

# 개인 정보 보호를 위한 화면 캡처 방지 모듈 구현

곽동욱, 윤동영, 이종혁

## Implementation of preventing screen capture modules for privacy

Dong-uk Kwak, Dong-young Yun, Jong-hyeok Lee

### 요 약

최근 컴퓨터의 보급과 정보사회의 발달로 인해 개인 신상 정보에 대한 관심이 증대되고, 이와 관련된 정책과 기술이 발전함에 따라서 개인 신상 정보를 보호하려는 시도가 다양하게 이루어지고 있다. 본 논문에서는 컴퓨터를 사용하면서, 개인의 중요한 자료나 신상정보 또는 회사의 기밀 내용을 다루는 기관 및 부서를 대상으로 중요한 자료와 신상정보 및 회사의 기밀을 보호하는 방안을 제안 하였다. 결과적으로 공공기관 또는 개인기관 내에서 타인의 정보를 악의적으로 도용하거나 도취하는 것을 방지 하고, 기관 내의 시스템들 사이에서 정보가 오가는 동안 중요한 자료와 신상 정보들의 노출을 1차적으로 막을 수 있다.

### ABSTRACT

Recently due to the development of the information society and the spread of computer, interest for personal information is increased and as policy and technology associated with the development, we have been various attempts to protect your personal information.

In this paper, for agencies and departments to computer use and to deal with Important data of individuals, personal information or the company's confidential information, we proposed modules to protect them. As a result, we prevent a public agency or private institutions within that using mean bad or stealing another person's information. When we communicate various information with the systems in the institutions, the module can be prevented critical data and personal information exposure.

### 키워드

화면 캡처 방지, 슈퍼 클래스링(전역 후킹), API, 클립보드, 기능키

Key word

Prevent Screen Capture, Super-Classing, API, Clipboard, Function keys

### 1. 서 론

최근 컴퓨터의 보급의 증가로 사용자의 편의성을 요구하는 일반대중은 인간에게 친숙한 인터페이스(Interface)의 출현을 바라고 있다.[1] 이러한 효과로 인해 컴퓨터 내에는 키보드, 마우스, 혹은 키패드를 이용하여 사용자가 조작할 수 있는 수많은 기능들을 내포하고 있다. 예를 들면 프린트 스크린 기능키, 복사 기능키, 붙여넣기 기능키를 들 수 있다. 이러한 기능들은 유용성과 사용성 등 인간 중심의 컴퓨터를 실현하기 위한 인터페이스로 굉장히 편리하게 사용할 수 있는 반면, 너무나 쉽게 개인의 중요한 자료

나, 신상정보를 훔칠 수 있는 기능마저 제공하여 오히려 보안에 대한 역효과가 대두되고 있는 실정이다.

보안의 종류를 간략히 살펴보면 네트워크 보안, PC 보안, 문서 보안, 출력 보안, DB 보안, 물리적 보안이 있다. PC보안의 특징을 간략히 소개하면 사용자가 PC에서 발생할 수 있는 여러 가지 문제들을 해결하기 위한 솔루션과 통합 보안, Antivirus(바이러스 침투를 방지하기 위한 솔루션), PC 방화벽이 있다.[2]

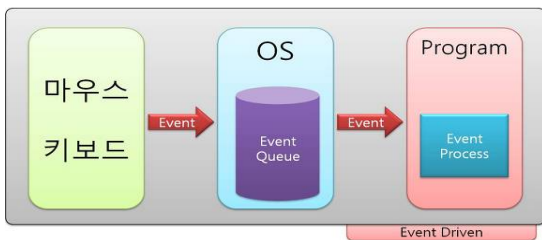
이러한 보안 정책들이 유지되고 있음에도 불구하고, '2012년 7월 KT에서 고객정보가 유출되는 보안사고 발생'[3], '2012년 9월 MBC 정보

수집 프로그램, 금융거래·의료정보 유출사건 발생[4], ‘2012년 9월 게임 앱 위장 개인정보 빼내’[5] 등 올해만 해도 개인정보가 유출된 사례가 셀 수도 없이 많이 일어나고 있다. 이런 전차로 우리는 개인정보 및 중요한 자료를 철저히 관리할 필요성이 있다.[6] 정보화 시대에 진입함에 따라 컴퓨터를 사용하지 않는다는 것은 거의 불가피한 상황이기 때문에 우리는 컴퓨터를 사용하면서 중요한 자료나 개인 정보를 다루는 공공기관이나 개인기관 뿐만 아니라 회사 내의 기밀문서를 다루는 부서를 대상으로 정보보호를 할 수 있는 실행 모듈인 화면 캡처 방지 모듈을 구현하고자 한다.

## II. 관련연구

### 2.1 화면 캡처 방지의 정의 및 특징

화면 캡처 방지란 컴퓨터와 연결된 모니터에서 디스플레이 되는 화면을 컴퓨터에서 제공하는 프린터 스크린 키, 복사 기능키, 붙여넣기 기능키를 통해 화면을 캡처 하거나, 마우스 드래그를 통해 정보를 복사하여 옮기는 것을 방지하는 것을 말한다. 위에 기술은 윈도우즈 운영체제의 이벤트 드리븐 방식에서 후킹 기법을 도입하여, 컴퓨터가 클립보드를 사용하게 될 경우를 백그라운드에서 쓰레드로 실행되고 있던 화면 캡처 방지 프로그램이 이를 감지하여 클립보드에 저장되어 있는 화면 캡처 내용 또는 텍스트 문서를 비워 주어 붙여넣기 기능을 사용하여도 화면 캡처 내용이나 텍스트 문서가 복사 붙여넣기 되지 않는다. 그림1은 화면캡처 방지모듈과 이벤트 드리븐 방식의 관계이다.



(a) 입력 (b) 후킹 (c) 클립보드 비움  
(a)Insert (b)Hooking (c)Clipboard Empty  
그림 1. 화면 캡처 방지 모듈과 이벤트 드리븐 방식과의 관계.

Fig. 1. Relation of Prevent screen capture modules and Event-Driven System.

### 2.2 WIN32 API 후킹

API는 후킹기술을 가능하게 해주는 모듈 중 하나이다. 후킹 기술은 크게 서브 클래싱(쓰레드 후킹), 슈퍼 클래싱(전역 후킹)으로 나눌 수 있다.[7] 서브 클래싱(쓰레드 후킹)은 윈도우 프로시저로 보내지는 메시지를 중간에 가로채는 기법으로 특정한 쓰레드에서 발생하는 메시지만을 가로챈다. 슈퍼 클래싱(전역 후킹) 같은 경우는 모든 쓰레드에서 발생하는 메시지를 가로챌 수 있다. 윈도우 메시지 발생하여 후킹 되는 과정을 그림 2에 나타내었다.

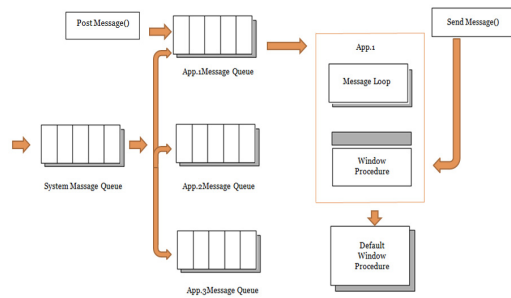


그림 2. 윈도우 메시지 후킹.  
Fig. 2. Window message hooking.

## III. 모듈 구현

### 3.1 구현 방법

화면 캡처 방지 모듈을 구현하기 전에 우선 모든 쓰레드에서 발행하는 윈도우 메시지를 가로챌 수 있도록 슈퍼 클래싱(전역 후킹) 기법을 사용하여 전역 후킹 모듈을 구현한다. 후킹 모듈 같은 경우는 반드시 dll형식으로 만들어 실행 시켜야 한다. dll형식의 파일을 실행시키기 위해서는 다른 응용 프로그램에 추가 종속시켜 혹 체인을 설치하도록 해야 한다. 혹 체인을 설치함으로써 인해 후킹 시에 자신이 만든 메시지 프로시저로 변경이 가능해진다. 설치 함수는 그림3과 같다.

```

HHOOK SetWindowsHookEx(
    int idHook,           // type of hook to install
    HOOKPROC lpfn,       // address of hook procedure
    HINSTANCE hMod,      // handle to application instance
    DWORD dwThreadId     // identity of thread to install hook for
);
    
```

그림 3. 혹 프로시저 설치 함수.  
Fig. 3. Hook procedure installed function.

화면 캡처 방지 모듈의 전체 방지 기능 구현 방법은 백그라운드에서 실행되고 있는 캡처 방지 모듈이 프린터 스크린 키가 사용되는지를 O/S 상에서 감시하고 있다가 이를 감지하게 될 경우 클립보드 내용을 모두 비워 버리는 방식을 사용하였고, 복사기능(Ctrl + V) 키 역시 화면 캡처 방지 모듈이 O/S 상에서 감시하고 있다가 Ctrl키를 감지하게 되면 클립보드로 접근하여 안의 내용을 모두 비워버리는 방법을 사용하였다. 부분 방지의 기능 구현의 경우 프린터 스크린 키를 감지하면 클립보드에 저장된 내용을 잠시 DC에 보관한 후, 방지 하고자 하는 특정 영역에 접근하여 RGB의 색깔을 덧 입혀 줌으로써 특정 부분에는 흰색 또는 어두운 색으로 채우는 형식으로 구현 하였다. 가로채 메시지를 사용자가 만든 메시지로 바꿔주는 함수는 그림4와 같다.

```
LRESULT CallNextHookEx(
    HHOOK hhk, //handle to current hook
    int nCode, //hook code passed to hook procedure
    WPARAM wParam, //value passed to hook procedure
    LPARAM lParam, //value passed to hook procedure
);
```

그림 4. 훅 체인 함수.  
Fig. 4. Hook chain function.

또한 이 프로그램은 MFC를 기반으로 만들었지만 VB등 다른 모듈에서도 실행하기 위해서 ATL COM이라는 방식을 사용하였다.

3.2 구현 알고리즘

캡처방지 기능을 실행시키면 후킹함수들이 윈도우상에서 눌러지는 버튼들을 감지한다. 감지를 하는 도중 원하는 키 값을 누르게 되면 함수의 기능이 실행이 되어 클립보드에 있는 내용들을 지우게 된다. 만약 원하는 키 값을 누르게 되지 않으면 계속해서 윈도우 버튼을 감시하게 된다. 그림5는 화면 캡처 방지 모듈의 흐름도이다.

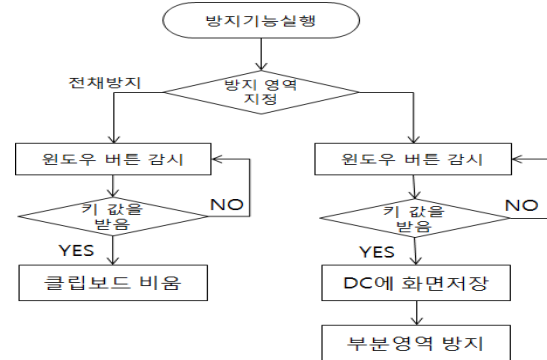


그림 5. 화면 캡처 방지의 흐름도  
Fig. 5. Flowchart of the prevent screen capture.

3.3 구현 결과

개인 정보를 취급하는 프로그램을 예로 들어 구현 결과를 설명하도록 하겠다. 그림6은 이력서에 자신의 개인 정보를 기록한 그림이다.

이 력 서

	이름	윤도영	영문	BONG YOUNG YOON	한문	
	주민번호	921225-1111111			나이	21
	휴대폰	00-000-0000	전화번호	000-0000-0000		
	E-mail	AB0000@naver.com	SNS	Blog/ Twitter/ Facebook		
	주소					

학력사항 (최종학력: OO대학교(4년) 졸업)			
제학기간	학교명 및 전공	학점	구분
0000.00.00	OO대학교 OO학과		졸업
0000.00.00	OO고등학교		

그림 6. 기존에 존재하는 이력서 작성 프로그램.  
Fig. 6. Application the program that currently exist.

이력서 프로그램에 화면 캡처 방지 모듈을 종속시켜 전체 방지 기능을 수행한 결과를 그림7에 나타내었다.



그림 7. 전체 방지 기능을 수행한 결과.  
Fig. 7. A result of performing the full protection.

개인 정보란에만 부분 방지 기능을 적용하였을 경우의 결과를 그림 8에 나타내었다.

이 령 서


	이름	윤동영	영문	DONG YOUNG YOON	한문	
	[Redacted]					
	주소	[Redacted]				
락터사명 (외종학번: OO대학교(4년) 졸업)						
계좌기좌	학교명 및 전공	학점	구분			
0000.00.00	OO대학교 OO학과		졸업			
0000.00.00	OO고등학교					

그림 8. 부분 방지 기능을 수행한 결과.  
Fig. 8. The result of partial protection.

IV. 결 론

본 논문에서는 PC보안에 중점을 두어 화면 캡처 방지 모듈을 구현하여 컴퓨터를 사용하면 개인의 정보나 중요한 자료를 다루는 기관을 대상으로 개인 정보 및 중요한 자료가 기관 시스템을 통해 오가는 동안 고의로 개인 정보가 유출 되는 것을 1차적으로 막기 위한 해결 방안을 제시하였다. 또한 화면 캡처 방지 모듈은 기존에 개인 정보나 중요한 정보를 다루는 프로그램에 DLL형태로 추가하여 캡처 방지 기능을 수행하도록 구현되어 별도의 환경을 구축할 필요가 없는 장점이 있다.

화면 캡처 방지 모듈로 인해 정보의 기밀성을 보장하여 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하여 비밀 보장을 유지하고, 원치 않는 정보의 공개를 막을 수 있다. 정보에 대한 무결성을 유지하여 정보의 수정할 수 없도록하며, 가용성 또한 높여 정보에 접근하려하고자 할 때 방해 받지 않고 정보를 보안할 수 있다.

참고문헌

- [1] 신수연·권태경, “개인정보보호를 고려한 HCI 기술에 대한 고찰”, 정보과학회지 제 27권 제 12호 pp68-77, 2009. 12
- [2] 조용태, 류경무, 양정이, “컴퓨터 보안 시스템”, 한국특허정보원, 2006. 06.
- [3] 황태호, “보안사고 ‘진퇴양난’ KT, 구체적 해결방안 안보여”, etnews, 2012. 07. 31
- [4] 이재진, “MBC 정보 수집 프로그램, 금융 거래·의료정보까지 빼갔다”, 오늘의 미디어, 2012. 09. 24
- [5] 백민제, “게임 앱 위장 개인정보 빼내”, Focus, 2012. 09. 21
- [6] 조영임, “개인정보보호와 지능형 에이전트 기술”, 한국정보기술학회지, 제6권, 제1호, 2008년.
- [7] 지식백과, “두산백과-컴퓨터와 인터넷-소프트웨어”, 두산백과 doopedia.