*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1225

# 피싱 및 파밍 공격에 의한 다수의 패스워드 유출 요인에 관한 연구*

유 홍 렬,† 홍 모 세, 권 태 경‡
연세대학교 정보대학원

# A Study of Multiple Password Leakage Factors Caused by Phishing and Pharming Attacks*

Hong Ryeol Ryu,† Moses Hong, Taekyoung Kwon‡
Graduate School of Information, Yonsei University

요 약

오늘날 많은 인터넷 서비스들은 사용자를 식별하고 데이터를 보호하기 위해 아이디와 패스워드 이용한 인증을 이용한다. 만약 피싱이나 파밍으로 인해 사용자의 아이디와 패스워드가 탈취되고 서비스 권한이 도용된다면 2차 피해가 발생할 수 있다. 본 연구는 피싱 및 파밍 사이트에서 아이디와 패스워드를 입력할 때 사용자의 부주의로 인해 탈취될 수 있는 요인들을 연구했다. 특히 사용자가 패스워드 관리를 기억에 의존하고, 무의식적인 인증 과정 수행할 때 얼마나 많은 패스워드를 유출할 수 있는지 실험을 통해 확인했다.

ABSTRACT

In this paper, we studied threats and risks that users might enter their passwords without awareness onto phishing and pharming sites, and particularly showed that it was highly likely to leak the secret information of multiple passwords by user experiments. The novel methodology of verifying those threats and risks is the major contribution of this paper. We will extend this work for further verification of our findings.

**Keywords**: Phishing, Pharming, Password, Authentication

## I. 서 론

오늘날 무선인터넷과 스마트폰이 보편화 되었고 이 서비스들은 개인, 가정, 직장에서 생활화 되었다. 많은 서비스들이 스마트폰과 인터넷을 통해 이루어짐으로서 클라우드 서비스와 같은 서버나, 스마트폰과 같은 클라이언트에 많은 양의 개인정보가 저장되고 있다. 최근 개인정보의 가치가 부각되면서 이것을 탈취하려는 다양한 공격이 이루어지고 있으며 특히, 사회공학을 이용한 공격이 증가하고 있다[1]. 대표적인 사회공학적 공격으로 피싱 공격을 들 수 있다. 국내외 피싱 사이트는 2010년부터 2013년까지 꾸준히 증가하고 있다[2].

피싱에 의해 유출되는 주요 개인정보 중 하나는 사용자의 아이디와 패스워드이다. 공격자는 특정 사이트의 실제 인증 화면과 동일한 환경을 만들어 놓고 사용

접수일(2013년 10월 15일), 게재확정일(2013년 10월 21일)
* 본 연구는 미래창조과학부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신)[10039180, 모바일 환경하에서 모바일 인증과 보안 강화를 위해 직관적이며 사용하기 편하고 안전한 인간-컴퓨터 상호작용(HCI) 기반 Usable Security 원천기술 개발]과 미래창조과학부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업 (NIPA-2013-H0301-13-1003)의 일환으로 수행하였음.
† 주저자, ryeol@yonsei.ac.kr
‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

자로부터 아이디와 패스워드 입력을 유도한다. 이때 사용자의 아이디와 패스워드가 유출되는 것은 사용자가 피싱에 대한 합리적인 의심이나 검증과정 없이 무의식적인 인증 과정이 수행되기 때문이다.

본 논문은 피싱(Phishing) 및 파밍(Pharming) 공격에서 아이디와 패스워드가 유출될 수 있는 요인들을 실험을 통해 분석한 것이다. 특히 소수의 아이디와 패스워드 쌍이 기억에 의존하여 관리되고, 사용자가 합리적인 의심 없이 인증 절차를 수행할 때 얼마나 많은 패스워드가 유출될 수 있는지 실험했다.

## II. 관련연구

### 2.1 피싱

피싱은 개인정보를 취득하기 위하여 변조된 웹사이트로 사용자를 유도하는 대표적인 사회공학적 공격이다[1]. 공격자는 인터넷 사용자를 속이고 개인정보를 수집하기 위한 웹사이트를 설계한다. 그리고 사회공학적 기법을 이용한 이메일 또는 문자메시지에 웹사이트 링크를 담아 전파한다. 만약 사용자가 공격자가 준비한 링크에 접속하면, 실제 웹사이트와 유사하여 정확하게 구별할 수 없는 웹사이트가 나타난다. 인터넷 사용자는 해당 웹사이트를 정상적인 사이트라고 판단하고 개인 정보를 입력하게 되며 입력된 정보는 공격자에게 유출된다[3].

### 2.2 파밍

파밍은 기존의 피싱 공격을 한 단계 발전시킨 공격기법이다. 공격자는 DNS 취약점을 이용해서 인터넷 사용자로 하여금 변조된 웹사이트로 이동하게 한다. 피싱은 정상 URL과 비교하면 변조된 웹사이트라는 것을 인지 할 수 있지만, 파밍은 동일한 URL로 접근해도 변조된 웹페이지로 이동하기 때문에 사용자가 위험을 인지하기가 어렵다[2][4].

## III. 연구가설

많은 인터넷 사용자들은 웹서비스를 이용하기 위해 다수의 웹사이트 계정(account)을 가지고 있다. 하지만 그에 비해 소수의 아이디(id), 패스워드(password)쌍을 가지고 있다. 계정의 수에 비해 소수의 아이디, 패스워드쌍을 보유하는 것은 패스워드 관리가 어렵기 때문이다. 이로 인해 많은 사람들이 소수의 패스워드를 암기에 의존하여 관리한다.

또한 사용자들은 아이디와 패스워드를 이용한 로그인 과정을 무의식적으로 시도한다. 아이디와 패스워드를 이용한 절차와 인터페이스는 매우 정형화 되어 있어 사용자에게 익숙하기 때문이다. 이와 같은 상황에서 만약 피싱 및 파밍 공격에 노출된다면 아이디와 패스워드를 노출할 가능성이 높다. 특히 불완전한 기억에 의존하는 상태에서는 다량의 패스워드를 노출할 가능성이 있다.

본 논문은 위와 같은 상황을 가정하여 Fig.1.과 같은 연구 가설을 도출했다.

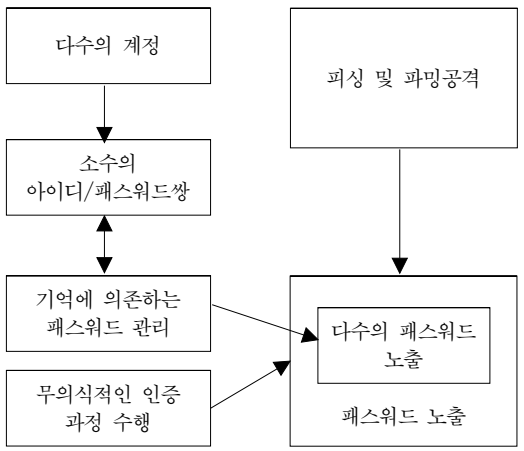


Fig.1. Research model

## IV. 실험설계 및 구현

### 4.1 측정변수 및 조작적 정의

연구가설을 통해서 측정하고자 하는 변수들과, 측정을 위한 조작적 정의를 Table 1.과 같이 설정했다.

Table 1. Measuring variables and operational definitions

| 변수 | 조작적 정의를 위한 질의 |
|---|---|
| 계정의 개수 | 얼마나 많은 사이트에 가입되어 있는가? |
| 아이디 개수 | 아이디의 개수(종류)는 몇 개인가? |
| 패스워드 개수 | 패스워드의 개수(종류)는 몇 개인가? |
| 패스워드 관리 방법 | {암기, 브라우저 자동저장, 파일 저장, 기타} |
| 인증 과정 수행 행태 | 피싱 또는 파밍을 막기 위한 검증 절차가 존재하는가? |
| 패스워드 노출량 | 몇 개의 패스워드를 노출하는가? |

### 4.2 실험절차 및 구현

실험은 Fig.2.와 같이 크게 '사전설문', '패스워드 노출 실험', '사후인터뷰' 순서로 진행된다. 또한 패스워드를 노출하기 위한 실험은 '파밍사이트 유도', '로그인과정 수행 유도', '실행종료'로 나눠진다.

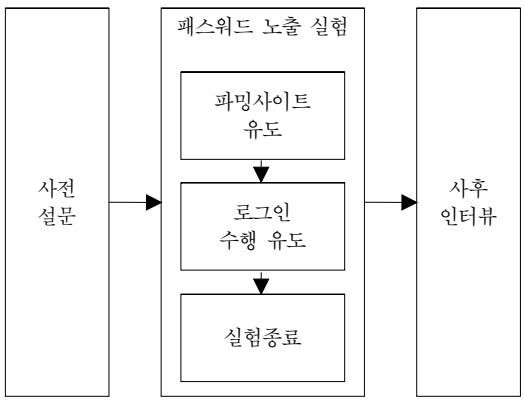


Fig.2. Experiment process

#### 4.2.1 사전설문

준비된 파싱 사이트는 총 4개(포털 2개, 쇼핑몰 1개, SNS 1개)이다. 이 중 피실험자들을 대상으로 사이트 이용 빈도를 조사했다. 기억에 의존하는 암호 관리의 위험성을 증명하려면 기억의 불확실성을 높여야 한다. 따라서 피실험자가 자주 이용하지 않는 사이트를 실험 대상으로 선택했다.

#### 4.2.2 패스워드 노출 실험

파밍 사이트를 재현하기 위해서 유명 웹사이트 4개(페이스북, 트위터, 구글, G마켓)를 실제 웹페이지와 동일하게 제작, 운영했다. 실험을 위한 PC의 호스트 파일을 변조함으로서 실제 웹사이트에 대한 요청을 준비된 파밍 사이트가 응답하도록 했다.

피실험자의 패스워드를 자연스럽게 유출하기 위해, 실험 목적과 무관한 수행과제를 부여하여 로그인을 유도했다. 또한 올바른 아이디, 패스워드를 입력해도 로그인이 실패하도록 설계하여 로그인을 재시도하도록 유도했다. 만약 로그인을 재시도하면 실험은 계속 진행되나, 피실험자가 스스로 로그인 시도를 중단하거나, '비밀번호 찾기' 기능을 수행하는 경우에는 실험을 종료했다.

피실험자가 입력하는 아이디와 패스워드는 데이터베이스에 저장되도록 설계했다. 이것은 실험 결과를 확인하기 위함이다.

#### 4.2.3 사후인터뷰

실험이 종료된 직후 저장된 아이디와 패스워드 파일을 피실험자가 직접 열람하도록 했으며, 그 순간 관찰자는 열람하지 않았다. 기록된 파일에는 입력된 아이디, 패스워드, 시도 횟수, 수행시각이 담겨 있다. 이 파일을 바탕으로 피실험자와 인터뷰를 진행했으며, 인터뷰를 바탕으로 실험 결과를 도출했다. 저장된 파일은 피실험자로 하여금 스스로 삭제할 수 있도록 설계하여, 인터뷰가 종료된 직후 피실험자에 의해 파기되었다.

## V. 실험결과

피실험자들은 남성 37명, 여성 28명으로 총 65명이며 평균나이 26.5세, 전공과 무관한 대학생 및 대학원생을 대상으로 실험했다.

### 5.1 계정, 아이디, 패스워드의 수

Table 2.의 결과와 같이 피실험자들은 평균 75.6개의 사이트에 가입하고 있었으며, 이 계정들을 평균 4개의 아이디와 4.1개의 패스워드만으로 이용하고 있었다.

Table 2. Number of account items

| | |
|---|---|
| 가입된 사이트의 개수 (평균) | 75.6 |
| 아이디 보유 개수 (평균) | 4.0 |
| 패스워드 보유 개수 (평균) | 4.1 |

Table 3.의 결과와 같이 피실험자가 가진 계정의 수가 많다고 해서 아이디나 패스워드의 수가 많지는 않았다. 하지만 아이디를 많이 보유한 피실험자 일수록 패스워드의 수가 많아지는 경향을 보였다.

Table 3. Correlation coefficient

| | |
|---|---|
| 〔계정-아이디 개수〕의 상관계수 | -0.09 |
| 〔계정-패스워드 개수〕의 상관계수 | 0.10 |
| 〔아이디-패스워드 개수〕의 상관계수 | 0.41 |

### 5.2 패스워드의 관리 방법

Table 4. Password management methods

| | | |
|---|---|---|
| 1 | 관리함 (파일,브라우저,도구이용) | 7.69% |
| 2 | 관리하지 않음 (암기에 의존) | 92.31% |

피실험자들의 대다수는 Table 4.의 결과처럼 암기에 의존하여 패스워드를 관리하고 있었다. 특별한 관리 방법 없이 암기에 의존하는 피실험자들은 Fig.3.의 결과와 같이 유출된 패스워드 수의 평균과 최대값이 상대적으로 높음을 알 수 있다.

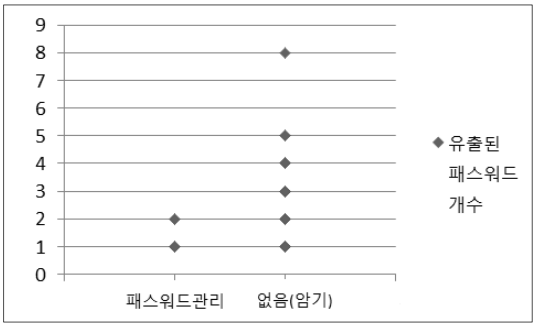


Fig.3. Number of leaked passwords

### 5.3 인증 과정 수행 관찰

피실험자들은 준비된 실험 사이트에서 평균 5.8번의 로그인을 시도했다. 이것은 최초 로그인 수행이 포함된 수치이며, 이것을 제외해도 인증과정을 여러번 재시도 했음을 확인할 수 있다. 실험 후 인터뷰에서 대다수의 피실험자들은 로그인 실패 이후에도 이것이 파밍 사이트임을 의심하지 못했다고 말했다.

### 5.4 패스워드 노출량

Table 5. Experimental results

| | |
|---|---|
| 로그인 시도 횟수 (평균) | 5.8 |
| 유출된 패스워드 개수 (평균) | 2.2 |
| 〔로그인 시도 횟수-유출된 패스워드 개수〕의 상관계수 | 0.50 |

평균 5.8번의 로그인 시도에서 유출된 패스워드의 개수는 평균 2.2개다. 나머지 3.6개는 동일한 패스워드를 재입력했거나 오타를 입력한 경우이다. 피실험자들이 보유한 패스워드가 평균 4.1개이므로 54%의 높은 비율로 유출됨을 알 수 있었다. 또한 인증 시도 횟수가 높을수록 더 많은 패스워드가 유출되는 것으로 나타났다.

실험 후 인터뷰에서, 유출된 또 다른 패스워드는 피실험자가 다른 사이트에서 실제 이용하고 있는 패스워드라고 밝혔다. 이것은 공격자가 피해자의 노출된 패스워드를 활용한다면, 피해자가 이용 중인 또 다른 웹 사이트에 접근할 수 있음을 말해준다.

## VI. 결론

실험을 통해 피싱 및 파밍 공격 시 사용자들이 보유한 패스워드가 얼마나 노출되는지를 확인했다. 사용자들은 피싱 및 파밍 사이트에 대한 합리적인 의심과 검증 절차 없이, 사이트에서 무의식적으로 아이디와 패스워드를 입력하고 있었다. 또한 암기에 의존한 패스워드는 불확실한 기억을 야기하고, 무의식적인 시도와 결합하여 다수의 패스워드를 노출하는 결과를 낳았다.

이에 대한 대책으로 로그인 과정에서 사용자의 인식을 개선하는 연구가 필요하며, 인증 시도 횟수의 한계를 설정하는 합리적인 연구가 필요하다. 피싱 및 파밍 사이트를 통해 노출된 아이디와 패스워드 쌍을 조합하면 다른 사이트에서 악용될 소지가 있다. 그리고 그 피해가 드러나지 않는 한 유출 사실은 알기 어렵다. 파밍은 실제 사이트와 동일한 인터넷 주소에서 구현되므로 사용자들의 의심을 피할 수 있으며, 무의식적으로 입력하는 사용자들의 행동 특성상 다양한 보안 기법들이 요구된다.

## References

〔1〕 D. Rachna, J.D. Tygar and M. Hearst, "Why phishing works," Proceedings of the SIGCHI conference on Human Factors in Computing, pp. 581-590, Apr. 2006

〔2〕 S.H. Kim, S.H. Lee and S.H. Jin, "Active Phishing Attack and its Countermeasures," Electronics and Telecommunications Trends, vol. 28, no. 3, ETRI, 2013.

〔3〕 D. Rachna and J.D. Tygar, "The battle against phishing: Dynamic security skin," Proceedings of the Symposium on Usable Privacy and Security, pp. 77-88,

Jul. 2005.
[4] S. Gastellier-Prevost and M. Laurent, "Defeating pharming attacks at the client-side," 2011 5th International Conference on Network and System Security, IEEE, pp. 33-40, Sept. 2011.

## 〈저자소개〉

유 홍 렬 (Hong Ryeol Ryu) 학생회원
2013년 2월: 서울과학기술대학교 산업공학전공 학사
2013년 3월~현재: 연세대학교 정보대학원 석사과정
〈관심분야〉 HCI, Usable Security, Social Engineering

홍 모 세 (Moses Hong) 학생회원
2010년 2월: 한국교통대학교 컴퓨터공학과 학사
2013년 3월~현재: 연세대학교 정보대학원 석사과정
〈관심분야〉 사회공학, 보안 정책 기획

권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 박사
1999년~2000년: U.C. Berkely Post-Doc.
2001년~2013년 8월: 세종대학교 컴퓨터공학과 교수
2007년~2008년: Univ. Maryland at College Park 교환교수
2013년 9월~현재: 연세대학교 정보대학원 부교수
〈관심분야〉 암호프로토콜, 네트워크 프로토콜, 센서네트워크 보안, HCI 보안 등