정 보 보 호 학 회 지
제28권 제1호, 2018. 2

스마트 디바이스 상의 안전한 개인식별번호 입력 연구 동향

이 문 규*

요 약

개인식별번호(personal identification number: PIN)는 숫자로 이루어진 짧은 패스워드로서, 은행 ATM, 디지털 도어락, 스마트 디바이스 등에서 사용자 인증을 위해 널리 쓰이고 있다. PIN을 입력하기 위한 전통적인 키패드 방식의 인터페이스는 엿보기나 녹화 등의 공격에 취약하며, 이를 방지하기 위해 다양한 PIN 입력 방식들이 제안된 바 있다. 그러나, 잘못 설계된 PIN 입력 방식은 무작위 대입 공격 등 다른 공격에 대한 안전성이나 사용자 편의성을 떨어뜨릴 수 있다. 이 논문에서는 특히 스마트 디바이스 상에서 PIN을 안전하게 입력하기 위한 다양한 방식들을 조사하고 이들의 특성을 분석함으로써 안전하고 편리한 PIN 입력 방식의 설계를 위한 방향을 제시한다.

Ⅰ. 서 론

사용자 인증은 어떤 시스템의 사용자로 하여금 해당 시스템에 대한 접근 권한을 획득하기 위해 자신의 신원을 증명하게 하는 과정이다. 현재까지 다양한 사용자 인증 방법이 제안되어 왔으나, 이들은 크게 지식 기반 인증(즉, 패스워드와 같이 사용자만이 알고 있는 정보를 확인하는 것), 소유물 기반 인증(ID카드 등과 같이 특정 객체를 소유하고 있는지의 여부를 확인하는 것), 바이오인식(사용자의 신체적 또는 행위적 특성에 기반한 인증) 등으로 구분할 수 있다. 최근 특히 바이오인식에 대한 관심이 높아지고 있으나, 여전히 지식 기반 인증이 널리 쓰이고 있다[1,5]. 숫자로만 이루어진 짧은 패스워드, 즉 개인식별번호(personal identification number: 이하 PIN)는 첫 번째 분류에 속하는 대표적인 인증 방식으로, 전통적으로 은행 자동화기기(ATM)에서 많이 쓰여 왔으며, 디지털 도어락, 스마트 디바이스 등에서도 널리 쓰이고 있다.

그러나 고정된 키패드 배열을 이용하는 전통적인 PIN 입력 방식(이하 Regular PIN)은 사용자가 키패드 상의 PIN 숫자를 직접 누르거나 터치하여 입력하게 함으로써 엿보기 공격(shoulder surfing attack)에 취약하다. 즉, 사용자의 인증 과정을 공격자가 관찰할 경우, 공격자는 이 PIN을 기억하여 사용자의 신원을 가장하고 인증에 성공할 수 있다. 또한, PIN은 보통 4자리 또는 6자리 등의 한정된 범위의 숫자들을 이용하기 때문에[5] 가능한 PIN 집합 내의 후보들을 무작위로 대입해 봄으로써 인증을 시도하는 무작위 대입 공격(random guessing attack) 또한 실질적인 위협이 될 수 있다. 이 논문에서는 이러한 공격들에 대응하여 안전하게 PIN을 입력하는 여러 방법들을 살펴본다.

Ⅱ. 챌린지-응답(challenge-response)에 기반한 PIN 입력 방식

Regular PIN에 대해 엿보기 공격이 가능한 본질적인 원인은 동일한 PIN에 대해 항상 동일한 내용이 입력되기 때문이다. 이러한 문제를 해결하기 위해, 사용자에게 무작위(random)의 챌린지(challenge)를 주고 사용자로 하여금 이 챌린지와 본인의 PIN 정보를 조합하여 응답(response)을 도출하여 입력하도록 하는 방식들이 제안되었다. 이 중 대표적인 것은 2004년 ACM CCS에 제안되었던 Roth, Richter, Freidinger의 방법[2]으로, 그림 1과 같이 Regular PIN 패드의 각 숫자 배경에 무작위로 흰색 또는 검은색의 바탕색을 부여하는 방법이다. 매 입력 시마다 10개 PIN 숫자들 중 시스템에 의해 임

* 인하대학교 컴퓨터공학과 (mklee@inha.ac.kr)

〔그림 1〕 BW PIN 입력 방식〔2〕

의로 선택된 5개는 흰색, 나머지 5개는 검은색의 바탕색이 칠해지며, 사용자는 본인이 입력하고자 하는 PIN 숫자의 배경에 있는 색을 확인한 후 하단의 검은색 또는 흰색 버튼 중 맞는 것을 터치하여 입력을 수행한다. 이 경우 사용자의 입력은 10개의 PIN 숫자들 중 5개와 일치하므로, 유일한 입력 숫자를 결정하기 위해서는 PIN 숫자 한 자리 입력에 4회 반복 작업이 필요하다. 즉, 4자리 PIN 입력에는 16회의 입력이 필요하게 된다. 입력 과정의 특징을 반영하여 이 방법을 Black-and-White 방법(이하 BW PIN)이라 부르기로 하자.

BW PIN의 입력에서는 같은 PIN 숫자라 하더라도 배경색이 흰색이 될 수도, 검은색이 될 수도 있으므로, 같은 PIN에 대한 사용자의 실제 입력값(검은색 또는 흰색의 시퀀스)은 매 입력 세션마다 바뀌게 된다. 이렇게 무작위 챌린지를 이용하는 입력 방법은 BW PIN과 거의 같은 시기에 제안된 Spy-resistant keyboard[3]부터 숫자 이외에 색깔 정보를 PIN의 일부로 추가로 이용하는 ColorPIN[4], 그리고 비교적 최근에 제안된, 기호와 숫자의 무작위 매칭을 이용하는 LinearPIN[8]이나 BW PIN에서 흰색과 검은 색 이외의 다른 입력을 부여한 방

〔그림 2〕 ColorPIN 입력 방식〔4〕

식[9] 등 다양한 방법들이 있다. PIN 입력에 무작위성을 부여한 이러한 방식들은 엿보기 공격 이외에도 스마트 디바이스 상에 남겨진 손자국(smudge)에 대한 이미지 처리를 통해 PIN을 유추해 내는 smudge 공격[6,7]에 대해서도 대응할 수 있는 장점이 있다.

Ⅲ. 부가 채널을 이용하는 PIN 입력 방식

앞에서 설명한 무작위 챌린지 기반의 PIN 입력 방식들은 더 진화된 형태의 엿보기 공격인 녹화 공격(recording attack)에는 대부분 취약하다. 녹화 공격은 사용자가 인지하기 어려운 소형의, 또는 숨겨진 녹화 장치를 이용하여 사용자의 PIN 입력 과정 전체를 녹화한 후 이를 재생하면서 오프라인으로 공격하는 방식으로, 실시간으로 사람의 능력만을 기반으로 하는 엿보기 공격보다 훨씬 강력하다. 예를 들어 BW PIN에서 공격자가 PIN 한 자리에 대한 4개 라운드의 챌린지와 응답을 모두 녹화하여 분석할 수 있다면, 10개 후보 숫자들 중 사용자의 4개 응답과 배치되지 않는 유일한 숫자를 구할 수 있으며, 이것이 사용자의 PIN 숫자이다. 스마트폰에 고성능 카메라가 장착되고, 초소형의 카메라를 쉽게 구할 수 있는 현재의 상황을 고려하면, 이러한 공격은 단순한 엿보기 공격보다 더 심각한 위협이 될 수 있다. 특히 최근에는 사용자의 안경에 투영된 챌린지, 응답 정보를 분석하거나, 다양한 녹화 정보를 자동분석하여 PIN을 도출하는 자동화된 툴이 개발되는 등 진화된 공격들이 등장하고 있다[10,11].

녹화된 정보로부터 PIN을 유도하는 것을 방지하기 위한 한 가지 방법은, 사용자의 응답이 유일한 PIN에 대응하지 않도록 하는 것이다. 예를 들어, BW PIN에서 PIN 한 자리 당 챌린지-응답 쌍을 2회만 수행하도록 하면, 10개 PIN 숫자 후보 중 사용자의 응답과 상응하는 후보는 평균적으로 $10 \times 1/4 = 2.5$개가 되므로, 공격자는 녹화물을 분석하더라도 PIN 숫자를 정확히 유추할 수 없게 된다. 이러한 방법은 사용자의 PIN 입력을 위한 전체 응답 수를 줄여 입력 시간을 감소시키는 효과도 기대할 수 있다. 그러나, 이러한 변형된 방식은 무작위 대입 공격의 성공 확률을 높이는 문제를 발생시킨다. 즉, PIN 한 자리 당 4라운드를 수행하는 원래의 BW PIN에서는 공격자가 응답을 무작위로 선택하거나 (PIN 한 자리 당 성공 확률은 $1/2^4 = 1/16$) PIN 숫

자를 무작위로 선택(PIN 한 자리 당 성공 확률은 1/10)하여야 하나, 2라운드만 수행하는 방식에서는 흰색 또는 검은색 중 하나인 응답을 2회만 맞추면 되기 때문에 무작위 대입 공격의 성공 확률이 PIN 숫자 한 자리 당 1/4로 증가한다. 그러나 이는 단지 BW PIN의 문제만은 아니며, 공격자에 의해 챌린지와 응답이 모두 관찰 가능한 상황에서는 어떠한 PIN 입력 방법에 대해서도 녹화 공격과 무작위 대입 공격에 대한 안전성은 서로 반비례함이 증명된 바 있다[8]. 정확히는, 다음 식이 성립한다.

(녹화 공격 성공률) × (무작위 대입 공격 성공률) ≥ 1/(PIN 후보 수) (1)

위와 같은 한계를 극복하는 방법으로, 공격자로 하여금 챌린지 또는 응답을 관찰하지 못하게 하는 방법을 고려할 수 있다. 즉, 챌린지 또는 응답의 전송 경로로, 공격자가 관찰 가능한 시각 정보 채널 이외에 다른 안전한 채널을 사용하는 방법인데, 대표적인 것으로 진동 정보를 활용하거나[12,14-17,19,20,26], 소리 채널을 활용하는[13,16-19] 방법들이 있다.

예를 들어 그림 3은 [19]에 제안된 TimeLock으로, 소리 채널을 이용하는 Audio version과 진동 채널을 이용하는 Haptic version이 있다. 화면 상단의 네 개의 사각형은 각각 4자리 PIN의 각 자리에 해당하며, 해당 자리를 사용자가 터치하면 Audio version의 경우에는 짧은 beep 신호음들이, Haptic version의 경우에는 짧은 진동 신호들이 순차적으로 발생된다. 사용자의 손가락이 버튼에 접촉된 상태가 유지되는 동안 beep 또는 진동 신호가 계속 발생되며, 사용자는 본인의 PIN 숫자에 해당하는 횟수의 신호가 발생했을 때 손가락을 뗌으로써 입력을 완료하게 된다. Audio version에서는 이어폰 등으로 소리 정보가 사용자에게만 전달되게 하며, Haptic version에서는 진동 신호의 강도를 조절하여 디바이스에 직접 접촉하고 있는 사용자 이외에는 진동을 감지하기 어렵도록 하였다. 따라서, 공격자가 관찰할 수 있는 정보는 사용자가 손가락을 터치하고 떼는 동작이 전부이므로, 이 방법은 녹화 공격과 무작위 대입 공격 모두를 막을 수 있는 방법이 될 수 있다.

〔그림 3〕 TimeLock 입력 방식〔19〕

그러나, 부가 채널의 사용이 반드시 안전한 PIN 입력을 보장하는 것은 아니다. 일례로, [23-25]에서는 잘못 설계된 PIN 입력 방법에 대해서는 응답 없이 챌린지만을 관찰하고 이에 대한 통계 분석을 수행하여 PIN의 정보를 획득할 수 있음을 밝혔다. 또한, 위에 설명된 TimeLock에 대해서는 일종의 부채널 공격을 수행할 수 있는데, PIN 숫자가 클수록 손가락의 터치 유지 시간이 길어지기 때문에, 이 시간을 공격자가 관찰함으로써 PIN을 간접적으로 유추할 수 있다. 따라서 [19]에서는 PIN 숫자와 터치 유지 시간 간의 상관관계를 최소화하기 위해 터치 시작부터 최초 신호 발생시까지의 시간을 변화시키거나, 신호 발생 간의 시간 간격을 무작위로 바꾸는 방법 들을 제안하였다. 그러나, 최근에 연구된 결과에 의하면, 이와 같은 조치가 상관관계를 완전히 없애지는 못하기 때문에 동일한 사용자 PIN에 대한 여러 세션을 녹화하여 분석할 경우 PIN을 복원할 수 있음이 밝혀진 바 있다[20]. TimeLock 이외에도 현재까지 제안된 부가 채널을 이용하는 방법들 중 많은 방법들이 시간 정보를 이용하는 부채널 공격에 의해 공격될 수 있음이 밝혀졌다[21,22]. 따라서, 부가 채널을 이용한 PIN 입력 방법을 설계할 때는 챌린지가 PIN 숫자와 무관하게 독립적으로 선택되는 동시에 PIN 숫자와 응답의 입력 시간이 서로 독립적으로 분포되도록 하는 것이 중요하다.

그러나, 이와 같은 조치에도 불구하고 만약 공격자가 카메라 이외에 고성능 장비를 보유할 경우 다른 공격들도 시도할 수 있다. 예를 들어 소리 채널의 경우 고성능의 방향성 마이크를 이용하면 이어폰으로 전달되는 미세한 챌린지를 획득할 가능성이 있으며, 진동 신호 역시 진동과 동시에 발생하는 미세한 소리 신호를 획득하거나 고성능의 이미지 처리 기법을 이용하여 진동과 함께 발생하는 디바이스의 움직임을 포착하여 분석을 시도할

수도 있다.

한편, 소리나 진동 이외에 다른 부가 채널을 활용하는 방안들도 제안된 바 있는데, Pass-thoughts[28]와 같이 brain-computer interface를 이용하거나, eye-tracker를 이용하여 응답의 관찰을 어렵게 하는 방법[29], 무안경 3차원 디스플레이 상에서 3차원 객체들의 깊이 차이를 이용하여 챌린지를 전달함으로써 특정 지점(sweet spot) 이외에 위치한 공격자는 챌린지를 인식할 수 없도록 하는 방법[30,31], Google glass와 같은 개인형 디스플레이를 이용하여 챌린지의 관찰이 어렵도록 한 방법[32,33], 손 등으로 공격자의 관찰 시야를 막도록 한 방법[34,35] 등 다양한 방법이 제안되었다. 그러나 이러한 방법들은 대부분 현재의 디바이스들에서 제공되는 소리 또는 진동 이외의 매체들을 필요로 하기 때문에 범용으로 사용되기에는 어려운 한계가 있다.

Ⅳ. PIN 입력 방식 설계시의 고려 사항

식 (1)에서 확인된 바와 같이, 챌린지 및 응답이 관찰 가능한 PIN 입력 방식에 대해서 안전성을 높이는 데에는 한계가 있다. 즉, 별도 채널이 없는 PIN 입력 방법에서는 녹화 공격과 무작위 대입 공격 성공률을 모두 낮추는 데 한계가 있다. 그러나, 잘못 설계된 입력 방법은 이러한 하한조차 달성하지 못하며, 녹화 공격 또는 무작위 대입 공격에서 공격자가 더 높은 확률로 성공할 수 있다. 또한, 이미 앞에서 설명한 바와 같이 잘못 설계된 PIN 입력 방법에 대해서는 응답 없이 챌린지만을 관찰하여 PIN의 정보를 획득한 사례도 있음을 확인할 수 있다[23-25]. 이러한 공격을 막기 위해서는 챌린지가 PIN과 무관하게 균일한 분포로 선택되도록 설계하여야 한다. [23]에서는 이러한 요구사항을 포함하여 안전한 PIN 입력 방법을 설계하기 위한 가이드라인을 제시하였다.

PIN의 안전성에 있어 한가지 더 고려할 사항은 PIN의 분포이다. 예를 들어 4자리 PIN의 경우 선택 가능한 PIN의 가능성은 $10^4 = 10{,}000$가지이나, 실제 사용자들의 PIN은 각각 $1/10{,}000$ 확률로 균일하게 분포되어 있지 않다. 최근의 연구에 따르면, 실제로 사용되고 있는 PIN의 분포는 Zipf's law를 따른다[5]. 즉, PIN 사이에는 명확한 빈도 차이가 발견되었다. 따라서, 공격자가 이러한 분포를 알고 있다면 무작위 대입 공격이 아닌 사전 공격(dictionary attack)에 의해 성공률을 현저히 높일 수 있다. 이러한 공격을 막기 위해서 사용자의 PIN의 선택에 제약을 가하는 방법이 쓰이고 있으며, 또 다른 방법으로는 가능한 PIN 공간을 늘리기 위해 PIN 자릿수를 늘리거나, ColorPIN[4]에서와 같이 색깔 등 다른 정보를 PIN의 일부로 추가하는 방법 등이 고려될 수 있다. 그러나 이 경우 기존의 PIN과 호환성 문제가 발생할 수 있는데, 예를 들어 전통적인 숫자 기반의 PIN을 이용하는 은행 시스템의 안전성을 높이기 위해 색깔을 추가하여 PIN 공간 자체를 바꾼다면, 기존의 은행 시스템을 모두 수정하고 일부 단말에서는 입력 자체가 불가능하게 되는 문제가 발생한다. 또한, PIN 입력 방식을 바꿈으로써 생기는 사용자 편의성 문제도 고려하여야 한다. 대부분의 안전한 PIN 입력 방법, 특히 부가 채널을 고려하는 방식들은 PIN 입력 시간이나 입력 오류율 등 사용자 편의성 측면에서 전통적인 Regular PIN 입력 방식에 비해 불리한 경우가 많기 때문이다.

위와 같은 문제들을 최소화하기 위해서는 PIN 공간은 유지한 채로 PIN 입력 방식만 다양화하는 것이 바람직하다. 예를 들어 창구에서의 입출금, ATM, 스마트폰 뱅킹 등에서 같은 계좌라면 모두 같은 PIN을 사용하되, 안전한 장소(예를 들면 집안)에서는 편리한 기존의 Regular PIN 방식을 사용하고, 잠재적으로 녹화 공격 가능성이 있는 공개된 장소에서 뱅킹 업무를 수행해야 하는 경우 좀더 안전한 입력 방식을 사용하는 것을 고려할 수 있다. 물론, 안전성을 높이기 위해 상황별로 인증 메커니즘을 추가하거나, 다른 매체와 조합한 다중 요소 인증(multi-factor authentication) 방식도 고려할 수 있다. 최근에는 주변 상황을 인지하여 적절한 인증 방식을 사용자에게 자동적으로 제시해주는 방법[27]도 제안된 바 있다.

참 고 문 헌

[1] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, "Usable security: User preferences for authenticationmethods in eBanking and the effects of experience," Interacting with Computers, vol. 22, no. 3, pp. 153-164, 2010.

[2] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder

surfing," ACM CCS '04, pp. 236-245, 2004.

[3] D. S. Tan, P. Keyani, and M. Czerwinski, "Spy-resistant keyboard: more secure password entry on public touch screen displays," ACM OZCHI '05, 2005.

[4] A. De Luca, K. Hertzschuch, and H. Hussmann, "ColorPIN - securing PIN entry through indirect input," CHI '10, pp. 1103-1106, 2010.

[5] D. Wang, Q. Gu, X, Huang, P. Wang, "Understanding Human-Chosen PINs: Characteristics, Distribution and Security," ASIACCS '17, pp. 372-385, 2017

[6] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in Proceedings of the 4th USENIX Conference on Offensive Technologies (WOOT '10), 2010.

[7] E. von Zezschwitz, A. Koslow, A. De Luca, and H. Hussmann, "Making graphic-based authentication secure against smudge attacks," in Proceedings of the 18th International Conference on Intelligent User Interfaces (IUI '13), pp. 277-286, 2013.

[8] M.-K. Lee, "Security notions and advanced method for human shoulder-surfing resistant PIN-entry," IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 695-708, 2014.

[9] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6, pp. 716-727, 2014.

[10] R. Raguram, A. M. White, D. Goswami, F. Monrose, and J.-M. Frahm, "iSpy: Automatic reconstruction of typed input from compromising reflections," ACM CCS '11, pp. 527-536, 2011.

[11] F. Maggi, A. Volpatto, S. Gasparini, G. Boracchi, and S. Zanero, "A fast eavesdropping attack against touchscreens," Information Assurance and Security (IAS 2011), pp. 320-325, 2011.

[12] H. Sasamoto, N.Christin, and E.Hayashi, "Undercover: authentication usable in front of prying eyes," CHI '08, pp. 183-192, 2008.

[13] T. Perkovi´c, M. ˇCagalj, and N. Raki´c, "SSSL: shoulder surfing safe login," in Proceedings of the International Conference on Software, Telecommunication and Computer Networks 2009, pp. 270-275, 2009.

[14] A. De Luca, E. Von Zezschwitz, and H. Hußmann, "Vibrapass - secure authentication based on shared lies," CHI '09, pp. 913-916, 2009.

[15] A. Bianchi, I. Oakley, J. K. Lee, and D.-S. Kwon, "The haptic wheel: design and evaluation of a tactile password system," CHI '10, pp. 3625-3630, 2010.

[16] A. Bianchi, I. Oakley, V. Kostakos, and D.-S. Kwon, "The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices," ACM TEI '11, pp. 197-200, 2011.

[17] A. Bianchi, I. Oakley, and D. S. Kwon, "Spinlock: A singlecue haptic and audio PIN input technique for authentication," in Haptic and Audio Interaction Design (HAID 2011), vol. 6851 of Lecture Notes in Computer Science, pp. 81-90, 2011.

[18] M.-K. Lee, H. Nam, and D. K. Kim, "Secure bimodal PIN-entry method using audio signals," Computers and Security, vol. 56, pp. 140-150, 2016.

[19] A. Bianchi, I. Oakley, and D. S. Kwon, "Counting clicks and beeps: Exploring numerosity based haptic and audio PIN entry," Interacting with Computers, vol. 24, no. 5, pp. 409-422, 2012.

[20] M.-K. Lee, J. Yoo, H. Nam, "Analysis and Improvement on a Unimodal Haptic PIN-Entry Method," Mobile Information Systems, vol. 2017, Article ID 6047312, 17 pages, 2017.

[21] T. Perkovi´c, S. Li, A. Mumtaz, S. A. Khayam, Y. Javed, and M. ˇCagalj, "Breaking

undercover: Exploiting design flaws and nonuniform human behavior," SOUPS '11, 2011.

[22] M. Cagalj, T. Perkovic, and M. Bugaric, "Timing attacks on cognitive authentication schemes," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 584-596, 2015.

[23] Q. Yan, J. Han, Y. Li, and R. H. Deng, "On limitations of designing leakage-resilient password systems: attacks, principles and usability," NDSS '12, 2012.

[24] H. J. Asghar, S. Li, R. Steinfeld, and J. Pieprzyk, "Does counting still count? revisiting the security of counting based user authentication protocols against statistical attacks," NDSS '13, 2013.

[25] H. J. Asghar, R. Steinfeld, S. Li, M. A. Kaafar, and J. Pieprzyk, "On the linearization of human identification protocols: attacks based on linear algebra, coding theory, and lattices," IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1643-1655, 2015.

[26] T. Kwon and J. Hong, "Analysis and improvement of a PINEntry method resilient to shoulder-surfing and recording attacks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, article no. A6, pp. 278-292, 2015.

[27] E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley, "CASA: context-aware scalable authentication," SOUPS '13, pp. 3:1-3:10, 2013.

[28] J. Thorpe, P. C. van Oorschot, and A. Somayaji, "Pass-thoughts: authenticating with our minds," in Proceedings of the 2005 workshop on New security paradigms (NSPW '05), pp. 45-56, 2005.

[29] M. Kumar, T. Garfinkel, D. Boneh, and T.Winograd, "Reducing shoulder-surfing by using gaze-based password entry," SOUPS '07, pp. 13-19, 2007.

[30] M.-K. Lee and H. Nam, "Secure and fast PIN-entry method for 3D display," SECURWARE 2013, pp. 26-29, 2013.

[31] M.-K. Lee, J. B. Kim, and M. K. Franklin, "Enhancing the security of personal identification numbers with three-dimensional displays," Mobile Information Systems, vol. 2016, Article ID 8019830, 9 pages, 2016.

[32] D. K. Yadav, B. Ionascu, S. V. Krishna Ongole, A. Roy, and N. Memon, "Design and analysis of shoulder surfing resistant PIN based authentication mechanisms on Google Glass," in 1st Workshop on Wearable Security and Privacy (In Association with Financial Crypto 2015), 2015, paper 8.

[33] P. Lantz, B. Johansson, M. Hell, and B. Smeets, "Visual cryptography and obfuscation: a use-case for decrypting and deobfuscating information using augmented reality ," Financial cryptography and data security, vol. 8976 of Lecture Notes in Computer Science, pp. 261-273, 2015.

[34] D. Kim, P. Dunphy, P. Briggs et al., "Multi-touch authentication on tabletops," CHI 2010, pp. 1093-1102, 2010.

[35] Q. Yan, J. Han, Y. Li, J. Zhou, and R. H. Deng, "Designing leakage-resilient password entry on touchscreen mobile devices," ASIACCS '13, pp. 37-48, 2013.

〈저자소개〉

이 문 규 (Mun-Kyu Lee)
종신회원

1996년 2월 : 서울대학교 컴퓨터공학과 졸업
1998년 2월 : 서울대학교 컴퓨터공학과 석사
2003년 8월 : 서울대학교 전기컴퓨터공학부 박사
2003년 8월~2005년 2월 : 한국전자통신연구원 선임연구원
2005년 3월~현재 : 인하대학교 컴퓨터공학과 교수
관심분야 : 암호 최적화, 사용자인증