정 보 보 호 학 회 지
제 25 권 제 3 호, 2015. 6

패턴 기반 사용자 인증 시스템 기술 연구 동향 및 비교

신 형 준*, 허 준 범**

요 약

최근 다양한 스마트기기의 대중화로 인해, 사용자의 개인 정보를 이용한 다양한 스마트 서비스들이 제공되고 있다, 이에 따라 해당 정보의 사용자를 확인하는 사용자 인증 기법의 중요성이 대두되고 있다. 가장 대표적으로 널리 쓰이는 인증기법인 패스워드 인증기법은 사용자가 기억하기 쉬운 형태로 패스워드를 설정하기 때문에 추측공격(Guessing Attack)과 사전공격(Dictionary Attack)에 취약하다. 또한 터치 스크린 기반의 시스템에서 사용할 경우, 가상 키보드의 불편함으로 인해 편리성이 떨어진다. 본 논문에서는 패스워드 인증 기법의 문제점을 해결한 여러 가지 패턴 기반 사용자 인증기법들의 연구 동향에 대해 분석하고, 해당 인증 기법들을 비교하여 분석한다.

Ⅰ. 서 론

최근 스마트 폰, 태블릿 PC 등을 비롯한 스마트 기기의 사용이 대중화 되면서 사용자에게 중요한 정보 저장과 개인 정보를 이용한 다양한 서비스들이 제공되고 있다. 특히 최근에는 다수의 서로 다른 스마트 기기들을 통해 하나의 통합된 서비스를 제공하는 플랫폼이 많이 사용되고 있다. 이러한 환경에서 안전하고 편리한 사용자 인증에 대한 요구사항이 지속적으로 증가되고 있다. 현재 스마트 기기를 이용한 서비스 환경에서 일반적으로 널리 사용되고 있는 사용자 인증 기법은 문자와 숫자의 조합을 이용한 패스워드 인증 기법이다.

문자와 숫자의 조합을 이용한 패스워드 인증 기법은 구현하기 쉽고, 변경이 용이하지만 두 가지 보안의 취약성을 가지고 있다. 첫 번째로 사용자는 복잡한 패스워드가 아닌 자신과 관련된 정보를 이용한 추측하기 쉬운 패스워드를 설정하거나 기억하기 쉬운 형태의 짧은 패스워드를 설정한다. 그렇기 때문에 사용자가 설정한 패스워드는 추측공격(Guessing Attack)[1]과 사전공격(Dictionary Attack)[2]에 굉장히 취약하다. 두 번째는 사용자가 하나의 패스워드를 여러 다른 장비나 서비스에서 사용한다는 점이다. 여러 개의 패스워드를 사용할 경우, 사용자는 각각의 패스워드를 기억하기 어렵기 때문에 여러 서비스나 장비 인증에 하나 혹은 두 개의 적은 개수의 패스워드를 이용하게 된다. 그렇기 때문에 만약 공격자가 어떤 특정 서비스나 장비에 접근하여 사용자의 패스워드를 획득할 경우, 이외의 다른 서비스나 장비를 통해 사용자로 위장하여 해당 사용자의 정보에 심각한 손상을 입힐 수 있다[3].

또한 터치 기반의 스마트 기기를 사용할 경우 패스워드 인증 기법은 사용자 편의성에 있어서도 단점이 존재한다. 예를 들면, 터치 기반의 시스템에서 사용자가 패스워드를 입력할 때, 사용자는 반드시 가상 키보드를 사용해야 한다. 만약에 가상 키보드의 각각의 요소들의 크기가 작다면, 다음의 두 가지의 문제점으로 인해 낮은 정확성을 갖게 된다[4]. 첫 번째 문제점은 넓은 손가락 문제(Fat Finger Problem)이다. 넓은 손가락 문제는 가상 키보드의 한 요소의 크기가 사용자의 손가락이 터치스크린에 접촉되는 영역보다 작을 경우에 낮은 정확성을 야기한다는 문제이다[5]. 두 번째 문제점은 폐색 문제(Occlusion Problem)이다. 폐색 문제는 아직 접촉하지 않은 상태임에도 불구하고, 손가락의 가리킴의 의해 가상 키보드의 요소들이 선택되는 문제로 낮은 정확성을 야기한다[6].

본 연구는 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2013R1A2A2A01005559).
* 중앙대학교 컴퓨터공학과(zxzx2512@cau.ac.kr)
** 고려대학교 컴퓨터학과(jbhur@korea.ac.kr)

스마트 기기 서비스 환경에서 이러한 패스워드 기반 인증 기법의 문제점을 해결하기 위해 지금까지 많은 인증 기법들이 제안되었다[7-11]. 이 중, 많은 제안된 인증 기법들은 패스워드를 문자와 숫자의 조합이 아닌 사용자가 생성한 일종의 패턴을 기반으로 인증을 진행한다.

본 논문에서는 패스워드의 취약점을 해결한 패턴 기반의 인증 기법들을 살펴보고 Joseph Bonneau [12] 가 제안한 인증 기법 비교 프레임워크를 이용하여 패턴 기반의 인증 기법들을 비교하고 분석한다.

Ⅱ. 패턴 기반 인증 기법

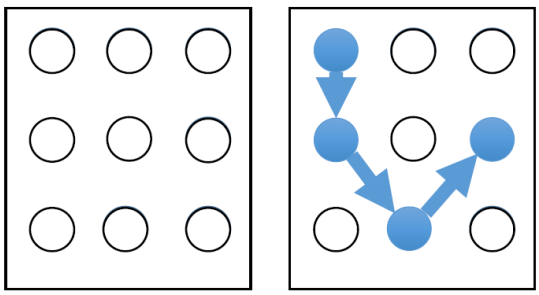
여기서는 패스워드의 취약점을 해결한 패턴기반 인증 기법들을 살펴본다. 패턴 기반의 인증 기법들은 그림을 이용한 그림 기반 인증 기법[8,9,10], 격자 형식의 무늬를 이용한 그리드 기반의 인증 기법[11], 터치 스크린 상에서의 터치 방식을 이용한 터치 기반의 인증 기법[7] 등이 포함된다.

2.1. Pattern Lock

Pattern Lock[15]은 일종의 그리드 기반의 인증 기법으로, 일반적으로 스마트 폰과 같은 장비에서 사용자를 인증할 때 사용한다.

그림 1은 Pattern Lock 인증 기법의 한 예를 보여주고 있다. Pattern Lock 인증 기법은 9개의 격자로 된 점들을 이용하여 사용자가 4개 이상의 점을 연결하는 방식으로 인증이 진행된다. 사용자는 자신 고유의 연결 패턴을 기억해야 하고, 후에 인증할 시 해당 연결 패턴을 이용하여 인증하게 된다.

Pattern Lock 인증 기법은 패스워드 인증 기법과 다르게 가상 키보드를 사용하지 않아 사용자 측면에서 편의성이 더 좋지만 안전성 측면에서는 여전히 문제가 있다. 특히 고정된 개수의 점을 이용한 Pattern Lock 인증 기법은 무작위 공격(Brute-force Attack)[13]이나 얼룩 공격(Smudge Attack)[14]에 취약하다.



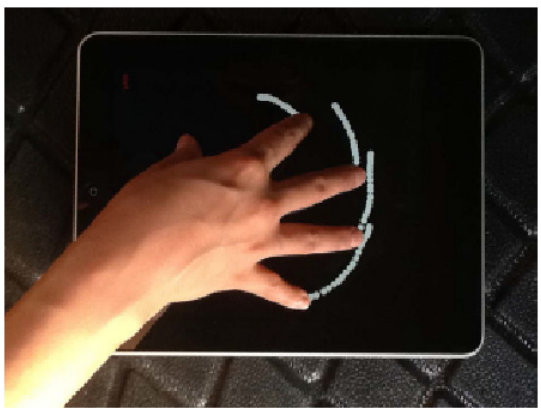
〔그림 1〕 Pattern Lock 인증 기법의 한 예

2.2. 멀티터치 동작기반 인증 기법

멀티터치 동작기반 인증 기법(Multitouch Gesture-based Authentication) [7]은 일종의 바이오 정보 기반의 인증으로, 사용자의 패스워드로써 사용자의 다섯 손가락을 전부 사용하는 방식을 이용한다.

그림 3[7]은 멀티터치 동작의 한 예를 보여준다. 멀티터치 동작기반 인증 기법은 그림 3과 같은 동작 패턴을 사용자의 인증 수단으로 사용하게 된다. 사용자 등록 단계에서 사용자는 자신의 비밀을 여러 번 동작하면서, 해당 비밀에 대한 템플릿 값을 만들게 되고 사용자의 인증을 수행하는 장비는 해당 템플릿 값을 저장하게 된다. 사용자 인증 단계에는 인증을 수행하는 장비에서 사용자로부터 들어온 동작과 템플릿 값의 차이를 이용하여 해당 차이가 지정된 임계점보다 작을 경우에만 사용자 인증을 성공적으로 진행하게 한다.

[7]에서는 사용자가 직접 임의로 만드는 동작을 포함하여 미리 지정된 여러 가지 동작들을 이용한 해당 동작들의 연속적인 입력 형태로써 사용자 고유의 패스워드를 만드는 방안을 제안하였다. 이와 같은 방식은 여러 사용자를 구별하는 측면에서 하나의 동작만 사용할 경우보다 좋은 성능을 보이지만, 여전히 해당 인식률이 2%~16% 사이이기 때문에 좋지 못하다.



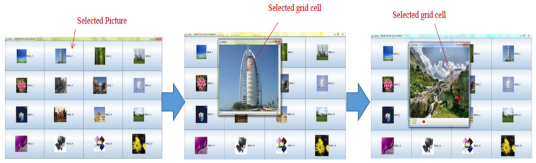
〔그림 3〕 멀티터치 동작 패턴 추적의 예

2.3. Select-to-Spawn

Select-to-Spawn은 일종의 그림기반 인증 기법이다[8]. 이 인증 기법은 여러 사진 중 하나의 사진을 고르고, 사용자가 해당 사진의 특정 부분을 지정함으로써, 사용자가 기억해야할 일종의 패스워드를 생성한다.

그림 4[8]는 Select-to-Spawn 인증 기법에서 사용자가 자신의 패스워드를 등록하는 과정을 보여주고 있다. 첫 번째 단계에서 사용자는 사진 하나를 선택하고, 두 번째 단계로 넘어가게 된다. 두 번째 단계에서 사용자는 선택한 사진의 특정 지점을 선택해야 한다. 두 번째 단계 이후부터 사용자는 다음에 나오는 사진에 대해서 특정 지점을 선택하거나 다른 사진으로 넘어가 자신이 원하는 특정 지점을 선택할 수 있고, 이런 일련의 방식으로 패스워드를 만들게 된다.

이러한 단계를 거치고 나면 사용자는 자신의 패스워드를 사진과 그 안에 있는 특정 지점으로 만들게 되고, 후에 사용자 인증을 진행하는 장비에서 인증할 경우 사용하게 된다.

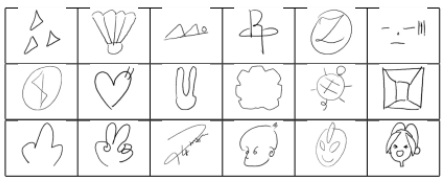


〔그림 4〕 Select-to-Spawn 패스워드 설정 단계

2.4. Scribble-a-Secret

Scribble-a-Secret 인증 기법은 사용자의 비밀로 사용자가 직접 그린 그림을 활용하는 일종의 그림 기반의 인증 기법이다.

그림 5[9]는 87명의 사용자로부터 추출된 그림으로, Scribble-a-Secret 인증 기법은 해당 그림으로부터 방향 패턴(Orientation Pattern)들을 추출하여 하나의 템플릿 벡터을 생성하고 이를 저장한다.



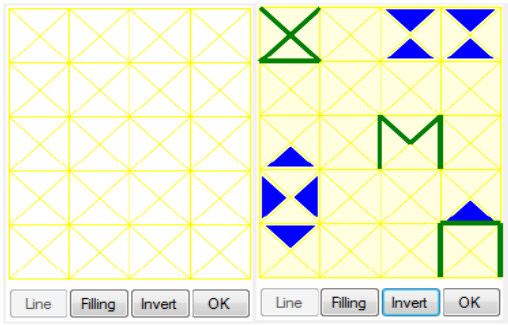
〔그림 5〕 사용자로부터 추출된 패스워드 그림

사용자 인증 단계에서는 사용자로부터 받은 입력 그림으로부터 새로운 방향 패턴들을 추출하여 새로운 벡터를 생성하고, 이 벡터와 저장된 템플릿 벡터의 유사성을 계산하여 인증을 진행한다.

2.5. Drawing Geometric

Drawing Geometric 인증 기법은 사용자의 선과 색이 채워진 삼각형으로 만든 기하학적 그림을 이용한 인증 기법이다.

그림 6[10]은 사용자가 그린 그림의 예를 보여준다. 그림 6과 같이 사용자는 선을 그릴 수 있고, 삼각형 부분을 클릭 혹은 터치함으로써 색을 채울 수 있다. 그림 6에서의 Invert 버튼을 누르면 선택되지 않은 선과 삼각형에 색이 채워지는 형식으로 그림이 나타나게 된다. 이와 같은 기하학적 그림을 사용자는 비밀로 가지고 있다가 인증 시 사용하게 된다.

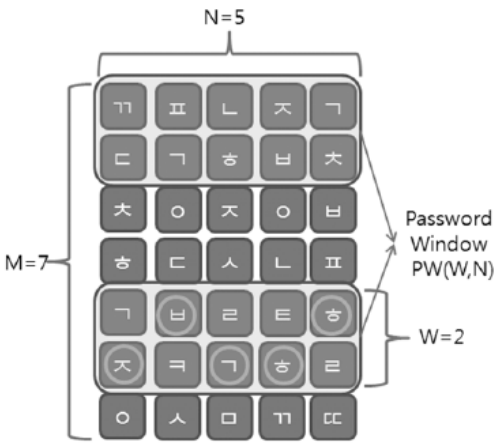


〔그림 6〕 Drawing Geometric 기법의 패스워드 예

2.6. 한글 자음을 이용한 그리드 기반 인증 기법

[11]에서는 한글 자음을 이용한 그리드 기반 인증 기법을 제안하였다. 해당 기법은 훔쳐보기 공격(Shoulder Surfing Attack)에 향상된 안전성을 보장하는 인증 기법으로 가상의 움직이는 패스워드 윈도우를 이용한다.

그림 7은 패스워드가 “ㅈㅂㄱㅎㅎ”인 상황에서 사용자가 $W \times N$ 크기의 패스워드 윈도우 범위 안에 해당 패스워드를 입력하는 예를 보여준다[11]. 한글 자음을 이용하기 때문에 위와 같은 패스워드일 경우 “정보과학회”와 같은 암기하기 쉬운 단어를 사용할 수 있어, 사용



〔그림 7〕 한글자음기반 인증기법의 예

자 입장에서 편하고, 패스워드 윈도우를 이용하여 물리적인 관찰자에 의한 공격에 향상된 안전성을 보장한다.

Ⅲ. 비교 및 분석

여기서는 2절에서 살펴보았던 인증 기법들을 Joseph Bonneau [12] 가 제안한 인증 비교 프레임워크를 이용하여 3가지 측면인 편의성(Usability), 활용성(Deployability), 안전성(Security) 측면에서 비교 분석한다.

표 1은 편의성, 활용성, 안전성 측면에 대해서 비교 분석한 결과를 보여준다. 편의성은 총 8개의 항목(U1~U8)로 구성되어 있고, 활용성은 총 6개(D1~D6), 안전성은 총 11개(S1~S11) 항목으로 구성된다.

3.1. 편의성

(1)U1 (기억의존성, Memorywise-Effortless): 본 항목은 해당 인증 기법을 사용하고 있는 자가 어떠한 비밀도 기억할 필요가 없어야 한다는 조건을 말하며, 본 논문에서 살펴 본 인증 기법들은 사용자가 패스워드와 같은 특정 패턴을 암기해야하기 때문에 이를 만족하지 않는다.

(2)U2 (계정확장성, Scalable-for-Users): 본 항목은 계정의 수가 많아져도 사용자의 부담이 늘어나지 않아야 한다는 조건으로, 패스워드를 사용할 시 각 계정마다 다른 패스워드를 사용한다고 가정한다면 그 부담은 계정의 수만큼 증가하기 때문에 여기서 살펴 본 인증 기법들은 만족하지 않는다.

(3)U3 (소지성, Nothing-to-Carry): 본 항목은 사용자가 인증을 위해서 부가적인 물건을 소지할 필요가 없어야 한다는 항목으로 여기서 살펴본 인증 기법들은 부가적인 물건이 필요 없기 때문에 해당 항목을 만족한다.

(4)U4 (물리의존성, Physically-Effortless): 본 항목은 인증 시 사용자가 버튼을 누르는 것과 같은 직접적인 입력을 할 필요가 없어야 한다는 항목으로 여기서 살펴본 인증 기법들은 사용자가 패스워드에 해당하는 패턴을 사용하기 위해 그리기와 같은 직접적인 입력을 해야 하기에 만족하지 않는다.

(5)U5 (용이성, Easy-to-Learn): 본 항목은 사용자가 해당 인증 기법을 배우기 쉬워야 한다는 항목으로, 여기서 살펴본 인증 기법들은 용이성이 검증된 MGB[7] 기법과 비슷한 수준의 용이성을 제공하므로 모든 기법들은 해당 항목을 만족한다.

(6)U6 (사용효율성, Efficient-to-Use): 본 항목은 사용자 인증 시 걸리는 시간이 실질적으로 적당히 짧아야 한다는 항목이다. PL은 최선의 경우 점 4개를 이용하여 인증을 하고 9개의 점에서 4개의 점을 잇는데 걸리는 시간은 굉장히 짧음으로 해당 항목을 만족한다. MGB는 [7]에서 41명의 사용자를 대상으로 가상 키보드로 패스워드를 입력하는 것보다 해당 기법의 인증 과정이 더 빠른지에 대한 조사를 진행 하였다. 그 결과로 38명의 사용자가 빠르다고 판단하였기 때문에 해당 항목을 만족한다고 하였다. DG는 [10]에서 25명의 사용자를 대상으로 조사를 한 결과 인증 소요 시간이 충분히 짧다고 하여 해당 항목을 만족한다고 하였다. STS는 검증된 DG기법과 같이 버튼을 이용하여 인증이 진행되기 때문에 만족한다고 하였다. 터치 스크린 상에 SAS에서 사용하는 그림은 PL과 같이 사용자가 그린 선으로 이루어져 있어, 사용자가 정확히 해당 그림을 기억하고 있다면, 걸리는 시간은 PL과 크게 차이가 없을 것이다. 그렇기 때문에 본 항목을 만족한다고 판단하였다.

〔표 1〕 인증 기법들의 비교 및 분석 결과표

구 분		PL [15]	MGB [7]	STS [8]	SAS[9]	DG [10]	한글기법 [11]
Usability	● U1:Memorywise-Effortless	×	×	×	×	×	×
	● U2;Scalable-for-Users	×	×	×	×	×	×
	● U3:Nothing-to-Carry	◎	◎	◎	◎	◎	◎
	● U4:Physically-Effortless	×	×	×	×	×	×
	● U5:Easy-to-Learn	◎	◎	◎	◎	◎	◎
	● U6:Efficient-to-Use	◎	◎	◎	◎	◎	◎
	● U7:Infrequent-Errors	◎	×	◎	◎	◎	◎
	● U8:Easy-Recovery-from-Loss	×	×	×	×	×	×
Deployability	● D1:Accessible	×	×	×	×	×	×
	● D2:Negligible-Cost-per-User	◎	×	◎	○	◎	◎
	● D3:Server-Compatible	×	×	×	×	×	×
	● D4:Browser-Compatible	◎	◎	◎	◎	◎	◎
	● D5:Mature	◎	○	○	○	○	○
	● D6:Non-Proprietary	×	◎	◎	◎	◎	◎
Security	● S1:Resilient-to-Physical-Observation	×	×	×	×	×	◎
	● S2:Resilient-to-Targeted-Impersonation	◎	◎	◎	◎	◎	◎
	● S3:Resilient-to-Throttled-Guessing	◎	◎	◎	◎	◎	◎
	● S4:Resilient-to-Unthrottled-Guessing	×	◎	◎	◎	◎	◎
	● S5:Resilient-to-Internal-Observation	×	×	×	×	×	×
	● S6:Resilient-to-Leaks-from-Other-Verifiers	×	×	×	×	×	×
	● S7:Resilient-to-Phishing	×	×	×	×	×	×
	● S8:Resilient-to-Theft	◎	◎	◎	◎	◎	◎
	● S9:No-Trusted-Third-Party	◎	◎	◎	◎	◎	◎
	● S10:Requiring-Explicit-Consent	◎	◎	◎	◎	◎	◎
	● S11:Unlinkable	◎	◎	◎	◎	◎	◎

◎: 매우 만족, ○: 만족, ×: 요구사항을 만족시키지 못함

(7)U7 (신뢰성, Infrequent-Errors): 본 항목은 합법적 사용자가 인증할 시 실패할 확률이 작아야 한다는 항목이다. MGB는 사용자의 멀티터치 동작을 패스워드로써 사용하고, 사용자의 동작을 정확히 인식할 확률이 낮기 때문에 해당 항목을 만족하지 못한다. MGB 이외의 인증 기법들은 패스워드 인식에 실패할 확률이 낮기 때문에 해당 항목을 만족한다.

(8)U8 (복구성, Easy-Recovery-from-Lose): 본 항목은 해 당 인증에 필요한 장비나 비밀을 잊어버릴 경우, 쉽게 복구가 가능해야 한다는 조건을 의미한다. 여기서 살펴 본 인증 기법들은 사용자의 비밀을 잊어버릴 경우 다시 얻기 위해 해당 인증 기법 전체를 다시 재설정해야하기 때문에 쉽지 않다. 그러므로 해당 항목을 만족하지 않는다.

3.2. 활용성

3.2.1. D1 (접근성, Accessible): 본 항목은 해당 인증 기법을 사용할 때, 신체적인 제약이 있더라도 인증 가능성의 차이가 없어야 한다는 조건으로, 여기서 살펴 본 인증 기법들은 사용자의 직접적인 입력을 필요로 하기 때문에 해당 항목을 만족하지 않는다.

3.2.2. D2 (합당성, Negligible-Cost-per-User): 본 항목은 사용자와 기기 간의 인증에 요구되는 총 비용에 대한

항목이다. 본 논문에서는 사용자 인증 시 일반적인 환경이 아닌 특정 환경에만 적용이 가능할 경우에 비용이 크다고 판단하였다. MGB 같은 경우에는 반드시 터치 스크린 환경이여야 가능하기 때문에 만족하지 않고, SAS 같은 경우에는 마우스나 손으로 충분히 사용자 그림을 그릴 수 있고, 터치 스크린 환경일 경우 더 수월하기 때문에 부분 만족으로 판단하였다. 다른 나머지 인증 기법들은 어떤 환경에도 단순 클릭만을 이용하여 인증이 가능하기 때문에 만족한다.

3.2.3. D3 (서버호환성, Server-Compatible): 본 항목은 기존 텍스트 기반의 패스워드 인증 기법과 호환이 가능한지에 대한 항목이다. 여기서 살펴본 인증 기법들은 추가적인 변경이 필요하기 때문에 해당 항목을 만족하지 않는다.

3.2.4. D4 (웹호환성, Browser-Compatible): 본 항목은 해당 인증기법을 사용하기 위해 웹 브라우저의 변경이 필요한지에 대한 항목이다. 본 논문에서 살펴 본 인증 기법들은 따로 웹 브라우저의 변경이 필요하지 않기 때문에 해당 항목을 만족한다.

3.2.5. D5 (성숙성, Mature): 본 항목은 인증 기법이 구현되었고, 널리 사용되고 있어야 한다는 항목이다. Pattern Lock은 현재 안드로이드 스마트 폰에서 실제로 널리 사용되고 있기 때문에 만족한다. 나머지 인증 기법들은 구현은 되었으나, 널리 사용되고 있는 인증 기법들이 아니기 때문에 부분적으로 만족한다.

3.2.6. D6 (공유성, Non-proprietary): 본 항목은 해당 인증 기법의 소유권이 어느 누구에게도 속해서는 안 된다는 조건으로, 패턴 락의 소유권은 Google에 있기 때문에 만족하지 않는다. 나머지 다른 인증 기법들은 해당 조건을 만족한다.

3.3. 안전성

3.3.1. S1 (물리 관찰 저항성, Resilient-to-Physical-Observation): 본 항목은 훔쳐보기 공격과 같은 물리적인 관찰에 의한 공격에 안전해야 한다는 조건이다. 한글 기법을 제외한 다른 모든 인증 기법들의 경우 물리적인 관찰에 의한 공격에 취약하다. 한글 기법은 패스워드 윈도우를 이용하여 훔쳐보기 공격과 같은 물리적인 관찰에 대한 안전성을 보장하여 해당 항목을 만족한다.

3.3.2. S2 (사용자 위조 저항성, Resilient-to-Targeted-Impersonation): 본 항목은 사용자의 정보로부터 인증 시 필요한 비밀 정보를 유추할 수 없어야 한다는 조건이다. 여기서 살펴 본 인증 기법들은 패스워드를 만들 시 사용자의 정보를 사용하지 않기 때문에 해당 항목을 만족한다.

3.3.3. S3 (추측공격 저항성, Resilient-to-Throttled-Guessing): 본 항목은 후보 패스워드를 뽑는 횟수의 한계가 있을 경우 추측공격에 안전해야 한다는 조건이다. 본 논문에서는 공격자가 20개의 후보 패스워드를 5번 획득할 경우 사용자의 패스워드가 속할 확률이 1이 아니면 만족한다고 하였다. 그럴 경우 여기서 살펴본 인증 기법들은 해당 조건을 만족한다.

3.3.4. S4 (비한계 추측공격 저항성, Resilient-to-Unthrottled-Guessing): 본 항목은 후보 패스워드를 뽑는 횟수의 한계가 없을 경우 추측 공격에 안전해야 한다는 조건이다. Pattern Lock 인증 기법의 경우에는 20개의 후보 패스워드를 뽑을 경우 6번만 시도를 하면 그 중 사용자 패스워드가 반드시 나타나기 때문에 해당 항목을 만족하지 못하고, 나머지 인증 기법들은 해당 항목을 만족한다.

3.3.5. S5 (내부관찰자 저항성, Resilient-to-Internal-Observation): 본 항목은 사용자의 인증에 대한 정보를 내부적으로 습득 가능한 공격자에 대해서 안전해야 한다는 조건이다. 여기서 살펴본 인증 기법들은 내부적인 관찰에 대해서는 안전성을 보장하지 못하기 때문에 만족하지 못한다.

3.3.6. S6 (정보노출 저항성, Resilient-to-Leaks-from-Other-Verifiers): 본 항목은 여러 증명 기관이 있는 환경에서, 한 증명 기관에서 노출된 정보에 의해 다른 증명 기관의 인증에 피해가 없어야 한다는 조건이다. 본 논문에서는 모든 증명 기관에서 해당 인증기법을 사용한다고 가정하였다. 그럴 경우, 사용자는 해당 증명 기관마

다 같은 인증 패스워드 패턴을 설정하기 쉽기 때문에, 한 증명 기관에서 사용자 패스워드를 얻은 공격자는 쉽게 다른 증명 기관에서 인증을 할 수 있게 된다. 그렇기 때문에 여기서 본 인증 기법들은 해당 항목을 만족하지 않는다.

3.3.7. S7 (피싱공격 저항성, Resilient-to-Phishing): 본 항목은 피싱 공격에 대해서 안전해야 한다는 조건으로, S5 항목과 같은 이유로 여기서 본 인증 기법들은 만족하지 않는다.

3.3.8. S8 (도난 저항성, Resilient-to-Theft): 본 항목은 사용자의 장비를 습득한 자가 인증을 시도할 시 성공하기 어려워야 한다는 조건으로, 해당 장비를 습득한 대상이 사용자의 패스워드를 알지 못하면 인증이 어렵기 때문에 여기서 본 인증 기법들은 해당 항목을 만족한다.

3.3.9. S9 (인증기관 부재, No-Trusted-Third-Party): 본 항목은 신뢰할 수 있는 제 3의 인증기관이 없는 환경에서 안전성을 보장해야 한다는 조건이다. 여기서 본 인증 기법들은 별도의 인증기관을 이용하여 인증을 시도하지 않기 때문에, 해당 항목을 만족한다고 하였다.

3.3.10. S10 (명확한 사용자 동의, Requiring-Explicit-Consent): 본 항목은 인증 시 사용자의 동의가 필요하다는 조건이다. 여기서 본 인증 기법들은 인증을 위해서는 패스워드를 이용한 사용자의 동의가 반드시 필요하기 때문에 만족한다.

(11)S11 (비연결성, Unlinkable): 본 항목은 여러 개의 제 3의 기관을 사용할 경우 각 기관사이의 어떠한 연결성도 존재해서는 안 된다는 조건이다. S9 항목과 마찬가지로 제 3의 기관을 여기서 본 인증 기법들은 사용하지 않기 때문에 만족한다고 하였다.

Ⅳ. 결 론

최근 스마트 기기의 사용이 보편화되면서, 사용자의 데이터 보호와 접근제어를 위해 인증 기법의 중요성이 대두되고 있다. 가장 대표적으로 널리 쓰이는 패스워드 인증 기법은 추측공격과 사전공격에 취약하고, 특히 터치스크린을 활용하는 스마트 기기 상에서는 가상 키보드로 인해 사용자 편의성이 떨어진다. 본 논문에서는 패스워드 인증 기법에서 나타난 편의성 문제와 안전성 문제를 해결한 여러 가지 패턴 기반 인증 기법들의 동향을 살펴보았고, 인증 비교 프레임워크를 이용하여 비교 분석하였다.

참 고 문 헌

[1] A. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp.125-143, June 2006

[2] D. V. Klein, "Foiling the cracker: a survey of, and improvements to, password security," *in Proc. 2nd USENIX Workshop Security,* 1990, pp.5-14

[3] William Stallings and Lawrie Brown, "Computer Security: Principles and Practice. 2nd Edition", *Pearson*, 2011

[4] L. Findlater, J. O. Wobbrock, and D. Wigdor, "Typing on flat glass: Examining ten-finger expert typing patterns on touch surfaces", *in Proc. Annu. Conf. Human Factors Comput. Syst.*,pp.2453-2462, 2011

[5] H. L and Y. Li, "Gesture avatar: A technique for operating mobile user interfaces using gestures", *in Proc. Annu. Conf. Human Factors Comput. Syst.*,pp.207-216, 2011

[6] Wigdor, D., Forlines, C., Baudisch, P., Barnwell, J., and Shen, C. "LucidTouch: a see-through mobile device",. *Proc. UIST 2007, ACM Press*., pp.269-278, 2007

[7] Napa Sae-Bae, Nasir Memon, Katherine Isbister, and Kowsar Ahmed, "Multitouch Gesture-Based Authentication", *2014 IEEE Transactions on Information Forensics and Security*, pp.568-582, April 2014

[8] Mohammad Sarosh Umar, Mohammad Qasim Rafiq, "Select-to-Spawn: A Novel Recognition-based Graphical User Authentication Scheme", 2012 IEEE International Conference on Signal

Processing, Computing and Control (ISPCC), pp.1-5, March 2012

[9] Mizuki Oka, Kazuhiko Kato, Yingqing Xu, Lin Liang, and Fang Wen, "Scribble-a-Secret: Similarity-Based Password Authentication Using Sketches", 19th International Conference on Pattern Recognition (ICPR), pp.1-4, Dec 2008

[10] Mohammad Sarosh Umar, Mohammad Oasim Rafiq, "A Graphical Interface for User Authentication on Mobile Phones", 4th International Conference on Advances in Computer-Human Interactions, pp.69-74, 2011

[11] 김종우, 김성환, 김광휘, 조환규, “훔쳐보기 공격에 견고한 그리드 기반 패스워드 시스템의 개선”, 정보과학회논문지, 17(4), April 2011

[12] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano, "The Quest to Replace Passwords: A Framwork for Comparative Evaluation of Web Authentication Scheme", 2012 IEEE Symposium on Security and Privacy, pp.553-567, May 2012

[13] Kim, I., "Keypad against brute force attacks on smartphones ", Information Security, IET, pp.71-76, June 2012

[14] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith, "Smudge Attacks on Smartphone Touch Screens", WOOT10 Proceedings of the 4th USENIX conference on Offensive technologies, Article no 1-7, August 2010.

[15] http://www.groovypost.com/howto/security/how-to-enable-pattern-lock-security-on-android-devices/, accessed May 2011

〈저자소개〉

신 형 준 (Hyungjune Shin)

2015년 2월 : 중앙대학교 컴퓨터공학부 졸업

2015월 3월~현재 : 중앙대학교 컴퓨터공학과 석사과정

관심분야 : 시스템 보안, 클라우드 보안, 빅데이터 보안,

허 준 범 (Junbeom Hur)

2001년 2월 : 고려대학교 컴퓨터공학 졸업

2005년 8월 : 한국과학기술원 전산학 석사

2009년 8월 : 한국과학기술원 전산학 박사

2009년 9월~2011년 8월 : University of Illinois at Urbana-Champaign 박사후연구원.

2011년 9월~2015년 2월 : 중앙대학교 컴퓨터공학부 조교수

2015년 2월~현재 : 고려대학교 컴퓨터학과 조교수

관심분야 : 클라우드 보안, 빅데이터 보안, 네트워크 보안, 응용 암호학