디지털산업정보학회 논문지 제5권 제1호 - 2009년 3월

# 피싱과 파밍 공격에 대응하기 위한 인증 프로토콜 설계

김 익 수* · 최 종 명**

# *Design Of A Secure Authentication Protocol Against Phishing And Pharming Attacks*

Kim, Ik Su · Choi, Jong Myung

〈Abstract〉

As individuals spend more time doing social and economic life on the web, the importance of protecting privacy against Phishing and Pharming attacks also increases. Until now, there have been researches on the methods of protection against Phishing and Pharming. However, these researches don't provide efficient methods for protecting privacy and don't consider Pharming attacks. In this paper, we propose an authentication protocol that protects user information from Phishing and Pharming attacks. In this protocol, the messages passed between clients and servers are secure because they authenticate each other using a hash function of password and location information which are certificated to clients and servers only. These messages are used only once, so that the protocol is secure from replay attacks and man-in-the-middle attacks. Furthermore, it is also secure from Pharming attacks.

Key Words : Phishing, Pharming, Authentication Protocol, Hash Function

## Ⅰ. 서론

컴퓨터 통신 기술의 발전으로 웹(web)을 통한 의사소통, 업무처리 등의 사회활동은 물론 쇼핑, 인터넷 뱅킹 등의 경제활동의 비중이 점차 커지고 있다. 이에 따라 악의적으로 인터넷의 개인정보를 약탈함으로써 경제적인 피해를 주는 피싱(Phishing)과 파밍(Pharming)의 위험이 커지고 있다[1, 2]. 피싱은 웹사이트를 위조함으로써 사용자가 개인정보(예: 사용자 아이디, 암호 등)를 입력하도록 유도함으로써 정보를 약탈한다. 반면에 파밍은 보다 지능적인 방법으로 DNS(Domain Naming Service) 정보를 변조해서 위조 사이트를 신뢰 사이트로 인식하도록 함으로써 사용자 정보를 약탈하는 방법이다[3]. 2007년 Gartner의 조사[4]에 의하면 피싱 공격으로 인한 피해액이 30억 달러 이상이었고, 향후 피싱과 파밍 기술이 점차 교묘히 발전하면서 피해액은 더욱 커질 것으로 예측된다.

피싱과 파밍을 통한 피해가 커지면서 이에 대응하기 위한 연구[5, 6, 7, 8, 9, 10, 11, 12, 13]들이 진행되어 왔지만, 이들은 다음과 같은 문제점들을 갖고 있다. 첫째로 파밍 공격을 방지하기 위한 기능을 제공하지 못한다. 파밍 공격은 DNS 위조를 통해서 이루어지기 때문에 현재

* (주)스카이컴
** 국립목포대학교 정보공학부 컴퓨터공학 교수(교신저자)

까지 제안된 피싱 방지 연구들은 파밍 공격에 대해서 방지 기능을 전혀 제공하지 못하는 문제점이 있다. 둘째로 피싱 공격에 대해서 효과적인 방지 기능을 제공하지 못한다. 예를 들어, URL 필터링 방법은 피싱 의심 사이트의 URL을 관리 혹은 피싱 사이트를 식별하는 규칙을 필요로 하기 때문에 새롭게 생성되는 피싱 사이트에 민첩하게 대응할 수 없다. 또한 인증서 기반의 신뢰성 있는 서버 방식은 일반 사용자가 인증서를 수시로 확인해야 하는 어려움과 중간자 공격에 의한 인증서 위조가 가능하다는 문제가 있다.

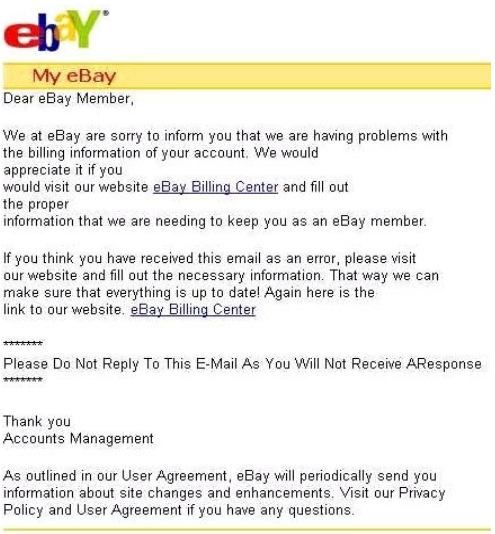
본 논문에서는 위에서 제시한 기존 연구들의 문제점을 해결하기 위해서 피싱과 파밍 공격으로부터 사용자 정보를 보호할 수 있는 인증 프로토콜을 제안한다. 사용자는 서버의 신뢰성을 확보하기 위해서 해당 사이트에 클라이언트 토큰(예: 사용자 ID)을 전송하고, 클라이언트 토큰을 기반으로 생성된 타당한 인증 정보를 서버로부터 수신함으로써 서버의 신뢰성을 확인한다. 만일 서버로부터 수신한 인증 정보가 타당하지 않을 경우에는 신뢰할 수 없는 사이트로 인식하여 인증 과정을 종료하며, 신뢰할 수 있는 경우에만 비밀 정보(예: 패스워드)를 서버에 전달한다. 클라이언트와 서버 간에 전달되는 인증 정보는 사용자 패스워드를 포함하여 랜덤 값과 위치 정보로 구성된 해시 값이기 때문에 패스워드를 획득하기 위한 도청 공격, 스푸핑을 위한 재생 공격과 중간자 공격으로부터 안전하며, 특히 최근 들어 큰 문제가 되고 있는 피싱과 파밍에 효과적으로 대응할 수 있다.

본 논문의 구성은 다음과 같다. 2장과 3장에서는 피싱과 파밍 공격을 소개하며, 이에 대응하기 위한 기존 연구에 관해 살펴본다. 4장에서는 제안 프로토콜을 기술하며, 제안 프로토콜의 안전성을 평가한다. 마지막으로 5장에서는 결론을 맺는다.

# II. 피싱과 파밍 동향

## 2.1 피싱 공격 방법

해커들은 사용자 정보를 탈취하기 위해 자신이 구축한 피싱 사이트로 인터넷 사용자의 접속을 유도하는 이메일을 보낸다[14]. 이메일에는 링크된 주소가 포함되어 있어 사용자가 클릭할 경우 피싱 사이트로 접속이 되며, 사용자는 아무런 의심 없이 자신의 정보를 입력하게 된다. 피싱이 사회적으로 주목을 받게 된 것은 2003년 eBay 사건이며, 이후에 피싱을 통한 피해는 지속적으로 증가하고 있다. eBay 피싱 사건에서 공격자들은 eBay를 사칭해 보안 위험으로 계정이 일시 차단되었으니 첨부된 링크를 클릭해 eBay 홈페이지를 통해 재등록하라는 메일을 무작위로 발송하였다. 메일을 수신한 사용자들은 ID와 패스워드와 같은 개인정보를 입력하였으며 공격자들은 이 정보를 탈취하였다. <그림 1>은 e-Bay를 사칭한 피싱에 사용된 메일의 내용이다.



My eBay

Dear eBay Member,

We at eBay are sorry to inform you that we are having problems with the billing information of your account. We would appreciate it if you would visit our website eBay Billing Center and fill out the proper information that we are needing to keep you as an eBay member.

If you think you have received this email as an error, please visit our website and fill out the necessary information. That way we can make sure that everything is up to date! Again here is the link to our website. eBay Billing Center

*******
Please Do Not Reply To This E-Mail As You Will Not Receive AResponse
*******

Thank you
Accounts Management

As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

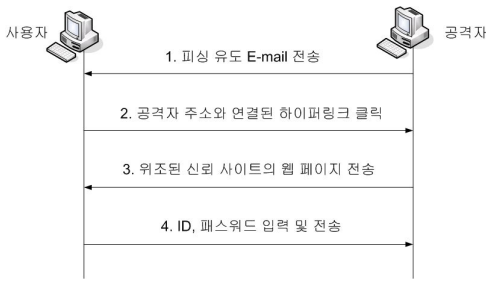
<그림 1> eBay 피싱에 사용된 메일

일반인들은 eBay 피싱에 사용된 메일 내용 중에서 하

이퍼링크 'eBay Billing Center'를 클릭하면 eBay 홈페이지로 연결된다고 생각하지만, 실제로는 공격자의 컴퓨터 혹은 사용자 정보를 수집할 수 있는 서버로 연결된다. 이것은 HTML에서 <a> 태그의 href 속성 값과 화면에 나타나는 내용을 달리 만들기 때문에 가능한 것이다. 예를 들어, 'eBay Billing Center' 링크는 다음과 같이 작성된다.

<a href="http://xxx.xxx.xxx.xxx">eBay Billing Center</a>

위 태그의 href 속성에 지정된 IP 주소는 실제 eBay 홈페이지의 IP 주소가 아닌 공격자 컴퓨터 혹은 자신이 공격에 성공한 서버의 주소이다. 따라서 사용자가 하이퍼링크를 클릭하게 되면 ID와 패스워드를 입력할 수 있는 새로운 웹 페이지로 이동하게 되며 사용자는 아무런 의심 없이 입력 양식에 자신의 개인정보를 입력하여 전송한다. 전송된 개인 정보는 신뢰 사이트가 아닌 피싱 사이트로 전송되기 때문에 공격자에 의해 악용될 수 있다. <그림 2>는 이러한 피싱 공격의 과정을 보여준다.




<그림 2> 피싱 공격 과정

## 2.2 피싱에서 파밍으로 진화

피싱은 초기의 링크를 위조하는 방법부터 점차 지능적인 해킹 방법으로 발전하고 있다. 초기의 링크를 위조하는 방법은 사용자가 실제로 하이퍼링크를 클릭했을 때 브라우저의 주소창 혹은 상태바에 나타나는 정보를 통해 어느 정도 피싱 공격을 탐지할 수 있다.

링크 위조 방법은 브라우저의 주소창을 통해 파악할 수 있기 때문에 링크 위조와 유사 도메인을 활용하는 피싱 방법이 등장하였다. 예를 들어 "www.trustedhostland.com"이라는 도메인을 가진 사이트를 가장하기 위해 공격자는 "www.trustedh0st1and.com"이라는 도메인을 획득하고 피싱 사이트를 구축한다. 숫자 0과 1이 포함된 두 번째 도메인명은 영문 o와 l이 포함된 첫 번째 도메인명과 엄연히 다르지만 대부분의 사용자는 두 도메인의 차이를 식별하지 못한다.

또 다른 형태로의 진화는 HTML, CSS, 자바스크립트 등을 결합하여 웹브라우저를 위조하는 방법이다[6]. 즉, 공격자는 window.open() 메소드를 이용하여 상태바와 주소창이 없는 새로운 창을 생성한 후, HTML의 프레임 관련 태그를 이용하여 주소창과 상태바, 클라이언트 영역을 할당한다. 이후 주소 입력창과 동일한 크기를 가지는 입력 폼을 주소 입력창과 동일 위치에 배치하고, 신뢰 사이트의 도메인 명을 입력 폼의 디폴트 속성 값으로 할당하면 이용자는 신뢰 사이트에 접속한 것으로 인식한다. 또한, 보안락(Security Lock) 이미지와 브라우저 로고 위치에 자신이 위조한 이미지들을 포함시킴으로써 주소창을 위조할 수 있다.

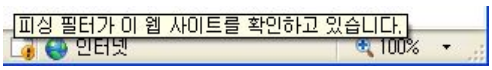
최근 들어, 피싱은 고급 해킹 기술과 결합하여 파밍 형태로 발전하고 있다. 파밍은 DNS의 정보를 변조함으로써 사용자들로 하여금 진짜 사이트로 오인하여 접속하도록 유도한 뒤에 개인정보를 훔치는 인터넷 범죄 수법이다. 피싱은 사용자가 웹 페이지나 웹 브라우저에 나타난 URL 주소를 주의 깊게 살펴보거나 웹 브라우저의 외형 변경 유무를 통해 어느 정도 식별이 가능하지만, 파밍은 DNS의 정보를 변조하는 공격이기 때문에 식별이 거의 불가능하여 더 많은 피해를 유발한다.

# Ⅲ. 안피 피싱과 파밍 연구 동향

## 3.1 안티 피싱 연구 동향

안티 피싱에 관련된 연구는 다양하게 분류될 수 있다. 구현 측면에서 보면 최근 들어 널리 사용하고 있는 방법 중의 하나가 브라우저의 확장 기능을 활용하여 피싱을 방지하는 것이다. 현재 널리 사용되고 있는 MS IE 와 Firefox 등 대부분의 웹브라우저는 확장 기능을 제공하며, 안티 피싱 연구자들은 이 기능을 이용해서 웹브라우저의 보안기능을 확장할 수 있다[15].

<그림 3>은 마이크로소프트사가 제공하는 MS IE 버전 7의 상태바를 나타낸다. 그림 3에서 좌측 이미지를 클릭하여 피싱 필터를 활성화하면 현재 방문 페이지가 피싱 사이트인지를 식별할 수 있는 기능을 사용할 수 있다.




<그림 3> MS IE의 피싱 필터

플러그 인 혹은 툴바를 이용한 안티 피싱 방법은 세부적으로 다음과 같이 분류될 수 있다. 첫 번째, 피싱이 의심되는 사이트를 블랙리스트로 등록하고 사용자가 해당 웹 사이트를 방문하는 경우에 사용자에게 경고 메시지를 전송하는 방법이다. 이 때, 블랙리스트 관리는 센터에서 등록하거나[7, 8] 사용자들의 참여를 통해서 등록 및 관리할 수 있다[9, 10]. 이 방법은 블랙리스트에 등록된 피싱 사이트에 대해서 효과적으로 사용자 접근을 예방할 수 있지만, 등록되지 않은 신규 피싱 사이트 혹은 파밍 공격에는 약하다는 단점을 갖고 있다.

두 번째는 사용자 정보를 제공할 때 도메인과 관련된 특정 정보로 변환해서 전달하는 방법이다[11, 12]. PwdHash[11] 플러그인은 사용자 암호를 도메인과 관련된 내용으로 변경해서 서버에 전달하기 때문에 사용자는 동일한 암호를 여러 사이트에서 사용할 수 있다. 이 방법은 사용자가 동일한 정보로 여러 사이트를 이용할 때 한 사이트의 정보가 노출되더라도 다른 사이트의 정보를 안전하게 유지할 수 있지만, 이후에 소개할 파밍 공격에 무력하다는 문제가 있다.

세 번째는 사이트 내용 혹은 URL 정보를 분석해서 피싱 사이트인지 여부를 파악하는 방법이다[6]. 하지만 이 방법은 피싱 사이트인지 여부를 판단하는 기준의 정확성이 높지 않다는 문제가 있다.

## 3.2 안티 파밍 연구 동향

안티 파밍은 크게 세 가지 방법으로 분류할 수 있는데, 첫 번째 방법은 신뢰할 수 있는 DNS 정보를 활용하는 것이다. 이 방법은 파밍과 같이 위조 및 변조된 DNS 정보를 통해 사용자가 피싱 사이트로 유도되는 것을 막기 위해 운영체제의 호스트 파일에 신뢰 사이트의 IP 주소를 기록한다. 도메인 이름을 브라우저에 입력했을 때 무조건 DNS 질의를 생성하는 것이 아니라 우선 캐시에서 읽어들이며, 만일 존재하지 않을 경우에는 호스트 파일을 통해서 도메인 이름에 대한 IP 주소를 해석한다. 따라서 호스트 파일에 중요한 신뢰 사이트의 IP 주소를 기록하여 파밍에 대응할 수 있지만, 사용자가 직접 신뢰 사이트의 IP 주소를 등록하고 관리해야 하는 불편함이 존재한다.

두 번째 방법은 DNS 프로토콜에 보안 기능을 추가하는 방법이다. DNSSEC은 DNS 데이터가 위조 및 변조되어 이용자에게 전달되는 것을 방지하기 위해 DNS 표준 프로토콜을 확장하고 보완하는 표준 프로토콜로서 DNS 포이즈닝 공격을 불가능하게 만든다[16]. 하지만 DNSSEC을 적용할 경우, 도메인 존의 서명된 데이터가 급증하고, 일반 도메인에 대한 대량의 위임설정 정보에 대한 서명처리로 인해 DNSSEC 비용이 과다하게 발생한다는 문제점이 있다.

세 번째 방법은 신뢰할 수 있는 제 3의 기관이 서명한 인증서를 웹 서버가 제시하고, 사용자가 이를 확인하여 신뢰 사이트를 인증한다[17]. 하지만 인증서는 보통 웹

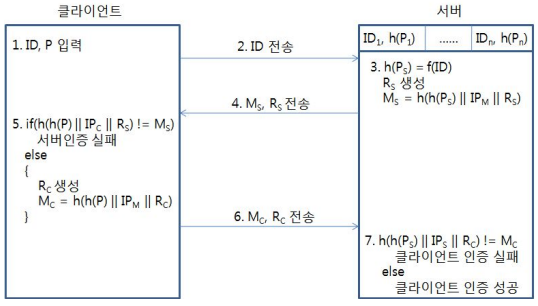
브라우저에 숨겨져 있으며, 일반 사용자가 인증서를 직접 확인하기에는 어려운 문제가 있다. 그리고 중간자 공격을 통한 인증서의 위조 공격이 충분히 가능하기 때문에 이에 대한 대응 방안이 요구된다[6].

## Ⅳ. 제안하는 상호 인증 프로토콜

### 4.1 상호 인증 프로토콜

제안 시스템의 인증 프로토콜을 설명하기 위해 사용될 용어 및 표기 방법은 다음과 같다.

ID : 사용자 입력 ID
P : 사용자 입력 패스워드
PS : 서버에 등록된 패스워드
h() : 해시 함수
f() : ID에 대한 패스워드 해시 값을 추출하는 함수
$M_C$ : 클라이언트가 생성한 인증 메시지
$M_S$ : 서버가 생성한 인증 메시지
$IP_C$ : 클라이언트 IP 주소
$IP_S$ : 서버 IP 주소
$IP_M$ : 메시지를 수신할 IP 주소
$R_C$ : 클라이언트가 생성하는 난수
$R_S$ : 서버가 생성하는 난수
|| : 연접 연산




<그림 4> 클라이언트와 서버 간의 인증 프로토콜

<그림 4>는 클라이언트와 서버 간의 신뢰 관계를 맺기 위한 상호 인증 프로토콜을 나타내며 부여된 숫자에 따라 인증 과정이 진행된다.

- 1단계: 클라이언트가 웹 페이지 입력 폼에 ID와 패스워드를 입력한다.
- 2단계: 클라이언트 모듈은 단지 ID만을 전송한다.
- 3단계: 서버 모듈은 수신한 ID에 대해 패스워드 해시 값을 추출하고 랜덤 값을 생성한다. 이후 추출된 패스워드의 해시 값, 생성된 랜덤 값, 메시지 수신 IP 주소를 모두 연접한 후 해시 연산을 수행하여 메시지 $M_S$를 생성한다.
- 4단계: 서버 모듈이 메시지 $M_S$와 $R_S$를 전송한다.
- 5단계: 클라이언트 모듈은 클라이언트가 입력한 패스워드의 해시 값과 클라이언트 IP 주소, $R_S$를 연접한 후 메시지 $M_S$와 비교한다. 만일 두 값이 일치하지 않을 경우에는 서버 인증이 실패한다. 두 값이 일치하면 서버 인증에 성공하며 패스워드의 해시 값, 메시지 수신 IP 주소, 생성 랜덤 값을 연접한 후 해시 연산을 수행하여 $M_C$를 생성한다.
- 6단계: 클라이언트 모듈이 메시지 $M_C$와 $R_C$를 전송한다.
- 7단계: 서버 모듈은 저장된 패스워드의 해시 값과 서버 IP 주소, $R_C$를 연접한 후 메시지 $M_C$와 비교한다. 두 값이 일치하지 않을 경우에는 클라이언트 인증이 실패하며 일치할 경우에는 클라이언트 인증에 성공한다.

### 4.2 프로토콜 안전성 평가

#### 4.2.1 도청 공격

일반적으로 공격자들은 클라이언트와 서버 간에 전송되는 메시지를 도청하여 패스워드를 획득하려 한다. 제안 프로토콜에서는 패스워드를 IP 주소와 랜덤 값을 연접한 후 해시 연산을 수행하여 전송하기 때문에 공격자

는 도청을 통해 평문의 패스워드를 추출할 수 없다.

#### 4.2.2 재생 공격

재생 공격은 공격자가 클라이언트와 서버 간에 전송되는 해시된 메시지를 도청하여 저장한 후 저장된 메시지를 차후에 재전송함으로써 인증에 성공한다. 이 공격은 클라이언트와 서버가 항상 동일한 메시지를 전송할 때 발생한다. 하지만 제안 프로토콜에서는 인증 메시지를 구성하는 랜덤 값이 수시로 변경되기 때문에 메시지를 재사용할 수 없다.

#### 4.2.3 반사 공격

반사공격은 공격자가 한 개체로부터 생성된 메시지를 저장하고 다시 그 개체에게 재전송하여 인증을 통과하는 방법이다. 시도-응답 프로토콜에서는 신뢰되는 두 개체가 인증 과정에 사용하기 위한 동일한 키 K를 공유하며, 서로 간의 식별을 위해 난수를 생성한다. 개체 A가 난수 $N_1$을 전송하면 개체 B는 암호 값 $E(N_1, K)$와 난수 $N_2$로 응답한다. 개체 A는 개체 B로부터 수신한 $E(N_1, K)$와 자신이 계산한 암호 값을 비교함으로써 개체 B를 인증한다. 인증에 성공하면 개체 A는 $E(N_2, K)$를 개체 B에게 전송하며, 개체 B는 수신한 $E(N_2, K)$와 자신이 계산한 암호 값을 비교하여 개체 A를 인증한다.

공격자는 공유키 K를 모르기 때문에 송신 개체가 전송한 난수의 암호 값을 송신 개체에게 전송할 수 없다. 하지만, 공격자는 송신 개체가 보낸 난수에 대한 암호 값을 알기 위해서 수신한 난수를 송신 개체에게 재전송하고, 이를 수신 개체의 난수로 인식한 송신 개체는 이에 대한 암호 값을 공격자에게 전송하게 된다. 암호 값을 수신한 공격자는 이 암호 값을 다시 송신 개체에게 전송함으로써 타당한 개체로 가장할 수 있다. 하지만 제안 프로토콜에서는 클라이언트와 서버 간의 응답이 서로 다른 해시 연산을 통해 수행되기 때문에 반사 공격이 이루어질 수 없다.

#### 4.2.4 중간자 공격

중간자 공격은 공격자가 클라이언트와 서버 사이에 전송되는 메시지를 재전송하거나 위조된 메시지를 전송하여 정당한 클라이언트 혹은 서버로 위장하는 공격이다. 제안 프로토콜을 통해 전송되는 메시지에는 메시지를 수신하게 될 개체의 IP 주소가 패스워드와 랜덤 값으로 연접한 후 해시 연산이 수행되어 전송되기 때문에 이 메시지가 수신자 측에서 자신의 IP 주소와 랜덤 값, 패스워드로 계산된 해시 값과 일치하지 않으면 메시지 위변조로 간주하여 인증이 거부된다.

#### 4.2.5 피싱 공격

피싱은 사용자를 위조 사이트로 유도하여 패스워드를 탈취하기 위해 다음과 같은 공격 과정을 거친다.

- 1단계: 공격자가 자신의 서버에 신뢰 사이트와 동일하게 위조 홈페이지를 구축
- 2단계: 위조 홈페이지와 연결된 하이퍼링크를 포함하는 악의적인 이메일을 공격 대상자에게 전송
- 3단계: 공격 대상자가 수신 이메일의 하이퍼링크를 클릭
- 4단계: 공격 대상자는 공격자에 의해 구축된 홈페이지로 접속
- 5단계: 공격 대상자는 수신한 웹페이지 입력 폼에 자신의 ID와 패스워드를 입력하여 전송
- 6단계: 공격자는 공격 대상자의 ID와 패스워드를 획득

위 시나리오는 가장 단순한 피싱 공격으로서 사용자는 웹 브라우저의 주소창의 URL 정보를 확인하거나 로그인 실패가 발생할 경우 피싱 공격을 탐지할 수 있다. 하지만 앞서 기술했듯이 대부분의 사용자는 URL 정보를 면밀히 검토하지 않으며, 로그인 실패 메시지를 수신하여 피싱 유무를 파악할 경우에는 이미 패스워드가 공격자에게 전달되었기 때문에 매우 위험한 탐지 방법이다. 특히, 공격자 서버가 사용자와 서버 사이에서 패킷을 포워딩 하는 경우에는 사용자의 ID와 패스워드가 공격자에 의해 신뢰 사이

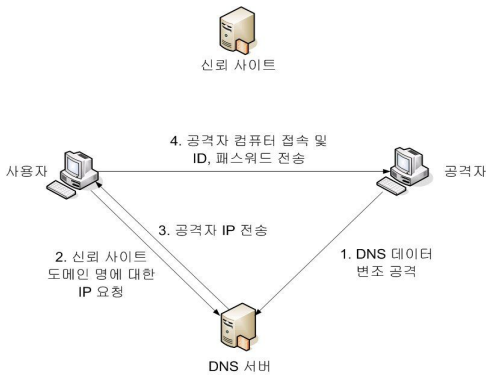
트로 전달되기 때문에 정상적인 로그인이 가능하여 공격 대상자는 아무런 의심 없이 서비스를 이용하게 된다.

제안 프로토콜은 패스워드 정보를 다른 인증 정보와 함께 해시 값으로 전달하기 때문에 평문의 패스워드 탈취가 불가능하며, 랜덤 값에 의해 항상 변하는 값을 가지기 때문에 피싱을 위한 재생공격이 불가능하다. 또한, 클라이언트와 서버는 메시지를 전송한 호스트의 IP 주소를 인증 과정에서 확인하기 때문에 패킷 포워딩에 의한 피싱에 안전하다.

#### 4.2.6 파밍 공격

사용자 정보를 탈취하기 위한 파밍 공격 과정은 <그림 5>와 같다.

- 1단계: 공격자가 DNS 서버를 공격하여 DNS 서버 정보를 변조
- 2단계: 사용자는 신뢰 사이트에 해당하는 IP 주소 정보를 요청하기 위해 주소창에 도메인 명을 입력하여 DNS 서버에 쿼리 전송
- 3단계: DNS 서버가 신뢰 사이트의 IP 주소가 아닌 공격자에 의해 위조된 사이트의 IP 주소 전송
- 4단계: 사용자가 위조 사이트에 접속한 후, 자신의 ID와 패스워드를 입력하여 전송
- 5단계: 공격자가 ID와 패스워드를 획득




<그림 5> 파밍 공격 과정

파밍은 실제로 공격 대상자는 자신이 원하는 신뢰 사이트와 동일한 웹페이지를 보게 되며 주소창에 표기되는 도메인 정보가 타당한 정보로 보이기 때문에 공격을 식별할 수 없다.

제안 프로토콜에서는 파밍 공격 과정 4에서 사용자로부터 입력된 ID와 패스워드 중 ID만을 전송하며, 서버가 사용자의 패스워드 정보를 기반으로 생성한 올바른 인증 정보를 반드시 전송해야만 사용자의 패스워드를 전송하기 때문에 패스워드를 보유하지 않은 위조된 사이트로의 패스워드 유출이 차단된다. 비록 공격자 서버가 패킷 포워딩을 통해 신뢰된 사이트로부터 수신한 인증 정보를 전달할지라도 IP 주소 정보가 포함된 해시 값이 서로 다르기 때문에 제안 프로토콜은 파밍 공격에 안전하다.

## V. 결론

웹의 활용이 사회 및 경제활동으로 확장됨에 따라 피싱과 파밍 공격에 의한 피해가 급속히 증가하고 있다. 이들 공격에 대응하기 위해 지금까지 진행되어 온 연구로는 블랙리스트를 사용하는 방법, 사이트 내용에 따라 판단하는 방법 등이 있지만, 신규 피싱 사이트 차단 및 피싱 사이트 판단의 정확성, 파밍 공격 차단 등에서 많은 문제점들이 있었다.

본 논문에서는 사용자와 서버간의 상호 인증을 통해 신뢰성을 판단한 후, 서버에 사용자의 비밀 정보를 안전하게 제공하는 프로토콜을 제안하였다. 이 프로토콜은 신규 피싱 사이트의 식별이 가능하며, 특히 파밍 공격에 대응이 가능한 효과적인 프로토콜이다.

향후 연구로는 본 프로토콜을 구현하는 사이트와 웹 브라우저 플러그인을 개발함으로써 시스템 구현의 용이성 및 확장성을 파악하는 것이다.

## 참고문헌


[1] 새로운 사이버위협 : 피싱, 한국정보보호진흥원, 2005.

[2] 피싱과 안티피싱 기술의 동향, 정보통신연구진흥원, 2008.

[3] Cunter Ollmann, "The Pharming Guide", 2005.

[4] Gartner, available at http://www.gartner.com/it/page.jsp?id=565125

[5] Daisuke Miyamoto, Hiroaki Hazeyama, and Youki Kadobayashi, "SPS: A Simple Filtering Algorithm to Thwart Phishing Attacks", LNCS 3837, 2005, pp. 195-209.

[6] Tie-Yan Li and Yongdong Wu, "Trust on Web Browser: Attack vs. Defense", In proceedings of the International Conference on Applied Cryptography and Network Security, 2003, pp. 241-253.

[7] Google Safe Browsing, available at http://www.google.com/tools/

[8] Microsoft Phishing Filterin IE7, available http://www.microsoft.com/windows/ie/

[9] Cloudmark, available at http://www.cloudmark.com/desktop/download/

[10] EarthLink Toolbar, available at http://www.earthlink.com/free/toolbar/

[11] B. Ross, et al., "Stronger Password Authentication Using Browser Extentions", In proceedings of Usenix Security Symposium, 2005.

[12] Thomas Raffetseder, et al., "Building Anti-Phishing Browser Plug-Ins: An Experience Report".

[13] Chow, et al., "Client-Side Defense against Web-based Identity Theft", In proceedings of Network and Distributed System security Symposium, 2004.

[14] Christine E. Drake, Jonathan J, Oliver, and Eugene J. Koontz, "Anatomy of a Phishing Email", In proceedings of CEAS'04, 2004.

[15] Lorrie Cranor, et al., "Phinding Phish: An Evaluation of Anti-Phishing Toolbars", 2006.

[16] Giuseppe Ateniese and Stefan Mangard, "A New Approach to DNS Security(DNSSEC)", In proceedings of the 8th ACM conference on Computer and Communications Security, 2001, pp. 86-95.

[17] David Wagner and Bruce Shenier, "Analysis of the SSL 3.0 protocol", The Second USENIX Workshop on Electronic Commerce Proceedings, 1996.


### ■ 저자소개 ■


김 익 수
Kim, Ik Su

2006년 1월-현재 (주)스카이컴 과장
2008년 2월 숭실대학교 컴퓨터학과(공학박사)
2002년 2월 숭실대학교 컴퓨터학과(공학석사)
2000년 2월 숭실대학교 컴퓨터학과(공학사)

관심분야 : 시스템 보안, 네트워크 보안, 모바일 보안, 시스템 소프트웨어
E-mail : iksuplorer@nate.com

최 종 명
Choi, Jong Myung

2004년 3월-현재 국립목포대학교 정보공학부 컴퓨터공학 교수
2003년 8월 숭실대학교 컴퓨터학과 (공학박사)
1996년 8월 숭실대학교 전자계산학과 (공학석사)
1992년 2월 숭실대학교 전자계산학과 (공학사)

관심분야 : 프로그래밍 언어, 유비쿼터스 컴퓨팅, 컨텍스트-인지 시스템
E-mail : jmchoi@mokpo.ac.kr



논문접수일 : 2009년 2월 2일
수 정 일 : 2009년 월 일
게재확정일 : 2009년 2월 20일