JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 12 : 2899~2910 Dec. 2014

입력 메시지 암호화를 통한 보안 키패드의 설계와 구현

서화정 · 김호원*

Secure Keypad with Encrypted Input Message

Hwa-jeong Seo · Ho-won Kim*

Department of Computer Engineering, Pusan National University, Pusan, Korea

요 약

본 논문에서는 기존의 가상 키보드 입력 방법에서 마지막 글자를 그대로 보여주는 대신 적합한 입력이 들어올 경우 화면에 올바른 입력이 되었음을 확인할 수 있는 기법을 제안한다. 이는 비밀정보에 대한 암호화를 통해 올바른 입력이 들어오는 경우에만 확인 메시지를 보여줌으로써 공격자가 입력창을 통해 쉽게 확인할 수 있었던 비밀번호 정보를 단순한 어깨너머 공격으로는 확인이 되지 않도록 하였다. 해당 키패드는 기존의 오자에 대한 확인역시 특정 메시지로 표시되는 피드백 정보를 통해 사용자가 오탈자를 확인할 수 있는 장점도 가진다. 해당 제안 기법은 실제로 안드로이드 폰 상에 구현 및 실험되었으며 기존의 기법에 비해 68.23% 향상된 보안성을 제공하며 100%의 정확도를 제공한다. 이와 더불어 기존의 기법과 유사한 신속성을 가진다. 이는 기존의 스마트폰 상에서의 보안 키보드를 안전하게 대체할 수 있는 기술로써 그 효용성이 매우 높다고 할 수 있다.

ABSTRACT

In this paper, we present method that verifies the validity of inputted message rather than showing last character on virtual keyboard. This encrypts password and valid input only can receive right feedback. This is implemented on Android phone and tested. This shows higher security than former method by 68.23% and accuracy shows 100%. This secure keypad is practical and secure so this can replace current input keypad without difficulty.

키워드 : 가상키패드, 보안키패드, 암호화, 구현

Key word : Virtual Keypad, Secure Keypad, Encryption, Implementation

접수일자 : 2014. 08. 15 심사완료일자 : 2014. 09. 12 게재확정일자 : 2014. 09. 26

* **Corresponding Author** Ho-won Kim(howonkim@pusan.ac.kr, Tel:+82-51-510-1010)
Department of Computer Engineering Pusan National University, Pusan, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2014.18.12.2899 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

스마트폰의 급속한 기술 발전과 보급 증대로 인해 대부분의 국민들이 언제 어디서나 온라인 금융서비스에 접속하여 인터넷 뱅킹을 사용하는 것이 가능하게 되었다. 이러한 스마트폰용 모바일 뱅킹 어플리케이션은 스마트폰 내부의 공인 인증서와, 보안 카드의 보안 정보를 이용하여 사용자 인증을 받은 이후 편리하고 안전하게 은행 업무를 처리하는 것이 가능하게 하는 서비스이다. 현재 인터넷 뱅킹서비스 이용률은 지속적으로 증가하여 2013년 1/4분기 기준 모바일뱅킹 서비스의 하루 평균 이용률은 5,285 만 건으로써 전 분기 대비 10.8%의 성장률을 보여주고 있다. 또한 사용 연령대는 20~30대 비중이 75.2%에서 64.7%로 낮아짐에 따라 점차 전 연령대가 자유롭게 모바일 뱅킹을 사용하고 있음을 확인할 수 있다[1-2].

현재 모바일 뱅킹 어플리케이션에서 사용되는 보안 솔루션은 크게 보안카드, 공인인증서 그리고 키보드 보안 솔루션으로 나누어 볼 수 있다. 보안카드는 은행에서 발급해주는 비밀 정보들을 적어놓은 카드로써 불규칙적인 난수 규칙에 의해 생성되었기에 공격자가 해당 정보를 유추하는 것이 불가능하다. 공인인증서의 경우에는 사용자가 신분을 법적으로 증명하여 공인된 기관으로부터 발급받은 인증서를 통해 온라인상에서도 신분을 증명하도록 한다. 키보드 보안 솔루션은 크게 두 가지 기술이 널리 사용되고 있다. 먼저 숫자 키패드의 경우에는 숫자 배열을 무작위로 배치하여 공격자가 누르는 위치를 유추하는 키 로깅 공격이 어렵게 하는 방식이 사용되고 있다. 쿼티 키패드에서는 각 버튼의 배열 간격을 달리하여 내부적으로는 키 로깅 공격에 대비하고, 외부적으로는 어깨 너머 공격에 대비할 수 있도록 비밀번호를 별표로 표시하고 있다. 다른 한 가지는 내부에서 적용되는 일련의 암호화 보안 기술로서 해킹에 의한 위협을 막는다.

하지만 현재 널리 사용되고 있는 키패드의 입력은 화면상에 입력된 비밀번호의 마지막 글자를 보여주는 방법을 통해 입력 값에 대한 피드백을 줌으로써 어깨너머 공격에 취약하다. 이렇게 위험한 방법으로 피드백을 주는 이유는 터치 키패드의 입력 오타율이 기존의 키패드에 비해 높아 사용자에게 입력한 글자에 대한 적절한 피드백이 없다면 비밀번호 입력 시 사용자가 많은 오타를 입력하기 때문이다. 현재 스마트폰 모바일 뱅킹은 언제 어디서나 사용 가능한 장점 때문에 공공장소에서도 손쉽게 서비스 이용이 가능하다. 만약 주위의 사람이 우연히 사용자의 스마트폰을 어깨너머로 살펴보게 된다면 비밀번호가 유출 될 수 있고, 유출된 정보로 인해 실제적인 피해를 받을 수 있다.

본 논문에서는 주위의 사람에 의해 쉽게 노출될 위험이 있는 어깨너머 공격에 강인한 보안 키패드를 제안한다. 해당 제안 기법은 암호입력의 완결성을 위해 입력에 대한 피드백을 사용자에게 보내주면서도, 입력한 글자를 공격자에게 노출시키지 않는 기술이다. 따라서 해당 기법을 통해 기존의 보안 키패드의 기능을 모두 만족하면서 어깨너머 공격에 보다 안전한 키패드를 사용하는 것이 가능하다.

본 논문의 구성은 다음과 같다. 2장에서는 보안 키패드에 대한 관련 연구에 대해 살펴본다. 3장에서는 제안하는 키패드에 대해 제시하며 4장에서는 이에 대한 성능 평가를 한다. 마지막으로 5장에서는 본 논문의 결론을 내린다.

Ⅱ. 관련 연구

금융 보안 연구원에서 출판한 스마트폰 보안 가이드에 따르면 스마트폰의 보안을 위해서는 중요 입력 정보와 지점에 대한 보호기술이 적용되어야 한다[5]. 이는 네트워크의 전송구간 상 메시지 탈취와 메모리 분석 그리고 키 로깅을 통한 물리적인 정보 획득 공격을 사용자가 방지할 수 있어야 함을 의미한다. 현재 대부분의 금융 어플리케이션에서는 안전한 인터넷 뱅킹을 위해 보안 키패드를 제공하고 있으며 이를 통해 안전한 서비스의 제공이 가능하도록 하고 있다. 본 장에서는 실제 안드로이드 스마트폰 상에서 제공되는 금융 어플리케이션을 대상으로 구현 현황에 대해 확인해 보도록 한다.

2.1. 보안 요구 사항

2.1.1. 입력정보 보호 및 전달 구간 내 저장 및 노출 금지

입력정보 보호 및 전달 구간 내 정보의 노출 금지는 가상키보드를 통해 입력된 정보를 암호화하여 저장 및 전달함으로써 이용자의 중요 입력 정보가 공격자의 메

모리 혹은 네트워크 패킷 분석을 통해 쉽게 유출되지 않도록 한다. 따라서 서버와 클라이언트 사이에서 암호화된 송수신 정보는 공격자에게 노출되더라도 서버와 클라이언트 간에 공유된 비밀 키가 유출되지 않는다면 공격으로부터 안전하다.

2.1.2. 입력지점에 대한 입력정보 보호

입력지점에 대한 입력정보 보호를 위해서는 정보 입력 시 키패드에 발생하는 물리적인 특징으로 키를 유추하는 키 로깅을 방지해야 한다. 키 로깅 공격기법이란 사용자의 PC 혹은 스마트폰 상에서 사용자가 모르는 사이 키보드의 키 입력을 추적하거나 기록하는 기법으로서[10], 소프트웨어 기반 방식과 하드웨어 기반 방식 그리고 원격 RF와 음향 분석기법등이 있다[13].

첫 번째로, 소프트웨어 기반 코너 로거 방식[14]은 키 로깅 공격기법 중 가장 기본적인 방식으로서, 스마트폰의 모션 센서를 기반으로 키보드의 중간과 좌우상하의 코너에 대한 입력을 인식하는 방법이다. 따라서 모션 센서를 통해 받은 데이터를 기반으로 필터를 생성하여 기계학습과 분류 알고리즘을 이용하여 비밀정보를 확인할 수 있다[7]. 두 번째로는 코너 로거 방식을 확장한 키패드 로거 방식으로, 기존의 코너 로거 방식에 비해 0부터 9까지의 숫자 입력에 대한 키 로깅 공격기법이다. 코너 로거방식에 비해 좀 더 복잡한 모션 필터와 학습 알고리즘을 기반으로 취약성을 분석할 수 있다[7]. 여기서 사용된 학습 알고리즘에는 베이시안 네트워크, 다층 퍼셉트론, J48 Tree, Random Forest알고리즘이 사용되었으며, 이 중에서 다층 퍼셉트론 알고리즘이 다른 학습 알고리즘에 비해 약 78%의 정확성을 가지고 있다[7]. 그리고 안드로이드 상에서 스마트폰의 3축 센서를 기반의 모션 센서 정보를 획득하여 공격하는 기법 또한 있다[9]. 이러한 공격기법은 키보드에 키 입력 시, 발생하는 스마트폰의 진동을 모션 센서를 통해 획득하여 공격하는 기법으로서, 모션 기반 키 입력 추론 공격기법이라고 한다[8].

다음으로 하드웨어 기반 방식에는 PC용 키보드 케이블 커넥터 형식으로 키 로깅을 하는 방식이 있으며[13], PC용 키보드 상에서 키 입력 시, 각키 마다 발생하는 소리가 다르다는 점에 기반으로 한 키보드 음향 발산 기반 공격이 있으며[11], 유선, 무선 키보드에 대한 전자기파 기반의 키 로깅 공격 기법도 제안되고 있다[12]. 하지만 하드웨어 기반의 공격 방식은 소프트웨어 기반의 공격 방식에 비해 신호에 대한 잡음을 처리하기 어려워 공격하기 어렵다는 단점이 있다[13]. 현재 키패드에 표기되는 문자를 무작위로 배열함으로써 공격자가 해당 키패드의 정보를 유추하는 것이 불가능하게 하는 기술이 실용화되어 있다. 여기서 무작위 배열이란 일반적인 숫자 키패드 배열에서 기존의 배치와는 달리 과같이 생성하여 공격자가 시도하는 키 로깅을 통해서 입력 위치를 파악하더라도 입력 정보를 유추하는 것이 불가능하게 한다.

쿼티 키패드에서는 입력하는 키가 많은 특성상 무작위 배열 시에 사용자에게 혼란을 가중시킬 수 있기 때문에 키의 배열순서는 그대로 두고 키 사이의 간격을 무작위로 늘리거나 줄임으로서 키 로깅에 효율적으로 대처할 수 있도록 하였다.

2.1.3. 사회 공학적 기법

사회 공학적 기법이란 시스템이 아닌 사람의 심리상태나 습관에서 발생하는 취약점을 공략하여 원하는 정보를 얻어내는 공격기법이다[21, 22, 24]. 이러한 사회 공학적 기법의 대표적인 예로서는 피싱, 파싱 그리고 어깨너머 공격이 있다[25]. 그 중에서도 어깨너머 공격은 사용자의 주위에서 어깨너머로 육안이나, 카메라, 비디오카메라 등을 이용하여 사용자의 기기를 훔쳐봄으로서 비밀정보를 얻어내는 공격 기법이다.

최근 발생한 ATM 상에서의 어깨너머 공격 역시 PIN(Personal Identification Number)을 통한 사용자 인증이 취약할 수 있음을 보여주었다[14]. 현재 스마트폰 금융 어플리케이션은 기존의 ATM 보다 많은 단계의 PIN정보를 입력함으로서 보안성을 강화되었지만 여전히 PIN 기반 인증을 해야 하는 한계를 가진다. 또한 어깨 너머 공격은 전문적인 지식 없이도 누구나 쉽게 할 수 있고, 만약 공격에 성공한다면 사용자의 비밀번호를 손쉽게 파악할 수 있다. 현재 스마트폰 금융 어플리케이션은 공공장소에서도 널리 사용되고 있으며 이는 사회 공학적 기법에 취약한 문제를 가진다. 현재 보안 키패드 상에서는 사용자의 비밀 정보 입력 시 마지막 정보를 사용자에게 피드백 정보로 알려주게 된다. 이는 사용자의 오타율을 낮출 수 있는 장점을 가지지만 공격자에게는 비밀정보를 쉽게 엿볼 수 있는 기회를 제공할 수 있다. 최근에는 어깨 너머 공격에 대처하기 위해

앞서 설명한 입력 숫자를 다른 이미지로 대치하여 방어하는 기법이 제시 되었다. 하지만 사용자가 일일이 모든 이미지를 기억해야하는 불편함이 있어 실질적인 실용성은 매우 떨어진다. 따라서 본 논문에서는 간편하면서도 어깨 너머 공격에 강인한 보안 키패드를 설계 및 구현하여 보안 안전하고 편리한 인터넷 뱅킹환경을 도모한다.

2.2. 어깨너머 공격에 대한 연구

스마트폰에서의 PIN값에 대한 입력은 어깨 너머 공격에 취약점을 가지며 이를 해결하기 위해 많은 연구가 진행되어 왔다. 본 절에서는 현재까지 진행된 어깨너머 공격에 관련 연구를 소개한다.

[18]에서는 cognitive trapdoor games 라 불리는 방식으로 기존 PIN을 대체하였다. 초기 입력 화면이 공격자에 노출된다고 하더라도 실제 입력하는 숫자가 노출되지 않는 방식을 취하기 때문에 어깨 너머 공격으로부터 안전하다. 하지만 확률을 기반으로 동작하여 실용적인 구현은 어렵다. 그래픽 기반 패스워드도 어깨 너머 공격을 방지하기 위해 제안되었다[19]. 특히 보다 개선된 그래픽 기반 패스워드인 CHC(Convex Hull Click) 스키마는 이미지 기반 입력 화면에 초기 설정된 이미지들을 사용하여 Convex Hull을 만들고 이미지들이 연결된 내부 도형을 선택함으로써 challenge를 발생시킨다. 이를 통해 안전하게 키를 선택하는 것이 필요하지만 초기에 3개의 이미지를 설정하여야 한다.

[20]에서는 EyePassword를 제안하였다. 이는 직접 키를 터치하여 입력하는 방식이 아니라 시선 추적을 통하여 버튼을 입력하도록 하였다. 빨간 점을 키패드 각각에 추가하여 시선이 키패드 버튼 중심에 고정될 수 있도록 하여 정확성을 증가시켰다. 하지만 입력에 비해 이를 처리하는 비용이 많이 드는 기법으로 실제 활용에는 적합하지 않다. 현재까지 진행된 연구에서는 공격자로부터 입력을 보이지 않도록 하는데 집중하여 이를 처리하는 비용이 증가했으며 따라서 실제 응용에는 매우 적합하지 않다. 따라서 본 논문에서는 기존의 PIN 방식에서의 보안성을 증가시키면서 실제 바로 적용이 가능한 보안 키패드 방식을 제안한다.

2.3. 가상 키패드

스마트폰의 사이즈와 무게를 줄이기 위해 초기의 물리 키보드가 있던 모델의 사용 빈도가 줄고 대신 풀 터치 키패드를 내장한 스마트폰에 대한 사용이 증가하고 있다. 하지만 사용자가 터치를 하는데 주로 사용하는 엄지손가락이 키에 비해 상대적으로 크기 때문에 입력 속도가 느리고, 오타율이 높은 단점을 가진다[23].

이는 물리 키보드는 각 키가 오목한 면으로 구분되어 있어서 촉각적인 피드백을 통해 오타를 감지 할 수 있기에 사용자는 정확한 키 입력이 가능했다. 하지만 터치 키보드는 촉각적인 피드백을 주지 못하기 때문에 보다 높은 오타율이 발생하게 된다[3]. 이러한 터치 키패드의 오류율을 줄이기 위해서 누르고자 하는 키의 버튼에 대한 접촉 면적이 다른 버튼에 비해 높다는 예측적인 접근이 도입되면서 오류율이 줄어들었지만 원천적으로 타자 오류를 차단하는 것은 불가능하다[4].

터치 키패드에서는 키의 크기가 입력속도와 오류율에 큰 영향을 미친다[6]. 그림 1의 결과는 ATM기에 설치된 일반적인 정사각형 형태의 숫자 키패드에서의 오류율을 나타내고 있다. 그래프의 결과에서 알 수 있듯이 키패드의 크기가 커질수록 입력 오류율이 줄어들게 된다. 또한 입력오류율은 비밀번호에 큰 영향을 받아 입력 자릿수의 길이가 커질수록 오차율이 높음을 확인할 수 있다. 결과에서 살펴보듯이 가로, 세로 10mm의 자판 기준으로 10자리 비밀번호 입력 시 오타율이 19%를 나타냄을 확인할 수 있다.

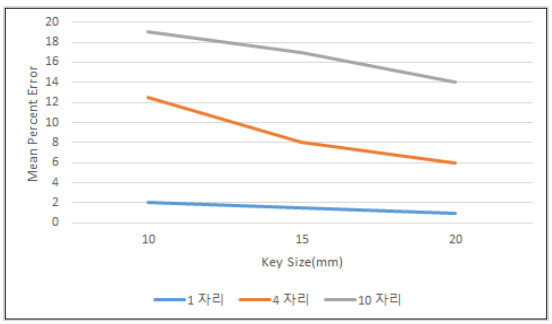

그림 1. 일반적인 키패드 상에서의 오류율[6]
Fig. 1 Error rate for normal keypad[6]

그림 1의 오차율을 실제 금융어플리케이션에 적용하여, 숫자 키패드로 계좌 비밀번호와 보안카드 비밀번호를 입력한다면 입력 값의 길이가 4자리를 넘지 않고, 각 키 사이즈가 갤럭시 S2기준 가로 30mm * 세로 20mm

라고 할 때 오타 입력 확률은 2~4% 대로 수렴함을 확인할 수 있다. 그에 반해 쿼티 키패드에서는 키패드의 크기가 20mm*10mm의 크기이므로 입력하는 비밀번호가 10자리 비밀번호라고 생각해볼 때 오타율은 14~16% 임을 확인할 수 있다. 물론 금융어플리케이션에서는 재배열이라는 과정을 거치나 이것이 오타율에 미치는 영향은 적다[6].

그림 2. 오타 발생 시나리오
Fig. 2 Scenario for error

따라서 사용자가 자신의 오타를 인식하고 이를 알맞게 수정하는 피드백 작업을 효율적으로 수행하기 위한 방법이 사용되고 있다. 기존의 물리 키보드를 사용하는 PC 환경에서는 오타율이 비교적 낮았기 때문에 피드백 없이 화면에 비밀번호를 '*'기호를 이용하여 나타내었다. 하지만 터치 키패드에서는 높은 오타율에 대한 피드백을 주기 위해 입력한 마지막 키 값을 화면에 그대로 표시하고 이전 입력 값은 '*'를 통해서 은닉 하는 방법을 사용하고 있다. 오타율과 그에 대한 피드백에 대한 시나리오를 그림 2를 통해 쉽게 생각해 볼 수 있다. 만약 사용자가 키 'j'를 눌렀을 경우에 오타를 누를 가능성이 있는 주변의 키들은 i, h, k, n, m이다. 따라서 사용자가 누르고자 했던 j와 주변키들 간에 차별화된 피드백을 사용자에게 비밀리에 전달할 수 있다면 사용자는 오타를 인식할 수 있을 뿐 아니라 비밀번호를 주위의 공격자에게 노출하지 않게 된다. 이러한 입력방식은 터치 키패드의 높은 입력 오류율의 해결에는 효과적이지만 공공장소에서 악의적인 공격자의 어깨너머 공격에 매우 취약한 단점을 가진다. 따라서 비밀번호를 주위의 악의적인 공격자에게 숨기면서 사용자에게는 적절한 피드백을 줄 수 있는 방안에 대한 연구가 필요하다. 본 논문에서는 해당 문제를 해결하기 위한 새로운 보안 키패드를 제안한다.

2.4. 암호화

메시지를 암호화하기 위해서는 대표적인 대칭키 알고리즘인 AES를 사용한다. 해당 알고리즘은 2001년에 NIST에 의해 선정된 알고리즘으로써 128 비트의 블락 크기를 가지며 128-, 192-, 256-비트의 키길이를 통해 높은 보안 강도를 제공한다[15, 16]. AES 연산은 안드로이드와 자바 상에서 간단히 javax.crypto API를 통해 호출을 통해 수행이 가능하다. 본 논문에서는 입력되는 메시지를 안전히 암호화하기 위해 128-비트 AES 암호화 연산을 수행한다.

2.5. 암호화 모드

암호화는 제공하고자 하는 응용에 따라 다양한 암호화 모드를 제공한다. ECB 모드는 가장 간단한 보드이며 각각의 평문을 암호문으로 암호화한다. 암호문과 평문이 일대일 관계를 유지하고 있기 때문에 암호문과 평문 사이의 변화 패턴을 관찰하는 것만으로도 공격이 가능하다. 따라서 가장 기밀성이 떨어지는 암호화 모드이다[4, 27, 28]. CBC 모드는 이름에서 알 수 있듯이 암호문 블록을 체인처럼 연결하는 구조를 이룬다. 이전 암호문과 암호화 할 평문을 XOR 연산하여 입력으로 사용한다. 중간 블록에 변경이 가해지면 전체 암호문 블록의 영향을 미치는 특징을 가지며 일부 암호문 블록만을 가지고는 평문을 유추할 수 없어 기존 ECB의 단점을 극복하는 암호화 모드이다. CFB 모드는 이전 암호문을 다음 암호화의 입력으로 사용하는 것은 CBC모드와 동일하나 CBC 모드의 경우 암호화 알고리즘을 적용하기 전에 평문과의 XOR 연산을 수행하지만 CFB 모드에서는 암호화 알고리즘을 적용한 후 평문과의 XOR 연산을 수행하는 것이 차이점이다. 따라서 실제로는 XOR에 의해 암호화가 수행된다. CTR 모드는 블록 암호화를 수행할 때 마다 카운터 값을 사용하며 카운터 값은 블록 암호화를 수행할 때마다 값이 1씩 증가하도록 되어 있다. 카운터 값과 평문을 XOR 연산 수행한 값을 암호화 알고리즘의 입력으로 사용하게 된다. OFB 모드에서 암호화 수행 중 중간 블록이 우연히 같은 값을 가지면 이

후 결과가 같아지는 단점이 있지만 CTR 모드는 카운터 값이 변화하기 때문에 이러한 문제가 발생하지 않는 장점이 있다. 본 논문에서 제안하는 보안 키패드에서는 전체 메시지에 대한 암호화 ECB 암호화를 수행하였다. 하지만 실제 응용에서는 체인 방식으로 수행하는 CBC 모드를 통해서 메시지를 암호화하는 것이 더 좋을 것이다. 해당 기법의 경우 이전 메시지가 잘못된 것인지를 확인할 수 있기 때문에 16 바이트 이상의 암호화 메시지를 입력하는 경우 전체에 대한 확인이 가능한 장점을 가지기 때문이다.

2.6. 아스키 코드

아스키 코드는 문자를 컴퓨터상에서 나타내기 위한 하나의 프로토콜로써 8비트 안에 일상적으로 사용되는 알파벳을 효과적으로 나타낼 수 있도록 한다. 일반적으로 키패드에서 입력하는 값은 문자들인 33~126에 해당하는 값이다. 이외의 값들은 특수한 기능키와 같은 값으로써 비밀번호에 사용되지 않는 값들이다. 본 구현에서는 메시지 값이 정의된 아스키 값의 범위에 들어오는 경우에 대해 확인하는 방식을 통해 비밀 메시지를 확인하는 기법을 사용한다. 해당 기법을 통해 실제로 비밀 메시지를 알지 못하더라도 복호화 수행이 아스키 코드로 나타내어지지 않을 경우 메시지를 버리도록 설계하였다. 이와 더불어 실제로 보안 키패드 상에서 하나의 문자가 가지는 정보의 양이 8비트가 아니므로 이를 높이기 위한 기법에 대해서는 추후 연구를 해볼 생각이다.

2.7. 난수 생성기

암호화에 사용되는 비밀 키 값은 공격자가 예상할 수 없는 임의의 값이 선택 및 사용되어야 한다. 따라서 비밀 키의 생성은 난수 생성기와 같이 높은 암호화 강도가 제공되는 기법을 사용하여야 한다. 여기서 난수 생성기는 NIST에서 권장하는 block-cipher 방식의 DRBG 알고리즘[26]과 이산대수의 강도를 가지는 Blum-Blum-Shub 알고리즘[17]로 생각해 볼 수 있다. 본 논문에서 구현에 사용한 난수 생성기는 구현의 편의 상 임의로 난수 값을 선택하였지만 난수 생성기는 하나의 모듈 형식으로 얼마든지 원하는 암호화 강도에 따라 DRBG 혹은 BBS로 변경하여 사용하는 것이 가능하다.

Ⅲ. 제안하는 보안 키패드

본 논문에서는 어깨너머 공격에 강인한 보안 키패드를 제안한다. 위에서 제시한 기법들을 사용하여 기존의 실제 문자를 화면에 띄워주는 방식과는 달리 올바른 입력에 대한 메시지를 제공해 줌으로써 공격자의 어깨너머 공격을 효과적으로 방어한다. 이는 사용자의 비밀번호가 제대로 입력되었는지를 스마트기기단에서 먼저 확인하여 값을 확인하는 기법이다. 스마트기기단에서 비밀번호를 확인하기 위해 사용하는 기법은 메시지 복호화 시 아스키 코드로 사람이 읽을 수 있는 형식으로 출력되는 경우이다. 암호화는 AES로 수행되었으므로 공격자가 스마트기기 안의 암호화된 비밀정보를 절취하는 경우에도 128비트 이상의 암호화 강도를 가진 AES로 암호화가 되었기 때문에 공격자가 이를 복호화하는 것은 불가능하다. 따라서 이와 같은 특징은 기존의 보안키패드에 비해 보안성이 한층 높아졌다고 할 수 있다.

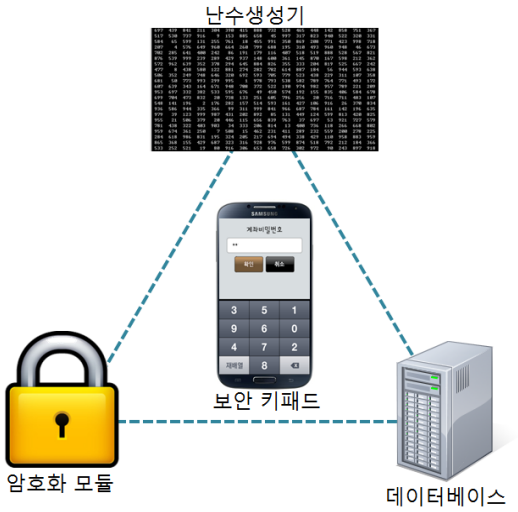

그림 3. 시스템 구성도
Fig. 3 System architecture

본 시스템의 구성은 그림 3과 같다. 스마트 폰 상에서 비밀정보 생성을 위한 난수생성기, 비밀정보를 암호화하기 위한 암호화 모듈 그리고 해당 비밀정보를 저장하는 데이터베이스가 보안 키패드를 생성하기 위한 기본적인 요소로 사용된다.

3.1. 시스템 플로우

본 시스템의 수행 순서는 그림 4과 같다. 먼저 사용자는 비밀번호를 입력해야 하는 사이트에 접속한다. 접속된 사이트에서는 사용자에게 보안 가상 키패드를 생성하여 보여준다. 먼저 난수 생성기를 이용하여 비밀정보를 생성한다. 여기서 주의 할 점은 비밀정보는 ASCII 코드로 우리가 인식할 수 있는 문자와 숫자로 이루어지도록 한다. 만들어진 비밀정보는 암호화 과정을 통해 암호화된다. 사용자는 해당 홈페이지에 대한 비밀정보를 사이트의 이름과 같이 저장한다. 홈페이지에서는 로그인시 사용자가 입력하는 비밀번호를 실시간으로 해석하여 제대로 된 입력이 된 경우에만 확인 메시지가 도출되도록 한다. 만약 입력된 비밀번호를 통해 비밀정보 복호화 시 도출되는 값이 문자 혹은 숫자로 나타내지 않는다면 키패드는 확인 메시지가 도출되지 않는다. 따라서 사용자는 이를 확인하여 나타낼 수 있어야 한다.

그림 4. 시스템 플로우
Fig. 4 System FLOW

3.2. 보안 키패드 생성 알고리즘

비밀정보를 생성하기 위해서는 알고리즘 1과 같은 형식으로 사용이 가능하다. Step 1에서는 난수 생성기에 Seed값을 넣어 비밀정보를 생성한다. 비밀정보는 아스키 코드 중 문자와 숫자로 나타나는 범위에 한해서만 선택이 되며 그렇지 않은 경우 다시 값을 생성한다. 이런 생성방식은 스마트기기에서 해당 비밀정보를 저장하고 있을 경우 물리적으로 스마트폰의 비밀정보를 가져가는 경우를 방지하기 위해서이다.

표 1. 알고리즘 1. 비밀정보 생성
Table. 1 Algorithm 1. secure information generation

입력: Seed 출력: 비밀정보(P)	
1.	Seed값을 난수 생성기에 넣음
2.	For t=0 to 15 do
3.	if(난수 > 47 && 난수 <123)
4.	P[t] = 난수
5.	다시 난수를 생성하여 P[t]에 넣음
6.	End For

알고리즘 2에서는 알고리즘 1을 이용하여 비밀정보를 생성한다. 생성된 비밀정보는 사용자의 비밀 키를 통해 암호화되며 암호화된 메시지 C가 생성된다. 생성된 암호문 C는 데이터베이스에 저장된다. 여기서 비밀정보 및 사용자의 비밀 키는 저장되지 않으며 오직 암호문 C만이 데이터베이스에 저장된다.

표 2. 알고리즘 2. 비밀정보 생성 및 암호화
Table. 2 Algorithm 2. secure information generation and encryption

입력: Seed, 사용자의 비밀 키(K) 출력: 암호문(C)	
1.	알고리즘 1을 이용하여 비밀정보 (P)를 생성
2.	비밀정보 (P)를 사용자의 (K)로 암호화
3.	암호화된 암호문(C)을 생성
4.	해당 사이트에 대한 암호문을 데이터베이스에 저장

알고리즘 3에서는 비밀 키를 보안 키패드로 입력하는 경우를 나타내고 있다. 먼저 데이터베이스에 접근하여 해당 사이트에 대한 암호문(C)을 가져온다. 비밀번호를 보안키패드를 통해 입력하도록 한다. 여기서 전수조사를 방어하기 위해서 Step 3, 4에서는 입력횟수에 제한을 두어 일정 횟수 및 시간을 초과하는 경우 false를 return하도록 한다. 해당 조건을 만족할 경우 입력된 비밀번호를 통해 암호문(C)을 복호화하며 해당 메시지가 문자와 숫자를 만족하는 경우에 true를 return하도록 한다.

표 3. 알고리즘 3. 보안 키패드 입력 확인
Table. 3 Algorithm 3. secure keypad for input check

입력: 사용자의 비밀 키(K) 출력: 확인메시지	
1.	데이터베이스에 접근하여 해당 사이트에 대한 암호문(C)을 받아옴
2.	입력되는 비밀 키 값을 통해 암호문(C)을 복호화하여 메시지 (X)를 출력
3.	if 입력횟수>기준횟수 return false
4.	if 입력시간>기준시간 return false
5.	For t=0 to 15 do
6.	if(X[t] > 47 && X[t] <123)
7.	return true
8.	else
9.	return false
10.	End For

3.3. 실용적인 응용 분야

본 논문에서 제안한 기법은 파일럿 프로젝트로써 이를 활용하여 보다 많은 응용 및 발전이 가능하다. 크게 두 가지의 확장성에 대해 설명한다. 먼저 Hybrid기법에 대한 적용이 가능하다. 본 구현에서는 전체 메시지에 대해서 암 복호화를 수행하였다. 하지만 보다 피드백을 원활하게하기 위해 입력되는 패스워드가 전체가 아닌 부분적으로도 해당 입력이 제대로 되었는지 확인할 수 있도록 구성할 수 있다. 만약 4개의 문자마다 피드백을 준다면 8바이트에 대해서는 임의의 난수 값으로 비밀번호를 패딩하여 복호화를 수행하는 기법이 가능하다.

또한 본 논문은 우리가 일상적으로 사용하는 카카오톡이나 문자메시지 서비스의 경우 뒤에서 혹은 몰래 메시지를 훔쳐 볼 경우를 대비하여 특정 인물이나 물건에 대해서 암호화하여 나타냄으로써 보안을 높일 수 있다. 예를 들어 표에서와 같이 일반메시지에서는 여과 없이 정보가 공개된다면, 보안메시지의 경우 해당 메시지에 대한 패딩이 수행되어 보안이 제공된다.

Ⅳ. 구현 및 성능 평가

본 논문에서 설계한 보안 키패드는 실제 안드로이드 스마트폰에서 구현 및 성능이 평가되었다. 자세한 내용은 아래와 같다.

4.1. 구현 결과

4.1.2. 쿼티 키패드

쿼티 보안키패드는 이전 키패드와 겉모습은 동일하다. 하지만 비밀번호 입력 시 제대로 된 입력이 들어가게 되는 경우에는 done이라는 글자를 비밀번호 입력칸에 출력해주게 된다.

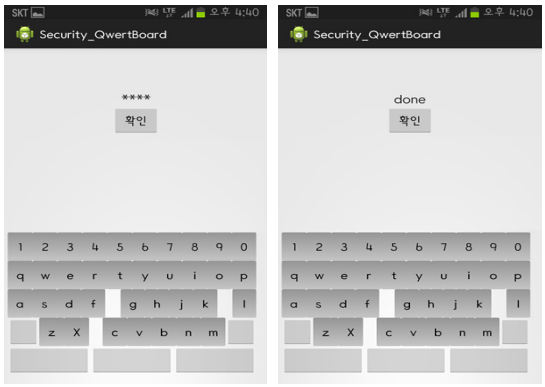

그림 5. 입력 및 동작
Fig. 5 Input and operation

그림 5에서는 입력 및 동작에 대해 설명한다. 왼쪽 그림에서는 비밀번호를 입력하는 중임을 확인할 수 있다. 현재 비밀번호가 제대로 입력이 되지 않았기 때문에 아직 done이라는 메시지가 출력되지 않음을 확인할 수 있다. 만약 메시지가 모두 입력이 되며 오른쪽 그림과 같이 done이라는 메시지가 출력됨을 확인할 수 있다.

4.2. 성능 평가

본 장에서는 보안성에 대해 테스트하기 위해 실제적 환경의 다양한 상황에서 어께 너머 공격을 실행할 경우에 비밀번호를 알아 낼 수 있는지 없는지에 대한 공격 성공률에 대해서 분석 한다. 또한 보안 키패드의 성능 분석을 위해서 키패드 상에서의 타자의 신속성 그리고 정확성을 비교 분석 한다.

사용된 타겟 보드는 그림 6과 같이 4개의 갤럭시 스마트폰을 사용하였다. 이는 다양한 해상도와 화면 크기 그리고 CPU 환경을 고려하여 보다 객관적인 지표를 제공하기 위해서이다. 하지만 갤럭시S1의 경우 실험결과 속도가 느리며 그림 6에서 보는바와 같이 스크린의 크기가 작고 해상도가 낮아 타자입력이 원활히 되지 않아

해당 성능 평가에서 제외되었다.

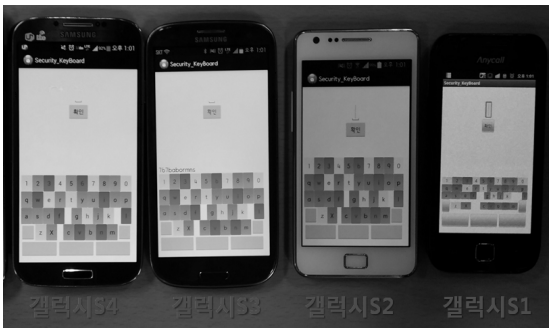

그림 6. 실험에 사용된 갤럭시폰에 보안 키패드를 설치한 화면
Fig. 6 Operating screen of secure keypad on galaxy

표 4에서는 갤럭시 시리즈에 대한 상세한 성능을 제시한다. 최신 스마트폰의 경우 가장 큰 화면과 해상도를 제공한다. 따라서 화면상의 버튼의 크기가 가장 커지게 되고 이는 추후에 실험에서 나타나는 바와 같이 높은 정확도와 빠른 타자 속도를 제공하게 된다.

표 4. 타겟 장비에 대한 상세 설명
Table. 4 Specifications for target devices

특성	갤럭시2	갤럭시3	갤럭시4
해상도	480X800	720X1280	1920X1080
디스플레이	4.3인치 슈퍼아몰레드 플러스	4.8인치 HD슈퍼아몰레드	5인치 풀HD 슈퍼아몰레드
버튼크기 (가로×세로)	0.5x0.8 (cm)	0.6x0.75 (cm)	0.6x0.85 (cm)
CPU	1.2GHz 듀얼	1.4GHz쿼드	1.6GHz옥타

실험에 참가한 4명의 실험자들에 대한 데이터 중 중요시 된 부분은 시력과 어깨너비이다. 시력은 1~2m 거리에서 스마트폰의 키에 대한 판별이 가능한 정도의 시력이며 어깨너비와 키의 경우 건장한 성인 남성의 평균으로써 실험에 적합한 표본이 선택되었다고 할 수 있다. 키패드의 정확성, 신속성 대한 실험은 현재 사용 중인 끝 글자가 보이는 키패드, 일반적으로 PC환경에서 사용되는 모든 글자가 '*'로 은닉되는 키패드, 그리고 제안된 키패드 3개를 비교한다. 실험에서는 3가지 키패드를 이용하여 정확도와 신속도 그리고 보안에 대한 실제적인 데이터를 수집 및 분석하였다.

4.2.1. 보안성

어깨너머 공격에 대한 보안성은 최근 출시되고 있는 구글 글라스에 의해 보다 그 중요성이 높아지고 있다. 공격자는 구글 글라스를 사용하여 아무런 제재 없이 사용자의 비밀번호 입력과정을 녹화하는 것이 가능하다. 만약 기존의 기법을 사용하여 비밀번호를 입력한다면 입력창 정보를 통해서도 공격이 가능한 취약점을 가진다. 하지만 제안된 보안 키패드는 어깨너머 공격에 노출되더라도 공격자가 비밀번호를 확인하는 것이 어렵다. 그 이유는 모든 비밀번호가 별표로 표현되기 때문에 공격자가 해당 비밀번호를 확인하기 위해서는 입력된 비밀번호의 개수의 지수승만큼을 전수조사를 해보아야 한다. 제안하는 알고리즘적인 보안강도는 AES의 보안강도와 동일하다. 비밀번호를 아스키인 경우에 제대로된 비밀번호라고 확인하는 기법은 휴리스틱한 기법이다. 하지만 특정 비밀번호로 아스키값이 나올 확률은 $1/a^{16}$로써 해당 false positive의 경우는 무시해도 될 정도로 확률이 낮다. 여기서 a는 해당 값이 아스키일 확률을 의미하며 전체 16자리의 수가 아스키가 나오는 확률을 의미한다.

다음은 보안성 확인을 위해 수행된 실험과정을 자세히 나타내고 있다. 먼저 사용자 한명을 선정하고 3명의 공격자가 뒤에서 사용자의 스마트폰을 지켜본다. 공격자는 사용자가 값을 입력 시 준비한 답변지에 예상되는 비밀번호를 입력하게 된다. 마지막으로 실제 입력 값과 예상답안을 확인하여 노출된 비밀정보를 확인한다.

그림 7에서는 평균 공격 성공률을 그래프를 이용하여 도식하고 있다. 기존기법 1과 제안기법은 공격자가 입력창만을 확인해서는 절대로 비밀번호를 확인할 수 없다. 그 이유는 모든 값이 '*'형식으로 표현되어 공격자가 얻을 수 있는 정보는 오직 비밀번호의 길이밖에 없다. 따라서 현재 스마트폰에서 가장 많이 사용되는 기존기법2에 대해서 공격 성공률의 평균을 스마트 폰에 따라 조사한 결과 갤럭시 S2에서 71.5%, 갤럭시 S3에서 67.8% 그리고 갤럭시 S4에서 66%임을 확인할 수 있었다. 여기서 흥미로운 점은 최신 장비로 갈수록 공격 성공률이 떨어진다는 점이다. 쉽게 생각해 볼 수 있는 점은 화면의 크기가 큰 최신모델이 보다 공격에 취약하다고 생각할 수 있다.

하지만 다음 장에서 설명된 바와 같이 최신 모델에서 타자 신속도가 가장 높다. 왜냐하면 스마트폰의 버튼 크기가 가장 커서 사용자가 타자입력을 원활히 할 수 있기 때문이다. 이처럼 기존기법2와 달리 제안기법은 정보 노출이 하나도 되지 않으므로 기존기법2에서 노출된 평균 공격 성공률인 68.23%의 보안 취약점이 개선되었다고 할 수 있다.

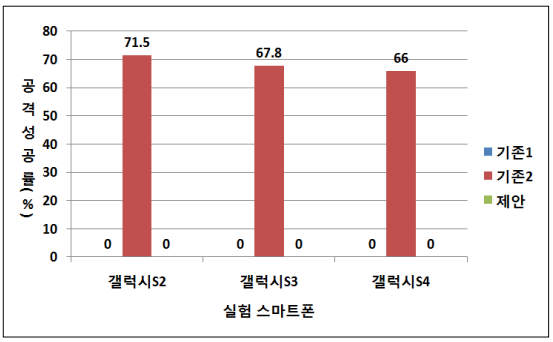

그림 7. 보안 키패드에 대한 공격 성공률
Fig. 7 Attack success rate for secure keypad

4.2.2. 정확성

비밀번호의 안전성을 보장하기 위해서는 비밀번호에 대한 정보 노출을 줄이는 것이 중요하다. 하지만 높은 오타율을 해결하기 위해 입력 값에 대한 피드백을 제공하는 기존하는 보안 키패드는 어깨너머 공격에 매우 취약하다. 하지만 본 논문에서 제안한 기법은 높은 보안성과 함께 사용자에게 피드백 정보를 제공하여 타자의 정확성를 100%로 유지할 수 있도록 설계되었다. 각각의 플랫폼의 평균 정확도는 그림 8에 그래프로 도식하여 나타내었다. 정확도를 플랫폼에 따라 확인해 보면 화면의 크기가 작을수록 버튼의 크기가 작아지므로 오타율이 높아짐을 확인할 수 있다. 기법에 대해 확인해 보면 정확도가 기존기법1에서 97.19%, 기존기법2에서 97.61% 그리고 제안기법에서 100%로 나타남을 확인할 수 있다. 이와 같은 정보를 통해 확인해 볼 때 제안기법이 기존기법과 비교해 볼 때 정확도가 월등히 높음을 확인할 수 있다. 그 이유는 제대로 된 비밀번호가 입력되는 경우에만 알림이 발생하도록 제작되었기 때문이다.

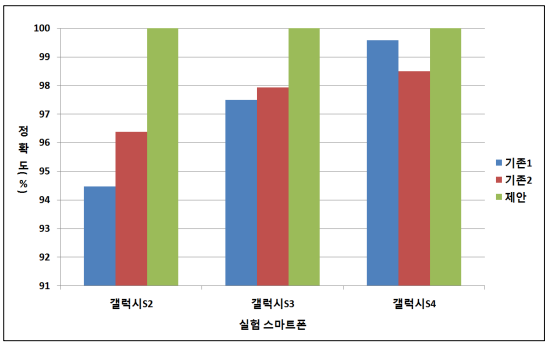

그림 8. 정확도 실험결과
Fig. 8 Accuracy results

4.2.3. 신속성

신속성이란 키패드를 통해 문자 입력 시 얼마나 빠른 속도로 원하는 목표를 작성하는 지에 대한 척도이다. 보안성 평가에서 확인해 본 결과 화면의 크기가 크더라도 신속하게 입력되는 정보가 보다 안전성이 높다는 것이 확인되었다. 따라서 비밀정보 입력을 신속하게 하여 정보의 노출을 최소화하는 것이 보안성을 높이는 하나의 방안이라 할 수 있다. 실험 결과 신속성에서 기존 기법들과 유사한 성능을 나타냄을 확인할 수 있었다. 그림 9에서는 타겟 장비에 따른 신속도의 비교가 그래프를 통해 확인할 수 있도록 나타나 있다. 화면의 크기에 따라 버튼의 크기가 결정된다. 따라서 화면의 크기가 클수록 버튼의 크기가 커지므로 타자 입력 속도가 빨라짐을 확인할 수 있다.

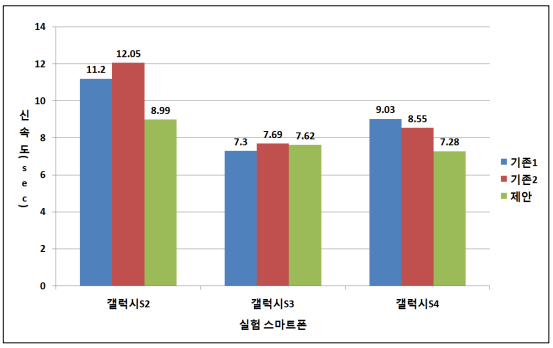

그림 9. 신속도 실험결과
Fig. 9 Speed results

Ⅴ. 결 론

기존 스마트폰에서 안전한 금융 서비스를 위해 사용되는 보안 키패드는 오탈자를 확인하기 위한 용도로 사용자에게 입력된 문자의 마지막 정보를 제공한다. 이로 인해 악의적인 공격자는 쉽게 사용자의 비밀정보를 어깨너머 공격을 통해 확인하는 것이 가능하다. 본 논문에서는 기존의 보안 키패드가 가지는 보안 취약성을 해결하기 위해 비밀번호에 대한 피드백을 암호화 기법을 통해 제공하는 새로운 개념의 보안 키패드를 제안한다. 기존의 오탈자 확인 정보가 문자 본연의 정보가 화면에 들어나는 방식이었다면 제안하는 방식은 비밀번호의 완결성을 한번에 확인할 수 있는 구조를 가진다. 해당 제안은 실제 구현을 통해 성능이 평가되었으며 보안성이 68.23% 향상되었으며 정확도는 100%를 나타낸다. 신속성은 기존의 기법과 유사한 결과를 도출하였다.

감사의 글

본 연구는 산업통상자원부 우수기술연구센터(ATC)사업의 연구비 지원으로 수행되었습니다 (10048537).

REFERENCES

[1] Korean bank, “Reports on Domestic Internet banking”, 2013.05.15.

[2] Miller, George. “The magical number seven, plus or minus two: Some limits on our capacity for processing information.” *The psychological review63*(1956):81-97.

[3] Kwon, Sunghyuk, Donghun Lee, and Min K. Chung. “Effect of key size and activiation area on the performance of a regional error correction method in a touch-screen QWERTY keyborad.” *International Journal of Industrial Ergonomics* 39.5(2009):888-893.

[4] Kohl, John T. ”The use of encryption in Kerberos for network authentication.” *In Advances in Cryptology CRYPTO89 Proceedings*, pp. 35-43. Springer New York, 1990.

[5] Financial research center, “Guide for smartphone security”, 2010.12.

[6] Soo Min Lim, Hyoung Joong Kim, and Seong Kee Kim, “Designing Password Input System Resistant on Shoulder Surfing Attack with Statistical Analysis”, *Journal of The Institute of Electronics Engineers of Korea* 2012, 49.9: 215-224.

[7] Darer, Alexander. “Mini Project 2: A key-logger which infers keystrokes on a touch-screen keyboard from smartphone motion.” (2013).

[8] Cai, Liang, and Hao Chen. “On the practicality of motion based keystroke inference attack.” *Trust and Trustworthy Computing*. Springer Berlin Heidelberg, 2012. 273-290.

[9] Cai, Liang, and Hao Chen. “TouchLogger: inferring keystrokes on touch screen from smartphone motion.” *Proceedings of the 6th USENIX conference on Hot topics in security*. USENIX Association, 2011.

[10] Gharaibeh, Natheer. "The Impact of Customer Knowledge on the Security of E-Banking." *International Journal of Computer Science and Security (IJCSS)* 7.2 (2013): 81.

[11] Asonov, D., Agrawal, R.: Keyboard acoustic emanations. In: *Proceedings of IEEE Symposium on Security and Privacy*, pp. 3-11 (May 2004).

[12] Vuagnoux, M., Pasini, S.: Compromising electromagnetic emanations of wired and wireless keyboards. In: *Proceedings of the 18th Conference on USENIX Security*.

[13] Gold, Steve. “Electronic countersurveillance strategies.” *Network Security* 2013.2 (2013): 15-18.

[14] Suo, Xiaoyuan, Ying Zhu, and G. Scott Owen. "Graphical passwords: A survey." *In Computer Security Applications Conference*, 21st Annual, pp. 10-pp. IEEE, 2005.

[15] Announcing the ADVANCED ENCRYPTION STANDARD (AES)". Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001. Retrieved October 2, 2012.

[16] Daemen, Joan; Rijmen, Vincent (9/04/2003). “AES Proposal: Rijndael”. National Institute of Standards and Technology. p. 1. Retrieved 21 February 2013.

[17] Sidorenko, Andrey, and Berry Schoenmakers. “Concrete security of the Blum-Blum-Shub pseudorandom generator.” *In Cryptography and Coding*, pp. 355-375. Springer Berlin Heidelberg, 2005.

[18] Roth, Volker, Kai Richter, and Rene Freidinger. “A PIN-entry method resilient against shoulder surfing.” In *Proceedings of the 11th ACM conference on Computer and*

communications security, pp. 236-245. ACM, 2004.

[19] Wiedenbeck, Susan, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. “Design and evaluation of a shoulder-surfing resistant graphical password scheme.” In *Proceedings of the working conference on Advanced visual interfaces*, pp. 177-184. ACM, 2006.

[20] Kumar, Manu, Tal Garfinkel, Dan Boneh, and Terry Winograd. “Reducing shoulder-surfing by using gaze-based password entry.” In *Proceedings of the 3rd symposium on Usable privacy and security*, pp. 13-19. ACM, 2007.

[21] BIANCHI, Andrea, et al. The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices. In: *Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction*. ACM, 2011. p. 197-200.

[22] Inseok, Kim. “Security enhancements for internet bank” J*ournal of The Korea Institute of Information Security & Cryptology* 15, no. 4 (2005): 43-48.

[23] hyunggyu yang "Security on Smartphone keypad." *Journal of The Korea Institute of Information Security & Cryptology* 21, no. 7 (2011): 30-37.

[24] Park, Kihong, Lee JunHwan, Cho HanJin"Countermeasure against Social Technologic Attack using Privacy Input-Detection" *Korean content journal*, 12, no. 5 (2012): 32-39.

[25] Dongil Seo. "Privacy preserving technology." J*ournal of The Korea Institute of Information Security & Cryptology* 16, no. 1 (2006): 40-48.

[26] Gjøsteen, Kristian. "Comments on dual-ec-drbg/nist sp 800-90 draft december 2005." (2006).

[27] Ehrsam, William F., Carl HW Meyer, John L. Smith, and Walter L. Tuchman. ”Message verification and transmission error detection by block chaining.” U.S. Patent 4,074,066, issued February 14, 1978.

[28] Kaufman, C., Perlman, R., & Speciner, M (2002). Network Security. Upper Saddle River, NJ: Prentice Hall. Page 319 (2ndEd.).

서화정(Hwa-jeong Seo)

2010년 2월: 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월: 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월 ~ 현재: 부산대학교 컴퓨터공학과 박사과정
※관심분야 : 정보보호, 암호화 구현, IoT

김호원(Ho-won Kim)

1993년 2월: 경북대학교 전자공학과 학사 졸업
1995년 2월: 포항공과대학교 전자전기공학과 석사 졸업
1999년 2월: 포항공과대학교 전자전기공학과 박사 졸업
2008년 2월: 한국전자통신연구원 정보보호연구단 선임연구원/팀장
2008년 3월~현재: 부산대학교 정보컴퓨터공학부 부교수
※관심분야 : 스마트그리드 보안, RFID/USN 정보보호 기술, PKC 암호, VLSI 설계, embedded system 보안, IoT