Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.2, Apr. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.2.345

메시지 인증 코드를 위한 디지털 인감*

정 창 훈,[1†] 신 동 오,[1] 장 룡 호,[1] 양 대 헌,[1] 이 경 희,[2] 염 흥 열[3‡]
[1]인하대학교, [2]수원대학교, [3]순천향대학교

Digital Legal Seal for Message Authentication Code*

ChangHun Jung,[1†] DongOh Shin,[1] RhongHo Jang,[1]
DaeHun Nyang,[1] KyungHee Lee,[2] Heung-Youl Youm[3‡]
[1]Inha University, [2]The University of Suwon, [3]Soonchunhyang University

요 약

이 논문에서는 디지털 인감이라는 보안 도구를 제안한다. 디지털 인감은 종이에 출력된 바코드를 스캔하고, 스캔한 바코드 데이터와 그 데이터에 대한 HMAC 태그를 디스플레이 장치에 출력한다. 생성된 HMAC 태그는 온라인 또는 오프라인에서 사용자 본인을 확인하거나 메시지의 인증에 사용될 수 있다. 우리는 디지털 인감을 온라인 뱅킹에 적용하여 보안카드나 OTP의 부족한 점을 보완할 수 있는지에 대해 검토한다. 또한 오프라인 차용증에 일반 인감대신 사용하여 인감의 위조 가능성을 낮출 수 있는지도 검토한다.

ABSTRACT

In this paper, we present a security tool which called Digital Legal Seal. The Digital Legal Seal scans a barcode on a paper and print it with the tag generated by Hash-based Message Authentication Code(HMAC) in text format on a display device. The result of HMAC can be used for user authentication or secure message transmission on both online and offline. We examine not only how the Digital Legal Seal can make up the weak points of security card and OTP (One Time Password), but also the possibility of reducing the forgery of promissory note on offline.

Keywords: Authentication Protocol, Hash-based Message Authentication Code, Digital Legal Seal, Online Banking, Promissory Note

I. 서 론

전자 금융이란 각종 금융 서비스에 정보통신기술을 적용시킨 것으로서, 온라인 뱅킹, 텔레뱅킹, ATM 거래 등을 의미한다. 전자 금융 시스템을 이용할 경우, 은행에 직접 가지 않아도 된다는 점과 은행 영업시간이 종료되어도 은행 서비스를 이용할 수 있다는 점 등 다양한 장점이 있다. 이러한 장점으로 온라인 뱅킹 중 특히 인터넷 뱅킹의 이용률은 점점 증가하고 있는 추세이다. 한국은행 금융결제국 지급결제 뉴스레터 제2015-8호에 따르면 2015년 2/4분기 국내 인터넷 뱅킹 서비스 등록 고객수는 1억 1,327만명으로 전분기말대비 4.3% 증가하였고, 일평균 이용건수와 이용금액은 7,725만건, 40조 4,627억원으로 전분기대비 각 0.4%, 7.7%가 증가하여 꾸준한 증가세를 보이는 것으로 조사되었다[1].

온라인 뱅킹은 사용자가 직접 은행에 가지 않고 온라인상의 PC나 스마트폰에서 이용하는 비대면 서비스이다. 그렇기 때문에 은행은 사용자의 신원을 확

Received(02. 15. 2016), Modified(03. 16. 2016), Accepted(03. 22. 2016)
* 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구(No.R0127-15-1051, IoT 환경에서 프라이버시 보호 국제 표준화)이며, 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(2014R1A1A2059852)임.
† 주저자, jcptk677@gmail.com
‡ 교신저자, hyyoum@sch.ac.kr(Corresponding author)

인하기 위하여 공인인증서와 계좌비밀번호 뿐만 아니라 보안카드, 일회용 비밀번호, ARS 인증 등 다양한 인증 요소와 채널을 이용하고 있다. 보안카드는 사용자가 소지할 수 있는 형태의 비밀이며, 중복이 없는 4자리 숫자 30여개로 구성된다. 사용자는 온라인 뱅킹으로 계좌이체 등의 서비스를 이용할 때 보안카드의 번호 중 특정 번호를 입력하도록 요구받으며, 이를 올바르게 입력함으로써 은행으로부터 발급받은 보안카드를 소지하고 있는 본인임을 인증한다. 일회용 비밀번호 생성기(OTP, One Time Password)는 30초 또는 1분 간격으로 은행 서버와 동기화된 6자리의 일회용 비밀번호를 생성한다. 사용자는 보안카드 대신 OTP 장치에 표시된 일회용 비밀번호를 입력함으로써 사용자 본인이 맞음을 인증한다.

비대면 거래를 위한 사용자 인증이 다양한 보안 수단을 통해 이루어지면서, 공격자는 보안 수단의 취약점보다는 사회공학적 기법을 이용하여 온라인 뱅킹 사기를 시도하는 경향을 보인다. 특히 피싱, 파밍 공격을 통하여 사용자의 보안카드 번호를 모두 훔치는 수법[2]으로 인한 피해가 지속적으로 발생하고 있으며, 이학영 국회의원이 2015년 9월 7일에 발표한 대한민국 국회 보도자료에 따르면, 2014년에 피싱과 파밍으로 인한 피해건수와 피해액은 32,568건, 1,637억원으로 전년대비 각각 39%, 65%가 증가했다는 것을 알 수 있었다[3]. 이로 인해 보안카드의 보안성은 앞으로 점점 낮아질 것으로 보이며, 이 문제를 보완하기 위하여 SMS 또는 ARS를 통한 사용자 인증 기법이 도입되었다[4].

일회용 비밀번호는 피싱, 파밍 공격에 안전하다고 여겨지나, MITB(Man In The Browser) 공격에는 여전히 취약하며[5], 이를 이용한 공격이 실제로 발생하기도 하였다[6]. 이 취약점을 해결하는 것은 아직 어려운 문제로, 단순한 SMS 또는 ARS가 아닌, 이용서비스의 상세 내용을 먼저 안내하는 방식으로 인증 방법이 바뀌었다.

이러한 보안적 문제들은 결과적으로 사용자들에게 금전적인 피해를 가져다주게 되며, 그로인해 더 높은 보안성을 가진 보안 수단이 필요 되고 있다.

이 논문에서 제안하는 디지털 인감은 우선 데이터를 바코드화 하여 종이로 출력하고, 디지털 인감으로 출력된 바코드를 스캔하면 바코드 데이터와 그에 대한 해시 기반 메시지 인증 코드(HMAC, Hash-based Message Authentication Code)의 태그(Tag)가 출력되는 도구이다. 우리는 이 디지털 인감을 온라인 뱅킹에 적용하여 사용자 본인인증 및 안전한 온라인 뱅킹 서비스를 구현할 수 있음을 보인다. 뿐만 아니라 차용증과 같은 오프라인 문서에 디지털 인감을 적용하여 위조하기 어려운 인감으로도 활용할 수 있음을 보인다.

이 논문의 구성은 다음과 같다. 2장에서는 메시지 인증 코드, 아두이노 우노, TCRT5000 센서, 보안카드, 일회용 비밀번호에 대해서 알아보고, 3장에서는 디지털 인감에 대해서 알아본다. 4장에서는 디지털 인감의 사용성 실험을 진행하고, 온라인 뱅킹 및 오프라인 차용증에 적용 가능성을 검토한다. 마지막 5장에서는 결론과 향후 연구에 대해 논의한다.

II. 관련 연구

2.1 메시지 인증 코드

메시지 인증 코드(MAC, Message Authentication Code)란, 네트워크상으로 메시지를 송수신할 때 수신자가 메시지 발신자에 대한 인증과 메시지의 무결성을 확인할 수 있는 코드를 말한다[7].

HMAC은 암호학적 해시함수를 이용하여 MAC을 구현한 알고리즘으로, 임의의 길이의 메시지와 비밀키를 입력받아서 고정된 길이의 MAC을 생성한다[8]. HMAC으로 생성되는 태그의 길이가 충분히 길면 같은 태그 값을 갖는 서로 다른 두 개의 메시지를 찾는 일이 매우 어려워지며, 해시 함수의 특성상 일방향성을 갖기 때문에 생성된 태그로부터 원본 메시지를 숨길 수 있다.

2.2 아두이노 우노

아두이노는 마이크로프로세서와 입출력 모듈이 하나의 칩으로 만들어져 특정한 기능을 수행할 수 있는 작은 임베디드 장치이다. 오픈 소스에 기반을 두고 있으며, 다수의 센서나 스위치로부터 데이터를 수신하고, 보드에 연결된 장치들을 통제함으로써 물리적인 환경과 상호작용하는 기기를 비교적 쉽게 개발할 수 있다. 아두이노의 기본이 되는 모델은 아두이노 우노(Arduino UNO)이며, 성능에 영향을 주는 마이크로프로세서의 종류와 메모리의 크기, 입출력 핀의 개수 등의 따라 다양한 시리즈가 존재한다.

아두이노 우노는 ATmega328P 마이크로프로세

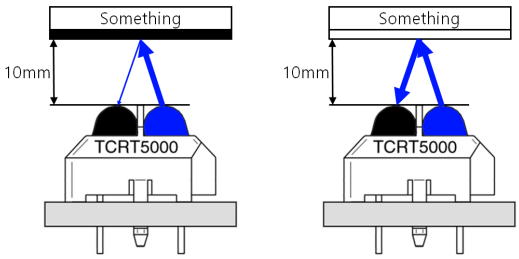

Fig. 1. The principles of TCRT5000. The TCRT5000 classifies the black and white by detecting reflection of infrared rays

서, 6개의 아날로그 입력 핀, 14개의 디지털 입출력 핀 그리고 32KB의 플래시 메모리 등으로 구성되어 있으며, USB 포트가 있기 때문에 USB 케이블을 이용해서 컴퓨터와 연결하여 프로그래밍이 가능하다[9]. 또한, 조도센서, 적외선센서, 와이파이 쉴드 같은 대부분의 컴포넌트 및 쉴드는 아두이노 우노와 호환이 되며, 사물인터넷(IoT, Internet of Things) 분야에서 많이 사용되는 모델이다.

2.3 TCRT5000 센서

TCRT5000 센서는 사물의 검은색과 흰색을 구별할 수 있는 적외선 센서로, 라인을 따라서 움직이는 라인 트레이서에서 선과 배경을 구분하기 위해 사용된다. TCRT5000 센서는 파란색 원형의 발광부와 검은색 원형의 수광부 그리고 음극 전류, 양극 전류, 저항, 입력 핀과 연결시켜야하는 4개의 다리로 구성되어 있다[10].

TCRT5000 센서는 Fig. 1.과 같이 동작한다. 우선 파란색의 발광부에서 10mm 이내 거리에 있는 사물에 적외선을 발산하면, 검은색의 수광부가 사물에 부딪혀 나온 적외선을 감지하여 빛의 양을 측정한다. 이때, 사물이 검은색이라면 적외선을 거의 반사하지 못하고, 사물이 흰색이라면 적외선을 잘 반사하는데, 이 차이를 이용하여 검은색과 흰색을 구별한다. 이 연구에서는 종이에 출력된 바코드를 스캔하기 위하여 디지털 인감에 TCRT5000 센서를 부착하였다.

2.4 보안카드

보안카드란 온라인 뱅킹으로 돈을 이체하려 할 때 사용자 본인을 확인하기 위한 보안 수단이며, 은행에

Fig. 2. The security card used in online banking

따라 다르지만 보통 10자리의 일련번호와 4자리의 번호 30여개로 이루어져 있다[Fig. 2.].

보안카드의 일련번호는 사용자와 보안카드를 1:1로 연결해주는 역할을 하며, 4자리의 번호 30개는 보안카드의 일련번호와 보안카드 번호 생성 알고리즘에 의해 생성되어 온라인 뱅킹시 본인여부를 확인할 때 쓰이게 된다.

보안카드를 사용하려면 우선 사용자는 직접 은행에 방문하여 대면인증을 통해 보안카드를 발급받는다. 이후 은행 웹사이트에 로그인하여 발급받은 보안카드의 일련번호와 웹사이트에서 요구하는 보안번호를 올바르게 입력함으로써 비대면 거래를 위한 비밀을 검증받는다. 사용자는 온라인 뱅킹으로 계좌 이체 등의 서비스를 이용할 때 공인인증서와 계좌 비밀번호뿐만 아니라 소유하는 형태의 비밀인 보안카드를 이용함으로써 비대면 거래를 위한 사용자 인증을 수행할 수 있게 된다[2].

하지만 보안카드의 번호는 고정되어 있으므로 장시간의 스니핑, 키로깅, 모니터링 등의 공격을 통해 유출될 수 있으며, 사용자의 부주의로 인한 사본의 생성이 가능하다는 보안 취약점이 있다. 뿐만 아니라 피싱(Phishing), 파밍(Pharming) 공격에 매우 취약하여[2] 보안 카드를 이용한 비대면 인증 기술은 가장 낮은 수준의 인증 수단으로 평가되고 있다.

2.5 일회용 비밀번호

일회용 비밀번호(OTP, One Time Password)는 일정 주기마다 일회성의 비밀번호를 생성하여 인증을 하는 보안 수단으로, 동일한 비밀번호의 반복적 사용으로 인한 보안 취약점을 해결할 수 있는 인증 수단이다. OTP는 보안카드보다 높은 수준의 비대면

Fig. 3. The OTP generator used in online banking

인증 도구이지만 제작비용이 보안카드보다 높아 사용자가 유료로 구입해야한다. 일회용 비밀번호를 사용하기 위해서는 은행에서 직접 Fig. 3.과 같은 일회용 비밀번호 생성기를 구입하고 온라인 뱅킹 웹사이트에서 인증 받아야한다.

일회용 비밀번호 생성기는 발급하는 은행마다 다르지만 보통 앞면에는 일회용 비밀번호를 생성하는 버튼과 6자리의 일회용 비밀번호가 출력되는 LCD로, 뒷면에는 10자리의 일련번호로 구성되어 있으며, 내부에는 작은 컴퓨터와 시계가 내장되어 있다. 일련번호는 사용자와 일회용 비밀번호 생성기를 1:1로 연결해주는 역할을 하고, 작은 컴퓨터는 일회용 비밀번호 생성 알고리즘과 내장된 시계를 이용하여 30초 또는 1분 간격으로 변하는 동시에 서버와 동기화가 되는[11] 일회용 비밀번호를 생성한다.

OTP는 장치의 특성상 피싱이나 파밍 공격을 당해도 짧은 시간 동안에만 그 비밀이 유효하기 때문에 공격자가 사용자의 비밀을 훔치고, 이를 나중에 이용하는 일은 굉장히 어려운 일이다. 보안카드와 OTP 모두 5회 인증 실패시 온라인 뱅킹 이용 금지 상태가 되므로 무작위 공격도 시도하기 어렵다. 하지만 OTP의 인증은 비밀을 소지하고 있다는 사실만을 인증할 수 있으며, 온라인 뱅킹의 이체 내용과는 무관하기 때문에 또 다른 공격에 의하여 무력화될 수 있다. Fig. 4.는 MITB(Man-In-The-Browser) 공격을 통하여 OTP를 사용하는 경우라도 온라인 뱅킹 이체가 조작될 수 있음을 보인다.

맹영재 등은 피싱이나 파밍 등의 공격 없이 국내 모 은행 사이트에서 MITB 공격으로 일회용 비밀번호를 무력화시키는 것을 증명해보였으며, 최근 이 취약점을 이용한 실제 온라인 뱅킹 이체 해킹 사고가 발생하기도 하였다[5, 6]. 이뿐만 아니라 일회용 비밀번호는 MITM(Man In The Middle)과 리버스 엔지니어링을 이용하여 공격하는 방법 또는 PC 환경을 이용하는 MITPC(Man In The PC) 공격에 대하여 취약점을 가지고 있다[12]. 현재 이러한 취약점을 보완하기 위하여 온라인 뱅킹의 이체 내용이 포함된 SMS, ARS인증 기법이 사용되고 있다.

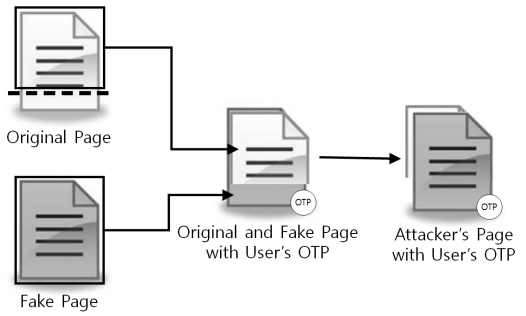

Fig. 4. The concept of MITB(Man-In-The-Browser) attack

III. 디지털 인감

이 논문에서 제안하는 디지털 인감은 적은 비용으로 제작 가능한 소형의 장치로, 온·오프라인에서 인감의 역할을 대신할 수 있는 인증도구이다. 디지털 인감은 종이에 출력된 바코드를 스캔하고, 스캔된 데이터와 HMAC으로 계산된 태그를 출력한다.

3.1 바코드

Fig. 5.는 디지털 인감이 스캔할 수 있는 바코드의 예시이다. 36×35 픽셀의 크기를 갖는 흰색 또는 검은색 셀을 가로 8개, 세로 27개로 출력하여 하나의 의미 있는 데이터를 구성한다. 이는 8개의 TCRT5000 센서를 이용할 때 A4용지 한 장으로 스캔할 수 있는 최대 크기의 바코드 데이터로, 센서의 크기가 작아진다면 동일한 공간에 더 많은 데이터를 담을 수 있을 것으로 기대된다.

검은색 셀은 1을, 흰색 셀은 0을 의미하며, 어떠한 데이터를 이진으로만 변환시킬 수 있다면 Fig. 5.와 같은 바코드로 표현할 수 있다.

8개의 셀로 구성된 한 줄의 바코드는 하나의 의미

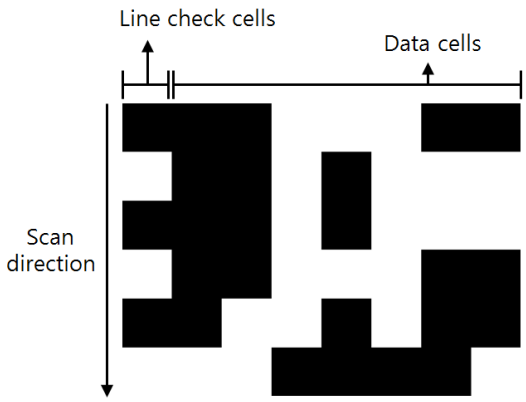

Fig. 5. Example of barcode consists of Line check cells and Data cells also user can scan this barcode lengthwise by using digital legal seal

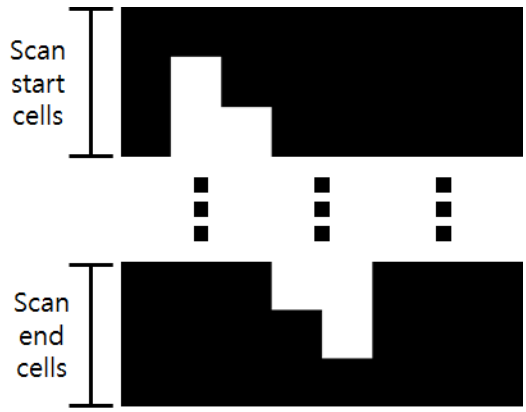

Fig. 6. Start/end signals for scanning

있는 데이터를 구성하며, TCRT5000 센서 8개를 동시에 이용하여 해당 데이터를 디지털 인감에서 입력받는다.

예를 들어, Fig. 5.의 첫 번째 줄은 데이터 11100011을 의미한다. 디지털 인감은 계속해서 세로 방향으로 바코드를 스캔하는데, 이 때 바코드의 첫 번째 셀을 검은색과 흰색이 반복되도록 구성함으로써 디지털 인감으로 하여금 바코드 데이터의 변경을 감지할 수 있도록 설계하였다. 따라서 실제 의미 있는 데이터는 첫 번째 셀을 제외한 7개 셀로 표현된다. 또한, 디지털 인감이 데이터의 시작과 끝을 정확히 인식할 수 있도록 바코드의 제일 위 3줄과 맨 마지막 3줄을 Fig. 6.과 같이 설계하였다. 즉, 디지털 인감의 스캔 결과가 11111111, 10111111, 10011111로 연속되면 그 다음 바코드부터 데이터로 받아들이고, 11100111, 11110111, 11111111이 연속적으로 스캔되면 데이터가 모두 입력되었다고 간주한다.

Table 1. ASCII code and binary data about integer and character

Int, Char	ASCII code	Binary data
0~9	48~57	110000~111001
a~z	97~122	1100001~1111010
A~Z	65~90	1000001~1011010

27줄의 바코드 중 시작과 끝을 감지하는 부분을 제외하면 실제 데이터는 21줄의 바코드로 표현되며, 첫 번째 셀은 데이터 변경 감지 셀이므로, 프로토타입에서 A4 용지 한 장에 표시할 수 있는 의미 있는 데이터는 147bit의 범위 내로 표현될 수 있다.

영어 알파벳과 숫자는 Table 1.과 같이 7비트 이내의 아스키코드로 표현 가능하므로 영문, 숫자로 구성된 어떠한 데이터를 바코드로 출력할 때에는 해당 문자를 아스키코드로 변환하고, 이를 이진수로 변환하여 1이면 검은색 셀로, 0이면 흰색 셀로 표현한다. 별도의 출력 양식을 정하지 않는 경우 한 줄당 하나의 의미 있는 데이터로 구성하여 21글자까지 표현할 수 있다. 하지만 숫자의 경우 6비트로 하나의 데이터를 표현할 수 있으므로, 사전에 데이터의 출력 형식을 약속한다면 숫자로만 구성된 데이터는 24글자까지도 표현 가능하며, 숫자와 영문을 혼합하여 숫자 19글자와 영문 4글자처럼 혼합형 데이터도 표현 가능하다.

3.2 디지털 인감의 구성 요소

디지털 인감은 Fig. 5.와 같은 바코드를 스캔하여, 바코드가 의미하는 데이터와 그 데이터에 의해 생성된 HMAC의 태그를 출력해주는 도구이다. 디지털 인감의 프로토타입은 아두이노 우노, 8개의 TCRT5000 센서, 1602 LCD, 2개의 400홀 브레드보드, 9V 배터리로 구성되어 있다.

Fig. 7.은 디지털 인감의 구성도이며, 왼쪽 브레드보드에 부착된 8개의 TCRT5000 센서들은 8×27의 바코드를 세로 방향으로 스캔할 수 있다. 스캔한 데이터는 아두이노 우노로 전송된다. 디지털 인감은 HMAC을 위한 비밀키를 가지고 있다고 가정한다. 디지털 인감은 스캔한 데이터를 숫자 또는 영문으로

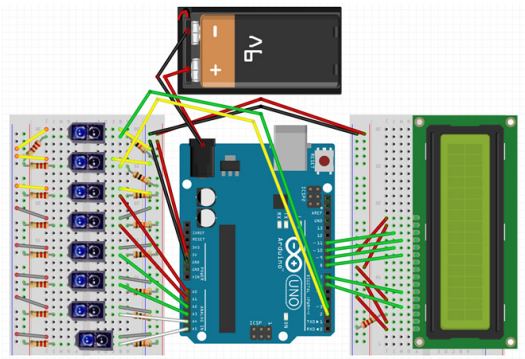

Fig. 7. Setup of our digital legal seal

변환하고, 이를 HMAC의 입력으로 받아 태그를 출력한다.

디지털 인감은 Fig. 7.의 1602 LCD와 같은 디스플레이 장치를 가지며, 데이터 스캔이 종료되면 HMAC의 태그를 출력한다. 프로토타입의 디지털 인감은 9V 배터리로부터 전원을 공급받도록 구성하여 휴대성을 갖도록 하였다. 또한 Fig. 8.과 같이 아크릴판을 이용해 외관을 감싸 다루기 쉽게 제작하였다.

Fig. 8.의 우측 사진은 8개의 TCRT5000 센서가 배치된 모습을 보여준다. 가장 우측 센서는 다른 센서들과 다르게 약간 위쪽에 둠으로써 바코드의 데이터가 변경됨을 나중에 감지할 수 있도록 하였다.

만약 8개의 TCRT5000 센서가 일렬로 되어 있으면서 사용자가 비뚤어진 각도로 바코드를 스캔한다면 가장 우측 센서는 데이터가 변경되었다고 인식하지만, 실제 나머지 센서들은 아직 이전 데이터를 스캔하는 경우가 발생할 수 있다. 이러한 잘못된 스캔 실수는 Fig. 8.과 같이 센서를 배치함으로써 사용자의 실수를 미연에 방지할 수 있다.

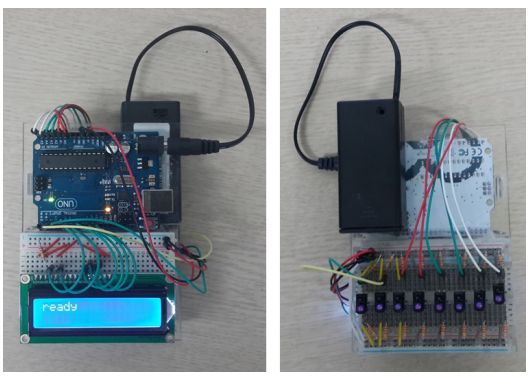

Fig. 8. Real setup of our digital legal seal

3.3 데이터 표시 형식

Fig. 9.는 "jchh1234987654321150716"이라는 데이터를 바코드 형태로 종이에 출력한 후, 디지털 인감으로 스캔하는 과정과 그 결과를 보여주는 사용 예시이다. 바코드 데이터는 "jchh 1234 987654321 150716"로 출력되고 그 데이터로부터 생성된 HMAC의 태그 중 앞 5글자인 "1546c"가 출력된다.

디지털 인감은 사용 목적에 따라 147bit 이내에서 영문(7bit)과 숫자(6bit)를 몇 글자씩 이용할 것인지 결정하고, 디스플레이 장치에서 최대로 표현 가능한 글자 수를 고려하여 설계해야한다. 예를 들어, Fig. 9.의 데이터 표시 형식은 1602 LCD의 최대 출력 글자 수인 32자를 고려하여 스캔 후 바코드 데이터와 HMAC의 태그의 앞 5글자를 출력하도록 설계한 것이다.

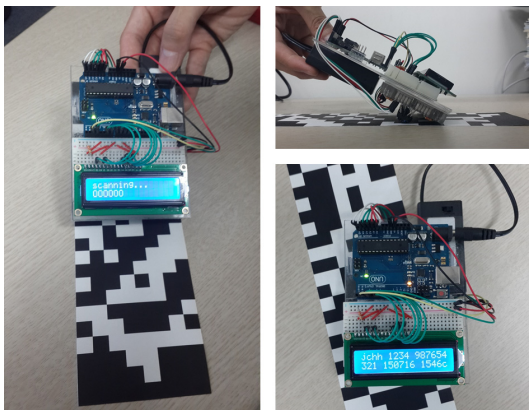

Fig. 9. Scanning method. Scanning digital legal seal from the start to end of barcode

3.4 스캔 보조대

디지털 인감은 사용자가 정확한 바코드를 스캔 능력을 요구한다. Fig. 10.은 아크릴판으로 제작된 스캔 보조대로, 사용자의 정확한 바코드 스캔을 돕는다. 하부판이 바코드출력물과 상부판을 고정하도록 제작되었으며, 상부판은 가이드를 설치하여 사용자가 쉽게 직선으로 바코드를 스캔할 수 있도록 하였다. Fig. 11.은 스캔 보조대를 이용하여 바코드를 스캔

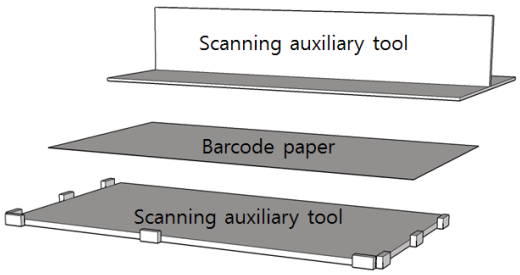

Fig. 10. Scanning auxiliary tool

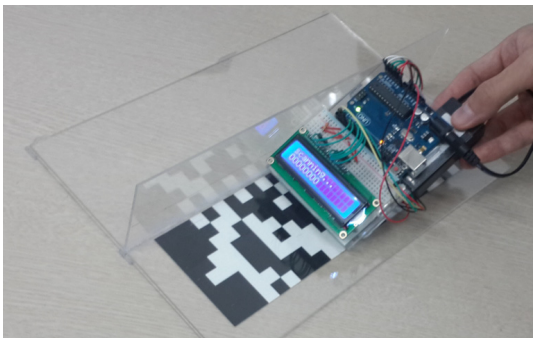

Fig. 11. The scanning auxiliary tool for improving success rate

하는 과정을 보여준다.

3.5 디지털 인감의 사용 방법

이 논문에서 제안하는 디지털 인감이 사용되는 과정은 다음과 같다. 우선, 온라인 뱅킹 계좌 이체 등의 데이터로부터 생성된 바코드를 종이에 출력하고 이를 스캔 보조대에 결합한다. 이 때, 디지털 인감은 서버와 사전에 공유된 비밀키를 가진다고 가정한다. 사용자가 디지털 인감을 이용하여 바코드를 스캔하면, 스캔된 데이터와 HMAC의 태그가 디스플레이 장치에 출력된다. 사용자는 디스플레이 장치에 표시된 데이터를 확인하고, 데이터를 올바르게 스캔한 것이 확인되면 온라인 뱅킹 계좌 이체 등의 내용에 대한 무결성을 보장하거나, 사용자를 인증하기 위한 목적으로 사용할 수 있다.

IV. 디지털 인감의 사용 방안

4.1 사용자 편의성 실험

이 논문에서 제안하는 디지털 인감은 사용자가 바코드를 정확하게 스캔해야지만, 올바른 바코드의 데이터와 HMAC의 태그가 출력된다. 우리는 디지털 인감과 스캔 보조대를 이용하여 사용자들이 편리하게 사용할 수 있는지에 대한 실험을 진행하였다. 실험은 3명의 피험자에게 디지털 인감과 스캔 보조대를 이용하여 연속으로 10번씩 스캔하게 하였으며, 우리는 스캔 성공률과 스캔하는 시간을 측정하여 사용자 편의성을 검토하였다.

Table 2.는 실험 결과이다. 피험자 1은 10번 중 9번을 제대로 스캔하였으며 스캔을 하는데 걸린 평균 시간은 2.3초였고, 피험자 2는 10번 모두 제대로 스캔하였으며 스캔 평균 시간은 2.5초 그리고 피험자 3은 10번 중 8번을 올바르게 스캔하였고 스캔 평균 시간은 3.5초였다. 우리는 이러한 실험을 통해서 평균 성공률 90%, 평균 스캔 시간 2.8초라는 결과를 얻을 수 있었고, 그로인해 사용자들이 사용하는데 그리 큰 불편함이 있지 않은 것을 확인할 수 있었다. 그렇지만 평균 성공률 90%라는 것은 10%의 확률로 오류가 발생할 수도 있으며, 사용자들이 사용하는데 어느 정도의 불편함이 존재한다는 의미이다. 우리는 이러한 불편함을 해소하기 위하여, 성공률 향상과 스캔 시간 단축에 대한 연구는 추후 연구로 남긴다.

Table 2. Results of user convenience experiments

	Success rate	Average time
Subject 1	90%	2.3sec
Subject 2	100%	2.5sec
Subject 3	80%	3.5sec

4.2 디지털 인감을 이용한 비대면 거래

HMAC은 공유된 비밀키를 이용하여 메시지에 대한 태그를 생성한다. 따라서 디지털 인감을 비대면 거래에 활용하려면 우선 금융기관 등과 사전에 비밀키를 공유해야한다.

4.2.1 디지털 인감의 발급 과정

디지털 인감은 제작될 때 일련번호를 부여받고 일련번호와 매칭되는 임의의 비밀키를 내장한다. 금융기관은 일련번호와 비밀키를 안전하게 등록하고 관리한다고 가정한다. 금융기관이란 개별 은행이나 증권사가 될 수 있으며, 현재의 OTP통합인증센터와 유

사하게 디지털 인감 통합인증센터 등에서 디지털 인감의 제작, 등록 관리를 대행할 수도 있다.

사용자는 금융기관에 방문하여 디지털 인감의 발급을 요청한다. 금융기관은 대면 인증을 통하여 사용자의 신원을 확인하고 디지털 인감을 발급해준다. 금융기관은 사용자 식별자와 사용자에게 발급된 디지털 인감의 일련번호를 안전한 방법으로 전산망에 저장한다. 사용자는 디지털 인감에 저장된 비밀키를 명시적으로 알 필요는 없으며, 디지털 인감으로부터 비밀키를 추출하는 것은 어렵다고 가정한다.

사용자는 PC를 통해 금융기관의 웹사이트에 로그인하여 대면 인증을 통해 발급받은 디지털 인감의 일련번호와 초기 메시지에 대한 인증 태그를 입력한다. 초기 메시지는 이름, 금융기관, 날짜 등을 포함하여 구성될 수 있다.

금융기관의 서버는 로그인한 사용자의 아이디와 입력된 일련번호, 메시지, 메시지에 대한 인증 태그를 수신한다. 사용자가 금융기관에 방문하여 디지털 인감을 발급받을 당시의 사용자 식별자와 일련번호가 웹사이트를 통해 입력받은 사용자의 사용자 식별자, 일련번호와 일치하는지 확인하고, 메시지에 대한 HMAC 태그의 일치여부도 확인하여 이상이 없을시 디지털 인감의 등록 과정을 마친다.

4.2.2 디지털 인감을 이용한 비대면 거래의 인증

현재 국내에서 이용되는 비대면 거래 인증 수단인 보안카드나 OTP는 사용자가 해당 비밀을 소지하고 있다는 사실에 대한 인증 기능을 가능하지만, 비대면 거래의 내용에 대한 인증 기능은 제공하지 않는다 [3].

디지털 인감에서 생성하는 HMAC의 태그는 거래 내용에 기반을 두므로 비대면 거래 내용에 대한 인증이 가능하며 데이터의 무결성도 보장된다. 디지털 인감의 비밀키는 대칭키이므로 디지털 인감 자체로는 부인방지의 기능을 제공하기 어려우나, 공인인증서를 이용하여 거래 내용과 HMAC 태그를 확인하고, 이에 대해 전자서명을 함으로써 부인방지의 기능을 수행할 수 있을 것으로 기대한다.

Fig. 12.는 금융기관 중 하나인 은행에서 제공하는 온라인 뱅킹으로 계좌 이체를 하는 과정에 대한 보다 구체적인 사용 예시이다. 이 논문은 디지털 인감의 아이디어와 프로토타입 제작을 통한 실현 가능성 검토에 중점을 두므로, 프로토타입 디지털 인감의

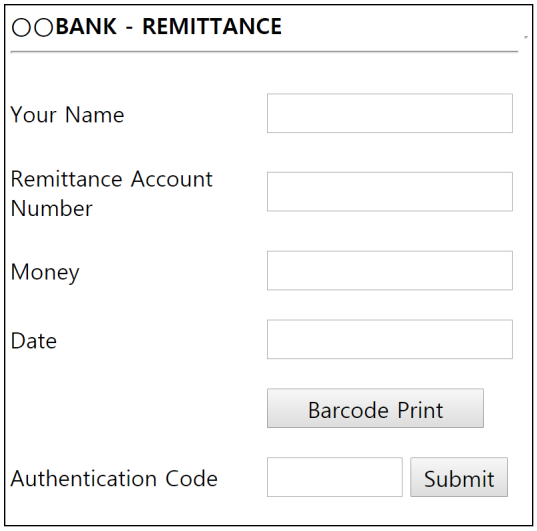

Fig. 12. The example of online banking site for using digital legal seal

크기에서 비롯되는 한계를 고려하여 메시지의 길이와 그 과정을 축약하여 설명한다.

사용자는 온라인 뱅킹 계좌 이체 페이지에서 본인의 이름(영문 네 자리), 수신자의 계좌번호(숫자 네 자리), 금액(숫자 아홉 자리), 날짜(숫자 여섯 자리)를 입력하고 바코드를 출력한다. 그리고 디지털 인감을 이용하여 바코드를 스캔함으로써 총 영문 4자리, 숫자 19자리의 데이터와 HMAC의 태그를 디지털 인감의 디스플레이 장치를 통하여 확인한다. 표시된 내용에 문제가 없을 경우 다섯 자리로 표현되는 HMAC의 태그를 '인증 코드'란에 입력한다.

Fig. 13.은 디지털 인감을 이용한 온라인 뱅킹 계좌 이체 중 이체 내용의 인증에 대한 프로세스를 보여준다. 예를 들어, 송신자의 이름은 "jchh", 수신자의 계좌번호는 "1234", 금액은 "987654321", 날짜는 "150716"이라 하자. 사용자는 위의 정보를 입력 후 'Barcode Print' 버튼을 눌러 입력된 데이터를 바코드 형태로 출력한다. 그리고 스캔 보조대를 이용하여 Fig. 14.처럼 바코드를 디지털 인감으로 스캔하면 입력한 계좌 이체 정보와 그 정보로 만들어진 HMAC 태그의 앞 다섯 글자 "1546c"가 출력된다. 이 값을 Fig. 12. '인증 코드'란에 입력한 뒤 'Submit' 버튼을 눌러 은행의 서버로 전송한다.

은행의 서버는 로그인한 사용자의 사용자 식별자, 식별자와 매칭되는 일련번호, 일련번호와 매칭되는 비밀키를 조회할 수 있으며, 사용자로부터 수신한 온

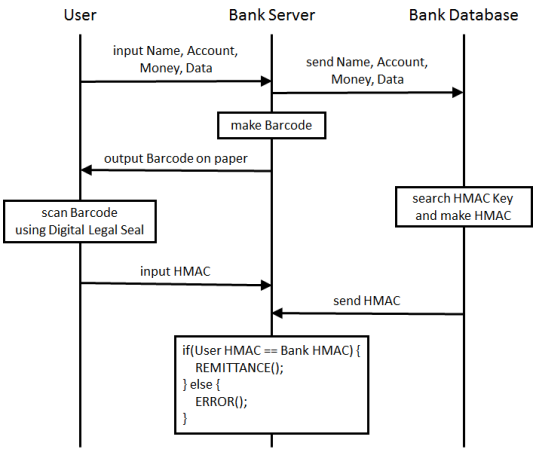

Fig. 13. The process of online banking transfer using digital legal seal

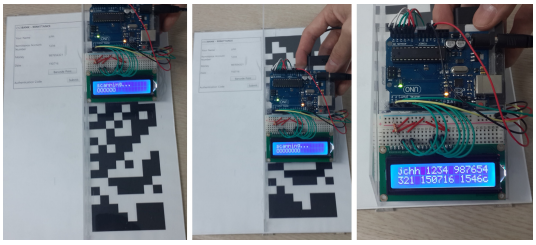

Fig. 14. The applying of digital legal seal on online banking

라인 뱅킹 계좌 이체 정보에 대하여 HMAC을 계산할 수 있다. 은행의 서버에서 계산한 태그와 수신된 태그의 일치 여부를 확인함으로써 사용자가 대면 인증을 통하여 발급 받은 디지털 인감을 소지하고 있으며, 온라인 뱅킹 계좌 이체에 대한 내용을 확인하고 이를 요청하였다고 가정할 수 있다. 태그가 일치하는 경우, 은행의 서버는 사용자의 요청에 따라 비대면 온라인 뱅킹 계좌 이체 업무를 수행할 수 있을 것이다. 송신자의 계좌번호, 계좌비밀번호, 공인인증서와 전자서명 및 부인방지에 대한 내용은 이 논문의 요지를 벗어나므로 생략한다.

4.3 디지털 인감을 이용한 차용증 공증

디지털 인감은 비대면 거래뿐만 아니라 차용증 공증에 활용될 수 있다. HMAC은 공유된 비밀키를 이용하여 메시지에 대한 태그를 생성한다. 따라서 디지털 인감을 차용증 공증에 활용하려면 우선 정부 표준 차용증 관리 시스템과 사전에 비밀키를 공유해야 한다.

4.3.1 디지털 인감의 발급 과정

디지털 인감은 제작될 때 일련번호를 부여받고 일련번호와 매칭되는 임의의 비밀키를 내장한다. 정부 표준 차용증 관리 시스템은 안전하게 차용증을 관리해주는 시스템의 예시이며, 모든 차용증은 정부에서 관리한다고 가정한다. 또한 이 시스템은 신뢰할 수 있는 시스템이며, 디지털 인감의 일련번호와 비밀키를 안전하게 등록 및 관리하고, 관리되는 디지털 인감 정보를 이용하여 스스로 차용증 발급 등 부정한 행위를 하지 않는다고 가정한다.

사용자는 정부행정기관에 방문하여 디지털 인감의 발급을 요청한다. 정부행정기관은 대면 인증을 통하여 사용자의 신원을 확인하고 디지털 인감을 발급해준다. 그리고 사용자 식별자와 사용자에게 발급된 디지털 인감의 일련번호를 안전한 방법으로 전산망에 저장한다. 사용자는 디지털 인감에 저장된 비밀키를 명시적으로 알 필요는 없으며, 디지털 인감으로부터 비밀키를 추출하는 것은 어렵다고 가정한다.

사용자는 PC를 통해 차용증 관리 시스템에 로그인 하여 정부행정기관으로부터 대면 인증을 통해 발급받은 디지털 인감의 일련번호와 초기 메시지에 대한 인증 태그를 입력한다. 초기 메시지는 이름, 주민등록번호, 날짜 등을 포함하여 구성될 수 있다.

정부 표준 차용증 관리 시스템은 로그인한 사용자의 아이디와 입력된 일련번호, 메시지, 메시지에 대한 인증 태그를 수신한다. 그리고 사용자가 정부행정기관에 방문하여 디지털 인감을 발급받을 당시의 사용자 식별자와 일련번호를 정부행정기관으로부터 전달받아 입력받은 사용자의 사용자 식별자, 일련번호와 일치하는지 확인하고, 메시지에 대한 HMAC 태그의 일치여부도 확인하여 이상이 없을시 디지털 인감의 등록 과정을 마친다.

4.3.2 디지털 인감을 이용한 차용증 공증

디지털 인감에서 생성하는 HMAC의 태그는 차용증 정보에 기반을 두므로 차용 정보에 대한 공증이 가능하며 데이터의 무결성도 보장되므로 차용사실증명 또한 가능하다.

Fig. 15.는 정부 표준 차용증 관리 시스템의 구체적 사용 예시이다. 채무자는 정부 표준 차용증 관

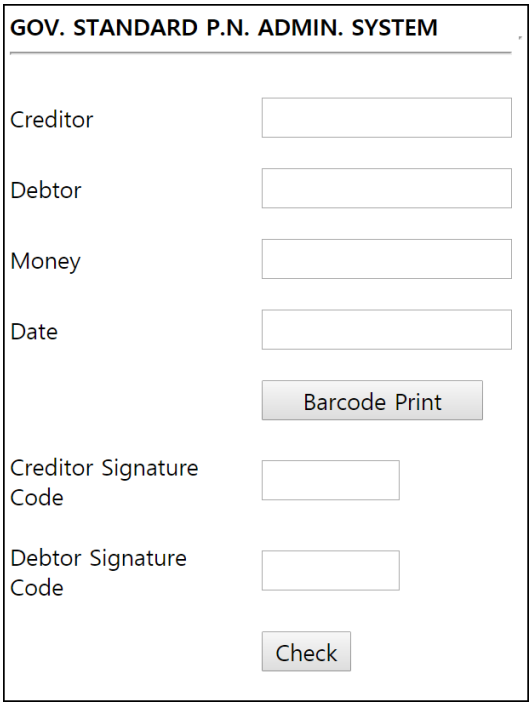

Fig. 15. The example of government standard promissory note administration system for using digital legal seal

리 시스템에서 채권자의 이름(영문 네 자리), 본인의 이름(영문 네 자리), 금액(숫자 아홉 자리), 날짜(숫자 여섯 자리)를 입력한 뒤 입력한 차용 정보와 바코드가 나와 있는 차용증을 출력한다. 그리고 채무자는 자신의 디지털 인감으로 바코드를 스캔한 다음 출력된 HMAC의 태그를 차용증 '채무자 서명 코드'란에 수기로 작성한 뒤 채권자에게 넘겨준다. 채권자는 차용증을 넘겨받아 자신의 디지털 인감으로 바코드를 스캔한 다음 출력된 HMAC의 태그를 차용증 '채권자 서명 코드'란에 수기로 작성하여 차용증 작성을 완료하고 보관한다.

차용증 작성 완료 후 채권자가 차용사실증명을 확인하기 위해서는 보관하고 있던 차용증을 가지고 정부 표준 차용증 관리 시스템에 접속한다. 그리고 차용증에 나와 있는 채권자 성명, 채무자 성명, 금액, 날짜, 채권자 서명 코드, 채무자 서명코드를 입력한다.

Fig. 16.은 디지털 인감을 이용하여 차용증 작성과 차용사실증명에 대한 프로세스를 보여준다. 예를 들어, 채권자의 이름은 "jchh", 채무자의 이름은 "sshh", 금액은 "987654321", 날짜는 "150716"이라

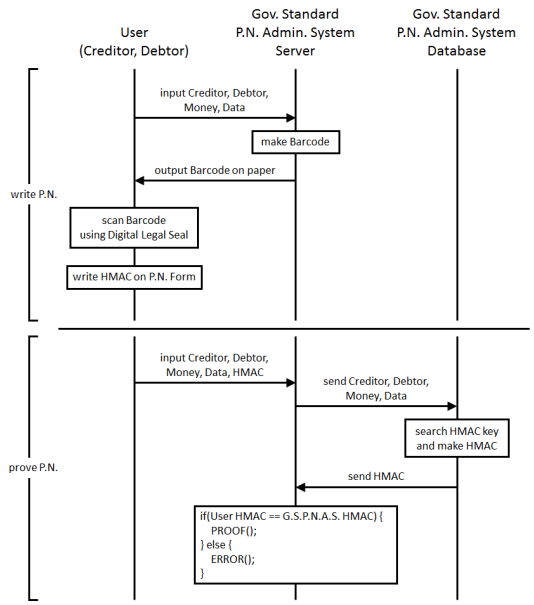

Fig. 16. The process of promissory note notarization using digital legal seal

하자. 채무자는 위의 정보를 입력 후 'Barcode Print' 버튼을 눌러 입력된 데이터와 바코드가 나와 있는 차용증을 출력한다. 그리고 Fig. 17.처럼 자신의 디지털 인감으로 바코드를 스캔한 다음 출력된 HMAC의 태그를 '채무자 서명 코드'란에 수기로 작성한 뒤 채권자에게 넘겨준다. 채권자는 차용증 넘겨받아 자신의 디지털 인감으로 바코드를 스캔한 다음 출력된 HMAC의 태그를 차용증 '채권자 서명 코드'란에 수기로 작성하여 차용증 작성을 완료하고 보관

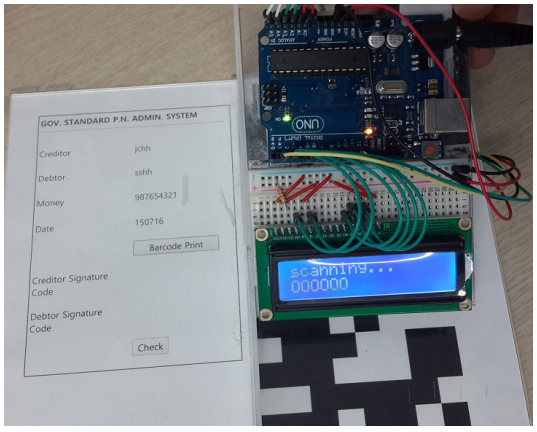

Fig. 17. The applying of digital legal seal on promissory note

한다.

차용증 작성 완료 후 채권자가 차용사실증명을 확인하기 위해서는 차용증에 나와 있는 정보와 채권자와 채무자의 서명 코드를 정부 표준 차용증 관리 시스템에 접속하여 입력한다. 정부 표준 차용증 관리 시스템은 정부행정기관을 통해 입력받은 채권자와 채무자의 식별자, 식별자와 매칭되는 일련번호, 일련번호와 매칭되는 비밀키를 조회할 수 있으며, 채권자로부터 수신한 차용정보에 대하여 HMAC을 계산할 수 있다. 정부 표준 차용증 관리 시스템은 계산한 태그와 채권자로부터 수신한 채권자와 채무자 태그의 일치 여부를 확인함으로써 채권자와 채무자가 대면 인증을 통하여 발급 받은 디지털 인감을 소지하고 있으며, 차용정보에 대한 내용을 확인하고 차용사실증명을 요청하였다고 가정할 수 있다. 태그가 일치하는 경우, 정부 표준 차용증 관리 시스템은 사용자의 요청에 따라 차용 사실을 증명하여 사용자에게 알려줄 수 있을 것이다.

4.4 평가

온라인 뱅킹에서 디지털 인감을 사용할 때에 생성되는 HMAC 태그는 정해져 있는 것이 아니며, 바코드 데이터인 계좌 이체 정보에 따라 달라진다. 그렇기 때문에, 공격자는 장시간의 스니핑 또는 피싱, 파밍으로 사용자의 HMAC 태그를 수집했어도, 사용자가 다음에 사용할 이체 정보를 예측하기 어려우므로 HMAC 태그를 알아내기 어렵다. 이를 통하여 온라인 뱅킹에서 쓰이는 보안카드의 취약점을 보완할 수 있게 된다.

사용자는 계좌 이체 정보 등을 바코드로 변환하여 프린트한 다음, 비밀키가 저장되어 있는 디지털 인감으로 스캔하여 HMAC 태그를 생성한다. 이 과정을 통해 우리는 공격자로부터 비밀키를 안전하게 보호할 수 있다. 만약 디지털 인감을 사용하지 않고, 비밀키를 컴퓨터에 저장 후 컴퓨터 자체에서 HMAC 태그를 생성하는 방법이라면, 공격자가 온라인을 통해 컴퓨터에 접속하여 사용자의 비밀키를 탈취할 수 있는 가능성이 있다. 그로인해 공격자가 비밀키를 이용해서 자신이 원하는 메시지에 대한 HMAC을 생성하는 등의 보안적 문제가 발생할 수 있다. 그러나 디지털 인감은 어떠한 서버와 통신을 하고 있는 것이 아니며, 사용할 때에 USB를 이용하여 컴퓨터와 연결을 할 필요가 없기 때문에, 원격지에 존재하는 공격자가 디지털 인감 내부의 HMAC의 비밀키를 원격으로 탈취하는 것을 어렵다. 따라서 비밀키는 공격자로부터 안전하게 보호 될 수 있다.

HMAC 태그는 온라인 뱅킹에서 사용자가 입력한 이체 정보에 의해 생성 된다. 만약 사용자가 이체 정보를 입력한 뒤 프린터로 출력하기 전에 공격자의 MITB 공격으로 이체 정보가 변경된다면, 사용자는 변경된 이체 정보로 만들어진 바코드를 출력하게 된다. 사용자가 그 바코드를 디지털 인감으로 스캔하게 되면 자신이 입력한 이체 정보가 아닌 공격자에 의해 변경된 이체 정보가 디지털 인감에 출력되므로 공격 여부를 쉽게 알아챌 수 있을 것이다. 뿐만 아니라 올바른 이체 정보로 만들어진 바코드를 디지털 인감으로 스캔하여 HMAC 태그를 생성한 후에 공격자로부터 MITB 공격으로 이체 정보가 변경되었다면, 은행은 올바른 HMAC 태그와 공격자의 이체 정보로부터 생성한 HMAC 태그의 일치 여부를 확인하여 서로 다른 경우 이체 요청을 거절 할 것이다. 이러한 과정으로 온라인 뱅킹에서 사용되는 일회용 비밀번호의 취약점을 보완할 수 있게 된다.

이를 통해 비대면 거래의 내용 확인 및 인증 코드를 작성한 뒤 확인된 내용에 대하여 현재의 공인인증서 전자서명 시스템으로 전자 서명한다면 부인방지의 기능까지 제공할 수 있을 것으로 기대된다. 또한 다채널 인증 과정인 ARS, SMS 인증 과정을 대체할 수 있을 것으로 기대된다.

유사하게, 디지털 인감은 온라인 뱅킹뿐만 아니라 차용증 같은 오프라인 문서에도 사용할 수 있으며, 결과적으로 인감의 위조 가능성을 낮출 수 있다. 디지털 인감에서 생성되는 HMAC 태그는 차용 정보에 따라 달라지므로, 한 사용자가 차용증마다 기입하는 HMAC 태그도 달라진다. 그러므로 형태가 하나로 정해져있는 일반 인감에 비해서 위조 당할 가능성이 낮아질 것으로 기대된다.

이 논문에서 제작한 디지털 인감은 프로토타입이며, 약 4만원의 비용으로 제작되었고 유지비용으로는 배터리 교체 비용만 요구된다. 이러한 비용은 제품화되어 대량생산 시스템이 갖추어졌을 시 상당히 저렴해질 것으로 예상되며, 각종 보안사고와 보안에 대한 중요성이 대두되는 사회분위기상 보안을 위해 충분히 투자할 수 있는 금액이 될 것이라 기대된다.

V. 결 론

디지털 인감은 어떠한 데이터가 들어있는 바코드를 스캔하여, 그 데이터와 HMAC 태그를 출력해주는 도구이다. 이 논문에서는 디지털 인감을 온라인 뱅킹에 적용하면 보안카드와 일회용 비밀번호의 취약점을 보완할 수 있다는 것의 대해서 검토하였다. 그리고 오프라인 차용증에 적용하면 일반 인감보다 위조당하기 어렵다는 것도 검토하였다. 디지털 인감에 대한 사용자 편의성을 높이는 방법, 바코드를 종이로 프린트 하지 않고 모니터에서 바코드 스캔하기 등은 추후 연구 주제로 남기며, 사물인터넷(IoT, Internet of Things) 등의 다양한 분야에서 활용될 것으로 기대된다. 조밀한 구성을 통하여 더 많은 데이터를 담게 되면 이 논문의 예시보다 더 긴 메시지에 대한 인증을 수행할 수 있을 것으로 기대하나, 스캔의 정확도를 높이기 위한 연구도 추가적으로 수행되어야할 것이다.

References

[1] Payment & Settlement Systems Department, "Payment & Settlement Newsletter," http://www.bok.or.kr/contents/total/ko/boardView.action?menuNaviId=109&boardBean.brdid=119573&boardBean.menuid=109, The Bank of Korea, Vol. 2015, No. 8, Aug. 2015.

[2] H. Seo and H. Kim, "Design and Implementation of Physical Secure Card for Financial Security," Journal of the Korea Institute of Information and Communication Engineering, Vol. 19, No. 4, pp. 855-863, Apr. 2015.

[3] H. Lee, "Press Releases," http://www.ofthepeople.kr/bbs/board.php?bo_table=b_0203&wr_id=188, Republic of Korea National Assembly, Sep. 2015.

[4] M. Wu, S. Garfinkel and R. Miller, "Secure Web Authentication with Mobile Phones," DIMACS Workshop on Usable Privacy and Security Software, 2014.

[5] Y. Maeng, D. Shin, S. Kim, D. Nyang and M. Lee, "A Vulnerability Analysis of MITB in Online Banking Transactions in Korea," Internet and Information Security, Vol. 1, No. 2, pp. 101-118, Nov. 2010.

[6] Electronic Finance Division, "Press Releases," http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=&sword=&r_url=&menu=7210100&chk=29613&no=29612, Financial Services Commission, Jan. 2014.

[7] M. Bellare, J. Kilian and P. Rogaway, "The Security of the Cipher Block Chaining Message Authentication Code," Journal of Computer and System Sciences, Vol. 61, Issue 3, pp. 362-399, Dec. 2000.

[8] M. Bellare, R. Canetti and H. Krawczyk, "Keying Hash Functions for Message Authentication," Lecture Notes in Computer Science, Vol. 1109, pp. 1-15, July. 2001.

[9] Arduino UNO, http://www.arduino.cc/en/Main/ArduinoBoardUno

[10] TCRT5000, http://www.vishay.com/docs/83760/tcrt5000.pdf

[11] T. Kim, J. Lee and D. Lee, "Study on Mobile OTP(One Time Password) Mechanism based PKI for Preventing Phishing Attacks and Improving Availability," Korea Institute of Information Security and Cryptology, Vol. 21, No. 1, pp. 15-26, Feb. 2011.

[12] B. Kang and H. Kim, "A study on the vulnerability of OTP implementation by using MITM attack and reverse engineering," Korea Institute of Information Security and Cryptology, Vol. 21. No. 6, pp. 83-99, Dec. 2011.

〈저자소개〉

정 창 훈 (Changhun Jung) 학생회원
2014년 9월~현재: 인하대학교 컴퓨터정보공학과 석사과정
〈관심분야〉 정보보호, 인증 프로토콜, 금융 보안, IoT

신 동 오 (DongOh Shin) 학생회원
2010년 2월: 인하대학교 컴퓨터정보공학과 학사
2012년 2월: 인하대학교 컴퓨터정보공학과 석사
2012년 9월~현재: 인하대학교 컴퓨터정보공학과 박사과정
〈관심분야〉 인터넷 보안, 네트워크 보안, 금융 보안

장 룡 호(RhongHo Jang) 학생회원
2013년 8월: 인하대학교 컴퓨터정보공학과 학사
2015년 8월: 인하대학교 컴퓨터정보공학과 석사
2015년 9월~현재: 인하대학교 컴퓨터정보공학과 박사과정
〈관심분야〉 네트워크 보안, 정보보호, 무선 인터넷 보안

양 대 헌 (DaeHun Nyang) 종신회원
1994년 2월: 한국과학기술원 과학기술대학 전기 및 전자공학과 학사
1996년 2월: 연세대학교 컴퓨터과학과 석사
2000년 8월: 연세대학교 컴퓨터과학과 박사
2000년 9월~2003년 2월: 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재: 인하대학교 컴퓨터정보공학과 교수
〈관심분야〉 암호이론, 암호 프로토콜, 인증 프로토콜, 무선 인터넷 보안

이 경 희 (KyungHee Lee) 정회원
1993년 2월: 연세대학교 컴퓨터과학과 학사
1998년 8월: 연세대학교 컴퓨터과학과 석사
2004년 2월: 연세대학교 컴퓨터과학과 박사
1993년 1월~1996년 5월: LG소프트(주) 연구원
2000년 12월~2005년 2월: 한국전자통신연구원 선임연구원
2005년 3월~현재: 수원대학교 전기공학과 부교수
〈관심분야〉 바이오인식, 정보보호, 컴퓨터비전, 인공지능, 패턴인식

염 흥 열 (Heung-Youl Youm) 종신회원
1981년 2월: 한양대학교 전자공학과 학사 졸업
1983년 9월: 한양대학교 대학원 전자공학과 석사 졸업
1990년 2월: 한양대학교 전자공학과 박사 졸업
1982년 12월~1990년 9월: 한국전자통신연구소 선임연구원
1990년 9월~현재: 순천향대학교 정보보호학과 정교수
1997년 3월~2000년 3월: 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재: 한국정보보호학회 총무이사, 학술이사, 교육이사, 논문지편집위원 위원장, 수석부회장(역), 학회장(역), (현) 명예회장
2005년~2008년: ITU-T SG17 Q9 Rapporteur(역)
2006년 11월~2009년 2월: 정보통신연구진흥원 정보보호전문위원
2009년~현재: ITU-T SG17 부의장/SG17 WP2/WP3 의장
〈관심분야〉 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜