논문 15-40-06-15 The Journal of Korean Institute of Communications and Information Sciences '15-06 Vol.40 No.06
http://dx.doi.org/10.7840/kics.2015.40.6.1107

일반 사용자를 위한 포털 사이트 경유 피싱/파밍 방지 방안

김 소 영◆, 강 지 윤*, 김 윤 정°

Countermeasures Against Phishing/Pharming via Portal Site for General Users

Soyoung Kim◆, Ji-yoon Kang*, Yoonjeong Kim°

요 약

피싱 및 파밍에 대한 공격이 증가하고 있어, 이를 방지하기 위한 많은 연구들이 진행되어 오고 있다. 피싱/파밍의 대상 사이트는 금융권 사이트 등이며, 이들은 포털 사이트 등에 비하여 사용자의 접속 빈도가 상대적으로 적은 편이다. 본 논문에서는, 포털 사이트가 건전하게 자사의 책임을 다한다는 가정 하에, 포털 사이트를 경유하여 금융권 사이트를 접속함으로써 피싱/파밍을 방지하는 방안을 제안한다. 본 방안은, 개발자나 전문적인 사용자가 아닌, 특별히 일반 사용자를 대상으로 한 피싱/파밍 방지안이라 할 수 있다. 이들 방안의 각 부분별 취약성을 나누어 안전성 분석을 수행함으로써, 본 방지안이 최대로 효과적일 수 있는 환경 분석도 수행하였다.

Key Words : phishing, pharming, anti-phishing, portal site, authentication

ABSTRACT

The number of phishing/pharming attacks occurring has increased and consequently, the number of studies on anti-phishing/pharming has also increased. The target sites of phishing/pharming are financial sites, and these have a low connection rate compared to those of portal sites. In this paper, we propose an anti-phishing/pharming method that uses a portal site as a stopover. The proposed method is based on the reliability of portal sites. This method is intended for general users rather than for professional users or developers. We also analyze the safety of the proposed method by separating the method into sub components of module safety assumption.

Ⅰ. 서 론

피싱(Phishing) 공격은 사용자가 자신의 이메일이나 문자메시지로부터 온 악성 URL을 클릭하여 공격자가 만들어 놓은 가짜 서버로 접속하여 개인정보들이 공격자에게 노출되어 금전적 피해나 사생활 침해 등을 받는 공격을 말한다[1]. 파밍(Pharming) 공격은 사용자가 올바른 웹 사이트의 주소를 입력하였음에도 불구하고 사용자의 DNS 서버 등이 침해되어 사용자가 공격자가 만들어 놓은 가짜 서버로 접속하게 되는 것을 말한다[2]. 이러한 피싱 공격과 파밍 공격의 악영향이 커짐에 따라 현재 온라인상의 많은 사용자들이

※ 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT 연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2015-H8501-15-1018)
◆ First Author : 서울여자대학교 정보보호학과, thdud2608@gmail.com, 학생회원(Seoul Women's University)
° Corresponding Author : 서울여자대학교 정보보호학과, yjkim@swu.ac.kr, 정회원(Seoul Women's University)
* KAIST 정보보호대학원, kangj1010@naver.com
논문번호 : KICS2015-03-070, Received March 23, 2015; Revised June 18, 2015; Accepted June 18, 2015

피해를 입고 있는 추세이다.

한편, 피싱/파밍을 방지하기 위한 많은 기술적인 연구들이 있어 왔다[3-18]. 이러한 기술적인 방지안이 효과를 가지려면 사용자가 피싱/파밍을 분별할 수 있도록 하는 교육이 필요하다. 그러나, 컴퓨터나 인터넷 사용에 익숙하지 않은 일반 사용자에게는 의미가 없을 수 있다. 본 논문에서는, 컴퓨터나 인터넷 사용에 익숙하지 않은 사용자도 피싱/파밍을 보다 손쉽게 막을 수 있는 방안을 제안하고자 한다. 제안방법은 일반 사용자들이 손쉽게 접속하는 포털 사이트를 이용하여, 금융권 등의 올바른 주소를 접근하도록 하는 방안이다.

Ⅱ. 기존 피싱/파밍 대응방안들

2.1 피싱사이트 탐지 기술

2.1.1 원시 사이트 HTTP 트래픽분석방법을 이용한 피싱사이트 탐지 방법[6]

본 연구는 피싱사이트를 탐지하는 방안에 대한 것으로, 피싱 사이트의 URL이 HTTP referer 헤더 필드를 통해 원시사이트로 유입되는 특성을 이용한다. 원시 사이트에 유입된 HTTP 트래픽을 수집하여 분석함으로써 피싱 사이트를 실시간으로 탐지하게 해 준다. 실제 제안 시스템을 피싱사이트 표적이 되고 있는 국내 기관 홈페이지에 적용한 결과 6 일 동안 40개의 피싱사이트를 탐지하였다.

2.1.2 검색엔진을 활용한 피싱 사이트 탐지방법[5,7]

진화된 형태의 피싱 공격인 이미지 기반의 피싱 페이지에 관한 연구로 검색엔진의 검색 결과를 활용한다. 검색엔진은 키워드를 입력 받아 그 내용과 가장 비슷한 내용을 가지는 웹 사이트의 결과를 보여준다.

사용자가 접속하고자 하는 웹페이지에 접근하면, 웹브라우저에 요청된 웹 페이지가 로드된다. 이 때 본 검색엔진 활용 안티피싱 시스템은 로드된 페이지와 실제 접속하고자 사이트를 검색 엔진을 활용하여 연관성을 보고 피싱여부를 판단하게 된다.

2.2 URL 스푸핑을 이용하는 피싱 공격을 방어하는 방법[8]

URL(Uniform Resource Location)이란 인터넷 상의 특정 정보를 지정하는데 사용하는 주소 표시 형식이다. 웹 브라우저의 취약점, DNS 스니핑 등을 이용한 URL 스푸핑 공격을 피싱 공격에 이용할 수 있다. 이에 대한 효율적인 방지안은 URL을 사용자가 직접 확인하는 것이다. 그러나, URL을 직접 확인하는 작업을 할 능력이 없는 사용자는 여전히 피싱 공격의 위험에 노출된다. URL 스푸핑을 이용한 피싱 공격을 해결하기 위한 또다른 방법은 사이트가 위조되지 않았음을 사용자가 신뢰하는 것이다. 이를 위하여 사이트는 사용자와 사이트가 모두 신뢰할 수 있는 제 3의 기관 (TTP, Trust Third Party)의 인증을 받는다.

2.3 인지 기반 접근기법[9]

인지 기반 접근기법에서는 프로그램이 IP나 사이트의 도메인을 분석하여 피싱/파밍 여부를 판단하는 기존의 방식이 아닌 플러그인과 서버 사이에서 HTML 코드의 변경 유무를 파악하여 피싱여부를 결정한다. 그리고, 그 결과를 풍선 도움말을 이용하여 사용자에게 알려줌으로써, 사용자가 직접 피싱/파밍 여부를 쉽게 결정할 수 있도록 한다.

2.4 모바일 기기를 이용한 추가 인증이나 대상 사이트 접속 지원[10-12]

범용 컴퓨터와 비교하여, 악성코드나 해킹 등에서 상대적으로 자유로운 모바일 기기를 이용하여 추가 인증이나 대상 사이트로의 접속을 수행함으로써 피싱을 방지하는 방안들도 있다.

2.4.1 PhoolProof 기법[10]

PhoolProof 기법은 Bryan Parno 등이 2006년에 제안한 것으로, 피싱 방지를 사용자에게 의존하지 않고, 사용자가 소유하고 있는 휴대전화 등을 이용한 암호연산을 통하여 얻는다.

2.4.2 MP-Auth 기법[11]

MP-Auth는 Oorschot 등이 2007년에 제안한 방법으로 사용자의 long-term 패스워드를 안전성이 보장되지 않은 PC에서 보호하는 프로토콜이다. 이 프로토콜은 모바일 기기가 존재해야하며 이 모바일 기기는 악성프로그램으로부터 안전하다는 가정이 필요하다.

2.4.3 oPass[12]

oPass는 Sun 등이 2012년 제안한 것으로, 패스워드 유출과 패스워드 재사용 공격을 방지하기 위하여, 사용자의 휴대전화와 SMS (Short Message Service)를 이용한다.

oPass는 가입, 로그인, 회복의 3가지 과정으로 구성된다. 가입 시 사용자는 휴대전화에서 oPass 프로그램을 실행하고 사용자의 ID와 서버의 ID를 입력한다.

이는 TSP (Telecommunication Service Provider)에게 전달되고 TSP는 서버로 정보를 전달함과 동시에 사용자와 서버에게 암호키를 교환한다. 이때 이동통신망을 사용한다. 교환이 끝나면 사용자는 long-term 패스워드를 휴대전화를 통해서 입력한다. 그리고 이를 휴대전화에서 SMS을 이용해 직접 제출한다. 로그인 할 경우, 사용자가 브라우저에 입력하는 것은 ID 뿐이다. 회복과정은 사용자가 본인의 휴대전화를 잃어버렸을 경우 진행된다.

2.5 인증 안전성 강화 방안[13-18]

피싱을 방지하기 위한 방안으로, 서버가 사용자를 인증하는 일방향 인증에서 나아가, 사용자도 서버를 인증하는 양방향 인증 등 안전성이 강화된 인증 기법들이 시도되고 있다.

2.5.1 OTP인증 강화[13]

OTP (One Time Password)를 이용한 인증의 안전성을 높이기 위하여, PKI 기반의 모바일 OTP를 이용하고 생성된 OTP를 모바일 단말기에서 인증서버로 직접 전송하는 기법에 대한 연구도 진행되었다

2.5.2 개인 비밀 정보 이용 기법[14]

사용자가 사용자와 웹사이트 간의 비밀정보인 사진과 키값인 사용자의 아이디를 통해 피싱사이트와 구분할 수 있도록 한다. 사용자로 하여금 자신의 e-mail에 온 정당한 은행사이트의 URL에 접속하게 함으로써 피싱 사이트로의 접속을 막을 수 있도록 해준다.

2.5.3 윈도우 맞춤화 이용 기법[15]

Dhamija와 Tygar 등은 로그인 화면의 백그라운드 이미지를 개인별로 다르게 함으로써 피싱/파밍을 방지할 수 있는 윈도우 맞춤화 (window customization)를 개선하여, Visual Hash를 이용하는 개선된 인증 방법을 제안하였다.

2.5.4 QR 코드를 이용한 상호 인증[16-18]

QR 코드를 활용한 다중채널, 다중요소 시스템을 통하여 상호 인증을 함으로써, 피싱이나 파밍을 방지하는 기법에 대한 연구도 진행되었다.

Ⅲ. 제안하는 피싱/파밍 대응 방안

현재 금융권 등의 사이트를 접속할 때, 사용자들은 금융권 사이트의 주소를 직접 입력하거나 본인의 웹 브라우저 상에 이 금융권 사이트를 즐겨찾기로 등록시켜 놓고 즐겨찾기를 통하여 접속한다. 이 방법은 사용자가 금융권 사이트 주소를 잘못 입력하거나 사용자가 이용하는 컴퓨터나 모바일 시스템이 바이러스 등에 의하여 공격을 당한 상태에서는 피싱/파밍이 발생할 수 있다.

본 논문에서는 금융권 등의 웹사이트를 접속할 때 포털 사이트를 경유하여 접속함으로써 피싱/파밍을 방지하는 방안을 제안한다. 포털 사이트는 개인사용자보다 상대적으로 보안 관리가 우수하여, 잘못된 피싱/파밍 사이트로 연결될 위험을 낮추자는 것이다. 제안 방안이 그림 1에 나타나 있다.

제안 방법의 성공을 위하여는, 우선 포털 사이트가 안전하여야 하고 다음으로 포털 사이트에서 금융권 사이트 정보를 신뢰하게 관리해 준다는 가정이 필요하다. 포털 사이트의 안전성 외에, 제안 방법이 성공적으로 수행되기 위하여 필요한 가정들에는, 사용자 컴퓨터의 안전성, 공유기나 DNS 서버 등 주위 환경의 안전성, 사용자 컴퓨터에서 포털사이트 접속 시의 인증 안전성, 포털 사이트에서 금융권 사이트 접속 시의 인증 안전성 등이 있다.

다음으로 생각할 것은, 제안 방안이 수행되기 위하여, 포털 사이트에서 지원해 주어야 하는 내용이다. 그리고, 제안 방안의 세부 내용으로 포털 사이트를 경유하여 은행 등 다른 사이트에 접속하는 접속 시나리오에 대한 고려가 필요하다.

이들을 각각 3.1절부터 3.3절에서 세부적으로 설명하면 다음과 같다.

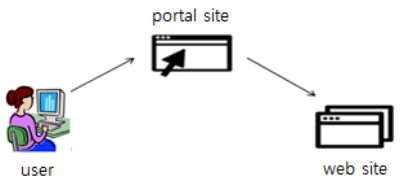

그림 1. 포털 사이트를 경유한 금융권 사이트 접속 방식
Fig. 1. financial web site access via portal site

3.1 제안 방법 성공을 위한 안전성 가정

3.1.1 포털 사이트의 신뢰성

제안 방법은, 포털 사이트의 신뢰성 및 포털 사이트에서 금융권 사이트 정보를 신뢰하게 관리해 준다는 가정에 근거한다. 이 가정은 현재의 네이버, 구글, 다음, 네이트 등의 포털이 건전하게 업무를 수행하고 있는 상황을 볼 때 타당한 가정이라 하겠다.

3.1.2 사용자 컴퓨터의 안전성

사용자가 사용하는 컴퓨터가 악성코드에 감염되지 않은 안전한 컴퓨터여야 한다. 예를 들어, 사용자가 북마크를 통해 포털 사이트에 접속할 때 아무리 포털 사이트가 안전하다 할지라도 사용자의 컴퓨터가 악성코드에 감염되어 있다면 북마크내의 잘못된 주소로 접속이 가능하다. 또한 파밍공격을 통해 사용자의 DNS정보를 가지고 있는 프로세스의 메모리가 변조되어 DNS서버가 허위 응답을 준다면 사용자는 공격자가 만들어 놓은 가짜 포털 사이트에 접속할 가능성이 있다. 따라서, 본 기법의 성공을 위하여는, 사용자가 이용하는 컴퓨터가 외부 악성코드에 감염되지 않은 안전한 컴퓨터이어야 한다.

3.1.3 공유기나 DNS 서버의 안전성

사용자 컴퓨터나 포털 사이트에서 이용하는 공유기나 DNS 서버가 안전해야 한다.

3.1.4 사용자 컴퓨터에서 포털 사이트 접속으로의 인증 안전성

사용자 컴퓨터에서 포털 사이트로 접속하여 사용자 인증을 받는 과정이 안전하게 진행되어야 한다. 여기에는 2.5절에서 언급한 인증기법이 사용될 수 있다.

3.1.5 포털 사이트에서 금융권 사이트로의 접속시 인증 안전성

포털 사이트를 경유하여, 금융권 사이트로 접속시 사용자 인증을 받는 과정이 안전하게 진행되어야 한다. 여기에도 2.5절에서 언급한 안전한 인증기법이 사용될 수 있다.

3.2 제안 방법을 위한 포털 사이트 지원 사항

사용자가 처음 이용시에 금융권 사이트를 개인 계정 페이지에 등록해 주는 메뉴 및 이 메뉴를 위한 서비스가 지원되어야 한다. 이 때 등록되는 금융권 사이트 정보는 포털 사이트에서 피싱/파밍에 노출되지 않은 순수한 사이트 정보로 준비하여야 한다. 이들 포털 사이트가 지원해야 할 사항을 정리하면 그림 2와 같다.

3.3 은행 등 사이트 이용시 포털 사이트 이용 시나리오

사용자 갑순이 I 은행을 N 포털 사이트를 경유하여 접속하고자 하는 경우, 먼저 N 포털 사이트의 자신의 개인 계정에 I 은행을 등록해야 한다. 이 때 N 포털 사이트는 3.2 절에서 기술한 것처럼 등록 메뉴 등을 지원해야 한다. 은행 사이트를 포털 사이트 개인 계정

① Portal site should have bank site list (bank name and its web site).

② Portal site should provide bank site registration menu on a user account window.

③ Portal site should provide customized user account window for each user (For example, a user who registered I bank has his/her customized user account window with I bank connection menu and a user who registered J shopping mall has his/her customized user account window with J shopping mall connection menu).

④ Portal site should provide secure authentication mechanism when users login to portal site (Portal site may use Section 2.5 Authentication Safety Strengthening Mechanism).

그림 2. 은행사이트 등 안전한 접속 지원을 위하여 포털 사이트가 지원해 주어야 하는 내용
Fig. 2. Protal Site's To-Do list that supports secure connection to banking web sites

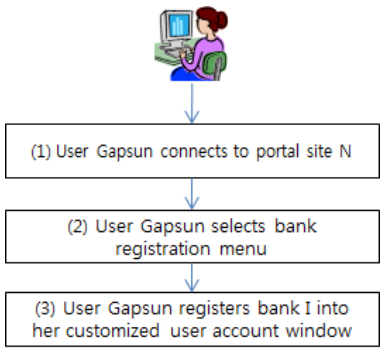

그림 3. 사용자 갑순이 N 포털 사이트 자신의 개인 계정에 I 은행을 등록
Fig. 3. User Gapsun registers Bank I into her account in Portal site N

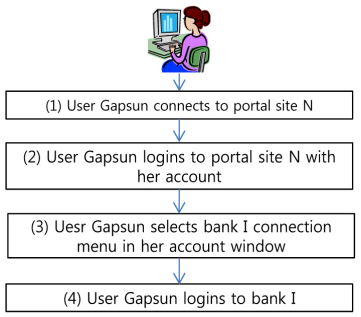

그림 4. 사용자 갑순이 N 포털 사이트를 경유하여 I 은행에 접속하는 절차
Fig. 4. User Gapsun connects to Bank I via Prtal site N

에 등록하는 과정이 그림 3에 나타나 있다.

이제, 실제로 사용자 갑순이 은행 업무를 위하여 I

은행에 접속하는 것은 다음과 같이 진행된다. 갑순은 먼저 N 포털 사이트에 접속하여 자신의 계정으로 로그인한다. 그리고, 자신에게 맞춤화된 화면에 있는 I 은행 접속 메뉴를 클릭하여 I 은행에 로그인한다. I 은행 로그인은 I 은행에서 제공하는 인증 기법을 따르면 된다. 이들 과정이 그림 4에 나타나 있다.

Ⅳ. 안전성 분석

4.1 제안 방법의 안전성 분석

본 절에서는 피싱/파밍 공격들에 대한 제안 방법의 안전성을 분석한 결과를 기술한다. 분석한 공격 기법은 피싱 공격, 파밍 공격, MITB, Key Logger, 패스워드 재사용 공격이다.

피싱 공격이란 공격자가 미리 만들어 놓은 가짜 웹 사이트를 포함한 URL을 사용자의 이메일로 보내는 것이다. 사용자는 그 URL을 클릭하여 가짜 웹 사이트에 접속하게 된다. 파밍 공격이란 공격자가 DNS 서버 등을 공격하여, 사용자가 올바른 경로를 통해 웹 사이트에 접속하려고 해도, DNS의 허위응답으로 인해 가짜 웹 사이트에 접속하게 되는 것을 말한다. MITB는 Man In The Browser의 약자로써, 브라우저 공격 기법이다. 이 기법은 공격자가 사용자의 컴퓨터 내에 악성코드를 심어놓음으로써 브라우저를 통하는 사용자의 웹 통신을 공격 할 수 있다. Key Logger는 사용자가 입력하는 키보드 문자를 공격자가 알아내는 공격 기법이다. 패스워드 재사용 공격은 공격자가 사용자의 패스워드를 알아내어 이 패스워드를 다시 사용하는 기법이다.

표 1에 이들 공격에 대한 제안 방안의 안전성이 분석되어 있다. 이메일을 클릭하여 대상 사이트에 접속하는 피싱 공격에 대하여는, 본 제안 기법을 이용하는 경우 별도의 가정 없이 안전성이 지원된다. 파밍 공격에 대하여는 사용자 컴퓨터의 안전과 공유기/DNS 서버의 안전을 가정하면, 본 제안 시스템을 이용하여 안전한 접속을 할 수 있다. MITB와 Key Logger 공격에 대하여는 사용자 컴퓨터의 안전을 가정시에, 안전한 접속을 할 수 있다. 패스워드 재사용 공격에 대하여는, 사용자 컴퓨터에서 포털 사이트로의 접속과 포털사이트에서 금융권 사이트로의 접속이 안전하다는 가정이 있으면, 안전한 접속을 할 수 있다.

표 1. 제안 방법의 안전성 분석
Table 1. Safety analysis of the proposed method

Attack	safety of the proposed method against the attack
phishing	safe (we need no assumption)
pharming	safe (if we assume user computer safety and router/DNS server safety)
MITB	safe (if we assume user computer safety)
Key Logger	safe (if we assume user computer safety)
password reuse	safe (if we assume connection safety from user computer to portal site and from portal site to financial site))

4.2 제안 방법과 기존 대응 방안들과의 안전성 비교

제안 방안은 컴퓨터 전문가가 아닌 일반 사용자가, 은행 등 피싱/파밍의 위험에 자주 노출되는 사이트에 접속할 때, 포털 사이트의 본인 계정을 경유하여 접속함으로써 포털 사이트에서 관리하는 안전성을 얻을 수 있게 하는 것이 목적이다. 즉, 일반 사용자를 대상으로 하는 것이다.

다음으로, 피싱/파밍 공격들에 대한 기존 대응 방안들과 본 논문에서 제안한 방법의 비교 분석을 수행하였다. 예를 들어, 2.1 절의 피싱 사이트 탐지 기술과 비교하여, 본 제안 방법은 피싱을 방지하고자 하는 주 목적은 동일하다. 그러나, 피싱 관리기관이 주로 이용하는 피싱 사이트 탐지에 관한 기술이 아닌, 일반사용자가 쉽게 이용할 수 있는 포괄적인 피싱 방지 방안을 제안한 것이다. 전체적인 비교 내용이 표 2에 나타나 있다.

표 2. 제안 방법과 기존 대응 방안들과의 안전성 비교
Table 2. Safety Comparison analysis of the proposed method and the previous countermeasures

Previous countermeasure	Comparative feature or advantage of the proposed method
2.1 phisphing site detection [6,7]	• a comprehensive method including phishing site detection
2.2 prevention of URL spoofing-phishing[8]	• a comprehensive method including prevention of url-spoofing-phishing
2.3 Cognitive approach[9]	• users only need to do procedurally (we don't need user's judgement based on the cognitive methods)
2.4 using mobile device [10-12]]	• we don't need separate mobile devices
2.5 strengthening authentication safety[13-18]	• we also use the authentication strengthening method (Section 3.1.4 and 3.1.5).

Ⅴ. 결론 및 추후 연구

본 논문에서는 포털 사이트의 개인 계정 맞춤 화면 정보를 이용한 피싱 및 파밍 공격에 대한 대응방안을 제안하였다. 그리고, 제안 방안을 안전성을 지원되는 시스템의 가정들에 따라 분류하여 분석하였다.

추후, 공유기나 DNS 서버 변조 공격에 대응하는 방안 등 본 논문에서 가정한 사실들에 대한 연구가 필요하다.

포털 사이트의 협조를 얻어, 본 제안 방안이 이용된다면, 일반 사용자들이 피싱/파밍에 대하여 보다 안전한 인터넷 환경을 이용할 수 있을 것으로 기대된다.

References

[1] Korean National Police Agency, *Phishing* (2015), Retrieved June 2015, from http://www.police.go.kr/portal/main/contents.do?menuNo=200289

[2] Korean National Police Agency, *Pharming* (2015), Retrieved June 2015, from http://www.police.go.kr/portal/main/contents.do?menuNo=200288

[3] J.-Y. Kang, J. Yoon, and Y. Kim, "Phishing/pharming examples and countermeasure analysis," in *Proc. KIISE KCC*, pp. 738-740, Yeosu, Korea, Jun. 2013.

[4] S. Kim, J. Kang, and Y. Kim, "Security analysis of phishing countermeasures," in *Proc. KIISE Winter Conf.,* pp. 756-758, Pyongchang, Korea, Dec. 2014.

[5] J. S. Shin, "Study on anti-phishing solutions, related researches and future directions," *J. The Korea Inst. Inf. Security & Cryptology*, vol. 23, no. 6, pp. 1037-1047, Dec. 2013.

[6] J. H. Sa and S. Lee, "Real-time phishing site detection method," *J. The Korea Inst. Inf. Security & Cryptology*, vol. 22, no. 4, pp. 819-825, Aug. 2012.

[7] M. Lee, H. Lee, and H. Yoon, "An anti-phishing approach based on search engine," in *Proc. KIISE KCC*, vol. 37, no. 1(D), pp. 121-124, Jeju, Korea, Jun. 2010.

[8] D. Min, T. Shon, and J. Moon, "A study on the phishing attack protection using URL spoofing," *J. The Korea Inst. Inf. Security & Cryptology*, vol. 15, no. 5, pp. 35-45, Oct. 2005.

[9] J. H. Kim, Y. J. Maeng, D. H. Nyang, and K. H. Lee, "Cognitive approach to anti-phishing and anti-pharming," *J. The Korea Inst. Inf. Security & Cryptology*, vol. 19, no. 1, pp. 113-124, Feb. 2009.

[10] B. Parno, C. Kuo, and A. Perrig, "Phoolproof phishing prevention," *Financial Cryptography and Data Security, LNCS,* vol. 4107, pp. 1-19, 2006.

[11] M. Mannan and P. C. van Oorschot, "Using a personal device to strengthen password authentication from an untrusted computer," *Financial Cryptography and Data Security*, *LNCS,* vol. 4886, pp. 88-103, 2007.

[12] H. Sun, Y. Chen, and Y. Lin. "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," *IEEE Trans. Inf. Forensics and Security*, vol. 7, no. 2, pp. 651-663, Apr. 2012.

[13] T.-H. Kim, J.-H. Lee, and D.-H. Lee, "Study on mobile OTP(One Time Password) mechanism based PKI for preventing phishing attacks and improving availability," *J. The Korea Inst. of Inf. Security & Cryptology*, vol. 21, no. 1, pp. 15-26, Feb. 2011.

[14] G. Varshney, R. C. Joshi, and A. Sardana, "Personal secret information based authentication towards preventing phishing attacks," *Advances in Intell. Syst. and Comput.*, vol. 176, pp. 31-42, 2012.

[15] R. Dhamija and J. D. Tygar, "The battle against phishing: Dynamic security skins," *Symp. Usable Privacy and Security (SOUPS)*, pp. 77-88, Pittsburgh, PA, USA, Jul. 2005.

[16] J. Lee, H. You, C. Cho, and M. Jun, "A design secure QR-Login user authentication protocol and assurance methods for the safety of critical data using smart device," *J. KICS*, vol. 37C, no. 10, pp. 949-964, Oct. 2012.

[17] S. Seo, C. Choi, G. Lee, and H. Choi, "QR code based mobile dual transmission OTP system," *J. KICS*, vol. 38B, no. 5, pp. 377-384,

May 2013.
[18] J.-Y. Park, J. Kim, M. Shin, and N. Kang, “QR-code based mutual authentication system for web service,” *J. KICS*, vol. 39B, no. 4, pp. 207-215, Apr. 2014.

김 소 영 (Soyoung Kim)

2012년 3월~현재 : 서울여자대학교 정보보호학과 학사과정

강 지 윤 (Ji-yoon Kang)

2015년 2월 : 서울여자대학교 정보보호학과 학사
2015년 3월~현재 : KAIST 정보보호대학원 석사과정

김 윤 정 (Yoonjeong Kim)

1991년 2월 : 서울대학교 컴퓨터공학과 학사
1993년 2월 : 서울대학교 컴퓨터공학과 석사
2000년 8월 : 서울대학교 전기·컴퓨터공학부 박사
2000년 7월~2001년 5월 : (주) 엔써커뮤니티 제품개발연구소 차장
2001년 5월~2002년 2월 : (주) 데이타게이트 인터내셔널 보안기술연구소 차장
2009년 1월~2010년 1월 : Baylor 대학교 (TX, USA) 방문연구원
2002년 3월~현재 : 서울여자대학교 정보보호학과 부교수
<관심분야> 암호학, 시스템 보안, 암호 응용