 Linux이다.[1]]

Live-CD Linux name	Service
Knoppix	Desktop
KursLinux	Education
Trx Live Firewall	Firewalls
Plan-B	Forensics
Hakin9 Live	Security
Rxlinux	Server

[표 1] 대표적인 Live-CD 목록

[표 1]은 대표적인 Live-CD를 정리한 것이다. 현재 백개가 넘는 Live-CD가 배포중인 것으로 조사 되었다.[2]

2.2 Bios

Bios는 사용자가 PC를 켜면 곧바로 시작되는 프로그램으로 하드디스크, 비디오 어댑터, 키보드, 마우스 및 프린터 등과 같은 주변장치와 컴퓨터 운영체제 간의 데이터 흐름을 관리하기도 한다. Bios는 컴퓨터의 없어서는 안 될 핵심부분으로서 컴퓨터와 함께 딸려온다 (운영체

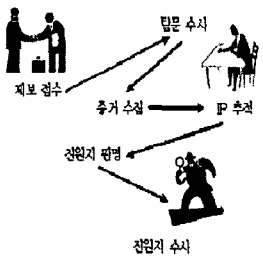
제가 제작자나 공급자에 의해 미리 설치되거나, 사용자에 의해 설치될 수 있는 것과는 대비된다). Bios는 EPROM 칩에 들어있으며, 마이크로프로세서에 의해 사용될 수 있도록 만들어져 있다. 사용자가 컴퓨터를 켜면, 마이크로프로세서는 EPROM의 항상 같은 장소에 위치하고 있는 Bios 프로그램에게 통제권을 넘긴다. 컴퓨터를 부팅시킬 때 Bios가 제일 먼저 모든 부착물이 제 위치에 있으며, 작동 가능한 상태인지를 확인한 뒤, 운영체제를 하드디스크나 디스켓, CD-ROM으로부터 읽어 램에 적재시킨다.[3]

2.3 컴퓨터 포렌식

컴퓨터 포렌식은 컴퓨터를 매개로 이루어지는 범죄행위에 대한 법적 증거자료 확보를 위하여 컴퓨터 저장매체 등의 컴퓨터 시스템과 네트워크로부터 자료를 수집, 분석 및 보존하여 법적 증거물로써 제출할 수 있도록 하는 일련의 절차이며 행위이다.[4]

2.3.1 대응분석

정보침해 사고가 제보되면, 관련 기관들은 컴퓨터 범죄 수사팀을 구성하여 침입자에 대한 신상정보를 파악하기 위해 탐문수사와 증거 수집을 시작한다. 탐문수사와 증거 수집은 침입자의 진원지를 파악하는 것이 최종목적이며 일반적인 순서는 [그림 1]과 같다.

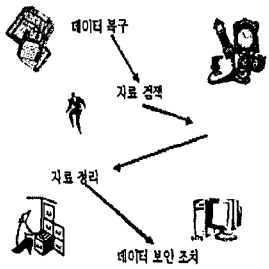


[그림 1] 대응분석 절차

피해자의 제보로 수사팀을 구성하고 피해 시스템의 분석을 통한 침입자의 정보를 획득하고 추출된 정보를 근거로 침입자에 대한 모니터링이 이루어진다. 침입자에 대하여 조사한 자료와 사이버 법규를 토대로 증거자료가 충분히 확보되면 진원지를 탐문 수사하게 된다.

2.3.2 위험분석

위험분석은 범죄에 사용되었다고 추정되는 디지털 증거를 확보하는 것으로 침입자에게 법적효력을 발휘하는 핵심근거가 된다. 디지털 증거 확보를 위한 컴퓨터 포렌식 절차는 [그림 2]와 같다.



[그림 2] 위험분석 절차

침입자가 범죄에 사용된 자료를 은폐 또는 삭제할 가능성이 높기 때문에 저장매체의 데이터 복구가 처음으로 이루어지고, 복구된 데이터는 암호가 걸려 있을 경우 역공학에 의해 해석되고, 분석의 용이함을 위해 파일 포맷의 분류를 통해 정형화된 형태로 정렬된다. 범죄가 발생했던 시간을 중심으로 단서가 되는 데이터를 분석하고 증거를 산출하게 된다. 필요한 증거가 최종적으로 산출되면 백업 디스크를 제외한 시스템 분석에 사용한 시스템의 자료들을 삭제하게 된다.

3. Live-CD를 이용한 컴퓨터 포렌식 우회 기법

Live-CD는 기반의 리눅스 운영체제로, 일반적으로 하드디스크에 설치하여 사용하는 Linux System과 동일한 역할과 기능을 수행한다. 분명한 차이점은 Live-CD가 Ramdisk상에서 작동한다는 것이다.

3.1 공격을 위한 Live-CD의 구성

자동 디바이스 설정: 80X86 계열의 모든 컴퓨터 환경에서 5분 안에 부팅 완료

기본적인 X-Windows APP: Editor, Graphic, Sound, Net, Shell, System, ETC.

공격 Exploit 포함: 실제 공격 시 사용가능한 Exploit 포함

크래킹 도구 포함: Finger Printing, Bug Scanner, Sniffering, Wireless, Cracking, Network/File analysis Tool, ETC.

3.2 Live-CD를 통한 컴퓨터 포렌식 우회

대응분석 및 위험분석의 컴퓨터 포렌식 절차가 Live-CD를 통해 어떤 방식으로 우회되는지 살펴본다.

3.2.1 대응분석 우회

피해시스템이 발생하면 관련 조사기관에 제보가 들어오고 사고조사팀이 구성된다. 사고조사팀은 피해 시스템의 네트워크 패킷 분석, 로그 분석을 통해 진원지 추적을 시작하게 된다. 최신 Live-CD는 H/W 자동인식 및 네트워크 인터페이스 자동설정을 지원하여 CD-ROM의 사용이 가능한 어떤 시스템에서도 원활하게 작동하기 때문에 피해 시스템의 네트워크 패킷 분석 결과로 침입자

의 진원지를 판명해 내더라도 그곳은 공격자와는 전혀 관계없는 곳일 수 있다. 진원지가 확실하다는 가정 하에 진원지 탐문수사를 통한 위험분석 단계로 간다.

3.2.2 위험분석 우회

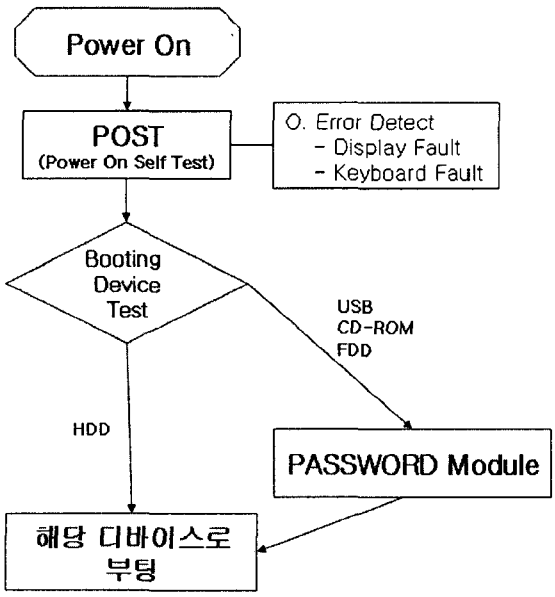
위험분석의 첫 번째 단계는 데이터 복구이다. 하지만, 공격자가 Live-CD를 이용한 포렌식 우회기법을 사용했다면 복구할 데이터 자체를 가지고 있지 않다.[5]

4. Live-CD를 통한 공격 방지를 위한 Bios 메커니즘의 설계

컴퓨터를 켜면 Bios는 POST(Power On Self Test)를 수행한다. POST가 display fault, keyboard fault등을 감지하고 Bios에 세팅 된 순서로 부팅 가능한 장치를 찾는다. 여기서 CD롬이 HDD보다 높은 순위의 부팅 장치로 되어 있을 경우 Live-CD를 통한 부팅이 가능하게 되고 결과적으로는 공격의 위험이 생긴다. Bios 세팅 시 처음 부팅 장치로 HDD를 해놓고 패스워드를 걸어 놓을 수도 있지만 이것 또한 Bios를 리셋하면 패스워드 확인 루틴이 사라지기 때문에 근본적인 위험을 해결할 수 없다.

4.1 Bios의 수행 순서 설계

[그림 3]과 같이 기존의 Bios 수행 과정에 password 모듈을 적용 한다.

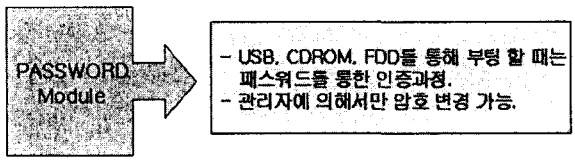


[그림 3] 제안하는 Bios 메커니즘

[그림 3]에서 볼 수 있듯이 Password 모듈을 삽입하여 HDD 이외의 장치로 부팅하는 것은 시스템 관리자에 의해서만 가능하도록 해야 한다.

4.2 Bios Password 모듈

[그림 4]에서는 Password 모듈의 특징을 보여준다.



[그림 4] Password 모듈의 특징

Bios Password 모듈은 MainBoard 제조사에서 MainBoard를 배포할 때 기본적으로 Password를 제공해야 하고 관리자에 의해서만 변경이 가능하도록 한다. MainBoard를 리셋 하더라도 기본적으로 Password가 존재하기 때문에 Password를 뚫지 않는 한 공격자는 HDD 이외의 장치로는 부팅이 불가능 하게 된다.

5. 결론

현재 Live-CD가 막 활성화 되는 단계이기 때문에 이를 이용한 공격 피해 사례가 적다. 하지만 익명성이 보장된 고성능의 컴퓨터를 쉽게 이용할 수 있는 환경과 Live-CD를 이용한 컴퓨터 포렌식 우회 공격이 가능하다는 점에서 잠재적 위험 요소는 매우 크다고 할 수 있다. 현재의 컴퓨터 아키텍처로는 일단 Live-CD로 부팅이 된 후에는 이를 이용한 공격에 무방비로 노출되어지게 되고 역추적 또한 불가능 하다. 현재 최선의 대응 방법은 HDD이외의 장치로 부팅을 할 시에는 시스템 관리자만이 부팅 권한을 갖도록 Password 모듈을 삽입하는 것이다. 지금 사용자들이 사용하고 있는 Bios는 이러한 Password 모듈이 없기 때문에 MainBoard 제조사에서는 본 논문에서 제안한 Password 모듈을 추가한 Bios Update를 반드시 해야 만 앞으로 발생할 가능성이 있는 피해를 최소화 할 수 있을 것이다. 그리고 MainBoard의 Password가 노출되면 심각한 문제점이 야기될 수 있기 때문에 향후 Bios에 최적화 된 Password 암호화 알고리즘에 대한 연구가 필요할 것이다.

6. 참고 문헌

[1] http://www.ikikldp.org/wikiphp/LiveCD-HOWTO

[2] http://www.frozentech.com/content/livecd.php

[3] http://www.terms.co.kr/BIOS.htm

[4] http://www.fbi.gov.hq/lab/fsc/backissu/oct2000/computer.htm

[5] 박재흥, 이상인, 김상돈, 강흥식, "컴퓨터 포렌식 우회기법에 대한 연구", ITFind 주간기술동향, 2004. 7