KIPS Tr. Comp. and Comm. Sys.
Vol.3, No.12 pp.463~478 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2014.3.12.463

Security Analysis on Password Authentication System of Web Sites

Heekyeong Noh[†] · Changkuk Choi[††] · Minsu Park[†††] · Seungjoo Kim[††††]

ABSTRACT

Portal site is not only providing search engine and e-mail service but also various services including blog, news, shopping, and others. The fact that average number of daily login for Korean portal site Naver is reaching 300 million suggests that many people are using portal sites. With the increase in number of users followed by the diversity in types of services provided by portal sites, the attack is also increasing. Most of studies of password authentication is focused on threat and countermeasures, however, in this study, we analyse the security threats and security requirement of membership, login, password reset first phase, password reset second phase. Also, we measure security score with common criteria of attack potential. As a result, we compare password authentication system of domestic and abroad portal sites.

Keywords : Password Authentication System of Web Portal, Threat of Web Portal, Security Requirement of Web Portal, Attack Potential

웹사이트 패스워드 인증 시스템의 보안성 분석

노 희 경[†] · 최 창 국[††] · 박 민 수[†††] · 김 승 주[††††]

요 약

포털사이트는 검색 엔진, 이메일 서비스뿐만 아니라 블로그, 뉴스, 쇼핑 등 다양한 서비스를 제공하고 있다. 국내 포털 업체인 네이버의 하루 평균 로그인 횟수가 3억 건에 달할 만큼 많은 사람들이 포털사이트를 이용하고 있음을 알 수 있다. 이와 같이 포털사이트가 제공하는 서비스의 종류가 다양해지고 더불어 이용자 수가 증가함에 따라 포털사이트를 대상으로 하는 공격도 증가하고 있다. 기존 패스워드 인증 시스템은 주로 로그인 단계에서의 보안 위협에 초점을 두고 이를 해결하기 위한 대안에 대한 연구를 진행한 반면, 본 연구에서는 패스워드 인증 시스템의 전체 절차인 회원가입, 로그인, 패스워드 재발급 1단계, 패스워드 재발급 2단계의 모든 단계에 대한 보안 위협 및 보안 요구사항에 대해 분석하였다. 또한 기존 공통평가기준의 공격 성공 가능성이 로그인 단계에만 국한되었던 것을 확대시켜 패스워드 인증의 모든 단계에 대한 공격 성공 가능성을 측정하였으며, 국내외 포털사이트 패스워드 인증 시스템의 보안성을 정량화된 수치로 비교 분석하였다.

키워드 : 패스워드 인증 시스템, 포털사이트 보안 위협, 포털사이트 보안 요구사항, 공격 성공 가능성

1. 서 론

포털사이트(이하 포털)는 사전적으로 '입구', '관문'을 의미하는데, 인터넷의 방대한 정보를 수집하여 사용자가 필요한 정보만 수집할 수 있도록 해주는 게이트웨이의 역할을 하는 사이트를 말한다. 초기에는 검색 엔진, 이메일 서비스를 주로 제공하는 형태였으나, 현재는 뉴스, 쇼핑, 블로그 등 다양한 종류의 웹 서비스를 제공하고 있다. 또한 포털사이트의 이메일 계정은 페이스북, 트위터와 같은 소셜 네트워크 서비스(SNS), 다른 웹 서비스나 웹 애플리케이션의 아이디로 사용되거나 사용자가 다른 포털 계정 가입 시 패스워드를 분실하는 경우에 인증 수단으로 사용되기도 한다. 이처럼 포털사이트의 계정은 단순한 이메일 통신이 아니라 쇼핑, SNS, 다른 웹 서비스 등에서 다양한 용도로 사용될 수 있다.

포털사이트의 계정이 다른 웹 서비스나 포털에서 사용되는 경우, '보안은 사슬처럼 연결되어있기 때문에 가장 약한 보안 강도가 전체의 보안 강도를 결정한다[1]'는 최소한의 원리에 따라 두 개의 서비스의 보안 강도는 더 약한 보안

※ 본 논문은 한국산업기술평가관리원의 IT R&D 프로그램(10043959, 모바일단말의 비인가접근차단 및 운영환경 보장을 위한 EAL 4급 군사용 융합 보안 솔루션 개발) 사 업의 연구결과로 수행되었음.
※ 본 논문은 한국인터넷진흥원의 시큐어코딩 기반 SW 개발 보안 기반 기술 연구(3차년도 연구결과로 수행되었음.
† 준 회 원 : 고려대학교 정보보호대학원 석사과정
†† 준 회 원 : 고려대학교 정보보호대학원 석·박사통합과정
††† 준 회 원 : 고려대학교 정보보호대학원 박사과정
†††† 종신회원 : 고려대학교 정보보호대학원 정교수
Manuscript Received : July 25, 2014
First Revision : October 14, 2014
Accepted : October 24, 2014
* Corresponding Author : Seungjoo Kim(skim71@korea.ac.kr)

강도로 동일해진다. 예를 들어, 사용자가 구글 계정을 생성할 때 기존에 사용 중인 이메일 주소를 네이버 계정으로 입력하였다. 구글 계정의 패스워드 생성 조건은 8자리, 영문 대/소문자, 숫자 조합 없음이며 네이버 계정의 패스워드 생성 조건은 6자리, 영문 대/소문자, 숫자 조합 없음이다. 따라서 두 개 계정의 패스워드 보안 강도를 비교하였을 때 네이버 계정이 더 약한 보안 강도를 가지므로 이 사용자의 구글 계정의 보안 강도는 네이버의 보안 강도로 귀결됨을 알 수 있다. 이러한 특성을 이용하면 두 개의 계정을 모두 획득할 수 있다(두 개 계정의 아이디가 동일하다고 가정). 위의 예시와 동일하게 구글과 네이버 계정을 사용하는 경우, 공격자는 구글 계정을 해킹하기 위해 패스워드 재발급을 요청하고, 인증 방법으로 네이버 계정으로 본인 인증을 요청한다. 이때, 네이버 계정의 패스워드 보안 강도가 더 낮으므로 전수조사 등의 방법을 이용하면 구글 계정보다 쉽게 네이버 계정의 패스워드를 획득할 수 있다. 공격자가 네이버 계정을 획득하면 공격자는 구글 계정의 사용자 인증도 수행할 수 있으므로 두 개 계정의 패스워드를 획득하여 모든 계정에 접근 가능하다.

따라서 본 연구에서는 포털 사이트 계정의 회원가입, 로그인, 패스워드 재발급-1단계, 패스워드 재발급-2단계의 인증 시스템 및 수행 절차를 분석한다. 이를 토대로 하여 각 사이트의 인증 과정에서 발생 가능한 보안 위협과 이에 대응하기 위한 보안 요구사항을 도출한다. 이후 포털 사이트의 안전성을 정량화하여 표현하기 위해 공통평가방법론의 공격 성공가능성을 이용하여 보안 위협에 대한 보안 요구사항이 적절하게 적용되었는지 평가하며, 결론적으로 각 포털 사이트 인증시스템의 안전성에 대해 분석한다.

2. 관련 연구

2.1 패스워드 인증 시스템 관련 연구

온라인 서비스와 애플리케이션이 발전함에 따라 사용자는 계정을 생성하여 해당 서비스를 이용해야 한다. 현재까지 제안된 인증 시스템의 보안에 관한 연구는 아이디-패스워드 기반의 인증 시스템이 가지는 보안 취약점과 이를 개선하기 위한 방안에 대한 연구가 주를 이루었다. 서비스의 종류가 다양해지고 이를 이용하기 위해 사용자들은 모든 서비스에 계정을 생성하는데, 기억력의 한계와 관리의 용이성 때문에 대부분의 사용자들은 동일한 아이디와 패스워드를 사용한다. 이러한 경우 공격자가 사용자의 한 개의 계정 정보를 취득하면 해당 사용자의 다른 계정에도 접근할 수 있다는 문제가 있다[2]. 사용자 계정이 탈취된 사이트가 포털사이트라면 피해 규모가 작지만 인터넷 뱅킹, 인터넷 쇼핑몰 등 금융 결제와 관련된 사이트의 계정이 탈취된다면 심각한 피해를 야기할 수 있다. 또한 사용자가 패스워드를 분실한 경우 패스워드 재설정을 위한 본인 확인 과정에서 사용자에게 보안 질문에 대한 답을 요청하는데, 이러한 보안 질문은 대부분 사용자가 아니더라도 추측할 수 있는 대답이거나, 사용자도 기억하기 어려운 것이 많다. 따라서 이러한 문제를 해결하기 위해 계정 등록 시 보안 질문 설계 및 선택의 안전성을 향상시키기 위한 연구도 진행되었다[3]. 이후 사용자가 여러 개의 아이디를 기억하기 어려운 문제를 보완하기 위해 많은 서비스 제공 업체에서 사용자가 주로 사용하는 이메일 주소를 아이디로 활용하고 있다. 이때, 각 업체에서 사용하는 패스워드 관리 방안, 사용자가 동일한 패스워드를 설정하는지에 대한 여부와 같은 요소로 사용자 계정의 보안 위협과 프라이버시 침해 가능성을 분석하고 이에 대한 대응 방법을 제안하였다[4].

그리고 패스워드 인증 시스템의 안전성 분석에 대한 연구가 주를 이루었는데, 연속적인 인증 시도에 대응하기 위해 사람만 분별 가능한 답으로 기기를 판별하는 캡차(CAPTCHA), 안전하게 패스워드를 암호화하여 저장하기 위해 패스워드를 해시함수에 적용시킬 때 난수를 넣는 salting 기법, 패스워드를 여러 차례 반복적으로 해시함수로 암호화하고 공격자의 연속적인 공격 시도에 해석 시간을 길게 하여 대응하기 위한 key strengthen algorithm 등의 연구가 이루어졌다. 또한 패스워드의 강도를 판별하고 보다 안전한 패스워드 생성을 효율적으로 수행하기 위한 알고리즘이 제시되었다. 이는 엔트로피를 기반으로 안전성을 평가할 수 있는데 엔트로피는 Claude Shannon이 처음 제시한 용어로 불확실성 또는 랜덤성을 측정하기 위해 정의되었다[5]. 패스워드의 엔트로피값을 측정하기 위해 패스워드 길이의 분포, 문자열 배치, 문자 종류의 개수 그리고 문자열의 내용을 기준으로 하였으며 해당 내용을 합한 값을 전체 엔트로피값으로 측정하였다[6]. 그리고 패스워드의 엔트로피를 고려하여 패스워드의 품질(보안 강도)을 측정할 수 있는 지표인 PQI (Password Quality Indicator)를 제시하여 안전한 패스워드를 정량적으로 확인할 수 있는 방법을 제안하였다[7].

사용자가 패스워드 생성 시에 보안 강도가 강한 패스워드를 생성할 수 있도록 빠르고 정확하게 보안 강도를 판별하기 위한 다양한 방법도 제안되었다. 높은 보안 강도를 가지는 패스워드와 낮은 패스워드의 패턴을 분석하고 두 부분으로 나누어 사전 공격을 효율적으로 수행할 수 있다는 것을 증명하였고[8], 사용자가 패스워드를 생성할 때 공격자가 쉽게 추측할 수 있는 패스워드를 선택하지 않도록 하여 사전 공격에 대응할 수 있는 방법을 제안하였다. 공격자가 사전 공격에 이용할 사전을 생성할 때 주로 사용하는 단어 목록을 분류하고, 사용자가 패스워드 생성 시 입력하는 패스워

드를 검사하여 사전에 작성한 단어 목록에 포함된 단어가 존재하는 경우에는 패스워드 생성을 방지하는 방법으로 패스워드의 보안 강도를 향상시켰다[9].

앞서 살펴본 바와 같이, 현재까지 제안된 연구는 패스워드 시스템 전반에 걸친 내용이 아니라 아이디-패스워드 기반 인증에 대한 문제점과 대응방안을 제안한다는 한계가 있으며, 전반적인 패스워드 인증 시스템이 아닌 패스워드의 안전성을 대상으로 연구하여 전체 패스워드 인증 시스템에서 발생 가능한 보안 위협이나 공격에 대해서는 파악이 어렵다. 따라서 본 논문에서는 포털의 패스워드 인증 시스템인 회원가입, 로그인, 패스워드 재설정-1단계, 패스워드 재설정-2단계를 분석하고 패스워드 인증 시스템 전반에 걸친 보안 취약점 분석 및 이를 대응하기 위한 보안 요구사항을 도출한다.

2.2 공통평가기준의 공격 성공 가능성

공격 성공 가능성이란 공통평가기준의 공통평가방법론(CEM; Criteria Evaluation Methodology)의 부록 B에서 제시하는 전문성, 자원 및 동기에 대한 함수로서 경과 시간, 전문지식, 공격 대상에 관한 지식, 공격에 노출되기 쉬운 기간, 장비들을 각 요소로 가지며 각각의 요소들에 값을 부여하여 공격 대상에 대한 공격 성공 가능성을 정량적으로 나타낸다[10]. 세부적인 요소에 대한 설명은 다음과 같다.

1) 경과 시간

경과 시간이란 공격자가 특정 잠재적 취약성이 존재함을 식별하고 공격 방법을 개발하고 공격을 위해 요구되는 노력을 지속하기 위해 걸린 시간의 총합이다. 이 요소를 고려할 때 요구되는 시간의 양을 추정하기 위해 최악의 경우가 사용된다.

2) 전문지식

전문지식은 기반 원칙, 제품 유형 또는 공격 방법의 일반적인 지식수준을 말한다. 패스워드 인증 시스템에 적용되는 지식수준은 다음과 같다.

- 일반인: 특정 전문지식이 없으며 전문가 및 숙련자에 비하여 비전문적인 사람
- 숙련자: 패스워드 공격 도구 사용 방법, 패스워드 공격 방법에 대해 익숙하며 박식한 사람
- 전문가: 패스워드 공격 도구 작동 및 생성 방법, 패스워드 인증 시스템에 적용된 알고리즘 등에 대해 지식이 박식하고 사용이 익숙한 사람

3) 공격 대상에 관한 지식

공격 대상과 관련된 구체적 전문지식을 의미하며, 전문지식은 정보의 민감도와 연결된다. 공격 대상에 대한 지식의 식별 수준은 다음과 같다.

- 공개 정보: 패스워드 조합 방법 및 길이 등 인터넷으로 획득할 수 있는 정보의 수준
- 제한된 정보: 개발 조직 내에서는 통제되며 비밀 유지 계약하에 있는 타 조직과 공유되는 지식
- 민감한 정보: 개발 조직 내 민감한 사안을 다루는 팀들 사이에서 공유되는 지식, 특정 팀의 구성원에게만 제한된 접근 권한
- 중대한 정보: 소수의 사람에게만 알려진 지식, 개인별 업무와 지식을 기반으로 하여 매우 엄격하게 통제되는 접근 권한

4) 공격에 노출되는 기간(기회)

공격자가 공격 대상에 접근할 수 있는 시간과 비용을 의미하며, 경과 시간 요소와 관련된다. 자세한 분류 기준은 다음과 같다.

- 불필요한/제한 없는 접근: 공격 대상에 접근 시 탐지될 위험이 없어 공격자가 공격 대상에 접근 가능
- 쉬운 접근: 하루 이내의 시간 소요
- 보통 접근: 한 달 이내의 시간 소요
- 어려운 접근: 한 달 이상의 시간 소요
- 접근 불가: 공격 수행하는 데 공격에 노출되는 시간이 불충분

5) 장비

공격 대상의 취약점을 식별, 악용하는 데 사용되는 장비를 의미한다. 패스워드 인증 시스템에 이용되는 장비는 주로 전수조사 공격에 이용되는 도구이다. 패스워드 공격에 이용되는 도구에 대한 자세한 내용은 Table 1과 같으며[11], 분류 기준은 다음과 같다.

- 표준 장비: 공격자가 쉽게 구할 수 있는 장비. Table 1에 나온 패스워드 공격 도구는 인터넷 검색으로 쉽게 획득 가능

Table 1. Password attack tool

Tool	Equipment
Cain and Abel	Standard
John the Ripper	Standard
SolarWinds	Standard
RainbowCrack	Standard
wfuzz	Standard
brutus	Standard
THC Hydra	Standard
Medusa	Standard
OphCrack	Standard
L0phtCrack	Standard
Aircrack-NG	Standard

- 전문 장비: 쉽게 구할 수는 없으나 큰 노력 없이 획득 가능
- 맞춤형 장비: 특별히 제작되거나 일반 대중이 쉽게 구할 수 없음. 전수조사 공격을 위한 대규모로 서버를 운영
- 복합 맞춤형 장비: 공격 단계별로 여러 유형의 맞춤형 장비가 필요한 상황. 전수조사 공격뿐만 아니라 패스워드 인증 단계별로 다양한 장비 필요

아래 Table 2는 앞서 언급된 공통평가기준의 공격 성공 가능성에 대한 평가지표를 구체적으로 점수화한 표이다.

Table 2. Attack Potential of Common Criteria

Factor		Values
Elapsed Time	≤ 1 hour	1
	≤ 1 day	3
	≤ 1 week	5
	≤ 1 month	7
	≤ 6 month	10
	> 6 month	15
Expertise	Layman	0
	Proficient	3
	Expert	6
	Multi Expert	8
Knowledge of object	Public	0
	Restricted	3
	Sensitive	7
	Critical	11
Access to object	Non-Restricted	0
	Easy	1
	Normal	4
	Hard	10
	None	*
Tools	None	0
	Standard	4
	Bespoke	7
	Multi bespoke	9

3. 국내외 포털사이트 인증 시스템 비교 분석

본 절에서는 국내외 포털사이트의 인증 시스템에 대해 비교하고 국내 인증 시스템의 개선 방안에 대해 살펴본다. 본 연구의 분석 대상 업체는, 국내 포털은 네이버, 네이트, 다음이며, 해외 포털은 구글, 야후, MSN이다. 또한 포털사이트의 인증 절차는 회원가입, 로그인, 패스워드 재발급-1단계 인증, 패스워드 재발급-2단계 인증의 총 4단계로 나뉜다.

Table 3. Collected Information in Membership Registration
(○: Required Input, △: Selected Input,
-: Not Applicable, ◐: Input One of the Two)

	Naver	Nate	Daum	Google	MSN	Yahoo
Name	○	○	○	○	○	○
ID	○	○	○	○	○	○
E-mail address	○	○	◐	△	◐	-
Mobile number	○	○	◐	△	◐	○
Country	-	-	-	○	○	-
Gender	○	○	-	△	○	○
Birth	○	○	-	△	○	○
Address	-	-	-	△	○	-

3.1 회원가입

최근 개인정보 유출 문제가 빈번히 발생함에 따라 서비스 제공을 위해 최소한의 개인정보만 수집해야 한다. 아래 Table 1은 국내외 포털사이트별로 수집하는 개인정보를 정리한 표이다. 대부분의 국내외 포털사이트는 사용자의 이름, 이메일 주소, 휴대전화 번호를 기본적으로 요구하고 추가적으로 성별, 생년월일과 같은 정보를 수집한다. 그러나 구글은 이름, ID만을 수집하는 것으로 나타났다. 이는 이름과 ID만을 가지고도 사용자에게 정상적인 서비스 제공이 가능함을 의미한다.

또한 자동가입 프로그램을 이용하여 계정을 무작위로 생성하는 것을 방지하기 위해 포털에서는 캡차 또는 휴대전화 인증, 이메일 인증 등의 방안을 제공해야 한다. 구글은 이메일 주소, 휴대전화 번호를 수집하지 않기 때문에 이메일 인증, 휴대전화 인증을 제공하지 않고 캡차 입력을 요구한다. 그러나 사용자가 캡차 입력에 실패할 경우, 휴대전화 인증을 수행한다. MSN은 캡차 입력을 요구하고, 야후는 캡차 입력 없이 휴대전화 인증만 요청한다. 국내 포털은 캡차 입력은 요구하지 않고 휴대전화 인증 또는 이메일 인증과정을 거치는데, 휴대전화 번호마다 발급 가능한 ID 개수를 3개로 제한하여 무작위한 계정 생성을 방지한다. 그러나 ID 발급 개수 제한 정책으로 인해 공격자들이 기존 사용자의 계정을 도용하여 이를 악용하는 문제를 야기하기도 한다.

Table 4. Automatic registration portal prevention service

	Naver	Nate	Daum	Google	MSN	Yahoo
CAPTCHA	-	-	-	○	○	-
Email	-	◐	◐	-	-	-
Mobile Phone	○	◐	◐	-	-	○

3.2 로그인 시도

사용자는 포털 서비스를 제공받기 위해 로그인 과정을 거친다. 이때, 사용자의 패스워드 분실이나 공격자의 잘못된 로그인 시도에 대응하기 위한 방법이 존재한다. Fig. 2와 Fig. 3은 국내와 해외 포털의 로그인 과정을 도식화한 것이다. 자세한 내용은 다음과 같다.

1) IP주소 보안

국내 포털은 IP주소 정보의 사용범위를 사용자의 인터넷 접속환경에 맞게 설정할 수 있도록 하여 타인이 로그인 권한을 부정 사용하는 것을 방지하는 'IP보안'이라는 서비스를 제공한다. Fig. 1의 IP보안 설정 여부를 확인하는 단계가 IP주소 보안을 확인하는 부분이며, 설정된 경우에 대한 자세한 보안 단계별 서비스는 각 포털 업체의 정책에 따라 달라진다. 네이버는 3단계 서비스를 제공하는데 각 단계의 서비스 제공 범위는 아래와 같다. 설정 단계는 사용자가 직접 선택하여 사용 환경에 맞는 서비스를 받을 수 있도록 한다.

Fig. 1. Blocking overseas IP

- 1단계: 원거리에서 로그인 시도가 발생하는 것을 차단하기 위한 보통 수준의 보안 제공, 최근 로그인 IP주소와 C클래스가 동일한 경우
- 2단계: 높은 보안 수준 제공, 최근 로그인한 IP주소들의 목록과 동일한 경우
- 3단계: 최고 보안 수준 제공, 마지막 로그인 IP주소와 동일한 경우

또한 포털사이트는 해외에서 발생하는 공격 시도에 대응하기 위해 해외 IP주소 차단 서비스를 제공해야 한다. 해외 IP주소 차단 서비스를 제공하고 설정 여부는 사용자의 선택에 따른다. Table 5의 결과는 각 포털별로 사용자가 해외IP주소 차단 여부에 대해 설정하지 않은 경우, 각 업체에서 기본으로 수행되는 서비스에 대해 조사한 결과이다. 국내 포털이 국외 포털보다 해외 IP주소 차단 서비스가 잘 구축되어있음을 알 수 있다. 아래 Fig. 1은 해외 로그인 시도가 발생한 경우 네이버에서 사용자를 인증하는 화면이다. 네이버는 이름과 생일을 입력받아 본인 인증한다.

Table 5. Status of international IP protection services

	Naver	Nate	Daum	Google	MSN	Yahoo
Authenticaiton	○	○	-	○	-	-
Email Alarm	○	○	○	○	-	○

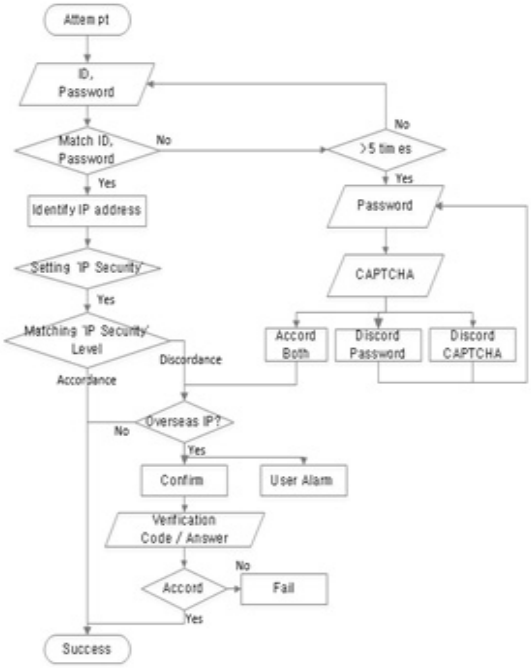


Fig. 2. Korean portal login procedure

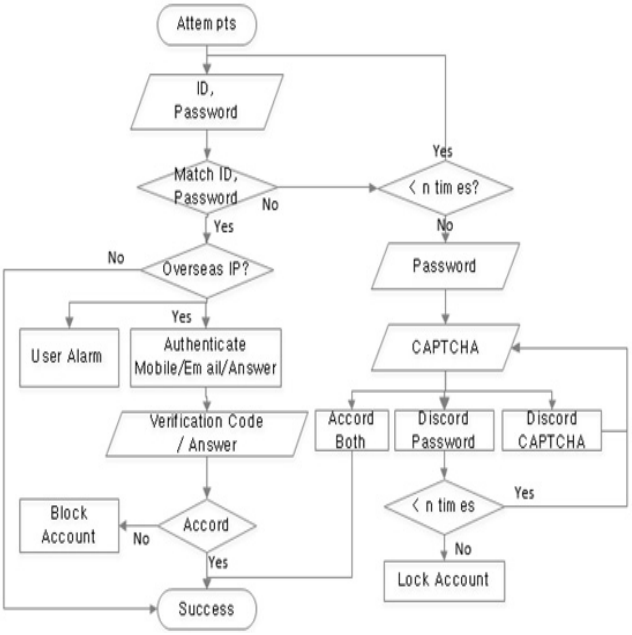


Fig. 3. Foreign portal login procedure

2) 연속적인 로그인 시도 발생 시

공격자는 봇을 활용하여 사용자 계정에 무작위로 로그인을 시도한다. 모든 포털에서는 봇을 이용한 계정 해킹에 대응하기 위하여 일정 횟수 이상으로 로그인에 실패할 경우 캡차 입력을 요청하고, 올바르지 않은 캡차값을 입력한 경우 패스워드와 캡차를 모두 재입력한다. 캡차 입력을 요구하는 로그인 실패 횟수는 각 포털마다 다른데, 구글의 경우 랜덤한 횟수로 캡차 입력을 요구하고, 다른 포털에서는 고정된 횟수로 캡차 입력을 요구한다. 구체적 횟수와 시행 여부는 Table 6과 같다.

Table 6. CAPTCHA and Account lockout threshold

	Naver	Nate	Daum	Google	MSN	Yahoo
CAPTCHA	5 Times	5 Times	5 Times	N Times	10 Times	5 Times
Account Lockout	-	-	○	○	○	○
Failed Count	-	-	5 Times	N Times	5 Times	5 Times
Lockout Time	-	-	3 Hours	24 Hours	24 Hours	12 Hours

또한 캡차 입력 이후로 추가적으로 로그인에 실패할 경우에는 일정 시간 동안 계정을 잠그고 더 이상의 로그인 시도를 차단해야 한다. 네이버, 네이트의 경우 계정 잠금 서비스를 제공하지 않으므로 공격자가 지속적으로 계정 해킹을 시도할 수 있다. Fig. 4는 야후에서 연속적으로 로그인에 실패하는 경우, 12시간 동안 계정 잠금을 사용자에게 알리는 경고메시지이다.

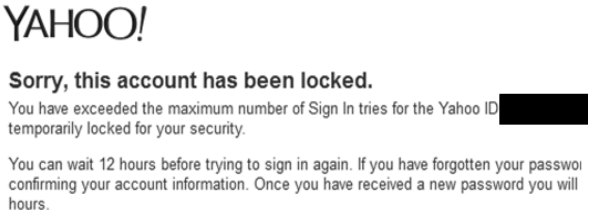


Fig. 4. Account lock

3.3 패스워드 재발급-1단계 인증

사용자가 패스워드 재발급을 요청할 경우 회원가입 시 등록한 이메일 주소 또는 휴대전화 SMS를 이용하여 사용자를 인증한다. 이메일 주소로 사용자를 인증하는 방법은 두 가지가 있다. 첫 번째 방법은 패스워드 재설정 페이지의 url을 메일로 전송하는 방법이다. 이 방법은 사용자가 등록한 이메일 계정에 로그인하고 발송된 메일을 확인하면 바로 패스워드를 재발급받을 수 있다. 두 번째 방법은 숫자로 구성된 인증번호를 메일에 첨부하여 전송하는 것이다. 사용자는 등록한 이메일 계정에 로그인하고 해당 메일의 인증번호를 패스워드 변경을 원하는 사이트에 입력하여 본인임을 인증한다. SMS를 이용한 인증은 이메일 인증의 두 번째 방법과 동일한 방식이지만, SMS로 인증번호가 전송된다는 점에서 차이가 있다. 국내외 모든 포털은 인증번호 전수조사 공격에 대응하기 위해 입력 횟수를 각각 1회에 5회, 3회로 제한하고, 정해진 횟수 이상으로 틀릴 경우 재발급을 요구한다. 또한 1일 인증번호 전송 횟수를 각각 10회, 5회로 제한하고 정해진 횟수 이상으로 인증번호 전송을 요구하는 경우 24시간 동안 일시적으로 계정을 잠근다.

구글의 경우, 회원가입 시 사용자에게 이메일 주소나 휴대전화 번호를 필수적으로 요청하지 않기 때문에 해당 정보를 입력하지 않은 경우가 발생한다. 따라서 위의 정보를 입력하지 않은 경우에는 2단계 인증으로 정당한 사용자임을 확인한다. 구글을 제외한 다른 포털에서는 회원가입 시 사용자에게 휴대전화 번호 또는 이메일 주소를 필수적으로 요청하기 때문에 1단계 인증으로 사용자를 확인할 수 있다.

3.4 패스워드 재발급-2단계 인증

1단계 인증에서 이메일 또는 SMS로 전송된 인증번호에 접근할 수 없는 사용자에 대해 2단계 인증을 수행한다. 국내 포털의 경우 2014년 8월 주민등록번호 수집 제한이 의무화되면서 기존의 주민등록번호를 이용한 사용자 인증을 폐지하였다. 이후 2단계 인증을 폐지하고 1단계 인증에서 통신사를 거친 본인 인증을 시행하고 있다. 해외 포털의 경우 2단계 인증에서 사용자를 확인하기 위해 사용자가 계정을 사용하면서 누적된 정보를 활용한다. 구글, MSN에서 2단계 인증을 위해 묻는 정보는 아래와 같다. 아래 정보를 단계별로 세분화하여 사용자로부터 값을 입력받는데, 입력된 값과 등록된 정보의 일치 여부를 확인하여 정상 사용자임을 확인한다. 구글의 경우, 사용자로부터 연락 가능한 이메일 주소를 입력받는데 사용자가 입력한 메일 주소가 사전에 등록해 놓은 이메일 주소와 동일하면 이후 입력값의 일치 여부와 관계없이 패스워드 재설정 url을 포함한 이메일을 해당 이메일 주소로 발송한다.

- 계정에 사용한 다른 암호
- 최근에 보낸 메일 제목
- 기본 폴더 외 다른 폴더
- 최근 보낸 메일의 수신자
- 선불카드번호 뒤 5자리
- 신용카드 이름
- 마지막 로그인 시기
- 계정 생성 시기
- 자주 연락하는 이메일 주소
- 최초 복구 이메일 주소
- 신용카드 번호 뒤 4자리
- 만료일

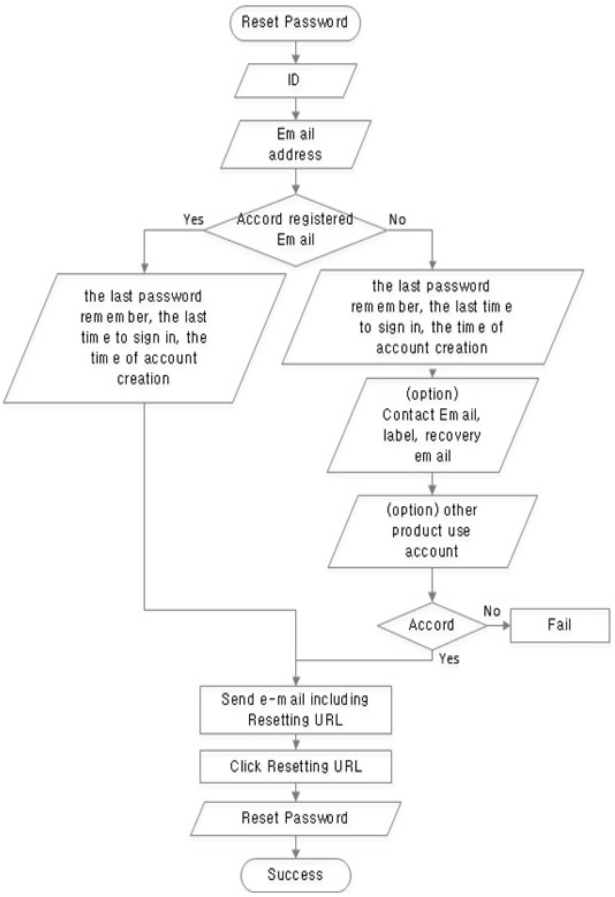


Fig. 5. Password reset second phasing procedure

4. 포털사이트 패스워드 인증 시스템의 보안 위협 및 보안 요구사항 분석

이 절에서는 앞서 분석한 국내외 포털사이트의 각 인증 단계에서 발생 가능한 보안 위협 및 보안 요구사항에 대해 분석한다. 발생 가능한 보안 위협은 로그인 과정에서 발생 가능한 위협, 패스워드 위협 등을 고려하여 분석하였다. Table 7은 각 포털별 패스워드 인증 단계에서 발생 가능한 보안 위협에 대해 정리한 표이다.

4.1 패스워드 인증 시스템의 보안 위협 분석

1) 회원가입 단계 보안 위협

T1. 자동가입

공격자들은 광고 목적의 스팸메일 발송, 피싱 사이트 유도, 광고용 게시글 작성 등 다양한 방법으로 금전적 이득을 취한다. 이용 가능한 계정의 수가 많을수록 더 많은 스팸메일을 발송하거나 광고용 게시글을 작성할 수 있기 때문에 자동가입 프로그램을 이용하여 계정을 생성한다.

2) 로그인 단계 보안 위협

T2. 연속적인 인증 시도

공격자는 사용자 계정의 패스워드를 획득하기 위하여 전수조사, 패스워드 추측 등의 방법을 이용한 연속적인 인증을 시도한다. 전수조사 공격은 가능한 패스워드 조합을 모두 대입하여 올바른 패스워드를 탐색하는 공격 방법이고, 패스워드 추측 공격은 사용자의 이름, 생년월일, 가족 관계 등의 정보를 조합하여 가능한 패스워드를 추측하는 방법이다. 또한 사용자들이 가장 많이 사용하는 패스워드와 같은 정보를 대입하여 인증 시도하는 공격 방법도 존재한다.

T3. 피싱(Phishing)

사용자가 포털사이트에 접속할 때, 악성코드 유포와 같은 방법으로 공격자는 정상 사이트가 아닌 위조 사이트를 사용자에게 출력한다[12]. 일반 사용자들은 정상 사이트와 위조된 사이트를 구분하기 어렵기 때문에 평소처럼 아이디와 패스워드를 입력하는데, 이때 공격자는 입력받은 아이디와 패스워드를 획득할 수 있다.

T4. 키로깅(Keylogging, Keystroke logging)

키로깅은 키보드로 입력하는 정보를 중간에서 가로채기하여 정보를 훔쳐가는 공격 기법이며, 키로깅 프로그램을 이용하여 공격을 수행한다[13]. 정상적인 처리과정은 키보드로 입력한 정보를 운영체제(OS)에서 처리하여 모니터에 해당 정보를 보여주지만, 키로깅 프로그램은 키보드에서 입력

Table 7. Security threats that can occur in the portal sites

		Naver	Nate	Daum	Google	MSN	Yahoo
Membership registration	T1. Automatically sign up	○	○	○	○	○	○
Login	T2. Consecutive login attempts	○	○	○	○	○	○
	T3. Phishing	○	○	○	○	○	○
	T4. Keylogging	○	○	○	○	○	○
Password Reset - first phasing	T5. Consecutive login attempts	○	○	○	○	○	○
	T6. Email Sniffing	○	○	○	○	○	○
	T7. Eavesdrop Smart Phone	○	○	○	○	○	○
Password Reset - second phasing	T8 Guessing user information	-	-	-	○	○	○
	T9. Disguise as user	○	○	○	-	-	-

한 정보를 운영체제에서 처리할 때 정보를 가로채 파일 등으로 저장하였다가, 지정된 서버로 파일을 전송하여 정보를 유출한다. 공격자는 사용자가 포털사이트에 로그인하는 순간 키보드에 입력한 키 값을 분석하여 아이디와 패스워드에 해당하는 값을 추측, 획득할 수 있다. 실제로 키로깅 프로그램을 사용하여 포털 및 소셜 네트워크 서비스(SNS) 계정을 획득한 공격이 발생하는데, 2013년 12월 페이스북 31만 8000건, 구글 7만 건, 트위터 2만 2000건 등 전 세계 9만 3000개의 웹사이트에서 사용자정보 200만 건의 사용자 계정이 키로깅 공격에 의해 해킹당했다. 공격자는 사용자 컴퓨터에 키로깅 프로그램을 설치하여 주요 웹사이트 아이디와 패스워드 등의 웹사이트 로그인 기록을 획득하였다[14].

3) 패스워드 재발급-1단계

T5. 연속적인 로그인 시도

공격자는 패스워드 재발급 단계에서 사용자가 본인 인증을 위해 이메일 인증을 선택한 경우 다른 계정의 패스워드를 획득하기 위하여 연속적으로 로그인을 시도할 수 있다. 이때, 사용자가 등록한 이메일 계정의 패스워드의 강도, 즉 요구되는 패스워드 자릿수, 문자 조합의 수가 적을 경우 공격의 난이도는 감소한다[15]. 따라서 공격자는 이러한 특성을 이용하여 전수조사 등의 방법으로 두 개의 계정의 사용자 패스워드를 획득할 수 있다.

T6. 이메일 스니핑(sniffing)

스니핑은 네트워크상에서 자신이 아닌 다른 상대방의 패킷을 도청하는 행위를 의미한다. 포털은 패스워드 재발급-1단계에서 사용자 인증을 위해 이메일 인증과 휴대전화 인증을 사용한다. 이 중 이메일 인증은 사용자가 회원가입 시 또는 사전에 등록한 이메일 주소로 인증번호 또는 패스워드 재발급 url을 포함한 이메일을 전송하는 방법이다. 이때, 공격자는 포털에서 전송한 이메일을 스니핑하여 인증번호를 획득하거나 패스워드 재발급 페이지로 이동하여 사용자 대신 사용자 계정의 새로운 패스워드를 설정할 수 있다.

T7. 휴대전화 도청

공격 대상이 스마트폰을 사용하는 경우 공격자가 사전에 악성코드를 설치하여 공격 대상의 SMS 또는 통화 내용을 도청할 수 있다. 이러한 공격 상황에서 사용자가 패스워드 재발급을 위해 인증번호를 포함한 SMS를 전송받는 경우 공격자는 공격 대상의 SMS를 도청하여 인증번호를 획득할 수 있다. 따라서 공격자는 사용자 계정의 새로운 패스워드를 재발급받아 사용자 계정 권한을 획득할 수 있다.

4) 패스워드 재발급-2단계

T8. 사용자 정보 추측

구글과 MSN의 경우 사용자가 이메일 인증이나 휴대전화 인증을 수행할 수 없는 경우, 사용자의 계정 정보를 활용하

Table 8. Correspondence table of the security requirements that can accommodate security threats

the Phasing of Security Threat / Security Requirement	Membership registration	Login			Password Reset - first phasing			Password Reset - second phasing	
	T1. Automatically sign up	T2. Consecutive login attempts	T3. Phishing	T4. Keylogging	T5. Consecutive login attempts	T6. Email Sniffing	T7. Eavesdrop Smart Phone	T8. Guessing user information	T9. Disguise as user
R1. CAPTCHA	×	×			×				
R2. Improved password security strength		×			×				
R3. Two channel authentication		×		×	×				
R4. Keyboard hacking prevention program				×					
R5. Virtual Keyboard				×					
R6. Log in identifying the IP address		×	×		×				
R7. Blocking abroad IP		×	×						
R8. Phishing prevention / response technology			×						
R9. Account Lockout		×							
R10. Encrypted communication			×		×	×			
R11. A reset of password security questions robustness								×	×
R12. Install anti-virus program (user)							×		

여 사용자를 인증한다. 이때, 포털에서 요구하는 정보는 최근 로그인 시기, 계정 생성시기, 연락처, 이메일 주소, 폴더 이름 등이 있다. 공격자는 특정 사용자를 대상으로 하는 공격에서 추측 가능한 정보를 입력하여 사용자로 가장한다. 특히, 야후처럼 보안질문을 활용하는 경우, SNS에서 공개된 계정 정보를 조합하면 해당 질문에 대한 답변을 추측할 수 있다[16]. 정확한 정보를 추측한 공격자는 해당 사용자의 패스워드를 재발급받을 수 있다.

T9. 사용자 위장

국내 포털의 경우 비밀번호 재발급-2단계에서는 사용자로부터 주민등록번호 또는 주민등록증 사본을 전달받아 주민등록번호를 활용해 사용자를 인증한다. 그러나 주민등록번호를 포함한 개인정보 유출 사건이 빈번하게 발생함에 따라 주민등록번호 및 성명의 일치 여부에 의하여 본인 확인을 하는 방식의 실효성이 의심되는 실정이다[17]. 공격 대상의 주민등록번호를 획득한 공격자는 공격 대상으로 위장하여 메일 또는 팩스로 개인정보를 전송한 후 비밀번호를 재발급 받을 수 있다.

4.2 패스워드 인증 시스템의 보안 요구사항 도출

이 절에서는 앞서 분석된 포털 인증 시스템의 보안 취약점에 대응 가능한 보안 요구사항을 도출한다. 또한 전체 패스워드 인증 시스템의 안전성을 분석하기 위한 공격 성공 가능성 평가지표를 제안한다. 공격 성공 가능성은 공통평가기준에 제안된 공격 성공 가능성을 기준으로 하며, 구체적인 요소는 제안된 보안 요구사항을 세분화하여 평가지표를 생성한다. Table 8은 패스워드 인증 시스템의 단계별 보안 위협에 대응 가능한 보안 요구사항을 나타낸 표이다.

R1. 캡차(CAPTCHA)

캡차는 어떠한 사용자가 실제 사람인지 컴퓨터 프로그램인지를 구별하기 위해 사용되는 방법이다. 사람은 구별할 수 있지만 컴퓨터는 구별하기 힘들게 의도적으로 비틀거나 덧칠한 그림을 주고 그 그림에 쓰여 있는 내용을 물어보는 방법이 자주 사용된다[18]. 자동가입 프로그램은 사람이 아닌 컴퓨터 프로그램으로 실행되므로 캡차를 이용하면 자동가입 프로그램을 이용해 계정을 생성하는 공격을 방지할 수 있다. 또한 전수조사 공격은 주로 컴퓨터 프로그램을 사용하여 무차별적으로 패스워드를 대입하여 올바른 패스워드를 획득하는 공격이다. 포털사이트의 계정을 획득하기 위하여 공격자는 전수조사 프로그램을 활용하여 연속적으로 인증을 시도한다. 따라서 로그인 시 캡차 입력을 요청하는 경우, 전수조사 프로그램을 이용한 공격에 대응할 수 있다.

R2. 보안 강도가 향상된 패스워드

전수조사 공격은 사용자의 패스워드 강도에 따라 공격 소요 시간과 난이도가 결정된다. 따라서 사용자가 안전한 패스워드를 생성하기 위해서는 다음 조건을 만족해야 한다[19].

- 영문 대문자, 소문자, 숫자, 특수문자 모두 포함
- 최소 8자리 이상
- 가족 이름, 전화번호 등과 같은 추측 가능한 개인정보에 기반한 패스워드 생성 금지
- 다른 웹사이트와 동일한 패스워드 사용 금지

R3. 2단계 인증

2단계 인증은 단일 인증의 보안 취약성을 보완하기 위하여 세 가지 사용자 인증 방법(사용자가 가지고 있는 정보, 유일한 정보, 알고 있는 정보) 중에서 서로 다른 두 개의 인증을 조합하여 사용자를 인증하는 것을 말한다. 가장 보편적인 방법은 '패스워드와 같은 알고 있는 정보'와 'OTP, 보안토큰, 스마트폰 등 가지고 있는 정보'를 조합하여 사용하는 것이다. 이러한 2단계 인증 방식은 원격 접속 및 ID 도용 피해를 줄일 수 있다.

R4. 키보드 해킹 방지 프로그램

키보드 해킹 방지 프로그램은 다음과 같은 방법으로 키로거를 활용한 패스워드 해킹에 대응한다[20]. 첫 번째 방법은 보안 키보드 드라이버를 설치하여 보안 키보드 드라이버와 연결된 보안 입력창에 "*" 등의 특수문자를 출력하고, 기존의 키보드 입력값이 전달되는 경로에는 NULL값을 전달하여 어떠한 키보드 입력값도 감지할 수 없도록 하는 것이다. 두 번째 방법은 사용자가 입력창에 값을 입력할 때마다 별도로 설치된 보안 키보드 드라이버에서 암호화한 값을 전송하는 것이며, 암호 키는 사용자가 입력창을 선택할 때마다 다른 값으로 생성된다. 공격자는 암호화된 값으로 받기 때문에 해당값이 어떤 키보드값인지 알 수 없다. 마지막 방법은 키로거 설치 여부를 확인하고 키로거가 가동 중인 경우, PC 화면에 가상 키보드창을 출력하여 사용자가 마우스로 입력값을 클릭하도록 하여 키로거에 대응하는 것이다.

R5. 가상 키보드

가상 키보드는 주로 금융 거래 시 공인인증서 암호, 계좌 패스워드 입력을 위해 화면에 출력되는 가상의 키보드이다. 사용자는 화면에 출력되는 키보드에 입력값을 마우스로 클릭하거나 스마트폰, 태블릿의 화면을 터치하는 방법으로 값을 입력한다. 따라서 공격자가 키로깅 프로그램을 설치하여 사용자의 패스워드를 획득하고자 하는 경우, 키 입력값을 획득하기 어렵기 때문에 패스워드 노출을 막을 수 있다.

R6. 로그인 IP주소 식별

사용자가 기존에 로그인한 IP주소를 저장하고 저장된 IP주소의 범위에서 벗어난 로그인 기록이나 마지막에 로그인한 IP주소와 동일하지 않은 IP주소에서 로그인 시도를 하는

경우에 대해 본인 확인 요청을 한다. 본인 인증에 성공한 사용자는 정상 사용자임을 인지하고 계정 접근을 허가하고, 이외의 경우에는 공격자로 간주해 계정 접근을 차단한다.

R7. 해외 IP주소 차단

스팸메일 발송은 중국, 미국에서 주로 이루어지는데 해당 지역에 서버를 두고 일반 사용자들의 계정을 해킹하는 경우가 발생하고 있다[21]. 따라서 포털사이트에서는 사용자가 등록된 국가가 아닌 다른 국가에서 로그인 시도를 할 경우, 본인 인증 단계를 거쳐 정상적인 사용자의 접근만 허가하고 사용자에게 해외 로그인 시도에 대해 공지하여 혹시 모를 공격 시도에 대해 알려야 한다.

R8. 피싱 방지/대응 기술

안티 피싱은 피싱 사이트 탐지 후 피싱 사이트로 추측되는 사이트를 차단하는 방법 또는 사용자가 스스로 피싱 사이트와 정상 사이트를 구분할 수 있도록 하는 방법을 의미한다. 피싱 사이트 탐지 방법에는 크게 유사 도메인 검색, HTTP 트래픽 분석이 있다. 첫 번째로, 유사 도메인을 통한 피싱 사이트 탐지는 블랙리스트, 화이트리스트 기법으로 분류할 수 있다. 블랙리스트 기반의 탐지 기법은 피싱 사이트로 알려진 서버들의 주소를 블랙리스트에 등록하고 이 리스트에 속한 주소에 대해 피싱 사이트임을 인지하는 방법이며, 화이트리스트 기반의 탐지 기법은 합법적인 서버들의 주소를 등록하여, 주어진 사이트가 아님을 판별하는 방법이다. 두 번째로 HTTP 트래픽 분석을 통한 탐지 방법은 정상 사이트의 그림 및 게시글을 링크하는 방식을 이용하여 정교하게 위장하는 피싱 사이트를 탐지하기 위해 사용된다. 피싱 사이트에서 참조하고 있는 게시글 및 그림을 정상 사이트에 요청하는 HTTP 트래픽을 모니터링 및 분석을 통해 피싱 사이트를 탐지하는 방법이다.

R9. 계정 잠금

공격자가 전수조사 프로그램을 이용하여 연속적인 인증 시도를 하는 경우, 무제한으로 인증 시도가 가능하다면 언젠가는 사용자 계정을 획득할 수 있다. 따라서 인증 시도 횟수를 제한함으로써 공격자가 무제한으로 공격을 시도하여 사용자 계정을 획득하는 것을 방지할 수 있다.

R10. 암호화 통신

암호화 통신이란 개체 간 통신 과정에서 타인이 통신 내용을 도청하거나 가로채는 것을 막기 위해 통신 내용을 공유된 키로 암호화하여 전달하는 것을 의미한다. 암호화된 통신 내용은 키를 소유하지 않은 사람은 패킷의 내용을 알아볼 수 없으므로 패킷이 노출되더라도 정보가 유출되지 않는다. 따라서 포털에서는 개체 간 통신의 기밀성, 무결성, 사용자 인증을 위해 암호화된 통신을 제공해야 한다.

R11. 패스워드 재발급 시 보안질문의 강력성

기존의 보안질문은 '어머니의 이름은 무엇입니까?'처럼 공격자가 추측하기 쉬운 형태 또는 '꿈의 직업은 무엇입니까?' 같이 사용자도 기억하기 어려운 형태로 제공되었다[22]. 이러한 질문은 보안성과 사용자 편의성이 모두 낮으므로 서비스 제공 업체에서는 이를 개선한 형태의 보안질문으로 사용자 인증을 수행해야 한다. 보안성이 강화된 보안질문은 하나의 질문이 아닌 복수 질문을 요청하고 정답률이 일정 수준 이상으로 입력될 경우에만 정당한 사용자임을 증명해야 한다. 또한 사용자의 편의성을 강화하기 위해 사용자가 즉석으로 생성하여 기억하는 답이 아닌 계정 이용 중 사용자의 경험, 행동에 의해 생성된 질문에 대한 답을 요청하여 사용자가 기억하기 쉽도록 해야 한다.

R12. 백신 프로그램 설치(사용자)

스마트폰 사용자가 스스로 공격자로부터 악성 프로그램을 이용한 휴대전화 도청, 정보 유출 등의 문제에 대응하고자 미리 스마트폰에 백신 프로그램을 설치하고 주기적으로 점검함으로써 안전하게 스마트폰을 사용할 수 있도록 한다.

5. 포털사이트별 공격 성공 가능성 측정 및 안전성 비교

본 절에서는 2.2절에서 언급한 공통평가기준의 공격 성공 가능성 지표를 기준으로 각 포털사이트의 패스워드 인증 시스템 단계별로 공격 성공 가능성을 측정하고, 안전성을 비교 분석한다.

5.1 포털사이트 공격 성공 가능성 측정

본 절에서는 앞서 도출한 포털사이트 패스워드 인증 시스템의 공격 위협 및 보안 요구사항을 기반으로 각 포털사이트의 공격 성공 가능성을 측정한다.

1) 회원가입

회원가입 단계에서는 자동가입 프로그램을 활용한 계정 생성이 주된 공격 위협이다. 회원가입 단계에서는 각 포털사이트의 보안 위협 및 대응 방안이 유사하므로 거의 동일한 공격 시나리오를 바탕으로 공격이 수행된다. 자동가입 프로그램을 활용하여 계정을 생성하는 데 소요되는 시간은 1시간 이내이다. 또한 이 프로그램은 구체적인 보안 지식이 없어도 쉽게 사용할 수 있으므로 일반인도 수행이 가능하며, 캡차, 휴대전화 인증을 자동가입 방지 대책으로 수행하고 있는데 이러한 정책은 이미 공개된 정보이다. 자동가입 프로그램은 사용료를 지불하거나 인터넷 커뮤니티에 소수의 사람들끼리 공개되므로 '전문 장비'로 분류된다.

공격 대상에 대한 접근성에서 국내외 포털사이트에 차이가 있다. 국내 포털사이트의 경우, 휴대전화 1개당 3개의 계정을 생성하도록 제한하고 있으므로 자동가입 프로그램을

활용하더라도 무제한으로 계정 생성은 불가능하지만, 해외 포털사이트는 계정 제한이 없으므로 무제한으로 생성이 가능하다. 회원가입 단계에 대한 공격 성공 가능성은 아래 Table 9와 같이 측정할 수 있다.

Table 9. Attack Potential of Membership Registration

	Naver	Nate	Daum	Google	MSN	Yahoo
Elapsed Time	1	1	1	1	1	1
Expertise	0	0	0	0	0	0
Knowledge of Object	0	0	0	0	0	0
Access to Object	1	1	1	0	0	0
Tools	7	7	7	7	7	7
Total	**9**	**9**	**9**	**8**	**8**	**8**

2) 로그인

로그인 단계에서 발생 가능한 공격 방법은 연속적인 인증 시도, 피싱, 키로깅이 있으며, 공격 성공 가능성을 측정하기 위해 각 공격 기법별로 분류한다. 따라서 각 포털사이트의 로그인 단계의 공격 성공 가능성은 각 공격 기법을 종합하여 최소한의 점수를 갖는 공격 기법을 기준으로 한다.

a) 연속적인 인증 시도

연속적인 인증 시도의 소요 시간은 포털사이트의 패스워드 강도에 따라 결정되며, 각 포털사이트의 패스워드 강도는 다음과 같다.

- 네이버: 6자리 이상, 영문 대/소문자, 숫자, 특수문자 조합 X
- 네이트: 6자리 이상, 영문 대/소문자 숫자 조합 O(특수문자 제외)
- 다음: 8자리 이상, 영문 대/소문자, 숫자, 특수문자 조합 X
- 구글: 8자리 이상, 영문 대/소문자, 숫자 조합 X
- MSN: 8자리 이상, 영문 대/소문자, 숫자 조합 O(특수문자 제외)
- 야후: 8자리 이상, 영문 대/소문자, 숫자 조합 O(특수문자 제외)

Table 10. Elapsed time for brute force attack

	Naver	Nate	Daum	Google	MSN	Yahoo
Elapsed Time	13 min	1 hour 32 min	6 days 4hours	6 days 4hours	82 days 21 hours	17 years 130 days

위의 Table 10은 공격 소요 시간을 측정하기 위하여 3.4GHz Intel Core i7-2600K의 사양을 갖는 공격자의 PC에서 공격 툴인 'John the Ripper'를 사용한다고 가정하고 측정하였으며, 사용 가능한 최소한의 조합을 이용하는 경우의 소요 시간이다. 네이버, 네이트는 6자리의 비밀번호를 사용하며, 계정 잠금 서비스도 제공하지 않으므로 공격에 소요되는 시간이 적게 나타났다. 야후는 영문 대소문자, 숫자 조합 사용을 의무화하므로 소요 시간이 가장 긴 것으로 나타났다. 또한 네이버, 네이트의 경우 계정 잠금 서비스를 제공하지 않으므로 공격 대상에 대한 접근이 다른 포털사이트보다 용이한 것으로 분석되었다.

연속적인 인증 시도를 위한 공격 도구는 Table 1에 언급된 바와 같으며, 인터넷에 쉽게 공개되어있어 누구나 쉽게 획득할 수 있다. 또한 보안에 대한 지식이 있는 숙련자라면 충분히 이용 가능하다. 따라서 로그인 단계의 연속적인 인증 시도에 대한 공격 성공 가능성은 아래 Table 11과 같이 측정할 수 있다.

Table 11. Attack Potential of Consecutive login attempts

	Naver	Nate	Daum	Google	MSN	Yahoo
Elapsed Time	1	3	5	5	10	15
Expertise	6	6	6	6	6	6
Knowledge of Object	0	0	0	0	0	0
Access to Object	1	1	4	4	4	4
Tools	4	4	4	4	4	4
Total	**12**	**14**	**19**	**19**	**24**	**29**

b) 피싱

피싱 공격은 공격자가 원본 사이트와 피싱 사이트를 얼마나 유사하게 제작하는가에 따라 공격 성공 여부가 달라진다. 각 포털사이트 로그인 화면의 소스코드가 그대로 노출되는 경우에는 누구나 쉽게 제작이 가능하며, 그 외의 경우에는 홈페이지 제작 도구를 활용하여 최대한 유사한 피싱 사이트를 제작한다. 이때, 공격자는 웹에 대한 기본 지식을 가지고 있어야 한다. 구글, MSN은 로그인 페이지에 소스코드를 그대로 노출시키지 않아 다른 포털사이트에 비해 공격 소요 시간이 오래 소요된다. 또한 페이지 소스를 그대로 복사하여 제작된 사이트는 원본 사이트와 유사하므로 보다 많은 공격대상의 패스워드를 획득할 수 있다. 피싱 공격에 대응하기 위해서 네이버, 구글, MSN은 툴바(MSN툴바-피싱필터, 네이버 툴바-안티 피싱), 브라우저(구글 크롬-피싱 및 멀웨어 알림)에 안티 피싱 기술을 적용하고 있으며, 야후는 보안씰 서비스를 제공하는데, 보안씰이란 사용자가 사전에 선택한 그림을 로그인 시 화면에 출력하여 해당 그림이 출력되면 정상 사이트의 로그인임을 인지할 수 있도록 하는 피싱 방지 기술이다. 따라서 네이버, 구글, MSN, 야후를 대상으로 하는 공격은 사용자가 해당 포털사이트가 제공하는 안티 피싱 기술을 이용한다면 네이트, 다음보다 접근이 어렵다. 로그인 단계의 피싱 공격에 대한 공격 성공 가능성은 아래 Table 12와 같이 측정할 수 있다.

Table 12. Attack Potential of Phishing

	Naver	Nate	Daum	Google	MSN	Yahoo
Elapsed Time	3	3	3	5	5	3
Expertise	3	3	3	6	6	3
Knowledge of Object	0	0	0	3	3	0
Access to Object	4	1	1	4	4	4
Tools	4	4	4	4	4	4
Total	**14**	**11**	**11**	**22**	**22**	**17**

c) 키로깅

키로깅은 포털사이트의 보안 정책보다는 사용자의 PC 환경에 따라 영향을 받으므로 모든 포털사이트가 동일한 공격 성공 가능성을 가진다. 키로깅 공격은 사용자 PC에 키로거 프로그램을 설치하고, 사용자가 아이디와 패스워드를 입력하고 그 값을 해독하면 사용자 계정을 획득할 수 있다. 키로깅 공격의 소요 시간은 공격자가 입력된 키 값을 해석하는 시간에 따라 달라지며, 일반적으로 1일 이내의 시간이 소요된다. 또한 키로거 프로그램은 인터넷에 공개된 도구이며, 키로거 프로그램은 스팸메일, 악성 게시글 등의 방법으로 유포되므로 해당 글이나 메일을 열람한 공격 대상에 쉽게 접근할 수 있으므로 쉬운 접근으로 분류된다. 로그인 단계의 키로깅 공격에 대한 공격 성공 가능성은 아래 Table 13과 같이 측정할 수 있다.

Table 13. Attack Potential of Keystroke Logging

	Naver	Nate	Daum	Google	MSN	Yahoo
Elapsed Time	3	3	3	3	3	3
Expertise	3	3	3	3	3	3
Knowledge of Object	0	0	0	0	0	0
Access to Object	1	1	1	1	1	1
Tools	4	4	4	4	4	4
Total	**11**	**11**	**11**	**11**	**11**	**11**

앞서 로그인 단계의 공격 성공 가능성을 분석한 결과, 키로깅 공격에 대한 공격 성공 가능성이 가장 낮은 것으로 분석되었다. 따라서 로그인 단계에서의 모든 포털사이트의 공격 성공 가능성은 가장 낮은 안전성을 갖는 키로깅 공격과 동일하다.

3) 패스워드 재발급-1단계

사용자가 패스워드 재발급을 요청한 경우, 공격자는 SMS 도청, 인증번호 전수조사, 다른 이메일 계정 접근의 3가지 방법으로 사용자 계정을 획득할 수 있다. 따라서 각 포털사이트의 패스워드 재발급 - 1단계의 공격 성공 가능성은 각 공격 기법을 종합하여 최소한의 점수를 갖는 공격 기법을 기준으로 한다.

a) SMS 도청

SMS 도청의 방법은 사용자가 스마트폰을 사용하는 경우에 해당 스마트폰에 도청 애플리케이션을 설치해 휴대전화로 전달된 인증번호를 획득하는 방법이며, 이러한 방법은 특정 공격대상으로 공격을 진행할 경우에 효과적이다. 도청을 위한 악성 애플리케이션은 공격자가 직접 제작하거나 구입 가능하며, 일반인도 쉽게 사용이 가능하다. 또한 휴대전화 인증 시 SMS로 전송된 인증번호는 3분간 유효하므로 해당 시간 안에 인증번호를 획득하고 패스워드를 재발급받아야 공격에 성공할 수 있다. 스마트폰의 취약점과 관련된 내용은 인터넷 검색을 통해 획득 가능한 정보이므로 공개된 정보로 분류한다. 사용자 스마트폰에 설치된 악성 애플리케이션에 의해 공격 성공 여부가 결정되므로 포털사이트의 보안 정책과는 무관하여 모든 포털사이트가 동일한 공격 성공 가능성을 가짐을 확인할 수 있다. 따라서 회원가입 1단계의 SMS 도청 공격에 대한 공격 성공 가능성은 아래 Table 14와 같이 측정할 수 있다.

Table 14. Attack Potential of SMS eavesdropping

	Naver	Nate	Daum	Google	MSN	Yahoo
Elapsed Time	1	1	1	1	1	1
Expertise	0	0	0	0	0	0
Knowledge of Object	0	0	0	0	0	0
Access to Object	4	4	4	4	4	4
Tools	4	4	4	4	4	4
Total	**9**	**9**	**9**	**9**	**9**	**9**

b) 인증번호 전수조사

인증번호는 6자리 숫자로 구성되어있으므로 경우의 수가 적기 때문에 전수조사를 통한 소요 시간이 더 짧다. 인증번호 전수조사에 대응하기 위해서 포털사이트에서는 연속적으로 인증번호 인증에 실패할 경우, 계정 잠금 서비스를 제공하는데 자세한 내용은 Table 15와 같다.

그러나 고정된 패스워드와 달리 인증번호는 재전송될 때마다 랜덤하게 전송되므로 10개의 숫자로 이루어진 6자리 숫자의 경우의 수인 100만 개 중에 10번 또는 5번의 입력

Table 15. Validation Code

	Naver	Nate	Daum	Google	MSN	Yahoo
Input	5 times	5 times	5 times	3 times	3 times	3 times
Transmission	10 times	10 times	10 times	5 times	5 times	5 times
Account Lock	24 hours	24 hours	24 hours	24 hours	24 hours	24 hours

기회만 존재하므로 이는 접근이 어렵고, 공격 소요 시간도 6개월 이상으로 소요됨을 알 수 있다.

전수조사 공격에 사용되는 도구, 지식수준, 공격자의 능력은 연속적인 인증 시도와 동일하며, 경과 시간과 공격 대상에 대한 접근은 포털사이트의 인증번호 입력/전송 횟수 제한에 따라 달라진다. 따라서 비밀번호 재발급 1단계의 인증번호 전수조사 공격에 대한 공격 성공 가능성은 아래 Table 16과 같이 측정할 수 있다.

Table 16. Attack Potential of Bruteforce Validation Code

	Naver	Nate	Daum	Google	MSN	Yahoo
Elapsed Time	15	15	15	15	15	15
Expertise	3	3	3	3	3	3
Knowledge of Object	0	0	0	0	0	0
Access to Object	10	10	10	10	10	10
Tools	4	4	4	4	4	4
Total	**32**	**32**	**32**	**32**	**32**	**32**

c) 다른 이메일 계정 접근

다른 이메일 계정 접근은 사용자가 패스워드 재발급 시 이메일 인증을 통한 본인 확인을 요청한 경우 발생 가능한 공격이다. 각 포털사이트는 Table 17과 같은 이메일 인증 방법을 이용하고 있는데, 야후는 이메일 인증은 제공하지 않고 휴대전화 인증만을 제공하므로 논외로 한다.

Table 17. E-mail Authentication

	Naver	Nate	Daum	Google	MSN	Yahoo
Authentication method	Code	URL	Code	URL	Code	-
Open	1st Character	all	1st Character	1st Character	all	-

다른 이메일 계정 접근을 통한 공격의 소요 시간은 포털사이트가 다른 계정의 정보를 공개하는지에 따라 결정된다. 이후 해당 계정으로의 로그인 시도는 로그인 단계에서의 공격 성공 가능성과 동일하다. 네이트와 MSN은 본인 확인 이메일을 전송한 다른 계정 정보를 공개하므로 공격자는 다른 계정 정보에 대해 추측하지 않고 해당 계정에 대해서 공격 시도가 가능하므로 공격 소요 시간이 짧고 쉽게 접근이 가능하다. 또한 특정 도구를 사용하는 것보다는 공격자가 획득한 정보를 이용하며, 보안 지식이 없는 일반인도 공격 수행이 가능하다. 따라서 비밀번호 재발급 1단계의 다른 이메일 계정 접근에 대한 공격 성공 가능성은 아래 Table 18과 같이 측정할 수 있다.

Table 18. Attack Potential of E-mail Account attack

	Naver	Nate	Daum	Google	MSN	Yahoo
Elapsed Time	3	1	3	3	1	-
Expertise	0	0	0	0	0	-
Knowledge of Object	0	0	0	0	0	-
Access to Object	4	1	4	4	1	-
Tools	0	0	0	0	0	-
Total	**7**	**2**	**7**	**7**	**2**	**-**

앞서 패스워드 재발급-1단계의 공격 성공 가능성을 분석한 결과, SMS 도청, 인증번호 전수조사, 다른 이메일 계정 접근의 공격 방법 중 다른 이메일 계정 접근 공격의 공격 성공 가능성이 가장 낮음을 알 수 있다. 따라서 패스워드 재발급 - 1단계의 공격 성공 가능성은 다른 이메일 계정 접근 공격과 동일하다.

4) 패스워드 재발급 - 2단계

국내 포털사이트는 2013년도 8월까지 주민등록번호를 활용한 본인 인증 과정을 제공하였으나, 현재는 2단계 인증 서비스를 제공하지 않는다. 본 논문에서는 해외 포털사이트와의 안전성 비교를 위하여 주민등록번호 수집을 통한 본인 인증 과정의 공격 성공 가능성을 측정한다.

주민등록번호는 인터넷 검색, 유통업자를 통해 소수의 사람들에게만 공유되는 정보이다. 공격 대상의 주민등록번호를 획득한 공격자는 계정 정보를 획득하고, 공격 대상의 주민등록증을 위조하거나 주민등록정보를 이용하여 포털사이트로부터 공격 대상의 패스워드를 제공받을 수 있다. 공격에 소요되는 시간은 아이디 검색, 주민등록번호 확인 등을 포함하여 1주일 이내로 이루어지며, 보안에 대한 지식이 없는 일반인들도 쉽게 수행할 수 있는 공격 방법이다.

해외 포털사이트는 사용자 인증을 위해 계정 사용 시 생성된 사용자의 경험 또는 행동을 기반으로 생성한 질의를 통하여 사용자를 확인한다. 공격자는 질문에 대한 대답을 위해 인터넷에 공개된 사용자에 대한 정보를 조합하여 정답을 추측할 수 있다. 해당 정보를 수집하고 분석하는 데 1주일 정도의 시간이 소요되며, 이러한 공격은 정보 수집에 능하고 분석이 가능한 숙련자가 수행할 수 있다. 또한 공격 수행을 위해 도구는 필요하지 않다. 그러나 질문에 대한 정답은 사용자만이 알고 있는 정보이므로 중대한 정보로 분류된다. 패스워드 재발급-2단계에 대한 공격 성공 가능성은 아래 Table 19와 같이 측정할 수 있다.

Table 19. Attack Potential of Password Reset-2nd Phase

	Naver	Nate	Daum	Google	MSN	Yahoo
Elapsed Time	5	5	5	5	5	5
Expertise	0	0	0	3	3	3
Knowledge of Object	3	3	3	11	11	11
Access to Object	4	4	4	4	4	4
Tools	0	0	0	0	0	0
Total	**12**	**12**	**12**	**23**	**23**	**23**

5.2 공격 성공 가능성을 기반으로 한 포털사이트 패스워드 인증 시스템 안전성 비교 분석

앞 절에서 측정한 공격 성공 가능성을 바탕으로 포털사이트 패스워드 인증 시스템의 안전성을 비교 분석한다. 각 단계별 공격 성공 가능성을 최종 분석한 표는 Table 20과 같다.

Table 20. Attack Potential Score of Password Authentication

	Naver	Nate	Daum	Google	MSN	Yahoo
Membership Registration	9	9	9	8	8	8
Login	11	11	11	11	11	11
PW Reset 1st Phase	7	2	7	7	2	9
PW Reset 2nd Phase	12	12	12	23	23	23

패스워드 인증 시스템의 단계별 안전도를 비교하였을 때, 패스워드 재발급 - 1단계의 안전성이 가장 낮은 것으로 분석되었다. 이는 로그인 단계에서의 취약점이 공격에 빈번히 이용되는 것에 반해, 실질적으로는 패스워드 1단계가 공격에 이용될 경우 공격자가 패스워드를 획득하기가 보다 용이한 것으로 분석되었기 때문이다.

각 단계별로 국내외 포털사이트의 안전성을 비교하고, 이를 강화하기 위한 방법은 아래와 같다. 회원가입 단계에서는 국내 포털사이트가 아이디 개수 제한을 시행하고 있으므로 해외 포털사이트보다는 무제한적인 자동가입에 안전함을 알 수 있다.

로그인 단계에서는 연속적인 인증 시도, 키로깅, 피싱의 공격 시나리오에 대해 공격 성공 가능성을 측정하였다. 키로깅은 모든 포털사이트가 동일한 값으로 분석되었으며, 국내외 포털사이트 모두 키로깅 공격에 대응 가능한 방법을 제공하지 않아 키로깅 공격에는 약한 것으로 나타났다. 연속적인 인증 시도는 국내 포털사이트가 해외 포털사이트보다 취약함을 알 수 있는데, 이는 네이버, 네이트가 계정 잠금 서비스를 제공하지 않으며 비밀번호 강도가 해외 포털사이트보다 낮기 때문인 것으로 분석된다. 이를 보완하기 위해 네이버, 네이트는 비밀번호 강도를 향상시키고, 계정 잠금 서비스를 제공해야 한다. 피싱 공격에 대해서는 네이버, 구글, MSN, 야후가 대응 기술을 제공하고 있으므로 네이트, 다음보다 안전한 것으로 나타났다. 그러나 국내 포털사이트 및 야후는 소스코드를 노출시키므로 피싱 사이트 제작이 용이한 것으로 분석되었다. 이를 보완하기 위하여 소스코드 해석을 어렵게 할 필요가 있으며, 네이버, 다음은 자체적인 안티 피싱 기술을 제공해야 한다.

패스워드 재발급-1단계에서 발생 가능한 SMS 도청 공격은 사용자 스마트폰의 안전성과 관련된 것이므로 사용자 스마트폰에 백신을 설치하도록 권고하는 것이 해당 공격에 안전할 수 있다. 인증번호 전수조사 공격은 국내외 포털사이트 모두 인증번호 입력 및 전송 횟수에 제한을 두어 인증번호 전수조사 공격에 안전함을 알 수 있었다. 특정 사용자를 공격 대상으로 하는 경우에는 패스워드 재발급 1단계의 이메일을 통한 인증 단계의 다른 이메일 계정을 통한 접근을 활용하면 로그인 단계보다 용이하게 패스워드를 획득할 수 있다. 사용자가 등록한 다른 계정이 노출되는 경우는 공개되지 않은 경우보다 소요 시간을 절약할 수 있고, 등록된 계정의 비밀번호 강도가 재발급받고자 하는 계정보다 낮은 경우에는 해당 계정을 공격하면 공격 난이도가 감소한다. 따라서 다른 계정 정보를 모두 노출하는 네이트, MSN은 계정의 일부만 노출시켜 안전성을 향상시켜야 한다.

국내 포털사이트는 패스워드 재발급-2단계 서비스를 2014년 8월 이전에 주민등록번호를 이용한 인증 방법을 기준으로 분석하였다. 개인정보 유출 사태가 빈번히 발생함에 따라 주민등록번호는 시중에 유통되고 있으며, 공격자는 쉽게 이를 획득할 수 있다. 따라서 공격자가 사용자로 위장하여 패스워드를 재발급받는 데 큰 어려움이 없다. 해외 포털사이트의 경우에는 사용자만이 알고 있는 경험에 기반한 내용을 이용하므로 정보의 내용이 공개되지 않아 공격자가 정답을 추측하기 어렵기 때문에 국내 포털사이트보다 안전함을 알 수 있다.

6. 결 론

본 논문에서는 국내외 포털의 패스워드 인증 시스템의 전체 절차를 분석하고 각 과정에서 발생 가능한 보안 위협과 보안 요구사항을 도출하였다. 또한 포털사이트의 패스워드 인증 시스템을 수치화하여 비교 분석하기 위하여 공통평가기준의 공격 성공 가능성 개념을 도입하여 국내외 포털사이트의 패스워드 인증 시스템의 안전성을 비교 분석하였다. 국내와 해외 포털 업체의 패스워드 인증 시스템을 분석한 결과, 국내 포털인 네이버와 네이트는 계정 잠금 서비스를 제공하지 않아 해외 포털보다 전수조사 공격에 취약한 것을 알 수 있었다. 그러나 해외 포털의 경우 구글을 제외하고 해외 로그인에 대한 차단이나 본인 확인 서비스를 제공하지 않는 것으로 분석되었는데, 이는 생성 가능한 ID 개수가 제한되지 않으므로 새로운 계정을 생성하는 것이 계정 탈취 공격을 시도하는 것보다 용이하기 때문인 것으로 파악된다. 하지만 스팸메일 발송 등의 목적이 아니라 정보 획득의 목적으로도 다양한 계정 탈취 공격이 발생할 수 있으므로 이에 대한 대비가 필요하다. 또한 국내외 포털 모두 사용자들에게 안전한 패스워드 생성을 필수적으로 요청하지 않고 있음을 알 수 있었다. 패스워드의 강도는 로그인 시도뿐만 아니라 패스워드 재발급 - 1단계에서도 공격 방법으로 응용될 수 있으므로 모든 포털사이트가 안전한 패스워드 생성 조건을 강화하는 것을 의무화해야 한다. 또한 국내 포털사이트는 패스워드 재발급 - 2단계에서의 사용자의 편의성 강화를 위해 해외 포털사이트처럼 사용자 행위 기반의 인증 방법을 사용하거나 새로운 방법을 제안하여 휴대전화 사용이 어려운 사용자들에게도 편의를 제공해야 한다.

References

[1] Bruce Schneier, “Applied Cryptography,” *John Wiley & Sons*, 1996.

[2] Perlman, Radia, and Charlie Kaufman, “User-centric PKI,” *Proceedings of the 7th Symposium on Identity and Trust on the Internet. ACM,* 2008.

[3] Just, Mike, and David Aspinall, “Personal Choice and Challenge Questions: A Security and Usability Assessment,” *Poceedings of the 5th Symposium on Usable Privacy and Security. ACM*, 2009.

[4] Jin, Lei, Hassan Takabi, and James BD Joshi, “Analysing security and privacy issues of using e-mail address as identity,” *International Journal of Information Privacy, Security and Integrity,* 1.1. pp.34-58, 2011.

[5] C.E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal,* Vol.27, pp.379-423, 1948.

[6] Komanduri, Saranga, et al., “Of passwords and people: measuring the effect of password-composition policies,” *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM,* 2011.

[7] Ma, Wanli, et al., “Password entropy and password quality,” *Network and System Security (NSS), 2010 4th International Conference on. IEEE,* 2010.

[8] Yan, Jianxin Jeff, “A note on proactive password checking,” *Proceedings of the 2001 workshop on New security paradigms. ACM,* 2001.

[9] Bishop, Matt, “Proactive password checking,” *4th Workshop on Computer Security Incident Handling,* 1992.

[10] “Common Methodology for Information Technology Security Evaluation,” Common Criteria, Version 3.1. Jul., 2009.

[11] Cazier, Joseph A., and B. Dawn Medlin, “Password security: An empirical investigation into e-commerce passwords and their crack times,” *Information Systems Security* 15.6. pp.45-55, 2006.

[12] Ji Sun Shin, “Study on Anti-Phishing Solutions, Related Researches and Future Directions,” *Journal of The Korea Institute of Information Security & Cryptology,* Vol.23, No.6, Dec., 2013.

[13] Leijten, Mariëlle, and Luuk Van Waes, “Keystroke Logging in Writing Research Using Inputlog to Analyze and Visualize Writing Processes,” *Written Communication* 30.3, pp.358-392, 2013.

[14] “2014 Trustwave Global Security Report,” *Trustwave*, 2014.

[15] Dell'Amico, Matteo, Pietro Michiardi, and Yves Roudier, “Password strength: An empirical analysis,” *INFOCOM, 2010 Proceedings IEEE. IEEE,* 2010.

[16] Irani, Danesh, et al., “Modeling unintended personal-information leakage from multiple online social networks,” *Internet Computing,* IEEE 15.3, pp.13-19, 2011.

[17] HyeongKyu Lee, “The Problems and Reformation of the Personal Identification by the Resident Registration Number on the Internet,” *Hanyang Law Review,* Vol.23-1, pp.341-371, Feb., 2012.

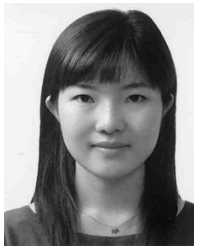
[18] Von Ahn, Luis, et al., “CAPTCHA: Using hard AI problems for security,” *Advances in Cryptology—EUROCRYPT 2003. Springer Berlin Heidelberg,* pp.294-311, 2003.

[19] Lei Jin, Hassan Takabi, James B.D. Joshi, “Analysing security and privacy issues of using e-mail address as identity,” *International Journal of Information Privacy, Security and Integrity*, Vol.1, No.1, pp.34-58, 2011.

[20] Goring, Stuart P., Joseph R. Rabaiotti, and Antonia J. Jones, “Anti-keylogging measures for secure Internet login: an example of the law of unintended consequences,” Computers & Security 26.6, pp.421-426, 2007.

[21] “Kaspersky Releases Q1 Spam Report,” *Kaspersky,* 2014.

[22] Lei Jin, Hassan Takabi, James B.D. Joshi, “Analysing security and privacy issues of using e-mail address as identity,” *International Journal of Information Privacy, Security and Integrity*, Vol.1, No.1, pp.34-58, 2011.



노 희 경

e-mail : hknoh@korea.ac.kr

2012년 덕성여자대학교 인터넷정보공학과 (학사)

2013년~현 재 고려대학교 정보보호대학원 석사과정

관심분야 : 정보보호제품 보안성 평가, Password Security

최 창 국

e-mail : necojin@gmail.com

2000년 광운대학교 화학공학과(학사)

2012년~현 재 고려대학교 정보보호대학원 석·박사통합과정

관심분야 : 해킹, CCTV 보안

박 민 수

e-mail : minsoon2@korea.ac.kr

2010년 신라대학교 컴퓨터 네트워크학과 (학사)

2013년 고려대학교 정보보호학과(석사)

2013년~현 재 고려대학교 정보보호대학원 박사과정

관심분야 : 정보보증, 정보보호제품 보안성 평가, 디지털 포렌식

김 승 주

e-mail : skim71@korea.ac.kr

1994년~1999년 성균관대학교 정보공학과 (학사, 석사, 박사)

1998년~2004년 KISA(舊한국정보보호진흥원) 팀장

2002년~현 재 한국정보통신기술협회(TTA) IT 국제표준화전문가

2004년~2011년 성균관대학교 정보통신공학부 조교수, 부교수

2011년~현 재 고려대학교 정보보호대학원 정교수

2004년~현 재 한국정보보호학회 이사

2005년~2006년 교육인적자원부 유해정보 차단 자문위원

2007년 국가정보원장 국가사이버안전업무 유공자 표창

2007년~2009년 전자정부서비스보안위원회 사이버침해사고대응실무위원회 위원

2010년 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원

2012년~2012년 선관위 디도스 특별검사팀 자문위원

2013년~2013년 IT보안인증사무국 자문위원

2013년~현 재 중앙선거관리위원회 자문위원

2014년~현 재 헌법재판소 자문위원

관심분야 : 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable Security