情 報 保 護 學 會 誌
第18卷 第3號, 2008. 6

키보드해킹에 대비한 새로운 영상기반 패스워드

정 태 영*, 이 경 률**, 임 강 빈***

요 약

본 논문은 기존의 패스워드 인증 시스템의 취약점 문제 및 이에 대응하여 제안된 다수의 영상 기반 인증 시스템을 소개하고, 인증 과정에서 2차원 또는 3차원 영상 내의 이동하면서도 기억하기 쉬운 다수의 화소 정보에 기반을 둔 향상된 영상 기반 전략을 소개한다. 최근 관심의 대상이 되고 있는 바와 같이, 인증 과정에서 입력되는 패스워드에 대한 감시 문제의 심각성에도 불구하고 그동안 취약한 사용자 신분증명에 대한 납득할 만한 대안이 부재하였다. 따라서 신중하게 설계된 보안 기반구조에도 불구하고 사용자 패스워드는 많은 응용에서 키보드 감시나 어깨너머로 훔쳐보기를 통하여 타인에게 쉽게 노출될 수 있다. 제안한 방안은 패스워드 인증에 문자열을 사용하지 않으므로 악의적 감시가 쉽지 않고, 소유자에게는 보다 기억하기 쉬우면서도 타인에게는 정보 노출을 최소화 할 수 있으므로 최근의 패스워드 유출 문제에 대한 훌륭한 대응책일 뿐만 아니라 키보드를 갖지 않는 휴대 장치를 위한 인증 방안으로도 활용 가능하다.

Ⅰ. 서 론

네트워크의 발전과 함께 인터넷을 이용한 상업적 행위가 일반화되었다. 초기 인터넷을 이용한 상업 거래는 특정 참여 기업에 의한 비공개적인 방법으로 이루어져 왔으나 현재는 그 참여 대상뿐만 아니라 거래 품목에서도 제한 없이 보편화되고 있다. 이는 인터넷을 이용한 거래가 신뢰를 얻고 있음을 입증하는 증거로서 앞으로는 대개의 재화 교환이 인터넷을 이용한 전자상거래 형태로 이루어질 것으로 전망된다.

전자상거래가 현재와 같이 일반인들로부터 신뢰를 얻게 된 데에는 정보보호와 관련한 많은 분야의 기술 발전뿐만 아니라 관련 업계와 상업적 거래 주체로서의 공급자와 일반 소비자들의 인식 변화 등에 커다란 공이 있었음을 부정할 수 없다.

기술적 측면에서는 많은 연구의 결과로 인터넷을 통한 전자거래의 안전성 지원을 위한 기반구조가 마련되었다[1]. 이러한 기반 구조는 안전성에 대한 기술적 검증뿐만 아니라 많은 경험과 실험을 통하여 그 실효적 안전성이 확인되고 있으며 따라서 실용 가능한 기술로 정립되고 있다. 그러나 이러한 안전한 보안 기반 구조를 확보한다 할지라도 최종적으로는 개인의 패스워드를 소유자가 보관, 관리해야 하는 것은 불가피하다. 따라서 사용자의 부주의나 해킹을 통한 패스워드의 유출은 공든 탑을 하루아침에 무용지물로 만들 수 있으므로 사용자에게는 최대한의 주의가 요구된다.

그럼에도 불구하고 대개의 일반 사용자는 패스워드 도용에 노출되어 있는 경우가 많으며 악의적인 공격 성향을 가진 실력 있는 해커에 의하여 얼마든지 패스워드가 유출될 수 있는 여지가 있다. 이러한 패스워드 유출의 가능성은 대개의 응용들이 사용자의 패스워드로서 문자열 형태를 요구하며, 문자열 형태의 패스워드를 사용자의 컴퓨터 키보드를 통하여 수집하는 방식을 고수하고 있음으로 인하여 더욱 더 증폭된다. 즉, 컴퓨터 키보드의 감시를 통하여 사용자의 패스워드를 훔쳐냄으로써 아무리 안전한 기반 구조라 할지라도 이를 무력화할 수 있는 것이다. 이러한 이유로 최근에는 키보드의 감시를 방지하기 위한 소프트웨어가 대개의 사이트에서 제공되고 있으나 현재의 컴퓨터나 운영체제의 구조적인 측면으로 볼 때 키보드 감시의 완벽한 차단은 현실적으로 불가능하다.

그 동안 상기와 같은 문제에 대응하기 위하여 다양

* 순천향대학교 (jtyworld@nate.com)
** 순천향대학교 (icon0001@nate.com)
*** 순천향대학교 (yim@sch.ac.kr)

한 연구가 진행되어 왔으며 대표적인 것으로서 사용자 인증에 키보드를 사용하지 않는 이미지 기반의 패스워드 인증방법[2] 등이 시도되고 있고 그 효율성에 대한 주장이 어느 정도는 설득력을 얻고 있다. 그러나 이러한 방법도 어깨 너머로 훔쳐보는 문제에 대하여 설득할 만한 대응책이 없어 현실적으로 그 안전성을 인정받지 못하고 있는 실정이다.

본 논문에서는 키보드 감시에 의한 패스워드 유출의 위험성을 분석하고 이에 대응하기 위한 몇 가지의 이미지 기반 패스워드 방식과 장단점을 소개하며 이들의 단점에 대하여 보다 개선된 새로운 이미지 기반 패스워드 입력 방안을 제안한다.

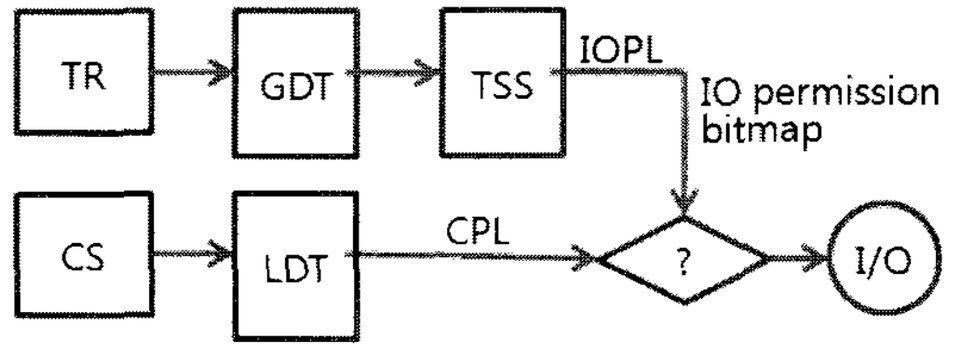
제안하는 이미지 기반 패스워드 입력 방안은 키보드의 입력을 사용하지 않음으로써 안전한 패스워드의 입력뿐만 아니라 차후 보편화될 이동성이 강조되는 무선 휴대 단말기나 원격지의 금융단말 등과 같이 키보드가 장착되지 않은 시스템에서의 직관적 패스워드 입력에도 이용이 가능하다는 점에서 효과적일 것으로 기대된다.

본 논문의 구성은 다음과 같다. 제2장에서는 문자열 기반 패스워드의 취약점 현재 사용 가능한 키보드 보안 기술에 대하여 소개하고 제3장에서는 키보드 보안이 가지고 있는 근본적인 취약점에 대하여 서술하였다. 제4장에서는 3장에서 서술한 취약점을 이용하여 구성 가능한 키보드 스니핑 프로그램의 실례를 보였으며 제5장에서 키보드 보안과 더불어 하드웨어 보안 취약점과 관련한 앞으로의 해결과제를 논하는 것으로 결론을 내린다.

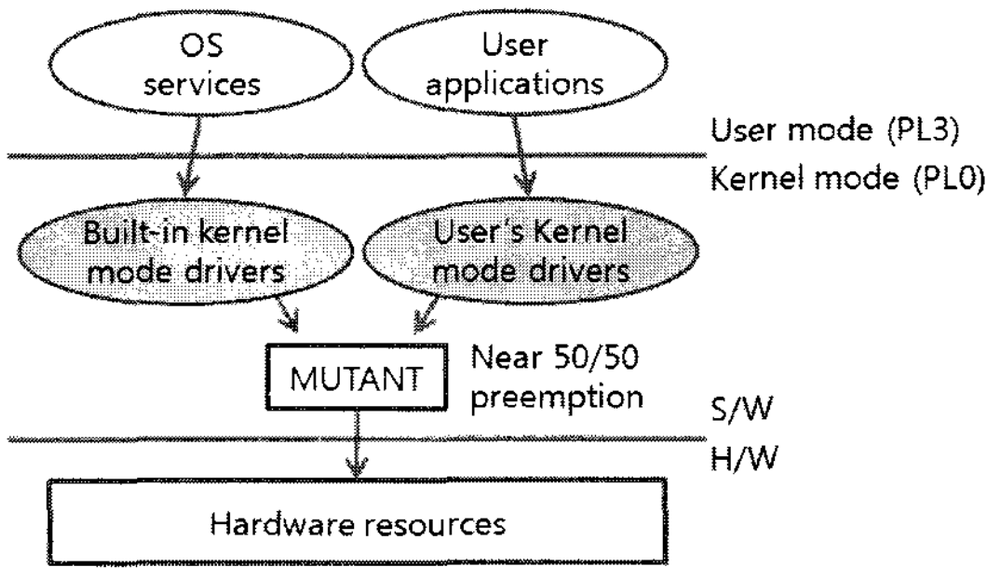
Ⅱ. 문자열 기반 패스워드 취약점 및 대응

문자열 기반 패스워드의 취약점은 인증의 주체인 소프트웨어 이외의 프로그램이 키보드로부터 입력되는 패스워드를 감시하여 그대로 탈취할 수 있다는 것이다. 이러한 가능성은 근본적으로는 운영체제의 허술한 접근관리로부터 비롯되며 이에 따라 부차적으로 하드웨어가 가지는 취약점이 사용자 프로그램에 그대로 노출된다는 점에서 기인한다.

1970년 이전, 범용 운영체제가 개발되던 초기의 하드웨어 플랫폼[3]은 그 위에서 실행되는 프로그램에 대하여 특권수준의 구별이 없었다. 다만, 이후 1970년대 후반에 몇몇의 프로세서 및 플랫폼[4,5]에서 수퍼바이저 모드와 유저 모드라는 두 실행 모드를 정의하고 각 모드에서 참조 가능한 메모리 영역을 물리적으로 분리하였으며 모드마다 서로 다른 특권수준의 접근권한 기능을 제공하였다. 이에 따라 당시의 운영체제들이 수퍼바이저 모드와 유저 모드라는 서로 다른 실행모드를 활용하여 자원에 대한 접근권한을 제공하였다. 이후 1980년대 하드웨어의 발전에 따라 다양한 프로세서에서 특권수준을 보다 세부적으로 구성함으로써 접근권한 관리 메커니즘을 강화하였다[6,7]. 그럼에도 불구하고 대개의 범용 운영체제에서는 새로운 하드웨어가 제공하는 접근권한 메커니즘을 수용하지 않은 채 기존의 수퍼바이저/유저라는 두 특권수준만을 고수하고 있다[8]. 일례로 현재의 펜티엄 프로세서는 그 전신으로 1983년 발표한 i80286 프로세서에서부터 입출력 포트에 대하여 [그림 1]과 같은 네 단계의 접근권한 관리를 하드웨어적으로 지원하며 MIPS 등의 프로세서도 커널/수퍼바이저/유저의 세 단계의 접근권한을 제공하고 있다. 그러나 [그림 2]에서 보는 바와 같이 윈도우 운영체제의 경우 사용자가 제공한 커널모드 드라이버와 기타의 커널모드 드라이버가 하드웨어 자원에 동시에 접근을 요청하는 경우 동등한 접근권한으로 서비스됨으로써 상호 동일한 기회로 접근이 보장되는데도 불구하고 커널은 사용자 드라이버의 접근에 대하여 제재하거나 감시할 만한 기구



〔그림 1〕 펜티엄 프로세서의 입출력 접근제어 모델



〔그림 2〕 운영체제에서의 하드웨어 자원에 대한 경쟁

를 가지고 있지 못하다.

현재 사용되는 키보드는 PS/2 인터페이스를 사용하는 방식과 USB 인터페이스를 사용하는 방식이 있는데 한동안은 USB 디바이스의 보편화로 인하여 키보드도 USB 방식이 많이 보급되었다. 그러나 USB 키보드의 취약성이 지적된 이후로 과거 정통부에서는 보안을 요하는 응용에 가능하면 PS/2 키보드를 이용할 것을 권고하여 왔다[9]. 더구나, 현재 생산되고 있는 노트북 컴퓨터의 키보드는 거의 모두 PS/2 인터페이스를 통하여 연결되어 있으므로 현재 노트북 컴퓨터의 보급 추세를 보면 PS/2 키보드의 보안문제는 매우 심각하다.

잘 알려진 키보드에 대한 공격과 방어는 키보드로부터 입력되는 정보를 누가 먼저 수집하는가를 경쟁하는 문제이다. 따라서 대개의 공격 방법은 방어 방안과 동일하며 그 반대도 성립하므로 그 동안 키보드와 관련한 보안프로그램과 감시프로그램 사이에서 이를 위한 경쟁이 지속되어 왔다.

키보드로부터 입력된 패스워드가 보안프로그램으로 전달되는 일련의 과정에서 감시 프로그램이 이를 탈취할 수 있는 방법은 다양하게 존재한다. 이러한 탈취 방법을 크게 나누면 운영체제의 키보드 인터럽트 처리기를 대체하는 방법과 키보드컨트롤러를 직접 제어하는 방법으로 구분할 수 있다.

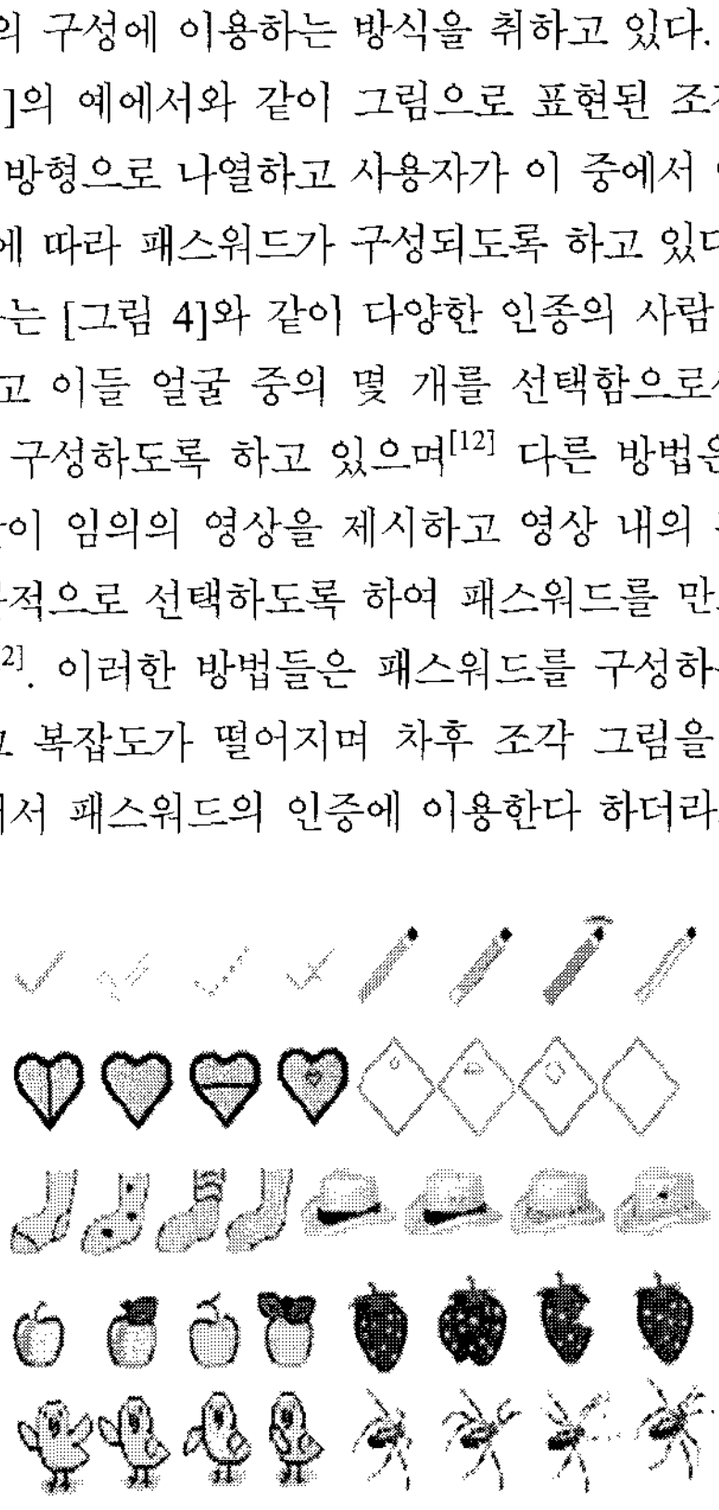
운영체제의 인터럽트 처리기를 대체하는 방법은 키보드뿐 아니라 다양한 부분에서 운영체제 커널의 서비스를 수정하거나 변경하기 위하여 사용되어 오던 고전적인 방법으로서 여기서 사용하는 대개의 기술들은 인터럽트 및 예외처리 과정에서의 매우 상식적인 선점(preemption)을 노린 경우이다. 이러한 방법들은 선점 이력에 대한 검출이 아주 용이하므로 이를 방어할 수 있는 기술들이 이미 공개되어 공유되고 있어 현 시점에서 이를 이용하여 키보드로부터의 패스워드를 탈취하는 일은 가능성이 없어 보인다.

키보드컨트롤러를 직접 제어하여 키보드 입력을 탈취하는 방법은 키보드컨트롤러의 입출력 포트에 직접 접근하는 방법으로서 방어자와 공격자가 경쟁상태(race condition)에 들어설 우려가 있으나 프로그래머가 하드웨어 제어 및 상호배제 메커니즘을 잘 활용할 경우 폴링에서 우선할 수 있다. 그러나 [그림 2]를 통하여 상기에서 서술한 바와 같이 이러한 선점은 늘 성공하는 것이 아니라 기회를 서로 공유하게 되므로 보안 프로그램이나 감시 프로그램 모두가 항상 선점할 수는 없다. 또한 이러한 선점을 위한 경쟁은 지나친 오버헤드를 유발하여 시스템이 정상적인 동작을 할 수 없을 만한 상황에 도달하게 된다. 따라서 이 방법을 보안프로그램이 사용하기는 어렵다.

보안프로그램이 감시프로그램과의 선점 경쟁을 포기하고 오히려 선점 기회를 감시프로그램에게 양보하면서도 키보드 입력을 보호할 수 있는 방법을 다양하게 고려할 수 있다. 다만 이러한 방법은 운영체제의 허술한 접근권한 관리를 통하여 키보드컨트롤러가 가지는 근본적인 취약점이 노출됨으로써 무력화되거나 그 효과가 크게 감소하는 문제가 발생한다[10] .

Ⅲ. 영상기반 패스워드

기존의 키보드를 이용한 문자열 형식의 패스워드 입력 방식이 가지는 패스워드 유출의 문제를 해결하기 위하여 이미지를 이용하여 패스워드를 입력 받는 방식이 몇 가지 소개되었다. 이들은 공통적으로 이미지 상에서의 포인트 장치의 클릭정보를 다수 입력 받아 패스워드의 구성에 이용하는 방식을 취하고 있다. 이들은 [그림 3]의 예에서와 같이 그림으로 표현된 조각난 기호를 정방형으로 나열하고 사용자가 이 중에서 여러 개 선택함에 따라 패스워드가 구성되도록 하고 있다[11]. 그 중 일부는 [그림 4]와 같이 다양한 인종의 사람 얼굴을 제시하고 이들 얼굴 중의 몇 개를 선택함으로써 패스워드를 구성하도록 하고 있으며[12] 다른 방법은 [그림 5]와 같이 임의의 영상을 제시하고 영상 내의 관심 점을 순차적으로 선택하도록 하여 패스워드를 만드는 방식이다[2]. 이러한 방법들은 패스워드를 구성하는 방식에서 그 복잡도가 떨어지며 차후 조각 그림을 복잡하게 섞어서 패스워드의 인증에 이용한다 하더라도 누구



〔그림 3〕 변종 기호를 이용한 패스워드

〔그림 4〕 얼굴 그림을 이용한 패스워드

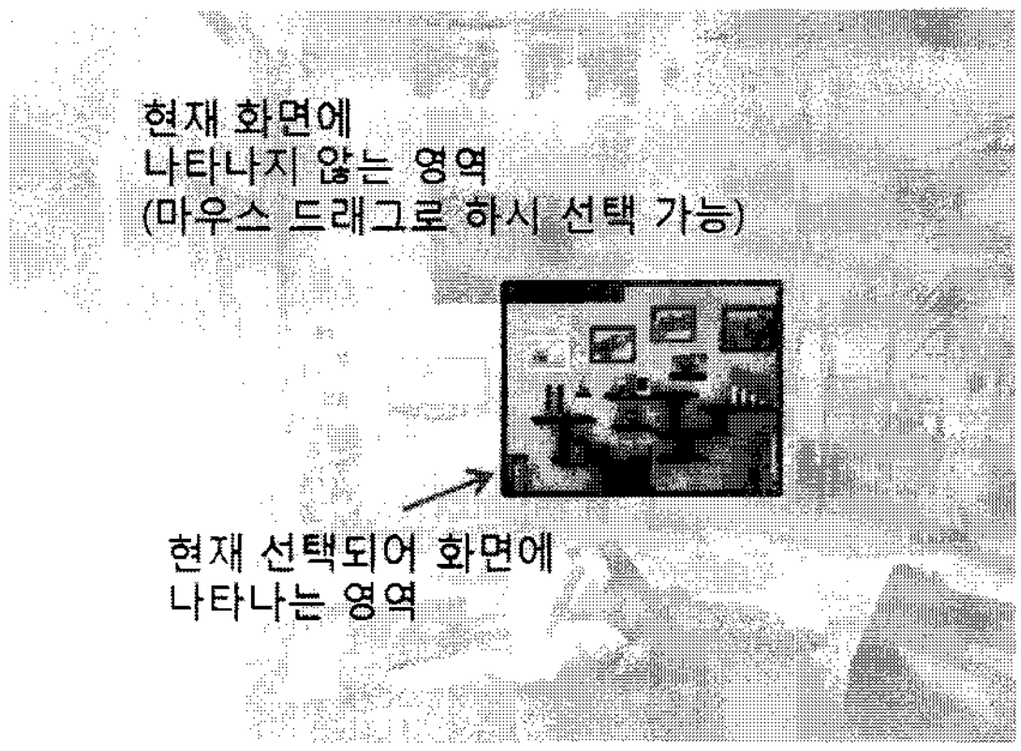
〔그림 5〕 영상 내의 관심 점을 이용한 패스워드

라도 쉽게 선택할 수 있는 형태이기 때문에 패스워드의 유출에 대하여 보다 강인한 방법이 요구된다.

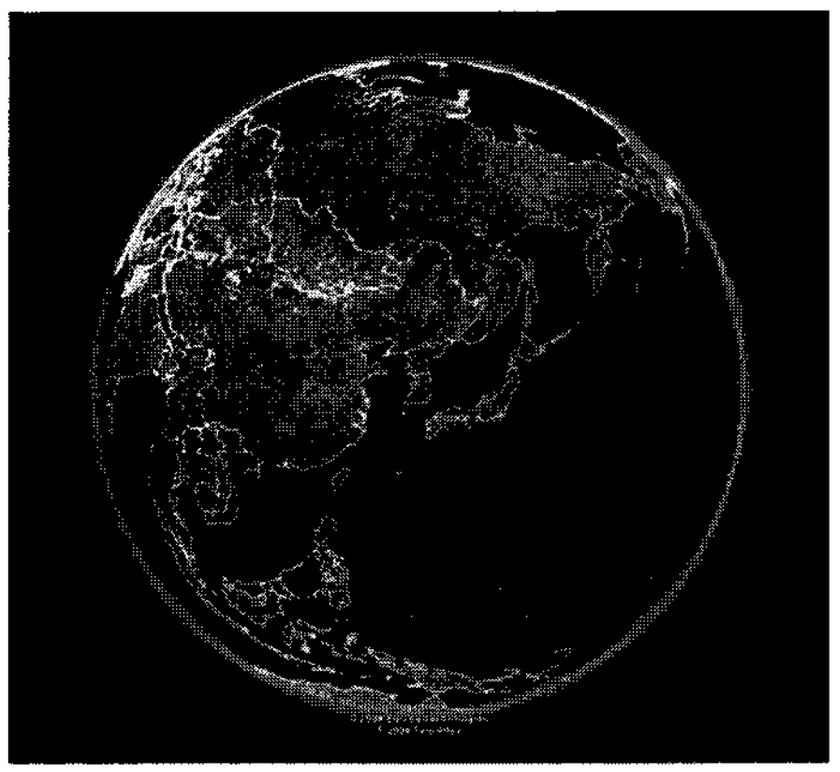
상기의 방안들이 가지는 공통적인 취약점은 각 논문에서 개선하고자 노력하고 있음에도 불구하고 제시되는 영상이 고정되어 있거나 변경되더라도 주어진 고정된 영상 집합 안에서 선택되므로 고도로 자동화된 소프트웨어를 구성하면 경험에 의한 패스워드 추출이 가능하다는 것이다. 또한 어깨너머로 패스워드를 훔쳐보는 경우에 대하여 내성이 강하지 못하다는 단점을 공통적으로 포함하고 있다.

Ⅳ. 영상기반 패스워드 시스템의 개선

본 논문에서는 영상기반 패스워드가 가지는 장점[13]을 살리면서도 기존의 방안들이 가지는 공통적인 취약점을 최소화함으로써 보다 효과적인 영상기반 패스워드 인증을 위한 방안을 제안한다.

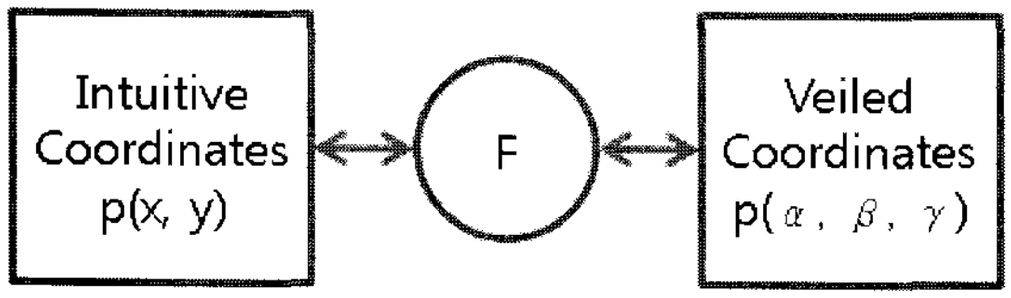


〔그림 6〕 가상공간의 임의 영역에서의 회전 및 이동이 가능한 객체를 이용



〔그림 7〕 회전 및 확대가 가능한 지형도를 이용

제안한 방안에서는 기호 기반이 아닌 비트맵 기반의 이미지를 토대로 패스워드 등록을 하고 이렇게 등록된 패스워드의 인증 시에는 이미지의 회전 및 대칭을 통하여 좌표 값을 얻는 방식을 취하고 있다. 더구나, 연산 능력이 충분한 시스템에서는 [그림 6]이나 [그림 7]에서와 같이 이미지를 3차원으로 구성할 수도 있으며 특히 [그림 6]의 경우와 같이 영상의 크기를 출력 프레임 크기보다 크게 선택하고 영상의 일부만을 출력 프레임 내에 출력되도록 하여 이외의 영역은 숨겨지도록 구성할 수 있다. 이와 같은 다양한 영상 모델 중에 하나가 선정되면 전체 또는 일부의 회전, 대칭, 이동, 확대 등을 통하여 영상을 제어하며 그 위에 기억하기 쉬운 관심 좌표 점을 선택하여 등록하며 이러한 과정을 수 회 수행함으로써 이전 좌표 점이 시야에서 사라지게 구성한다. 이렇게 함으로써 어깨너머로 훔쳐보는 경우에도 강인하면서 만일의 경우 공격자가 좌표 추측을 시도하



〔그림 8〕 좌표 값의 변환에 의한 추측의 교란

는 것에 대비함으로써 이미지 내에서의 좌표 점과 그 순서 정보에 대한 유출을 탈피할 수 있다.

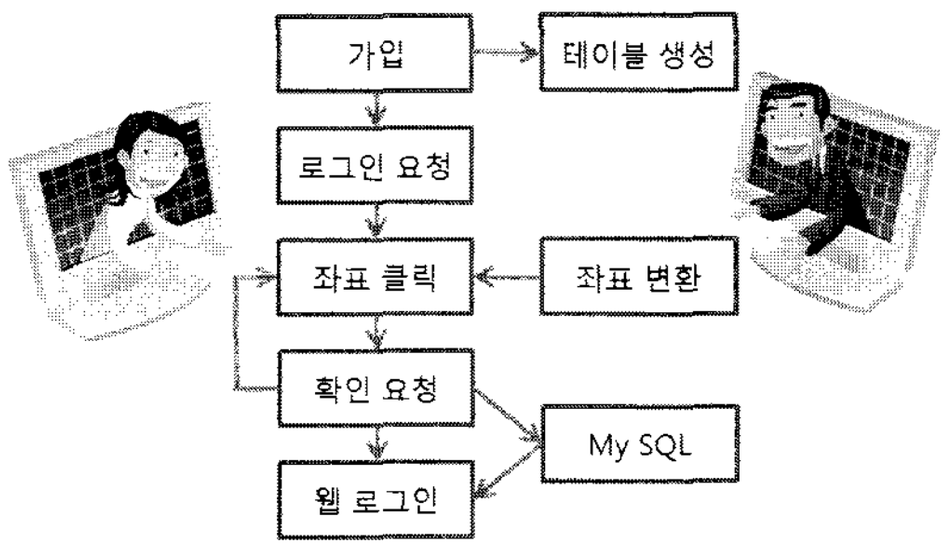
이렇게 구성된 패스워드의 경우 그 복잡도에 있어서도 문자열 형태의 패스워드에 비하여 유리하다. 문자열 형태의 패스워드가 7비트 아스키코드 8자리로 이루어진 경우를 가정하면 그 복잡도는 128×8로 계산된다. 그러나 제안한 패스워드 방식에서는 2차원 영상의 경우 이미지 크기를 270×418로 가정하면 같은 길이의 패스워드에 대하여 복잡도는 112860×8로 계산되므로 기존 문자열 형태의 패스워드에 비하여 무차별 대입 공격(brute force attack)이나 사전공격(dictionary attack)에 대하여 매우 강인하다.

특히, 3차원 영상의 경우 영상 내의 임의의 객체를 복수 개 선택하여 이를 회전, 대칭, 이동시킴으로써 새로운 영상을 만들어 낼 수 있으며 원 영상의 초기 좌표를 랜덤하게 선택하는 경우 다양한 초기 화면이 얻어질 수 있다. 또한 모든 경우에 대하여 화면 상에 표현되는 영상의 좌표는 [그림 8]과 같은 좌표변환을 통하여 이루어져 공격자의 입장에서는 3차원 좌표로부터 2차원 좌표로의 해시된 좌표만을 보게 되므로 자동화된 영상 추적 공격도구에 대하여 매우 강인한 특성을 가지게 된다.

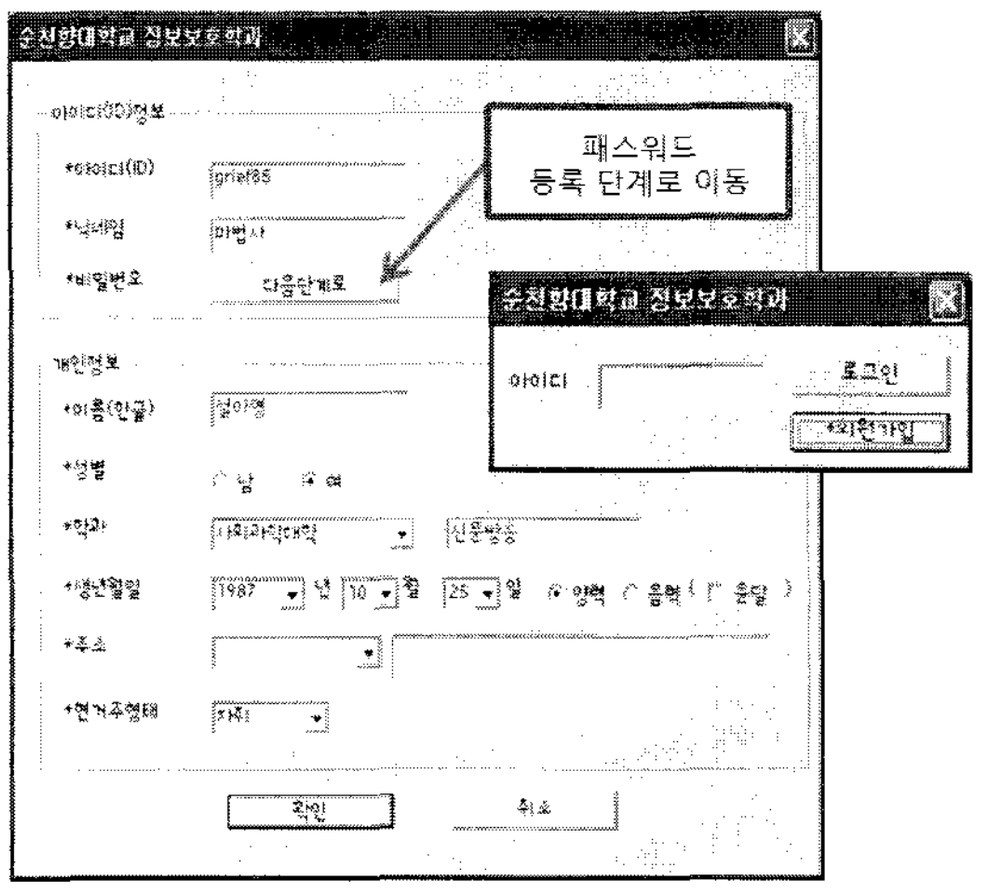
V. 영상기반 패스워드 시스템의 구현 예

이미지 기반의 패스워드 입력 방법을 실제로 활용하기 위해서는 준비된 이미지에 패스워드를 등록하는 과정이 필요하며, 이후에 등록된 패스워드를 기반으로 하여 로그인 시에 해당 이미지를 제시하여 사용자로부터 패스워드를 입력 받아 검증하는 절차가 이루어진다. 이러한 전체적인 절차를 [그림 9]에 보인다.

그림에서는 웹서비스를 제공하는 사이트에 로그인하는 과정에서의 절차를 보인 예이다. 우선 사용자가 신규 방문하는 경우라면 [그림10]과 같은 가입절차를 가지며 가입절차에서 사용자의 패스워드를 등록하는 과정을 거친다.



〔그림 9〕 이미지기반 로그인 절차

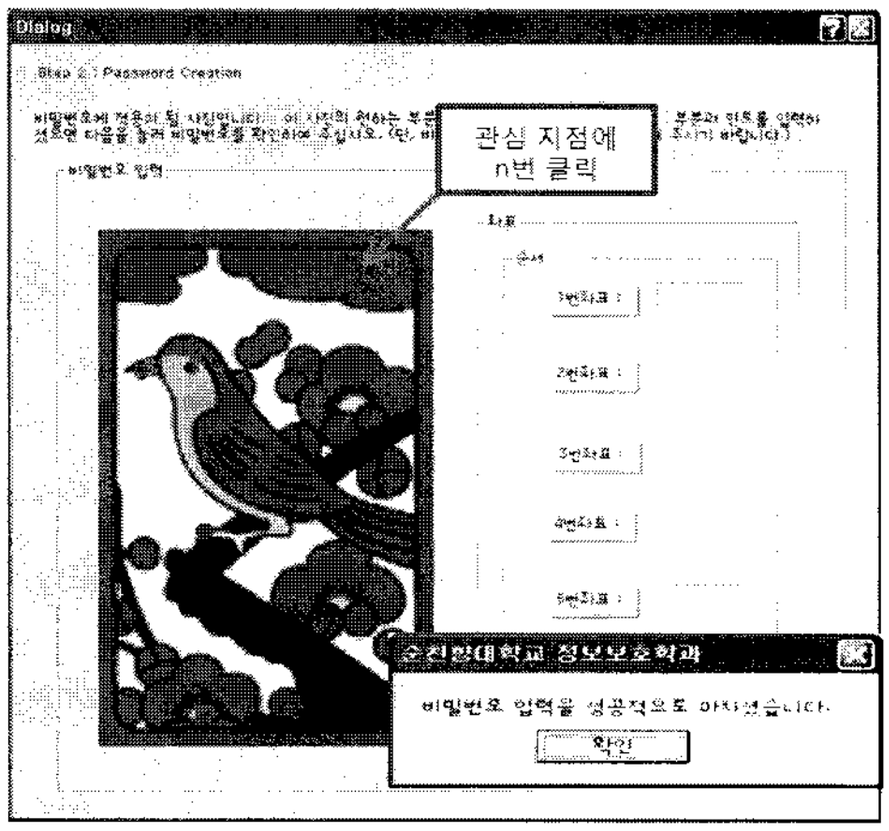


〔그림 10〕 패스워드 등록 요구

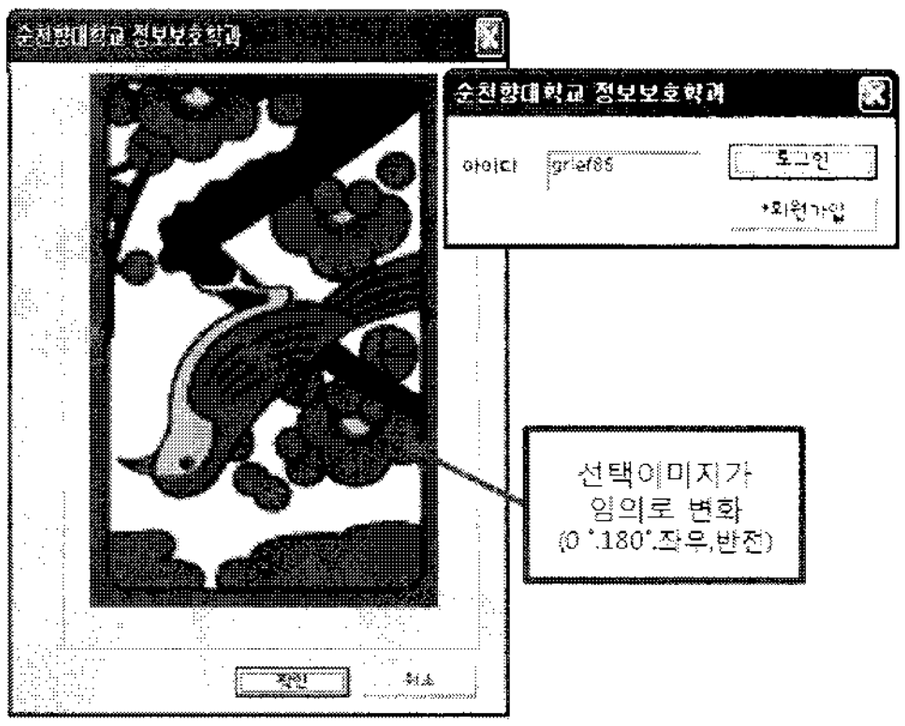
〔그림 11〕 사용할 이미지의 선택

패스워드의 등록과정에서는 [그림 11]과 같이 미리 준비된 다양한 이미지를 제시하여 사용자에게 택일하도록 유도된다. 물론 구현에 따라 사용자가 개별적으로 준비한 이미지를 제시하도록 유도할 수도 있다.

이러한 과정을 통하여 선택된 이미지는 [그림 12]와 같이 미리 준비된 수만큼의 좌표를 선택하여 클릭 하



〔그림 12〕 패스워드의 등록

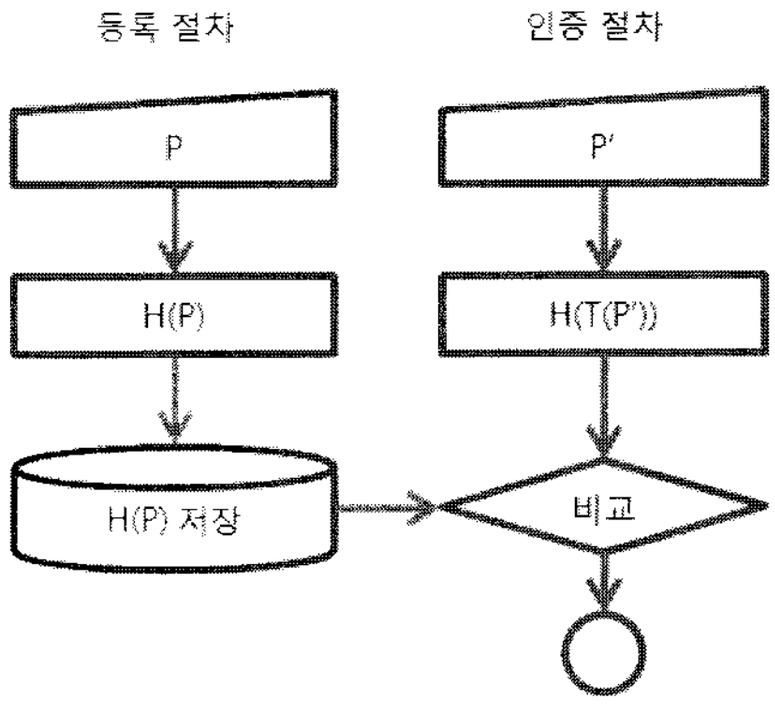


〔그림 13〕 패스워드의 입력

는 과정을 거친다. 클릭 하는 좌표는 선택된 이미지를 토대로 하여 사용자가 연상 기법에 의하여 엮은 이야기를 기반으로 선택되며 이렇게 얻은 좌표를 조합한 후 해싱 등을 통하여 사용자의 패스워드로 취하여 등록한다. 이 과정을 거쳐 등록되는 사용자, 즉 가입자에 대한 정보는 데이터베이스에 저장된다.

가입자는 차후 로그인 과정에서 아이디 만을 요청받으며 아이디를 제시할 경우 그에 따라 해당 가입자가 선택하였던 이미지가 제공된다. 이 때 제공되는 이미지는 제안한 방법에 따라 [그림 13]에서와 같이 회전 및 대칭을 통하여 표출된다. 이렇게 하여 구한 좌표 값은 보다 안전한 형태로 변환함으로써 유출시의 보안에 대비할 수도 있다. 이는 MD5와 같은 간단한 해싱을 통하여 구해질 수도 있으며 여타 보안 인증 메커니즘과 동일한 과정을 거쳐 구성될 수도 있다.

등록된 패스워드는 로그인시, 입력 받은 좌표 값에



〔그림 14〕 패스워드 인증 절차

대하여 해싱 등의 동일한 과정을 통하여 얻어진 대상 패스워드와 비교함으로써 사용자 인증에 사용된다. 이러한 등록절차 및 인증절차를 [그림 14]에 보인다.

Ⅵ. 결론 및 향후과제

본 논문에서는 문자열 기반 패스워드의 취약점에 대하여 분석하고 이에 대응하기 위하여 출현한 영상기반 패스워드에 대하여 소개하였다. 또한 기존의 영상기반 패스워드보다 안전한 새로운 영상기반 패스워드 구성 방안을 제안하고 제안한 방안에 대하여 구현 예를 보였다.

제안한 방안이 보다 더 개선되고 그 결과가 구현되어 실제 시스템에 적용됨으로써 최근 문제가 되고 있는 키보드의 취약점을 해결함으로써 보다 안전한 신분 증명을 위한 환경이 마련되기를 기대한다.

참고문헌

[1] 이만영, 염흥열, 송유진, 김지홍, "최신 정보보호개론", pp.201-220, 홍릉과학출판사, 2005년 2월

[2] Susan Wiedenbeck, et al., "PassPoints : design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies, v.63 n.1-2, p.102-127, July 2005

[3] "LSI-11, PDP-11/03 User's Manual", Digital Equip- ment Corporation, 1975

[4] "KDF11-AA User's Guide", Digital Equipment Corporation, 1979

[5] "M68000 8-/16-/32-bit Microprocessors User's Manual", 9th Ed., 1993

[6] Joe Heinrich, "MIPS R4000 Microprocessor User's Manual", 2nd Ed., MIPS Technologies Inc., 1994

[7] "Intel Architecture Software Developer's Manual : Vol.3 System Programming", Intel Corporation, 1999

[8] Mark E. Russinovich, David A. Solomon, "Windows Internals", Microsoft press, Dec. 2004

[9] http://www.boannews.com/media/view.asp?page=1&gpage=1&idx=6789&search=title&find=&kind=2

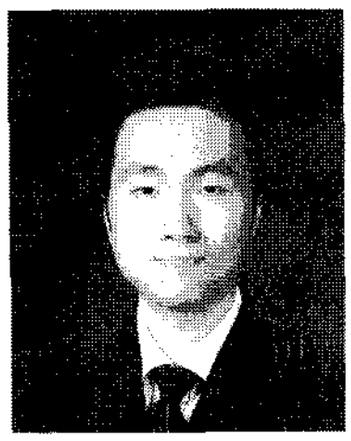
[10] 배광진, 임강빈, "키보드 보안의 근본적인 취약점 분석", 한국정보보호학회 논문집 제18권 제3호, 2008년 6월

[11] S. Man, D. Hong, B. Hayes, M. Matthews, "A password scheme strongly resistant to spyware", Proc. Int. Conf. on Security and Management, Las Vegas, pp.94-100, 2004

[12] "Passfaces : Next Generation Graphical Authentication", http://www.passfaces.com/enterprise/index.htm

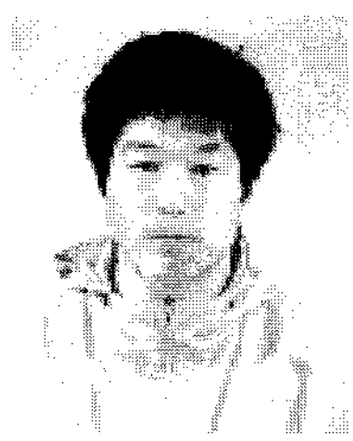
[13] L. Sobrado, J. C. Birget, "Graphical passwords", The Rutgers Scholar, vol.4, Sep. 2002

〈著者紹介〉



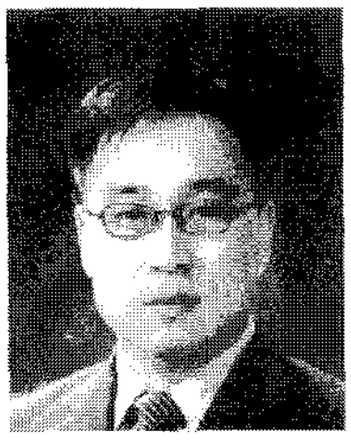
정 태 영 (Taeyoung Jeong)
학생회원

2007년 2월 : 순천향대학교 정보보호학과 학사
2007년 3월~현재 : 순천향대학교 정보보호학과 석사과정
<관심분야> 시스템보안, 운영체제 보안, 임베디드시스템보안



이 경 룔 (Kyungroul Lee)
학생회원

2003년 3월~현재 : 순천향대학교 정보보호학과 학사과정
<관심분야> 시스템보안, 운영체제 보안, 임베디드시스템보안



임 강 빈 (Kangbin Yim)
종신회원

1992년 2월 : 아주대학교 전자공학과 학사
1994년 2월 : 아주대학교 전자공학과 석사
2001년 2월 : 아주대학교 전자공학과 박사
1999년 3월~2000년 2월 : (미)아리조나주립대 연구원
2001년 5월~2003년 2월 : 삼성전자 첨단기술연수소, (주)아이지시스템 강사 (임베디드시스템, RTOS)
2003년 3월~현재 : 순천향대학교 정보보호학과 교수
2005년 3월~현재 : 한국정보보호학회 이사
<관심분야> 시스템보안, 운영체제 보안, 임베디드시스템보안, 접근제어