情 報 保 護 學 會 誌
第18卷 第3號, 2008. 6

시스템 제어 방식의 웹 데이터 유출 방지

윤 석 구*, 최 연 주**

요 약

웹상에서 표시되는 다양한 정보의 유출을 막기 위해서 접근 방법으로 캡처 프로그램이 필요로 하는 시스템 기능의 패턴을 분석한 후 분석된 시스템 기능을 제어하는 방식을 제안한다. 이것은 기존의 다양한 캡처 프로그램을 등록하는 방식과 비교하여 보안 위험 기간을 획기적으로 줄여줄 뿐만 아니라 미래의 잠재 위험에 대해서도 근본적인 대책을 가져다 준다는 점에서 강점이 있다. 향후 시스템 기능 제어 기술을 확장하여 안전한 가상 환경을 제공하는 가상화 보안 기술로 확대 연구를 진행할 계획이다.

Ⅰ. 서 론

다양한 해킹 프로그램들에 대한 지금까지의 보안기술의 접근 방법은 각 해킹 프로그램에 대한 Signature 정보를 바탕으로 Black List를 작성하고 실시간 모니터링을 통해 인식된 해킹 프로그램을 Disable시키는 방법을 채택하고 있다. 지금까지의 웹 상에서 표시되는 정보의 유출을 방지하는 웹데이터 유출 방지 기술의 경우도 이와 유사한 접근 방법을 취하고 있다. 그러나 효과적인 웹캡처 방지 기술을 개발하기 위해서는 최소 300종에서 최대 300만종 이상의 프로그램을 분석해야 하고, 시장에서 존재하는 대부분의 캡처 프로그램에 대한 정보를 가지고 있다 하더라도 프로그램 능력을 가지 해커가 해킹용으로 직접 제작한 프로그램의 경우는 정보를 가질 수가 없기 때문에 프로그램 등록 방식의 접근 방법은 한계를 가진다.

현대적인 운영체제하에서 응용 프로그램의 제작 방식을 살펴보면, 프린트, 파일저장, 네트워크 전송 등 프로그램들이 공통적으로 사용하는 기능은 운영체제에서 DLL(Dynamic Link Library)이나 API(Application Programming Interface) 형태로 제공되고 응용 프로그램에서는 이러한 운영체제의 기능을 필요에 따라 사용함으로써, 목적한 기능을 수행하게 된다. 웹 정보를 유출하기 위한 캡처 프로그램의 경우도 이러한 기본적인 동작방식에서 벗어나는 경우는 거의 없다. 유일한 예외는 디바이스 드라이버를 직접 포함하는 프로그램의 경우는 예외가 될 수 있는데, 이러한 예외사항에 대해서는 그 수가 제한적이므로 각 프로그램 별 분석 기법을 사용해서 큰 문제가 되지 않는다.

일반적인 응용프로그램 형태로 제작된 캡처 프로그램에 대한 방어를 구현하기 위한 방식으로, 본 논문에서는 캡처 프로그램과 운영체제 사이에서 캡처 프로그램이 시스템에 요청하는 System Call 중 캡처에 사용될 수 있는 Call을 Blocking함으로서 기능 수행을 근본적으로 차단하는 방식을 제안하고, 실제 제품화 사례를 소개한다.

Ⅱ. 본 론

2.1 기존 웹 데이터 유출 방지 시스템의 기능과 문제점

웹은 브라우저라는 표준화된 User Interface를 통해 사용자에게 동일한 사용환경을 제공하고, 언제 어디서나 접근이 용이하며, 필요에 따라 ActiveX, JavaScript 등을 통해 부가기능을 제공할 수 있다는 점에서 Blog 등의 형태인 개인정보 및 인트라넷 형태의 기업 데이터의 표준 Presentation Platform으로 자리매김하고 있다. 그러나 기능적인 측면만을 강조한 웹 브라우저의 개발은 상대적으로 보안의 취약성을 키워왔다. HTML 텍스트, 동영상, Flash™, 이미지 등 표시되는 콘텐츠 포멧의 다양성, 다양한 스크립트 기능, ActiveX등과 같은

* (주)테르텐 대표이사 (prinstone@teruten.com)
** (주)테르텐 기술연구소 주임 (valinor@teruten.com)

임의 다운로드 되는 프로그램 기능 등과 같은 다양한 브라우저의 기능은 시스템 복잡도를 증가시킴으로써 보안의 취약성을 증가시키고 있다.

지금까지 일반적인 웹 보안을 위한 접근 방법은 거의 모든 기업에서 사용 중인 방화벽을(Firewall)을 시작으로, 침입탐지시스템(IDS), 침입방지시스템(IPS), 종합보안관제 시스템(EMS)등을 사용하고 있다. 이러한 방법은 시스템 외부로부터의 해킹에 대한 방어는 상당 수준의 보안 레벨을 유지할 수 있으나, 시스템 내부에서의 해킹을 통한 데이터 유출에는 상대적으로 취약한 면을 보이고 있다. 시스템 내부로부터의 해킹의 유형과 취약성을 다시 정리하면 다음과 같다.

첫째로, 중요 정보가 사용자 인증 후 복호화되어 웹 브라우저 화면에 표시될 때 화면 캡처를 통해서 콘텐츠가 유출될 수 있다. 데이터가 DB에 저장되어 있을 경우에는 DB 보안 기능에 의해서 데이터가 암호화되어 보관되어 있기 때문에 안정성이 보장되고, 사용자 PC단의 웹 브라우저와의 통신은 SSL과 같은 보안 통신 기능을 사용한다면 보호될 수 있다. 그러나 보호된 데이터가 복호화되어 웹 브라우저를 통해서 해석되고 표시된 이후에 운영체제에서 제공하는 화면 캡처 기능 등을 이용한다면 손쉽게 데이터를 유출할 수 있다. 또한 '다른 이름으로 저장'과 같은 웹 브라우저의 기본 기능 또는 간단한 캡처 유틸리티 프로그램으로도 중요 정보 및 콘텐츠가 유출 될 수 있다.

둘째로, 데이터 유출 사고의 80%정도는 사용자 끝단에서의 해킹을 통해서 유출이 이루어지고 있다. 먼저 스팸 메일이나 네트워크 공격 등을 통해서 사용자 PC에 침투한 해커는 루트킷이나 트로이목마 프로그램을 사용자 PC에 심게 된다. 이후 사용자가 웹 브라우저 등을 통해 암호화된 데이터를 복호화한 상태로 표시할 때 임시파일이나 프로그램 메모리, 파일시스템 등 다양한 시스템 자원에 대한 공격을 통해서 데이터를 유출한다.

이러한 사용자 끝단에서의 해킹 공격의 가장 큰 문제점은 간단한 수준의 보안을 위하여서도 많은 비용과 시간이 요구된다는 것이다. 여러 가지 다양한 환경에서 많은 부가 기능 모듈들에 모두 적용되는 보안 시스템을 만들고 이를 적용하기까지 하나의 시스템이나 네트워크 트래픽만을 보호하는 서버 보안이나 네트워크 보안에 비해서 상대적으로 많은 시간과 비용을 필요로 한다. 따라서 이러한 보안의 문제를 해결하기 위해서는 지금까지와는 다른 접근 방법을 필요로 한다. 이에 대한 답을 하기 전에 먼저 이 장에서는 웹에서 데이터 유출을 방지하기 위해서 필요한 사용자 끝단에서의 각 보안 요소별로 구체적인 시스템의 요구사항과 문제점에 관하여 구체적으로 논하고자 한다.

2.1.1 화면 캡처 기능 제어

웹 상의 화면을 캡처하여 콘텐츠가 유출되는 것을 막기 위한 기능은 웹 보안 시스템의 가장 큰 부분을 차지한다고 할 수 있다. 일반적으로 캡처 기능 제어를 위해서 개별 캡처 프로그램의 리스트를 등록함으로써 캡처 프로그램의 작동을 막는 방식이 쓰이며, 이 방식은 기술적으로 캡처 프로그램의 실행 파일 패턴 비교를 통하여 캡처 프로그램을 검출하여 각각의 캡처 프로그램을 막아주는 형식의 방법이다. 그러나 이러한 방법은 범용적인 접근이 어렵고, 폭넓은 검출이 어렵기에 새로운 캡처 프로그램과 패턴이 나올 때마다 많은 시간과 비용이 들게 된다. 또한 화면 캡처 기능 제어를 위하여 일반적으

〔표 1〕 화면 캡처 방지 기술에 대한 요구 사항

기 능	설 명
클립보드 복사 방지	PrintScreen, 클립보드 복사 방지
캡처 프로그램 기능 상실	모든 캡처 프로그램 실행 시 캡처 이미지가 생성 안됨
최상위 윈도우	모든 윈도우의 최상위로 나타나게 함, 즉 다른 프로그램은 뒤로 나타남
마우스 영역 제한	마우스를 최상위 부모 윈도우의 영역 밖으로 나가지 않게 함
아이디 표시	플래쉬나 동영상 플레이 시 화면에 ID가 나타나고, 그림 안에 아이디를 숨겨둠
GDI 캡처 방지	GDI를 이용하여 캡처 시 다른 곳을 캡처하게 함
이미지 저장 방지	BMP, DIB, JPG, JPEG, GIF, TIF, TIFF, CMP, CAL, CALS, FAX, EPS, IMG, RAW, ICA, PCT, PICT, MSP, RAS, TGA, WFX, WMF, EMP, ICO, CUR, WPG, PCX, PNG, PSD, AVI, MPG, MPEG, WMV, WMA등으로 저장하지 못하게 함.
터미널 서비스 방지	Windows2000 Server/XP등에서 터미널 서비스를 이용하여 라이브 재생시 실행 안되게 함.
미러드라이브 방지	울트라 VNC, TCO Stream, 윈도우 XP 원격 데스크톱
DirectX 캡처 방지	DirectX를 사용한 멀티미디어 영상 캡처 방지
프린터 방지	프린트 드라이버로 화면 데이터 전송 불가

로 사용되는 API Hooking 기술은 윈도우 시스템과 커널에 대한 깊이 있는 이해와 기술을 필요로 하기에, 보안 시스템이 어떠한 경우에도 안정적으로 적용되도록 하는 것은 상당한 경험과 지식을 요구한다.

화면 캡처 기능을 제어하기 위하여 일반적으로 요구되는 사항은 [표 1]과 같다.

2.1.2 캐쉬 파일 보호 기능

사용자의 PC에 일단 웹 페이지의 콘텐츠가 다운로드된 후에는 그 PC안의 캐쉬 파일들을 쉽게 접근하여 콘텐츠를 유출할수 있게 된다. 이 문제를 해결하기 위하여 지금까지는 브라우저 종료 시 캐쉬를 삭제하여 콘텐츠를 보호하는 방법이 쓰여지고 있으나, 이 방식은 캐쉬 파일 전체를 삭제할 경우 많은 시간을 소모하게 되고, 관련된 파일만을 매번 검색하여 삭제한다 하더라도 마찬가지의 문제점이 있다. 특히 브라우저 실행 중 임의의 방법으로 캐쉬가 사용자에게 노출될 위험은 항상 존재하게 된다.

이에 대하여는 HTTP의 헤더경로를 변경하여 캐쉬파일의 저장경로를 변경해 사용자가 쉽게 캐쉬파일이 저장되어 있는 경로를 찾지 못하도록 하는 방법이 쓰여지기도 하나, 근본적으로 로컬의 특정 경로에 캐쉬 파일이 저장되어 있는 한 사용자에게 캐쉬가 노출될 위험이 존재하게 된다.

2.1.3 다중 정책 지원 기능

앞서 열거된 화면캡처 제어 기능과 캐쉬 파일 보호 기능이 어떠한 상황이나 사용자의 구별없이 일괄적으로 적용될 경우 그것이 웹이라는 매체의 편리한 접근성과 정보의 빠른 전달성이라는 장점을 살리지 못하게 된다. 일반적으로는 사용자별, 페이지별 고정된 권한 정책을 지원하게 되나 이러한 방식은 상황과 변수에 따라서 이분화된 정책 적용이 안되므로 보안 기능을 추가하기 위하여 웹의 특성을 어느 정도 제한적으로 사용할 수밖에 없게 된다. 또한 게이트웨이(별로 하드웨어)를 사용하여 HTML 패키징 작업을 하는 경우에는 별도의 프로세스가 추가되므로 비용과 자원의 추가적인 소모가 있게 된다.

2.1.4 외부 프로그램 지원 기능

외부 프로그램은 원격지원 프로그램 혹은, 메신저, VMWare 등을 통하여 웹 매체로의 접근이 가능한 프로그램들을 말하며, 이러한 외부 프로그램에 대한 지원은 보안이 이뤄지지 않고 있다.

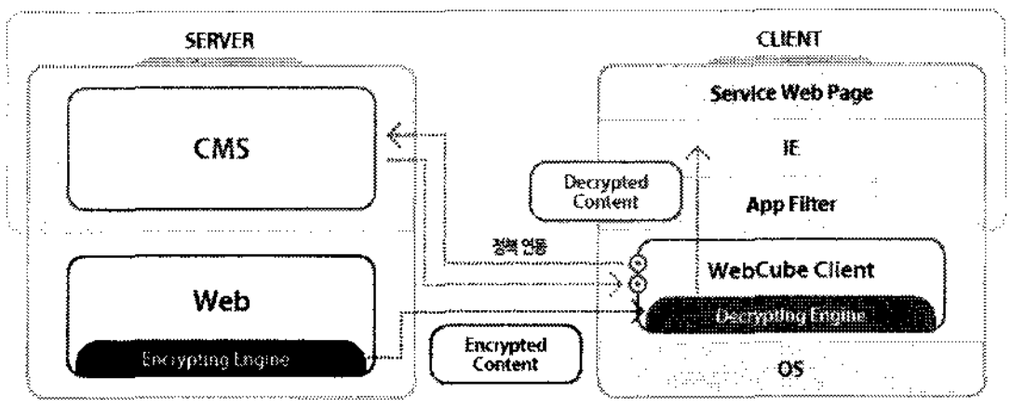
또한 시스템 외부에서 정책의 권한에 대한 변경이 불가능하므로, 일괄적인 정책을 적용할 수밖에 없다.

2.1.5 유지보수 및 업그레이드의 편리성 (확장성)

모든 보안 시스템과 마찬가지로 지금 우리가 논하고 있는 웹의 보안 역시 한번의 보안 시스템 설치로 영구적으로 사용 가능한 시스템은 현실적으로 존재하기 어렵다. 모든 시스템은 유지/보수라는 관리 단계가 존재하며, 서비스는 그 서비스의 확장이라는 단계가 이어지기 마련이다. 따라서 보안 시스템의 확장성이 부족할 경우 업그레이드 및 확장 페이지 적용이 불편하게 되어 안정적이고 원활한 서비스를 보장할 수 없게 된다.

2.2 웹큐브 웹 보안 시스템

본 장에서는 2.1장에서 제시한 요구사항을 만족하는 테르텐의 웹큐브 시스템 구현사례를 제시한다. 웹큐브 시스템은 사용자의 웹 브라우저에 도달한 콘텐츠를 보호하는 클라이언트 모듈, 정책 연동 인터페이스 모듈, 콘텐츠 실시간 암·복호화를 통한 네트워크 보안 모듈로 구성되며, 세 가지 모듈은 선택적으로 적용 가능하도록 되어 있다. 실제로 보안 시스템이 적용된 웹 콘텐츠는 Application Filter 기반의 프로세스 제어 기술을 이용하여 보호되고 있으며, 웹상의 다양한 콘텐츠를 하나의 논리적 단위로 묶어 접근을 차단하고 있다.



〔그림 1〕 테르텐의 웹 보안 시스템, WebCube의 프로세스 흐름도

2.2.1 브라우저 기능제어

웹큐브 시스템은 기본적으로 웹 브라우저의 기본 기

능 제어를 통해 콘텐츠 및 데이터의 유출을 방지하도록 한다. 웹 브라우저에서 제공하는 기본 메뉴, 툴바, 단축키, 컨텍스트 메뉴 중 보안과 관련된 메뉴만을 선택하여 철저하게 제어하여 일반 메뉴를 사용하는 사용자의 편의성을 저해하지 않도록 한다. 브라우저의 기능 제어를 위하여 제시되는 기능은 다음과 같다.

- 편집/저장/인쇄/보내기 등 보안 메뉴 제어
- 툴바, 단축키 등 제어
- 소스 보기 등 컨텍스트 메뉴 제어

2.2.2 화면 캡처 기능제어

화면캡처를 통한 데이터 및 콘텐츠의 유출은 보안 사고 발생에 있어 가장 손쉽고도 광범위하게 사용되는 방식이다. 캡처 제어 기술은 실행되는 프로세스의 패턴 분석 방식을 적용하였으며, API호출, DirectX 작동 패턴 등을 분석하여 캡처 패턴으로 감지된 모든 프로세스가 우리의 보안 시스템이 적용된 웹 페이지에 접근하는 것을 차단한다. 이는, 개별 캡처 프로그램의 리스트를 등록함으로써 동일 기능을 구현하는 방식에 비하여 절대적인 기능과 범용적인 적용이 가능하다라는 측면에 있어서 우위를 보여준다. 화면 캡처 제어를 위하여 제시되는 기능은 다음과 같다.

- Copy & Paste를 통한 화면 캡처 제어
- 프린트 스크린을 통한 화면 캡처 제어
- 화면 캡처 전용 툴의 작동 제어

2.2.3 캐쉬 파일 영역보호

웹큐브 시스템은 실행 중인 웹 브라우저의 캐쉬 파일 저장 경로를 지정된 Secure Storage로 변경하도록 한다. Secure Storage 는 보안 시스템 구동 시 생성되는 가상드라이브로서, 이 시스템과 바인딩된 브라우저 프로세스에 대해서만 접근이 허용되도록 한다. 따라서 사용자가 임의의 어플리케이션을 통해 Secure Storage에 접근을 시도할 경우 실행 중인 웹 브라우저 및 연결된 프로세스 이외의 접근이 차단됨으로써, Secure Storage 내에 저장된 콘텐츠 파일, 소스 파일 등에 대한 사용자 임의의 접근 및 유출을 제어한다. 캐쉬 파일 영역보호를 위하여 제시되는 기능은 다음과 같다.

- 웹 브라우저의 캐쉬 파일 저장 경로를 가상 드라이브로 변경
- 사용자 PC의 캐쉬 파일에 대한 접근 제어
- 이미지 및 플래시, 동영상 등의 Data 유출 제어

2.2.4 콘텐츠 암·복호화를 통한 네트워크 보안

웹 정보와 콘텐츠에 대한 보안은 단순히 사용자의 PC 내부에서의 정부 유출만으로 제한되어지지 않는다. 콘텐츠가 네트워크를 통하여 전달되는 동안 소프트웨어적으로 네트워크 보안상의 안정성을 보장하기 위하여 콘텐츠를 암·복호화하도록 한다. 암·복호화를 위하여 제시되는 기능은 다음과 같다.

- 보안의 등급에 따라 암·복호화 기능 적용
- 콘텐츠 전체에 암·복호화가 되도록 지정
- 콘텐츠가 존재하는 경로 중 특정 경로를 지정하여 암·복호화가 되도록 지정
- 콘텐츠의 특정 확장자 단위로 암·복호화가 되도록 지정

2.2.5 정책 적용 및 관리

웹큐브 보안 시스템은 사용자별, 페이지별 차별화된 정책 적용 기능을 제공하여야 한다. 이를 위해 서비스 업체가 보유하고 있는 사용자 DB 및 콘텐츠 관리 시스템(CMS: Contents Management System)과 연동이 용이한 인터페이스를 제공하여야 하며, 선택 적용 가능한

〔표 2〕 웹큐브에서 정책 적용 가능한 기능 리스트

분류	상세 항목
웹 브라우저 기능 제어	웹 브라우저 기본 메뉴를 통한 저장, 편집, 소스보기 등 제어
	인쇄 제어
	웹 브라우저 컨텍스트 메뉴를 통한 저장, 편집, 소스보기, 이메일로 보내기 등 제어
화면 캡처 기능 제어	캡처 전용 프로그램을 통한 화면 캡처 제어
	원격 프로그램을 통한 화면 캡처 제어
	PrintScreen 을 통한 화면 캡처 제어
클립보드 기능 제어	복사&붙이기 기능 제어
	클립보드 접근 제어
원격 프로그램 지원	허가된 사용자에 한해 VMWare, Terminal 등을 통한 원격 접속 허용
기타	마우스 기능 제어

정책은 다음과 같다.

2.2.5.1 사용자별, 페이지별 차별적인 정책 적용 기능 제공

웹큐브 시스템은 서비스 업체가 기 보유하고 있는 사용자 DB 및 CMS와 연동하여 편리하게 페이지별, 컨트롤별 정책 적용을 할 수 있는 인터페이스를 제공한다. 따라서 웹 페이지에 보안을 적용하기 위한 기존 시스템의 변경 또는 재개발이 불필요하며, 이를 위해 관리 서버 등 별도의 장비를 도입해야 하는 추가 비용 또한 매우 적어지게 된다. 이러한 점은 웹 관리 시스템 변경 및 페이지 확장에 따른 신속한 보안 변경 적용을 용이하게 한다.

2.2.5.2 원격 지원 프로그램을 통한 사용자 별 실시간 정책 변경 기능 제공

또한 개별 사용자에게 설정된 정책을 실시간 변경 가능하도록 지원한다. 이는 시스템이 자체적으로 제공하는 원격 지원 프로그램을 통해 가능하도록 하며, 이를 통해 관리자는 요청한 사용자의 권한 범위 변경 및 사용자 PC 장애에 대한 지원이 가능하도록 한다. 이는, 보안 적용이 곧 시스템의 사용 편의성 저하로 이어지는 솔루션에 비해서 빠르고 편리한 서비스를 제공해야 하는 웹 비즈니스의 특성을 잘 살릴 수 있다.

2.3 적용 기술

전 장에서 우리는 브라우저 기능 제어, 화면 캡처 기능 제어, 캐쉬 파일 영역보호, 콘텐츠 암·복호화를 통한 네트워크 보안 그리고 정책 적용 및 관리 등의 기능을 웹 보안 시스템의 주요 기능으로 제시하였다. 이 장에서는 이 중 화면 캡처 기능 제어와 캐쉬 파일 보호를 위한 기능을 위하여 적용된 기술에 관하여 기술하도록 한다. 본 논문에서는 운영체제가 윈도우일 경우를 가정하여 설명하였으며, Macintosh나 Linux 또는 Unix등 타 운영체제에서도 유사한 방식으로 구현 가능하다.

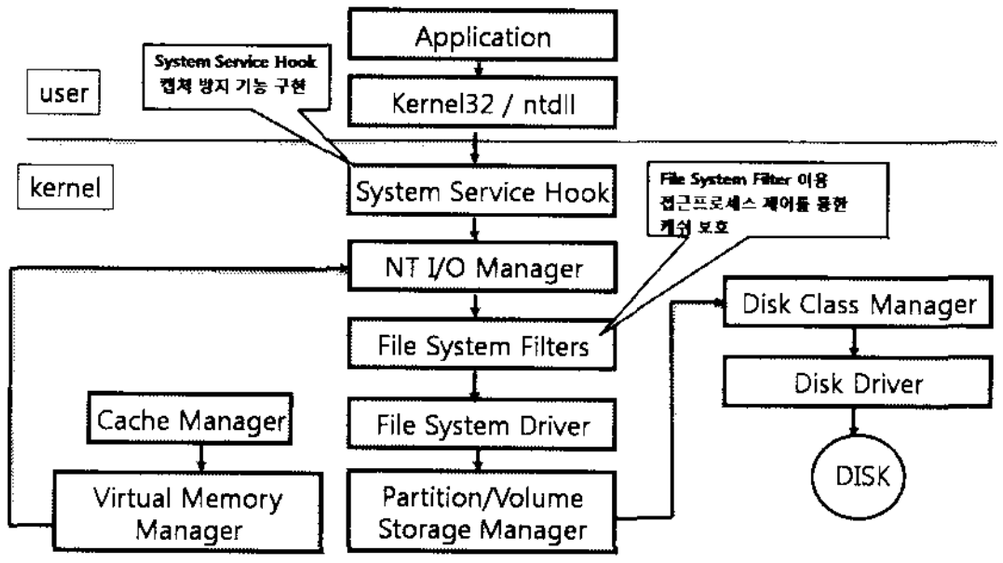
화면 캡처 기능 제어와 캐쉬 파일 보호 기능을 실제로 적용하기 위해서는 OS의 커널 레벨의 System Service Hooking 기술과 File System Driver 윗 단계에 적용되는 가상 드라이버인 File System Filter 기술이 필요로 하며 이것은 User 영역이 아닌 Kernel 영역에서 처리가 되어야 한다.

그 외에 콘텐츠의 암·복호화 기능은 네트워크적인 보안을 보장하며 암호화 부분은 웹 서비스 서버상에서 (Windows의 경우 IIS Server, UNIX/LINUX 의 경우 Apache Server) 필터 형식으로 구현되고, 복호화 부분은 웹 보안 시스템의 모듈의 일부로 구성되어져질 수 있다.

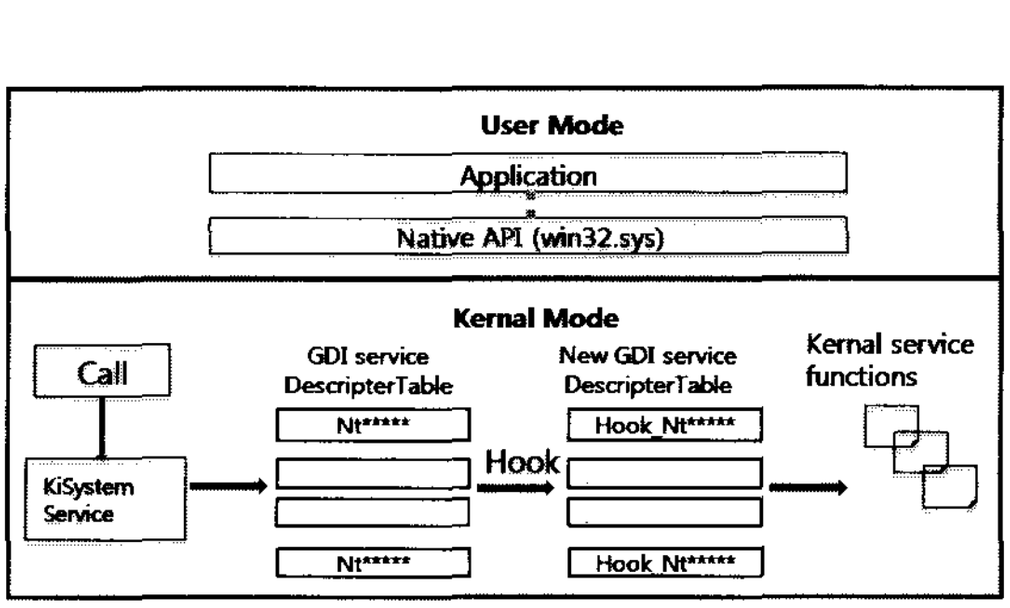
2.3.1 캡처 방지 기능 구현: System Service Hook

캡처 프로그램을 제어하기 위해서는 API 후킹을 통해 실행되는 프로세스를 확인한 후, 프로세스의 패턴 분석을 통해 캡처 프로세스를 인지하여, 그 캡처 프로세스가 이미지를 메모리에 저장하는 것을 차단하도록 한다.

GDI, DirectShow 방식의 캡처를 제어하기 위해서는 GDI 관련 Function 만을 Hook 하여 화면 캡처일 경우 그 기능을 차단하도록 한다. 이 때의 Hooking은 User 영역의 win32.sys의 호출이 발생하였을 때 Shadow System Service Table이라는 윈도우의 모든 서비스 주소를 담고 있는 테이블에 접근하여 API를 전역으로 후킹하도록 한다. 이 테이블은 Ring0 의 권한으로만 read/write 할수 있으며, 이 테이블의 후킹을 원하는 함



〔그림 2〕 Windows OS 시스템 프로세서 단계들과 커널모드에서의 기술 적용 구조



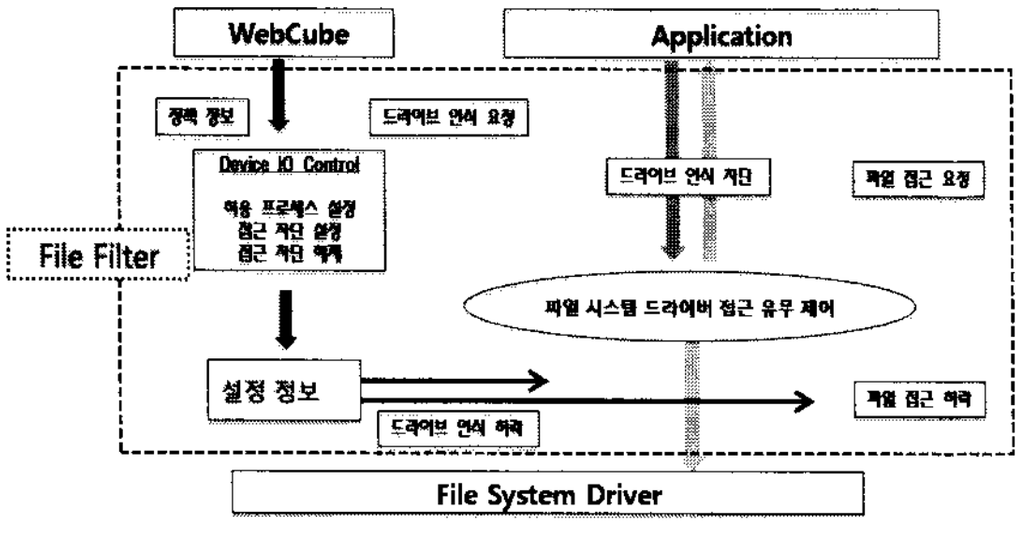
〔그림 3〕 웹큐브 System Service Hook 구조

수를 찾기 위해서는 커널 메모리상에 존재하는 Shadow System Service Table에서 관련된 정보를 찾거나, 후킹하고자 하는 함수의 패턴을 찾아 후킹하여 캡처와 관련된 부분을 제어하도록 한다. 이 과정은 아래의 그림으로 나타내어질 수 있다.

2.3.2 캐쉬 보호 기능 구현: File System Filter

캐쉬 보호를 위한 기능은 File System Filter를 사용하여 구현한다.

보안 시스템이 처음 구동될 때 File System Driver 윗 단계에 File System Filter를 넣어 가상드라이버를 만들게 된다. 보호를 받고 있는 웹 사이트의 주요 정보와 콘텐츠들은 Secure Storage 라고 명명된 가상 드라이버안에 저장이 되며, 이 가상 드라이버에 접근하는 것은 File System Filter를 통해서 제어한다. 따라서 시스템은 파일 시스템 드라이버에 접근 요청이 있을 경우 설정되어 있는 접근 허가 프로세스 정보를 Device IO Control를 통해 Filter에 전달한다. Filter는 전달 받는 정보를 이용하여 드라이브 인식 가상 디스크에 접근하는 프로세스에 대한 접근을 결정하게 된다.



〔그림 4〕 웹큐브 File System Filter 구조

Ⅲ. 결 론

지금까지 우리는 웹상에서 표시되는 다양한 정보에 대한 유출을 방지하기 위한 보안 시스템의 요구사항과 이를 구현한 시스템의 구조, 그리고 구현 시스템에 적용된 기술을 대해서 살펴보았다. 본 논문에서는 기존의 프로그램 등록 방식의 보안 접근 방식을 버리고, 시스템을 제어함으로써 보다 근본적인 보안 기능을 구현할 수 있는 방식을 제안하였다.

최근의 보안 기술의 흐름을 보면, 안티바이러스, 스팸 필터, 방화벽, 침입 탐지 등 다양한 분야에서 프로그램 시그니처 분석을 통한 주기적인 업데이트 방식보다 근본적인 접근 방식에 대한 해답을 찾고 있다. 본 논문에서 제안하는 시스템 제어형 보안 기술은 이러한 보안 시스템의 설계에도 응용될 수 있다고 판단된다. 향후에는 시스템 제어 기술을 확장하여 Java 기술에서 제안한 Sand Boxing 방식과 유사하지만 보다 근본적인 보안 실행 환경을 제공하는 가상화 보안 기술을 개발할 계획이다.

참고문헌

[1] Peter Szor, "*The Art of Computer:Virus Research and Defense*", Symantec. Press, USA, February 2005

[2] Markus Jakobsson, Steven Myers, "*Phishing and Countermeasures*", WILEY INTERSCIENCE, USA, 2007

[3] Markus Jakobsson, Zulfikar Ramzan, "*Crimeware : Understanding New Attacks and Defenses*", Symantec. Press, USA, April 2008

[4] John Viega, Gary McGraw, "*Building Secure Software*", Addison Wesley, USA, September 2001

[5] Charles P. Pfleeger, Shari Lawrence Pfleeger, "*Security in Computing*", Pearson Education, Inc., USA, October 2006

[6] Gary McGraw, "*Software Security*", Pearson Education, Inc., USA, January 2006

[7] Greg hoglund, James Butler, "*Rootkit*", Pearson Education, Inc., USA, August 2005

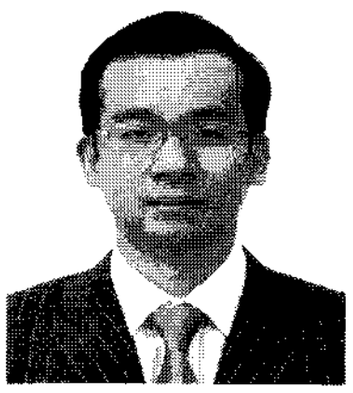
[8] Ross Anderson, "Security Engineering" second ed., WILEY Publishing, Inc, USA, 2008

[9] Jon Erickson, "*Hacking : The Art of Exploitation*"second ed., No Starch Press, January 2008

[10] Dafydd Stuttard, Marcus Pinto, "*The Web Application Hacker's Handbook : Discovering and Exploiting Security Flaws*", WILEY Publishing, Inc, USA, 2008

[11] Shon harris, Allen Harper, Chris Eagle, Jonathan Ness, Michael Lester, "*Gray Hat Hacking*", McGraw Hill Osborne Media, November 2004

〈著者紹介〉



윤 석 구 (Yun Seokgu)
(주)테르텐 대표이사

1990년 2월 : KAIST 전자공학과 학사
1993년 2월 : University of Southern California Computer Science 석사
1994년 1월~1999년 9월 : (주)삼성종합기술원 디지털통신 Lab 전문 연구원
2000년 6월~현재 : (주)테르텐 대표이사
<관심분야> 정보보호, 소프트웨어 보안

최 연 주 (Choi Yeon-Ju)
(주)테르텐 기술연구소 주임

1998년 2월 : 세종대학교 전산과학과 학사
2002년 6월 : France, Université Paris 8, Dep. d'Informatique 학사
2006년 6월 : France, Université Paris 8, Dep. d'Informatique 석사
2008년 1월~현재 : (주)테르텐 기술연구소 주임 연구원
<관심분야> 정보보호, 가상머신