키보드 해킹기법 및 대응기술 분석

2005. 11.

금융ISAC

차 례

Ⅰ. 분석 목적

○ 전자금융거래 확산 및 사용자 인증 강화 추세

– 정보통신 기술발전과 인터넷 사용 보편화로 인터넷을 통한 전자금융거래 및 전자상거래 이용 확산

– 한편, 대면확인이 불가능한 온라인 환경의 특수성 때문에 ID와 Password에 의한 기초적 인증 방식에서 전자공인인증서와 같은 고도의 인증 방식에 이르기까지 다양한 방법으로 고객의 정당성 여부를 확인

○ 키보드 입력정보의 해킹사고 증가 추세

– 각종 보안대책 도입에도 불구하고 고객PC의 키보드 입력값을 탈취하는 해킹기법의 출현 및 고도화로 인해 각종 관련사고가 발생

* 전자공인인증서 암호 유출위험성 보도(2005.5.27)
* 키보드 해킹을 통한 불법 자금이체사건 보도(2005.6.3)

– 각 금융기관은 고객PC에서 키보드 해킹을 방지하기 위한 보안솔루션을 갱신하거나 추가 도입하는 등 전산보안시스템의 보완·강화 추진

【참가기관 보안솔루션 적용현황】

키보드 보안 솔루션	PC 보안 솔루션	통신 암호화 솔루션
nProtect KeyCrypt (8)	nProtect Netizen (11)	INISAFEWeb (6)
Secure KeyStroke (8)	MyFirewall (6)	XecureWeb (6)
K-Defense (1)	LiveCall Suite (1)	Banktown Module (5)
MyKeyDefense (1)		STI J/SSWEB (1)

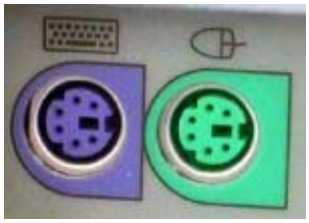
* ( )는 도입은행 수

따라서, 주요 정보입력 수단인 키보드의 해킹방지를 강화하기 위하여

- ▶ 개인용PC의 일반적인 키입력 처리과정과
- ▶ 이 과정에서의 키보드 해킹 기술 및 위협을 분석하고
- ▶ 이에 대응한 주요 솔루션의 특징 및 대응기술을 분석함

Ⅱ. 키보드 접속방식 및 처리절차

1. 키보드 접속방식

	PS/2 방식	USB 방식
접속 단자		
주요 특징	○ 키보드·마우스 전용 ○ Plug & Play* 미지원	○ 타 장비 공용 가능 ○ Plug & Play 지원

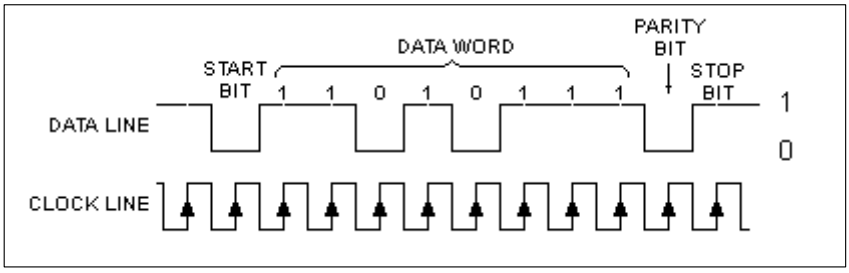
* PC 사용 중에도 재설정 또는 재부팅 없이 자동으로 주변장치를 설치·제거할 수 있도록 하는 기술로서, 'hot swapping'으로도 지칭

가. PS/2 방식

○ PS/2 포트는 IBM이 개발한 키보드 및 마우스 접속용 포트로서, 6개의 핀을 갖는 접속단자 사용

○ PC의 기본 입력장치인 키보드와 마우스를 연결하는 전용포트를 만들어 마우스가 사용하던 직렬포트(serial port)를 다른 주변장치들이 사용할 수 있도록 제공

○ PS/2 포트는 입력장치와의 통신을 위해 0 Volt를 논리값 0으로, +5 Volt를 논리값 1로 하여 신호전송에 사용하고, 장치제어를 위해 PC내부에 인텔 8042(i8042) 키보드 컨트롤러 사용



【PS/2 주변장치의 정보 전송】

나. USB 방식

○ USB 포트는 PC 관련업체들*이 참여한 USB-IF(USB Implementers Forum)에 의하여 현재 2.0 버전까지 설계되었으며, 4개의 핀을 갖는 접속단자 사용

* 미국 Apple, HP, Microsoft, Intel 및 일본 NEC 등

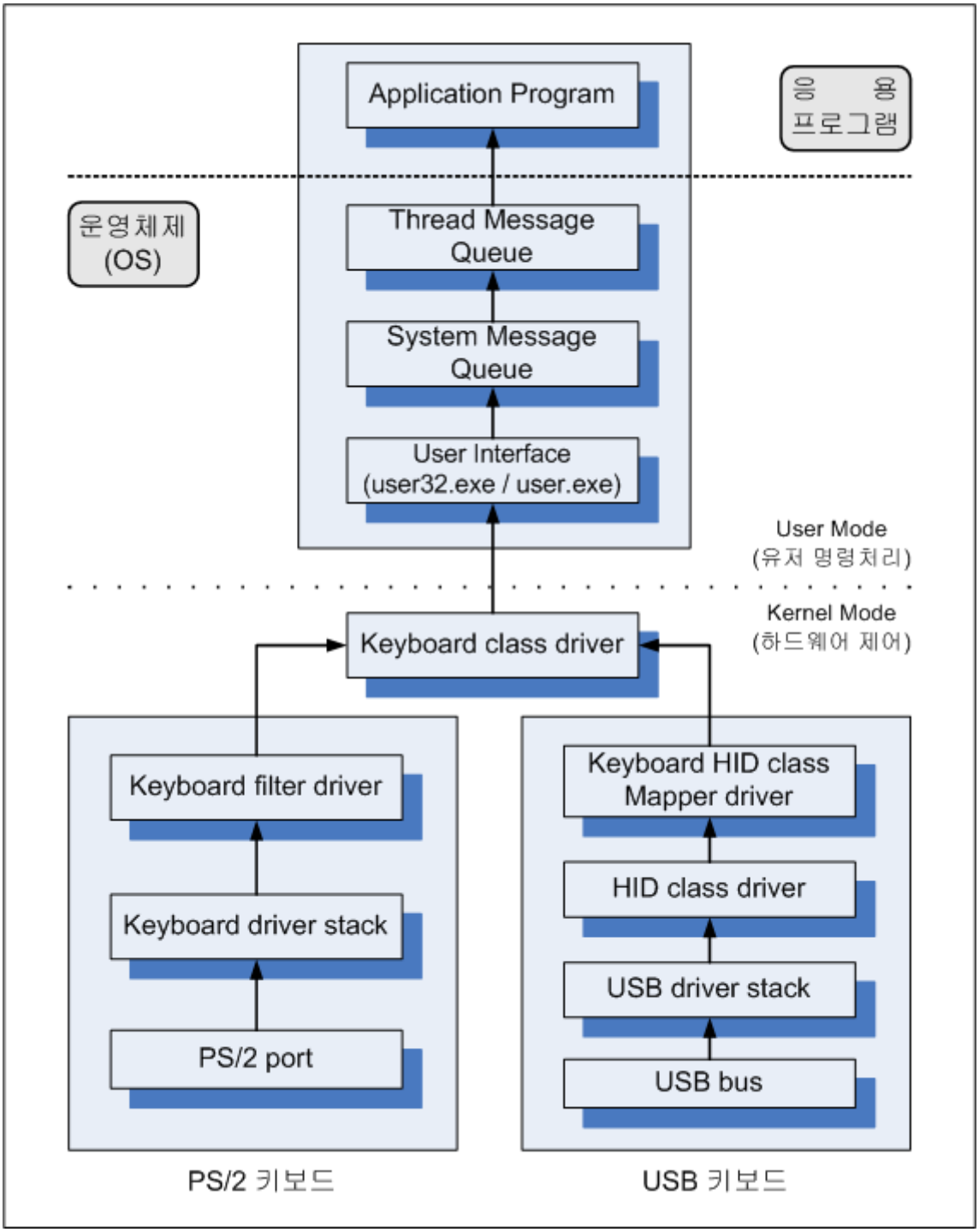
○ Plug and Play(PnP) 기능강화 및 PC 확장슬롯을 활용한 기능추가 방법의 불편함*을 개선하기 위하여 USB 접속방식을 설계·구현

* PC 내부의 확장슬롯에 그래픽·사운드 카드 등을 직접 설치해야 하므로 부주의에 의한 기기손상 및 시행상의 어려움 상존

○ USB 포트는 입력장치와의 통신을 위하여 신호선 2개(D+와 D-)를 사용하여 패킷 단위로 정보를 전송하고, 장치제어를 위하여 PC 내부에 USB 호스트 컨트롤러 사용

- USB 트랜잭션은 TCP/IP 프로토콜처럼 몇 개의 계층으로 나뉘어 있으며, 최상위 계층에서 USB 호스트 컨트롤러와 주변장치 사이에 송·수신되는 여러 패킷으로 구성됨

2. 정보전송 흐름도



* HID(Human Interface Device) : 키보드·마우스 등 사용자의 입력값을 받아주는 주변장치

3. 키입력 세부 처리절차

가. PS/2 키보드 입력처리

순 서	위 치	기 능
1	PS/2 Port	PS/2 방식 키보드로부터 키보드 입력값 접수
2	K/B driver stack	키보드 입력값 임시저장(버퍼)
3	K/B filter driver	키보드 입력값 필터링(선택사항)
4	K/B class driver	키보드 입력값의 메시지 변환 및 분기
5	User Interface	키 배열설정에 따라 가상키 값으로 번역
6	System Message Queue	윈도 메시지* 처리과정 * 키입력 등 event를 알리기 위한 전달값
7	Thread Message Queue	
8	Application Programs	최종적으로 키보드 입력값 접수

나. USB 키보드 입력처리

순 서	위 치	기 능
1	USB bus	USB 방식 키보드로부터 키보드 입력값 접수
2	USB driver stack	USB 장치 입력값 임시저장(버퍼)
3	HID class driver	입력장치(키보드/마우스) 제어
4	K/B mapper driver	PS/2 키보드 입력값으로 번역
5	K/B class driver	키보드 입력값의 메시지 변환 및 분기
6	User Interface	키 배열설정에 따라 가상키 값으로 번역
7	System Message Queue	윈도 메시지* 처리과정 * 키입력 등 event를 알리기 위한 전달값
8	Thread Message Queue	
9	Application Programs	최종적으로 키보드 입력값 접수

Ⅲ. 키보드 해킹 기술 및 위협 분석

1. 키보드 인터럽트 하이재킹

가. 기술분석

○ 키로거(KeyLogger) 프로그램이 키보드 입력시 발생하는 인터럽트를 가장 먼저 감지한 후 키보드 버퍼에서 키입력 정보를 빼내는 방식

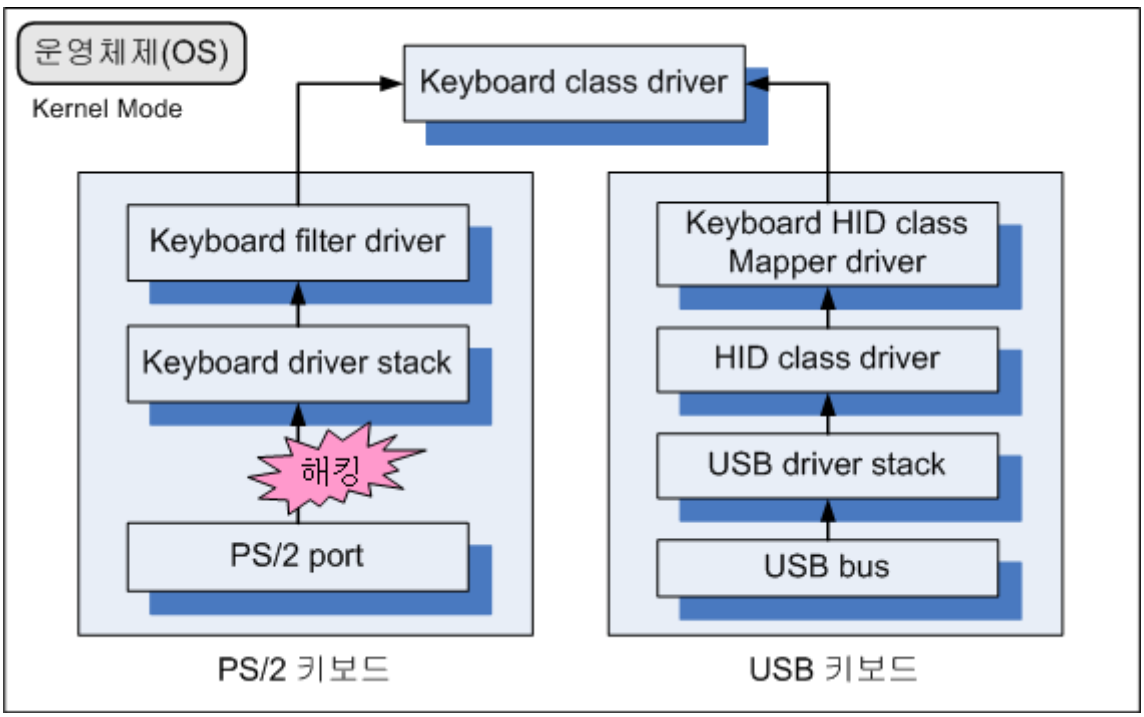
○ 일반적 PC는 키보드 컨트롤을 위하여 IRQ(Interrupt ReQuest) 1번 채널을 사용하며, 인터럽트 발생 즉시 키보드 인터럽트 핸들러(keyboard interrupt handler)가 호출되어 입력된 키의 스캔코드(scancode)* 및 상태정보 획득

* 키보드에 있는 각각의 키에 부여된 고유번호

나. 위협분석

○ 현재까지 발견된 사례는 없으나, 잠재적 위협요소로 간주

- 인터럽트 가로채기를 위하여 운영체제의 커널 해킹이 요구되지만, 윈도는 소스가 비공개인 상용 OS이므로 기술적 어려움 존재



2. 키보드 드라이버 해킹

가. 기술분석

○ 해킹용 키보드 드라이버를 개발해 키보드 입력값 처리를 담당하는 기존 키보드 드라이버를 대체하거나, 기존 키보드 드라이버보다 앞서서 수행되도록 실행순위 조정

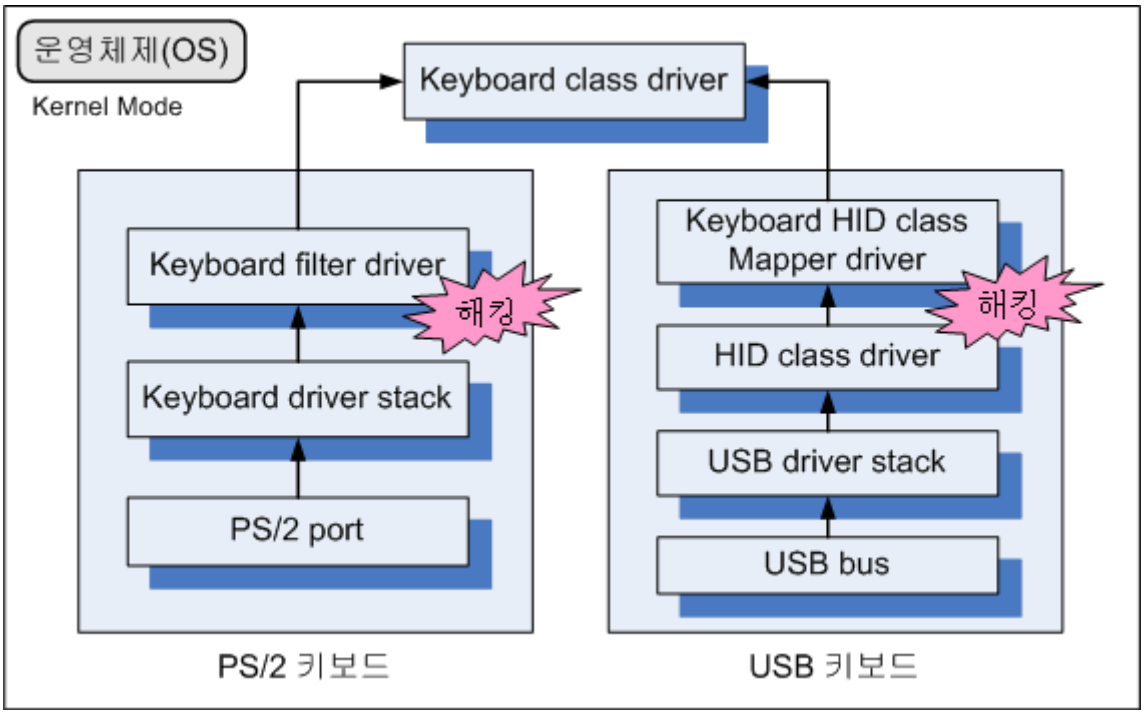
○ 이후 해킹용 키보드 드라이버는 정상적인 키보드 드라이버에 앞서 키 입력값 처리를 수행하면서 키보드 입력값 정보를 빼돌리는 방식

나. 위협분석

○ SC KeyLog, GhostKeyLogger 등 상용 키로거 프로그램이 대표적 예

○ 운영체제와 독립된 별도 보안 키보드 드라이버 방식*을 이용하는 현재의 키보드 보안 솔루션에 의해 차단 가능

* 다른 키보드 드라이버가 존재할 경우 이를 감지하고 실행순서를 조정하여 키보드 보안 솔루션이 먼저 수행되도록 함



3. DLL Injection 해킹

가. 기술분석

○ 키보드 입력값을 처리하는 실행코드(DLL* 코드)의 메모리 영역에 키보드 입력값을 빼내는 해킹코드를 기록한 후 실행시키는 방법

* Dynamic Link Library의 약자로, 특정 기능을 담당하는 프로그램이며 보조기억장치에 기록되고 필요시 읽어들여 실행함으로써 메모리 활용 및 기능확장이 용이하도록 함

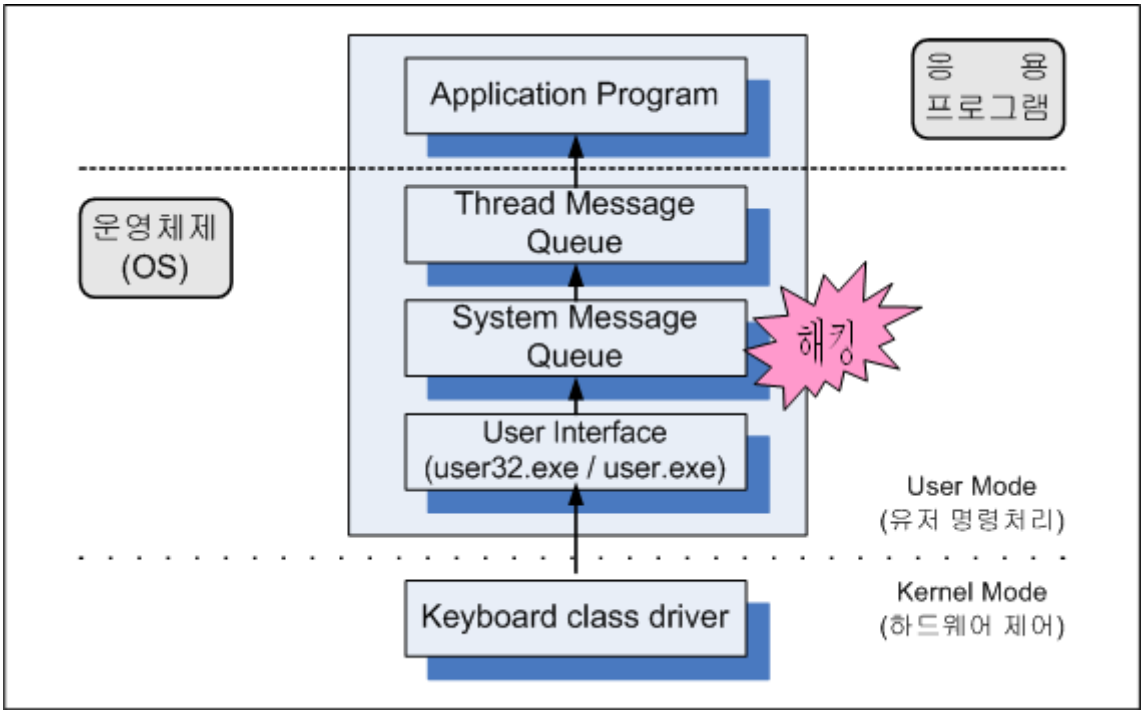
○ 해킹코드는 원래 호출되는 함수의 시작번지를 해킹코드가 위치한 주소로 바꿈으로써 실행되도록 조작

나. 위협분석

○ NetBus, NetDevil*, KGB KeyLogger 등 백도어 해킹 프로그램을 포함하여 대부분의 키로거 프로그램에서 사용되는 일반적인 방식

* 모 은행 인터넷뱅킹 불법 예금인출사고시 사용된 키보드 해킹 프로그램

○ 운영체제와 독립적인 키입력 처리경로를 갖고 있거나, 키보드 입력값을 암호화하여 전달하는 현재의 키보드 보안 솔루션에 의해 차단 가능



4. 메모리 저장값 유출

가. 기술분석

○ 컴퓨터 메모리 내부에 복호화된 키보드 입력값을 가로채는 방식

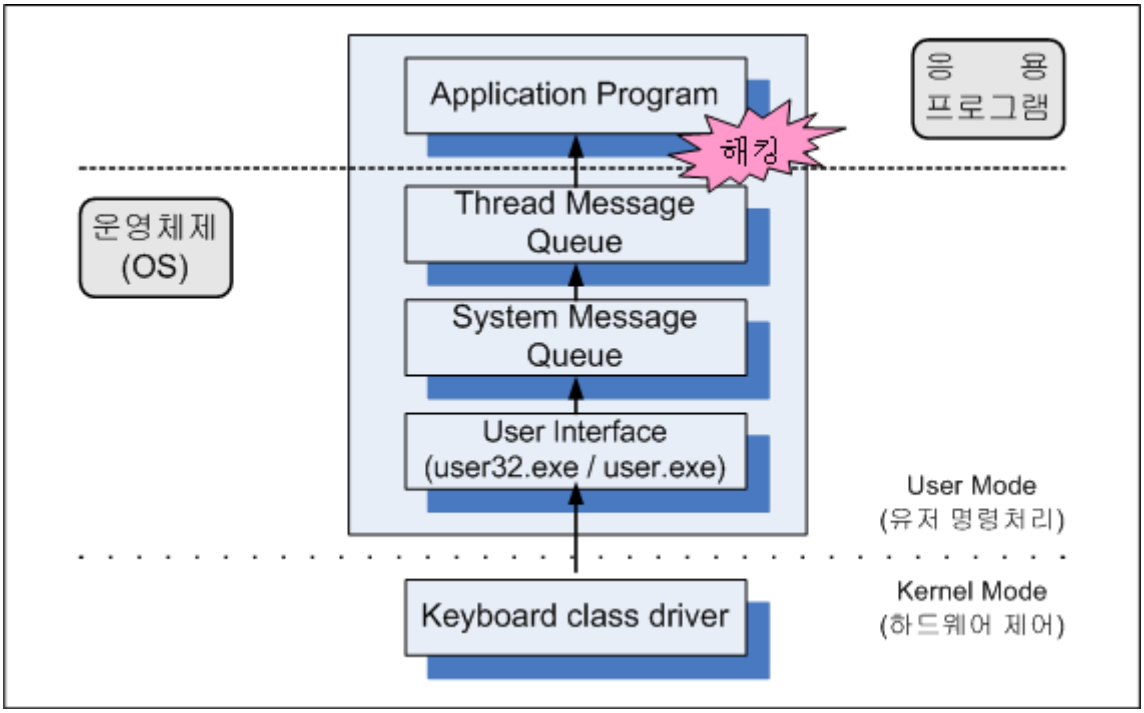
동 작 유 형	해당 키로거
인터넷 익스플로러의 BHO(Browser Helper Object)* 기능을 이용한 게임사이트 **ID 해킹**	IcyFox
윈도 OS의 메시지 처리 원리를 이용한 **비밀번호 해킹**	Personal Inspector
메모리 덤프(Memory Dump) 기술을 이용한 메모리 주소의 **데이터 취득 및 조작**	-

* 인터넷 익스플로러 제어 및 사용자 환경설정을 지원하기 위한 DLL

나. 위협분석

○ 최근 나타난 유형으로, ID·Password 등 키입력값을 복호화한 후 화면에 표시하거나 메모리에 임시 저장하지 않도록 관련 프로그램의 개발 필요

○ 해킹 프로그램이 무의미한 데이터를 가져가도록 속이거나, 아예 메모리에 접근하지 못하도록 함으로써 보호가능



Ⅳ. 키보드 보안솔루션 기술분석

1. 대상 범위 및 자료

가. 대상 범위

○ 현재 국내은행의 인터넷뱅킹 환경에서 키보드 보안솔루션으로 적용 중인 아래 4개 솔루션을 대상으로 기술분석

솔 루 션 명	제 작 사	비 고
nProtect KeyCrypt*	잉카인터넷	- 8개행 적용
Secure KeyStroke	소프트캠프	- 8개행 적용
K-Defense	킹스정보통신	- 1개행 적용(국민)
MyKeyDefense	안철수연구소	- 1개행 적용(SC제일은행)

* 현재 금융결제원에 도입·적용된 솔루션

○ 해당 키보드 보안 솔루션의 단독 기능을 대상으로 하여 분석하였으며, 동일 회사의 타 제품(PC 보안솔루션 등)과 함께 사용되는 경우 추가될 수 있는 기능 등은 분석 범위에서 제외

나. 분석 자료

○ 공신력 있는 자료를 근거로 하기 위해 특허청에 등록된 해당 솔루션의 최초 특허출원자료를 바탕으로 분석하였으며,

○ 특허출원자료에 기술되지 않은 추가 기능 등은 2005년 7월 금융결제원의 키보드 보안솔루션 도입시 제작사가 작성·제출한 기술제안서를 참고

2. 솔루션별 기술분석

가. nProtect KeyCrypt

1) 주요 대응기술

○ 사용자의 키보드 입력값의 자리수 노출방지

- 기존 시스템 메시지 대기열(System Message Queue)에는 NULL값(아무 입력이 없음을 의미)을 제공하여 어떠한 키입력도 감지할 수 없도록 설계
- 보안 키보드 드라이버와 응용 프로그램과 연결된 보안 입력창 제어부 간의 직접 통신을 통해 화면에 "*" 등의 특수문자를 표시함으로써 사용자에게 키입력 여부 표시

○ 해킹 성공시에도 원래 입력값 노출방지

- 보안 키보드 드라이버는 128bit AES* 암호화 알고리즘을 적용하여 키보드 입력값을 암호화하고,

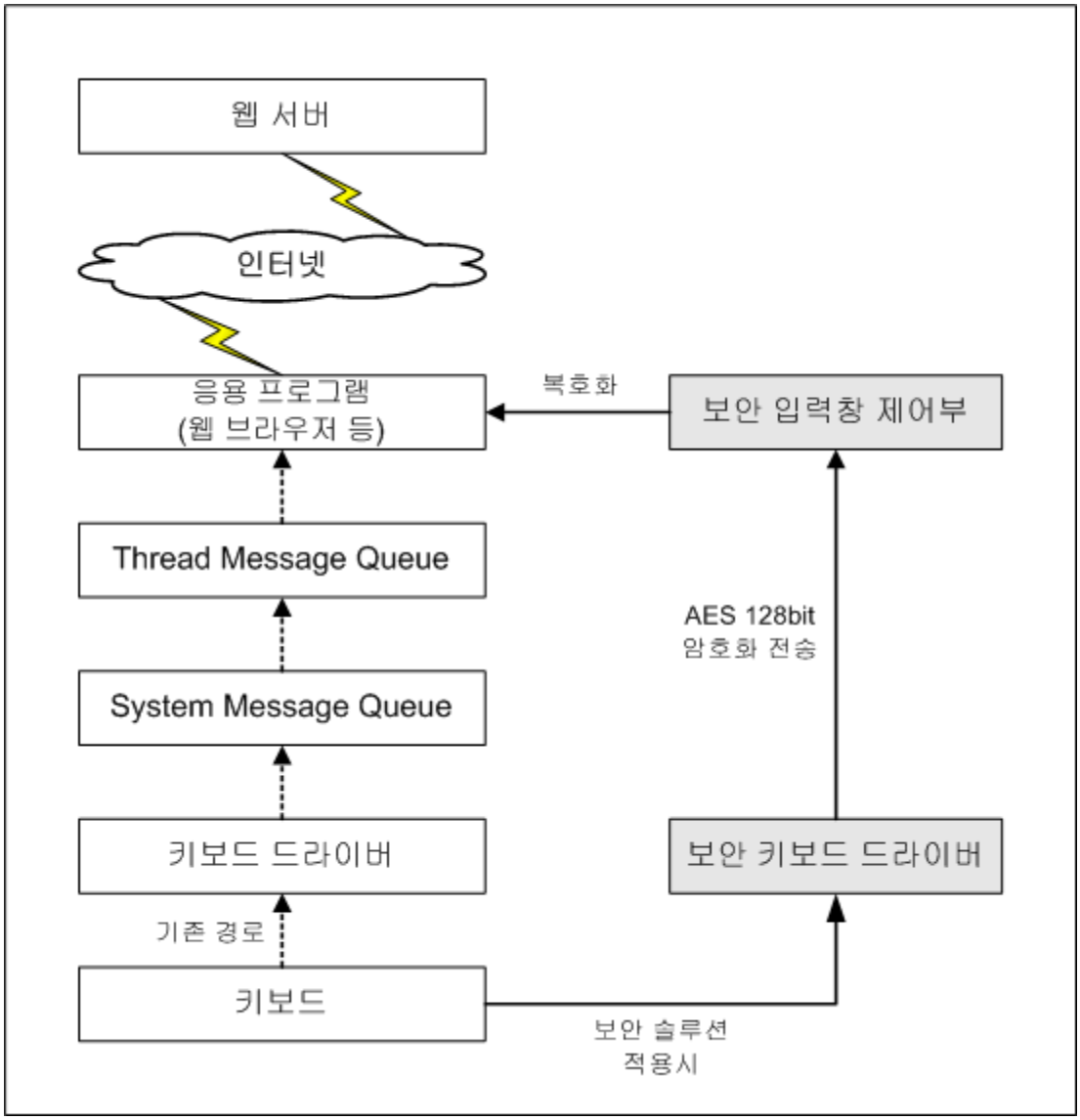
  * Advanced Encryption Standard의 약자로서, 구 표준인 DES(Data Encryption Standard)를 대체하여 美 기술표준원(NIST)이 신규 지정한 차세대 암호화 알고리즘

- 암호화된 입력값을 직접 보안 입력창 제어부로 전송하여 웹 브라우저 등 응용 프로그램에 전달

○ 프로그램 실행시 안정성 강화

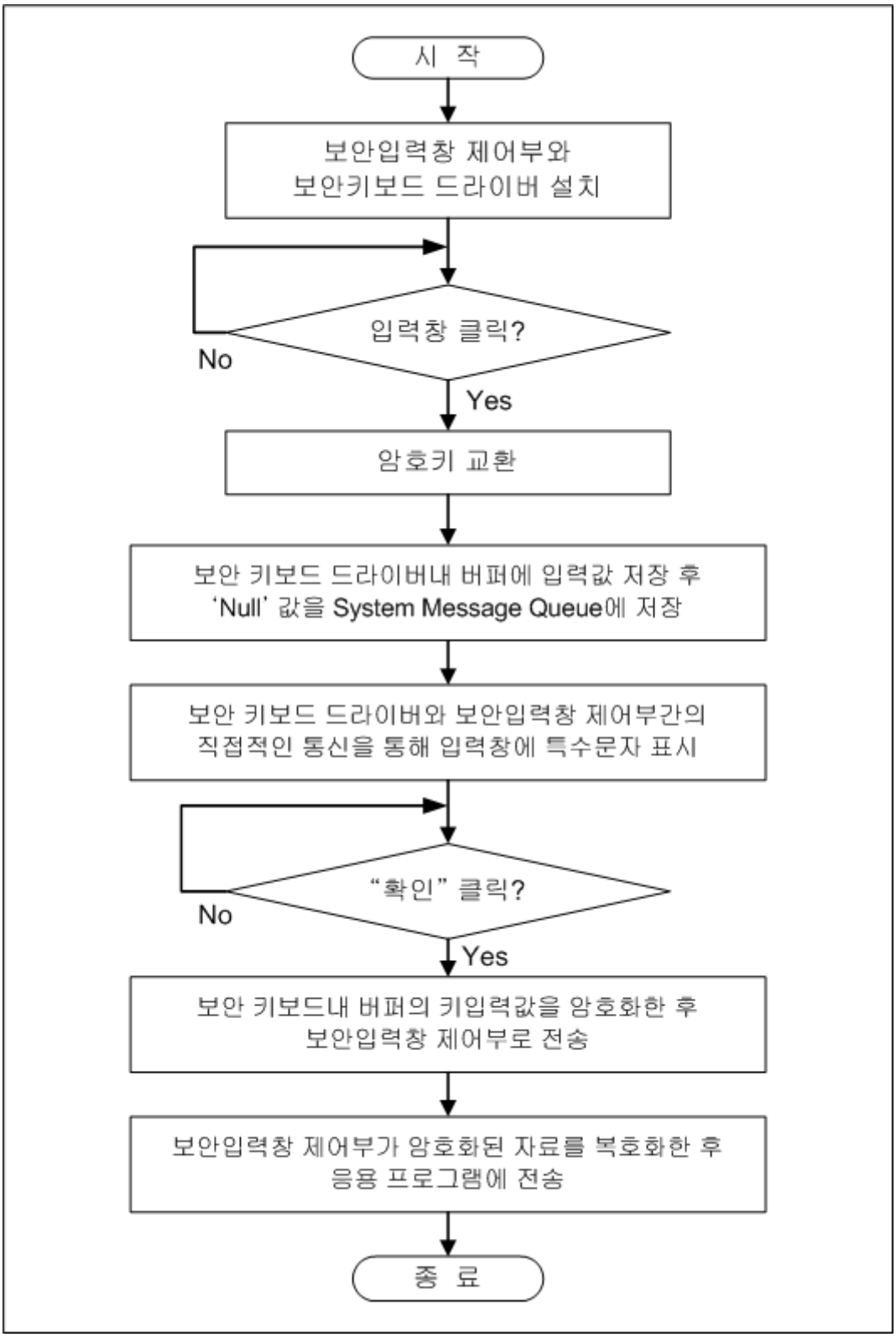
- 키보드 보안솔루션이 적용되는 입력창이 선택된 경우만 보안 키보드 드라이버가 실행되도록 설계
- 그 밖의 경우 즉시 보안 키보드 드라이버의 수행을 중단시키고, 기존 키보드 드라이버를 수행시키는 등 타 보안 프로그램(해킹도구 포함)과의 충돌을 방지하여 보안솔루션 실행시 안정성 강화

2) 입력정보 처리절차



* '기존 경로'의 키보드 드라이버로는 NULL 값을 전송하여 상위 계층에서 해킹도구가 동작하더라도 키보드 입력값을 얻지 못하도록 함

* 보안 키보드 드라이버는 키입력이 있을 때마다 '*' 표시가 나타나도록 보안입력창에 지시하고, 확인 버튼이 눌러지면 버퍼에 저장된 입력값을 암호화하여 보안입력창 제어부로 전송


시 작
보안입력창 제어부와
보안키보드 드라이버 설치
입력창 클릭?
No
Yes
암호키 교환
보안 키보드 드라이버내 버퍼에 입력값 저장 후
'Null' 값을 System Message Queue에 저장
보안 키보드 드라이버와 보안입력창 제어부간의
직접적인 통신을 통해 입력창에 특수문자 표시
"확인" 클릭?
No
Yes
보안 키보드내 버퍼의 키입력값을 암호화한 후
보안입력창 제어부로 전송
보안입력창 제어부가 암호화된 자료를 복호화한 후
응용 프로그램에 전송
종 료

나. Secure KeyStroke

1) 주요 대응기술

○ 매번 다른 암호키로 입력값 암호화

- 사용자가 입력창을 선택할 때마다 서로 다른 키테이블을 생성하고 보안 키보드 드라이버를 설치하도록 설계
- 다른 창이 선택되면 보안 키보드 드라이버를 자동으로 제거하여 다른 프로그램(타 보안 프로그램 등)과의 충돌 방지

○ 해킹 성공시에도 원래 입력값 노출방지

- 보안 키보드 드라이버는 미국 암호화 알고리즘 표준인 AES 또는 국내 개발된 SEED 암호화 알고리즘을 사용하여 입력값을 보호하도록 설계
- 사용되는 암호화 키의 크기는 128bit이고, 입력창 제어부가 암호화된 입력값을 키테이블에 따라 복호화한 후 웹 브라우저로 전송

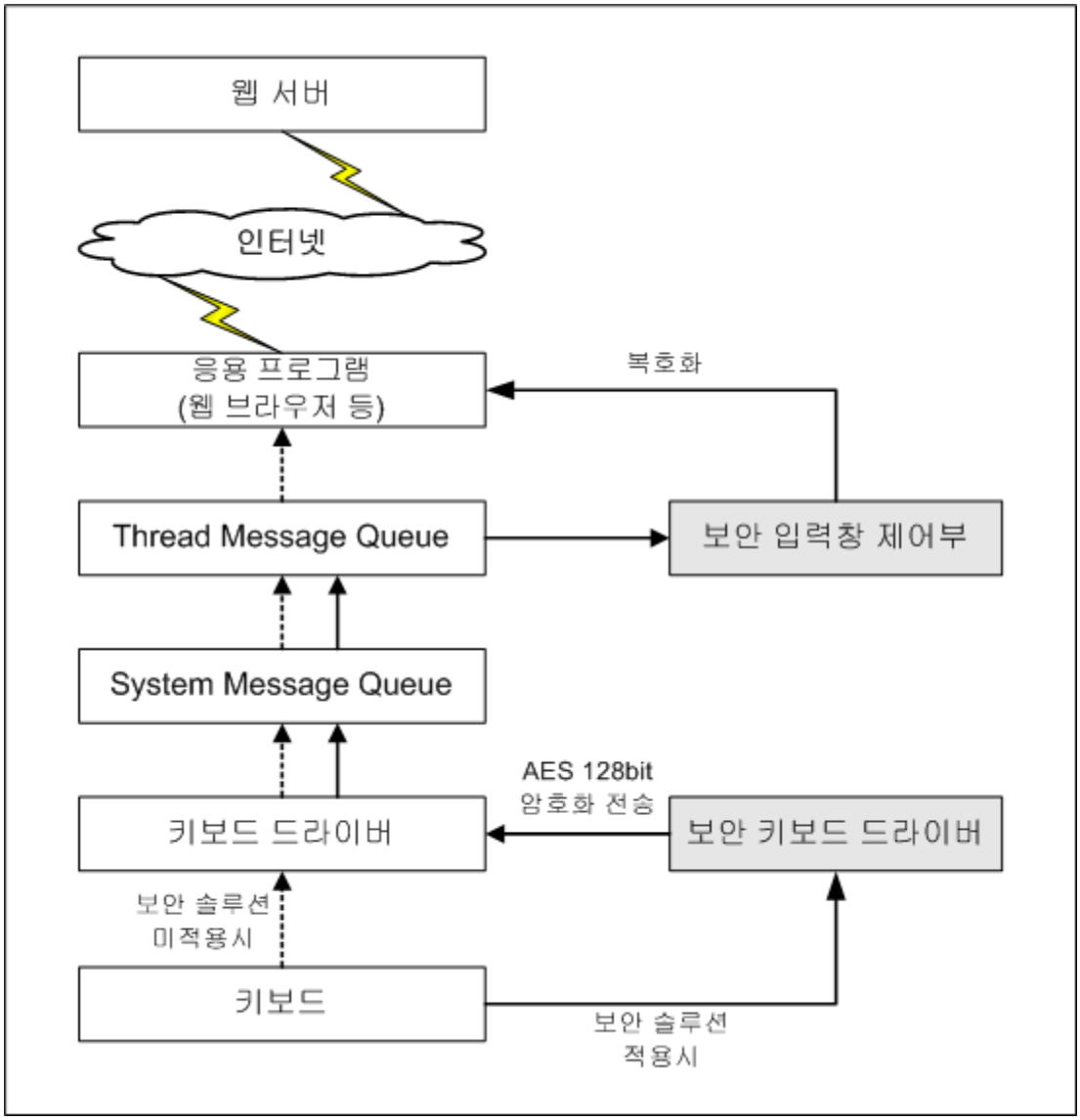
○ 디버깅 및 변조 방지

- 키보드 보안 프로그램을 구성하는 프로그램 파일들을 암호화함으로써 이들 파일의 분석을 통한 우회 및 무력화 공격을 사전 방지토록 개발

○ 프로세스 종료 방지

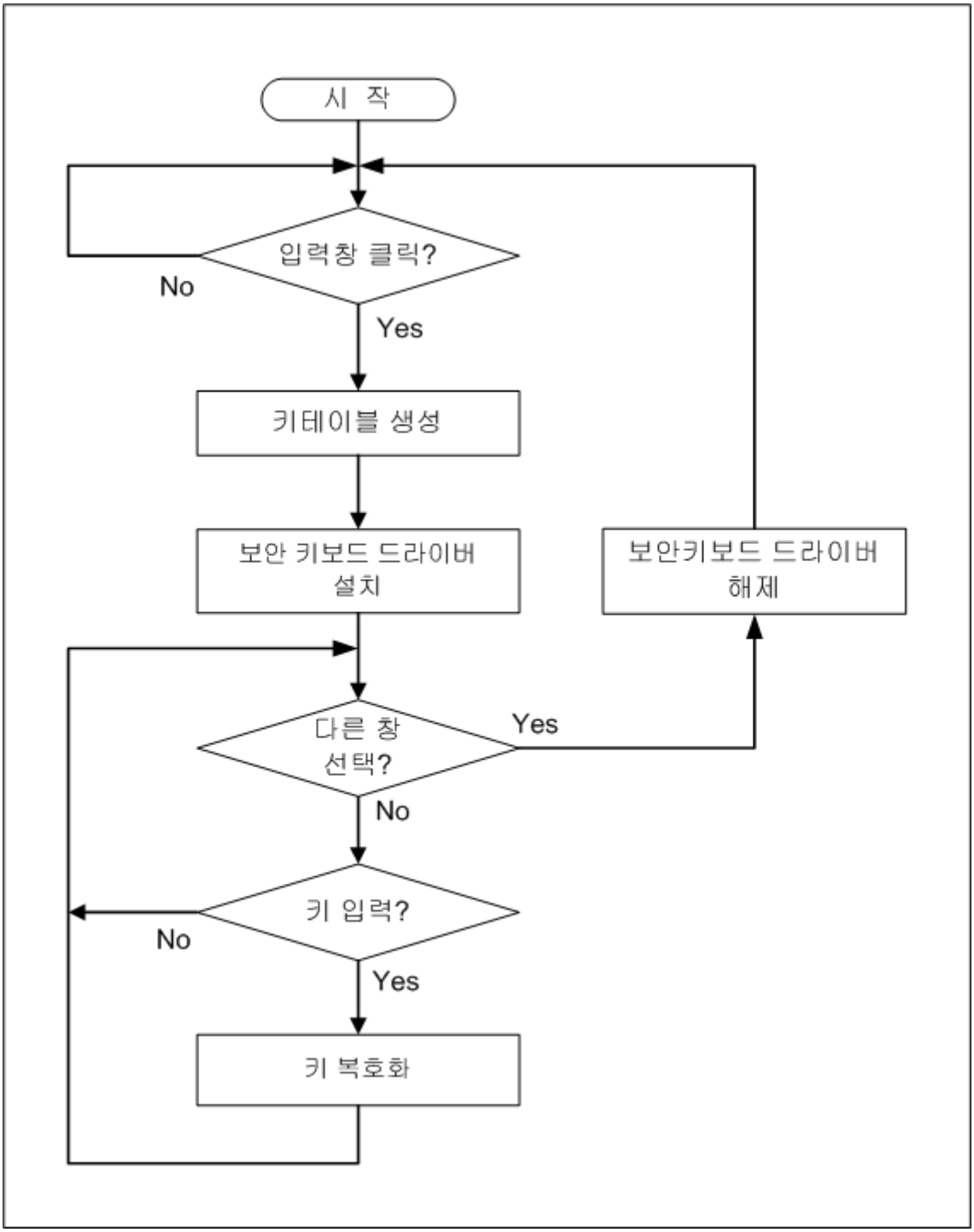
- 별도의 프로그램이 아닌 ActiveX 형태로 브라우저와 함께 동작하여 프로세스 목록에 나타나지 않으므로 실수에 의한 실행종료 방지

2) 입력정보 처리절차



* '보안 솔루션 미적용시' 의 처리절차를 따르되, 입력값의 입구와 출구에 해당하는 보안 키보드 드라이버와 보안 입력창 제어부를 통하여 키보드 입력값이 응용 프로그램에 전달되도록 함

* 보안 입력창 제어부는 타 프로그램(해킹 프로그램 등)의 키보드 입력값 접근 차단


시 작
입력창 클릭?
No
Yes
키테이블 생성
보안 키보드 드라이버 설치
보안키보드 드라이버 해제
다른 창 선택?
Yes
No
키 입력?
No
Yes
키 복호화

다. K-Defense

1) 주요 대응기술

○ 처리절차상 최하위 레벨에서 해킹차단

- 키보드 하드웨어 인터럽트를 처리하는 기존 루틴을 대신해 보안 입력 인터럽트 서비스 루틴을 실행하여 최하위 레벨에서 보호기능 수행토록 설계
- 최하위 레벨에서 해킹을 차단하므로 신규 운영체제 및 하드웨어 변경 외에는 해킹 프로그램의 패턴정보 등 정기적인 업데이트 불필요

○ 디버깅 및 변조 방지

- 키보드 보안 프로그램을 구성하는 프로그램 파일들을 암호화함으로써 이들 파일의 분석을 통한 우회 및 무력화 공격을 사전 방지

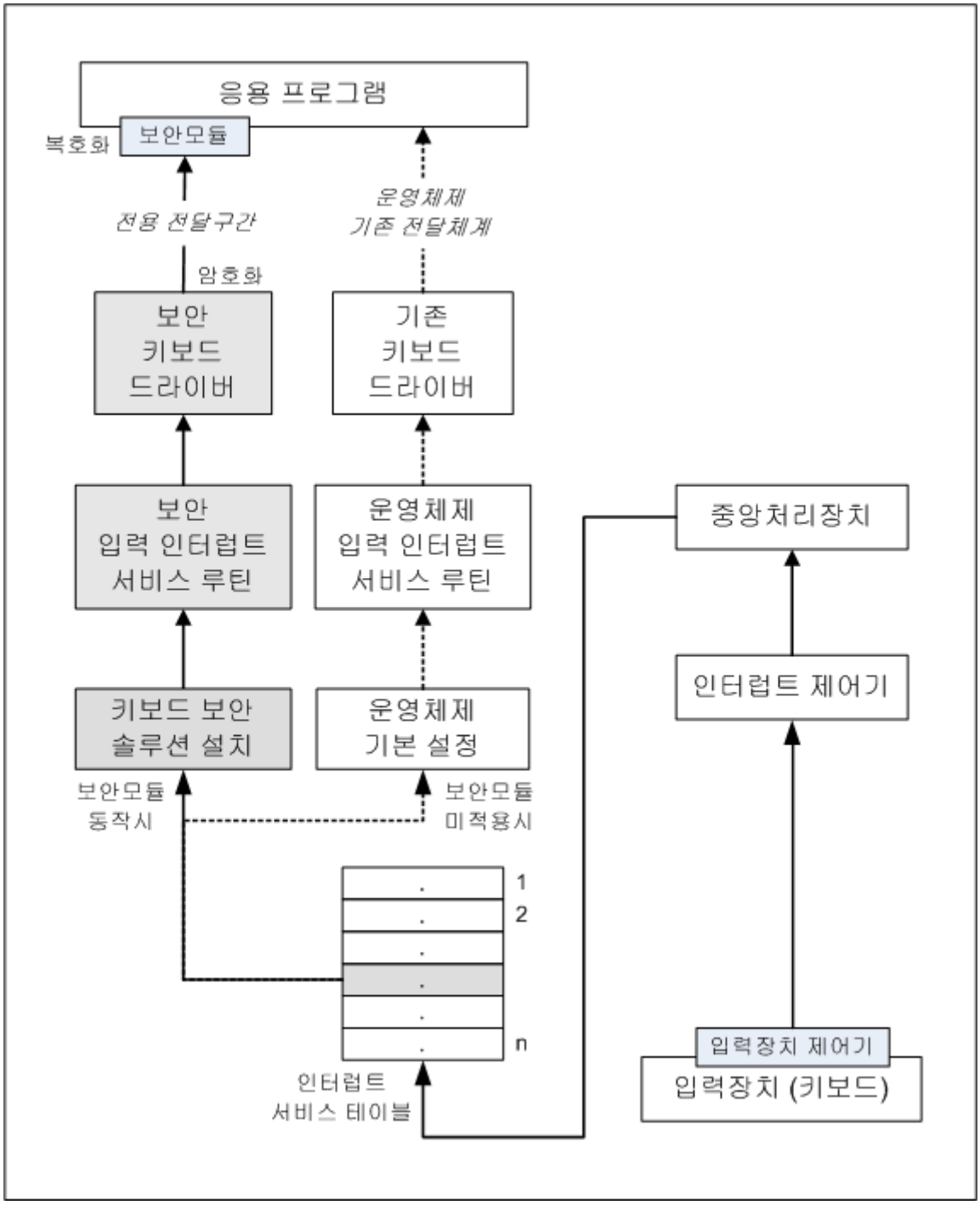
○ 키보드 입력값 암호화 및 전용 전달경로 활용

- 보안 키보드 드라이버는 미국 표준 128bit AES 암호화 알고리즘을 적용하여 키보드 입력값을 암호화하도록 설계
- 또한, 전용채널을 통해 보안모듈로 전달하고, 보안모듈이 복호화한 후 응용프로그램에 최종 전달

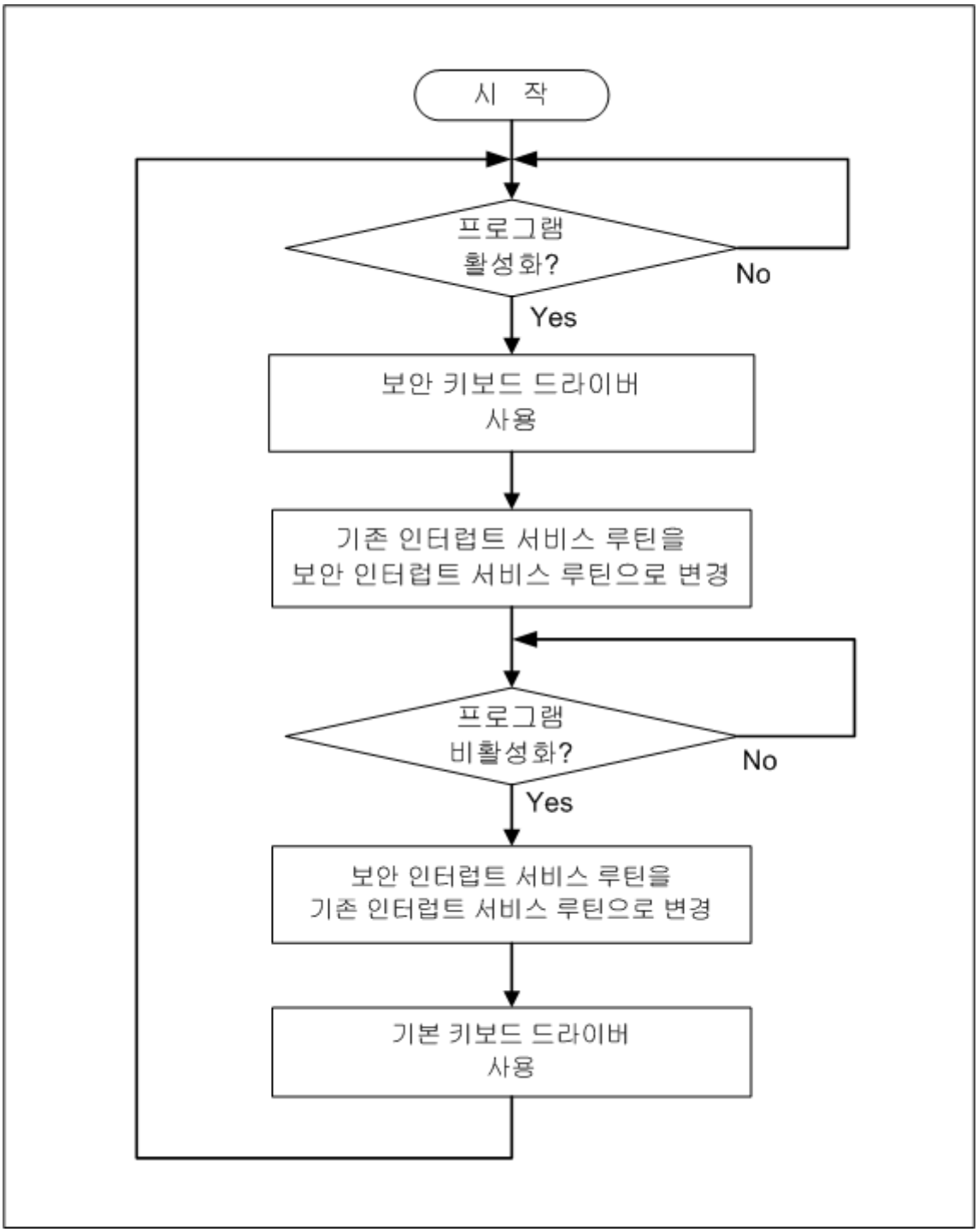
○ 강제 실행종료 방지

- 프로그램의 강제실행종료를 방지하여 키보드 입력값 보호가 중단되지 않도록 예방

2) 입력정보 처리절차



* 키보드 보안 솔루션이 실행되면 키보드 입력 발생시 보안 시스템이 호출되도록 인터럽트 서비스 테이블 수정


시 작
프로그램 활성화?
No
Yes
보안 키보드 드라이버 사용
기존 인터럽트 서비스 루틴을 보안 인터럽트 서비스 루틴으로 변경
프로그램 비활성화?
No
Yes
보안 인터럽트 서비스 루틴을 기존 인터럽트 서비스 루틴으로 변경
기본 키보드 드라이버 사용

라. MyKeyDefense

1) 주요 대응기술

○ 키로거 존재 여부 확인

- 프로그램이 실행 및 활성화되면, 보안 키보드 드라이버 설치 등 키입력값 보호조치에 앞서 해당 PC에 키로거가 존재하는지 여부를 확인

- 키로거 존재 여부는 시스템의 장치 드라이버 수준에서 아래와 같은 사항을 조사 및 확인

  ▶ 시스템 기본 드라이버 외 타 장치 드라이버의 존재 여부
  ▶ 장치 드라이버의 시작 주소 또는 주소 테이블의 변경 여부
  ▶ USB 키보드가 사용하는 HID class의 변조 및 변경 여부

○ 가상키보드 입력방식 전환기능

- 키로거가 가동 중이라고 의심되는 경우 키보드 해킹 가능성이 있는 보안 키보드 드라이버를 설치하지 않고,

- PC화면에 가상 키보드창을 표시한 후 마우스로 해당 입력값을 직접 클릭(입력)하도록 하여 키로거의 위협에 우회적으로 대응하도록 설계

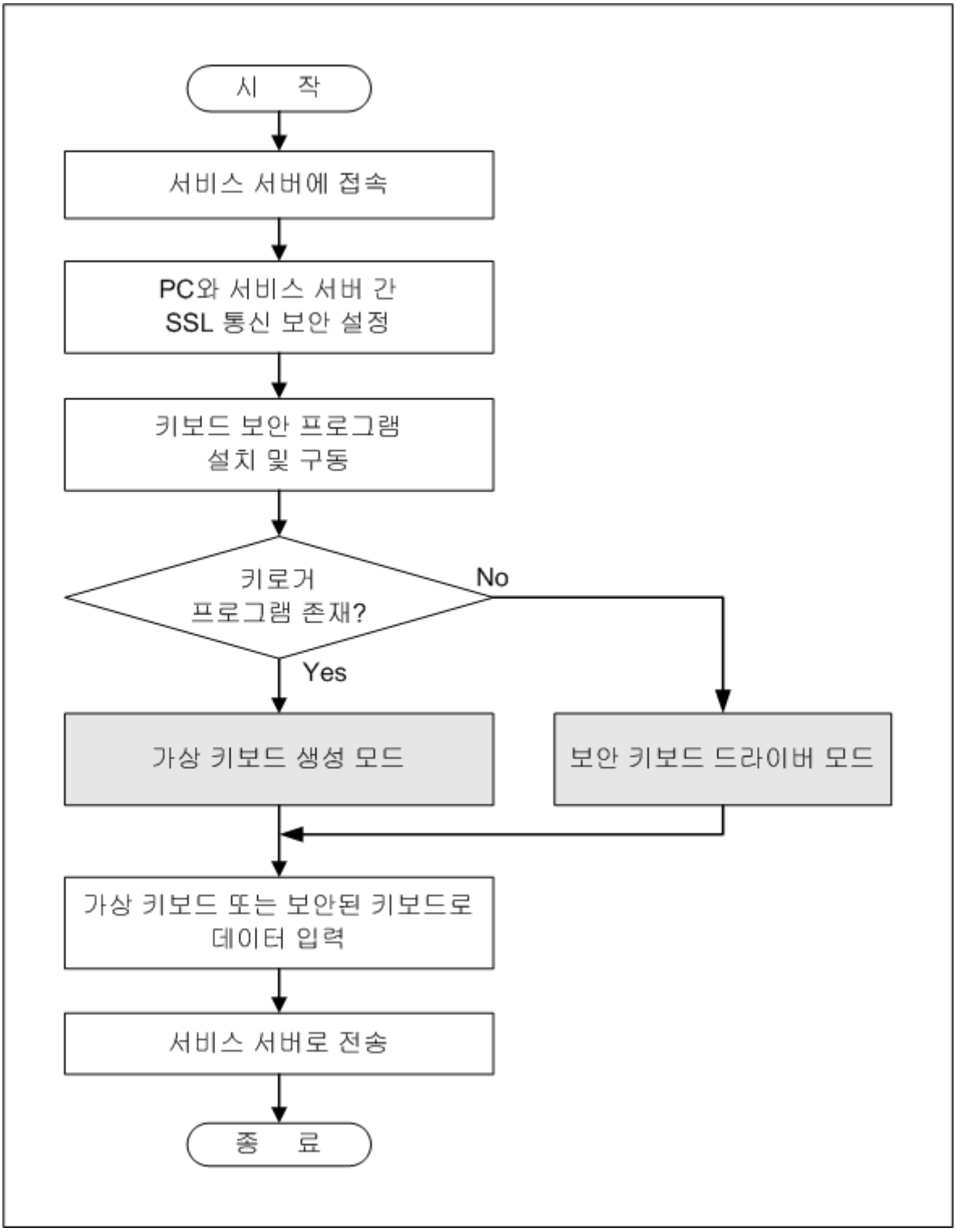
○ DHTML*을 이용한 직접적인 입력값 전달채널

- 인터넷 익스플로러의 DHTML(Dynamic HTML) 객체를 이용하여 직접 웹브라우저 또는 지정된 프로그램으로 입력값 전달

- 위와 같은 ActiveX 등 별도의 프로그램을 거치지 않는 직접 전달방식으로 인해 키보드 입력값을 암호화하지 않음

  * 웹 페이지에 각종 기능을 추가할 수 있도록 HTML, style sheet 및 JavaScript로 구성된 복합기술

2) 입력정보 처리절차


시 작
서비스 서버에 접속
PC와 서비스 서버 간
SSL 통신 보안 설정
키보드 보안 프로그램
설치 및 구동
키로거
프로그램 존재?
No
Yes
가상 키보드 생성 모드
보안 키보드 드라이버 모드
가상 키보드 또는 보안된 키보드로
데이터 입력
서비스 서버로 전송
종 료

Ⅴ. 시사점 및 향후과제

○ 국내은행의 보안솔루션 적용현황에서도 볼 수 있듯이 키보드 해킹사례가 알려진 후 모든 은행이 이에 대한 대응책 수립

○ 또한, 키입력값 보호 외에 메모리 해킹 및 스크린 덤프 공격 등 타 악성 프로그램에 의한 정보유출 등을 종합적으로 차단하기 위하여 모든 은행이 아래와 같은 기능을 갖는 PC 보안 솔루션을 동시에 구축·운영

- 개인PC 방화벽 기능 : 내·외부 접속시도 차단
- 해킹도구 진단 기능 : 정보유출 바이러스 등 악성 프로그램 탐지

○ 그러나, 현재 키보드 보안솔루션이 보호하는 구간보다 더 낮은 수준에서 발생하는 해킹시도에 대비할 수 있도록 지속적 관심 및 관련업체의 기술 개선 노력이 필요

* 윈도 운영체제 제작사인 미국 마이크로소프트사에서 키보드 보안강화를 위한 운영체제 차원의 수정 작업을 진행 중

○ 키보드 보안 솔루션의 적용방법 개선 및 안정성 개선이 필요

- 현재 적용 대상 웹페이지마다 설정작업이 요구되어 신규 또는 수정되는 웹페이지가 실수로 보호되지 않을 수 있는 불편함과 문제점을 해결하고,

- 키보드 보안 솔루션의 동작 중 보안 키보드 드라이버가 보호하지 못하는 키입력이 발생하지 않도록 실행시 안정성 및 활성·비활성화시 프로그램 전환처리 강화가 필요

【붙 임】 참가기관 보안솔루션 적용현황

(2005.11.8 현재)

은 행	키보드 보안	PC 보안	통신 암호화
경남은행	nProtect KeyCrypt	nProtect Netizen	INISAFEWeb
광주은행	Secure KeyStroke	MyFirewall	Banktown Module
국민은행	K-Defense	nProtect Netizen	XecureWeb
기업은행	nProtect KeyCrypt	nProtect Netizen	XecureWeb
농협중앙회	Secure KeyStroke	MyFirewall	INISAFEWeb
대구은행	nProtect KeyCrypt	nProtect Netizen	INISAFEWeb
부산은행	nProtect KeyCrypt	nProtect Netizen	Banktown Module
수협중앙회	Secure KeyStroke	nprotect Netizen	Banktown Module
신한은행	Secure KeyStroke	LiveCall Suite	INISAFEWeb
우리은행	Secure KeyStroke	MyFirewall	XecureWeb
전북은행	nProtect KeyCrypt	nProtect Netizen	Banktown Module
제주은행	nProtect KeyCrypt	nProtect Netizen	Banktown Module
조흥은행	Secure KeyStroke	nProtect Netizen	XecureWeb
하나은행	Secure KeyStroke	MyFirewall	INISAFEWeb
한국산업은행	nProtect KeyCrypt	nProtect Netizen	STI J/SSWEB
한국씨티은행	Secure KeyStroke	MyFirewall	XecureWeb
한국외환은행	nProtect KeyCrypt	nProtect Netizen	XecureWeb
SC제일은행	MyKeyDefense	MyFirewall	INISAFEWeb

【참고자료】

1. 소프트캠프, 특허정보(공개번호:특2002-0048313, 2002.3.7)
2. 킹스정보통신, 특허정보(공개번호:특2003-0036276, 2003.5.9)
3. 잉카인터넷, 특허정보(공개번호:10-2004-0009575, 2004.1.31)
4. 안철수연구소, 특허정보(공개번호:10-2004-0066237, 2004.7.27)
5. 강신범 外, 인터넷 뱅킹 해킹 유형과 대응 기술, 정보보호학회지, 2005. 8.
6. Writing Linux Kernel Keylogger, Phrack Vol.59, 2002.6.19