KIPS Tr. Comp. and Comm. Sys.
Vol.7, No.2 pp.41~48 pISSN: 2287-5891

https://doi.org/10.3745/KTCCS.2018.7.2.41

Password-Based Mutual Authentication Protocol Against Phishing Attacks

Iksu Kim† · Jongmyung Choi††

ABSTRACT

Until now, various studies on anti-phishing have been conducted. The most typical anti-phishing method is a method of collecting URL information of a phishing site in advance and then detecting phishing by comparing the URL of the visited site with the previously stored information. However, this blacklist-based anti-phishing method can not detect new phishing sites. For this reason, various anti-phishing authentication protocols have been proposed. but these protocols require a public key and a private key. In this paper, we propose a password-based mutual authentication protocol that is safe for phishing attacks. In the proposed protocol, the mutual authentication between the client and the server is performed through the authentication message including the password information. The proposed protocol is safe to eavesdropping attack because the authentication message uses the hash value of the password, not the original password, And it is safe to replay attack because different messages are used every time of authentication. In addition, since mutual authentication is performed, it is safe for man-in-the-middle attack. Finally, the proposed protocol does not require a key issuance process for authentication.

Keywords : Phishing, Authentication Protocol, MITM Attack, Replay Attack

피싱 공격에 대응하기 위한 패스워드 기반의 상호 인증 프로토콜

김 익 수† · 최 종 명††

요 약

지금까지 피싱에 대응하기 위한 여러 연구가 진행되어 왔다. 가장 대표적인 안티 피싱 방법은 피싱 사이트의 URL 정보를 미리 수집한 뒤, 사용자가 방문하는 사이트의 URL과 미리 저장된 정보를 비교하여 피싱을 탐지하는 방법이다. 하지만 이러한 블랙리스트 기반의 안티 피싱 방법은 새로운 피싱 사이트를 탐지하지 못하는 한계를 갖는다. 이에 다양한 안티 피싱 인증 프로토콜이 제안되어 왔지만 대부분 인증 과정에서 공개키와 비밀키를 필요로 한다. 이에 본 논문에서는 피싱 공격에 안전한 패스워드 기반 상호 인증 프로토콜을 제안한다. 제안된 프로토콜에서 클라이언트와 서버간의 상호 인증은 패스워드 정보가 포함된 인증 메시지를 통해 수행된다. 인증 과정에서 사용되는 인증 메시지에는 패스워드 원본이 아닌 패스워드의 해시 값이 포함되며, 인증 시 매번 다른 메시지가 사용되기 때문에 재생공격, 도청 공격에 안전하다. 또한, 상호 인증을 수행하기 때문에 중간자 공격에 안전하며, 인증을 위한 별도의 키 발급 과정이 필요없다.

키워드 : 피싱, 인증 프로토콜, 중간자 공격, 재생 공격

1. 서 론

개인정보를 약탈하여 금전적 피해를 유발하는 피싱 사고가 속출하고 있는 상황에서 이에 대응하기 위한 여러 솔루션 및 프로토콜들이 제안되어 왔다. 현재 사용되고 있는 대표적인 안티 피싱 솔루션으로는 마이크로소프트사의 인터넷 익스플로러에 탑재된 SmartScreen Filter가 있다. SmartScreen Filter는 사용자가 방문한 서버의 URL 정보와 사전에 구축한 블랙리스트 정보를 비교하여 피싱 사이트 방문 여부를 판단한다. 하지만 사용자가 블랙리스트 DB에 저장되어 있지 않은 새로운 피싱 사이트를 방문할 경우에는 사용자에게 올바르게 알려주지 못하는 한계가 있다. 이에 블랙리스트를 효과적으로 관리하기 위해 자동으로 피싱 사이트를 식별하

† 종신회원 : 숭실대학교 컴퓨터학부 교수
†† 종신회원 : 목포대학교 컴퓨터공학과 교수
Manuscript Received : June 29, 2017
First Revision : August 14, 2017
Accepted : September 19, 2017
* Corresponding Author : Jongmyung Choi(jmchoi@mokpo.ac.kr)

는 알고리즘 연구도 진행되었다[1-3]. 하지만 이러한 방법을 통해 피싱 사이트를 탐지하여 블랙리스트를 생성하더라도 그에 따른 시간이 소요되기 때문에 실시간 피싱 사고 방지에는 한계가 있다.

SSL/TLS 프로토콜은 응용 계층에 암호화 서비스를 제공하는 프로토콜로써 클라이언트가 방문하는 서버를 인증하기 위한 방법도 함께 제공한다. 서버 인증 방법은 신뢰할 수 있는 제 3의 기관이 서명한 서버 인증서를 웹 서버가 사용자에게 제시함으로써 신뢰 사이트임을 밝힌다. 하지만 SSL/TLS는 중간자 공격에 취약한 문제가 있다[4]. 이 공격에서 해커는 조작된 핸드셰이크 기법을 통해 서버와 클라이언트 사이에 전송되는 데이터를 복호화 및 암호화함으로써 데이터 조작이 가능하므로 클라이언트와 서버간의 상호 인증을 위한 보완이 필요하다. 이에 클라이언트와 서버 간의 상호 인증을 위한 다양한 프로토콜이 제안되어 왔지만 대부분의 프로토콜들이 여전히 메시지 재생 공격과 파밍 같은 다양한 공격에 취약하며, 상호 인증을 위한 공개키 및 비밀키 발급 과정이 필요하다. 그리고 인증 과정에서 개인의 메신저나 스마트 디바이스를 필요로 하는 경우도 있다.

본 논문에서는 피싱 공격에 안전한 패스워드 기반의 상호 인증 프로토콜을 제안한다. 제안하는 상호 인증 프로토콜에서는 패스워드를 알고 있는 실제 사용자와 서버만이 인증에 성공할 수 있다. 제안 프로토콜에 의한 인증 과정에서는 사용자와 서버 상호간에 인증 메시지가 전송되는데, 인증 메시지에는 원본 패스워드와 인증에 필요한 추가적인 정보들이 함께 해시 연산되어 포함된다. 따라서 해커가 중간에 인증 메시지를 도청하더라도 패스워드 원본을 추출할 수 없다. 특히 인증 메시지에는 메시지를 수신해야 할 대상의 IP 주소 정보가 포함되어 있기 때문에 중간자 공격이 진행될 경우 인증을 거부할 수 있다. 또한 매 인증 시마다 일회용 난수를 생성하여 인증 메시지에 포함하기 때문에 재생 공격에 안전하다. 마지막으로, 제안 프로토콜에서는 상호 인증을 위한 공개키 및 비밀키 발급을 필요로 하지 않기 때문에 사용자는 서버와 용이하게 인증을 수행할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 안티 피싱 연구 동향에 대해 살펴보고 3장에서는 제안하는 안티 피싱 프로토콜을 기술한다. 4장에서는 제안 프로토콜의 안전성을 분석한 후 5장에서 결론을 짓는다.

2. 관련 연구

2.1 피싱

해커는 피싱 공격을 수행하기 위해 먼저 위조 사이트를 구축하고 불특정다수의 사용자들에게 피싱을 유도하기 위한 이메일을 전송한다. 이 이메일에는 위조 사이트로 연결되는 하이퍼링크가 포함되어 있으며, 사용자가 이를 클릭할 경우 위조 사이트로 연결이 된다. 만일 사용자가 실제로 계정을 가지고 있으며 위조 사이트의 진위 여부를 식별하지 못하는 경우, 사용자는 자신의 패스워드를 위조된 페이지에 입력하게 되고 이 패스워드는 해커에게 그대로 전달된다. 이러한 전형적이고 단순한 공격방법은 사용자가 브라우저의 주소창을 살펴보면 쉽게 알아차릴 수 있다. 하이퍼링크를 통해 위조 사이트로 연결될 경우에는 주소창에 실제 사이트 주소나 도메인 이름이 아닌 위조 사이트의 IP 주소가 표시되기 때문이다.

좀 더 진보된 피싱 방법으로는 스크립트를 이용한 사용자 웹 브라우저 위조 방법이다[5]. 앞서 기술한 피싱 방법은 주소창 확인을 통해 쉽게 피싱 공격을 식별할 수 있지만 스크립트를 이용한 웹 브라우저 위조 방법은 사용자가 공격 사실을 쉽게 알아차리기 어렵다. 이 공격 방법은 공격 중에 주소창에 표시되는 위조 사이트의 IP주소나 도메인 이름을 스크립트로 숨기고 해커가 작성한 IP주소 혹은 도메인이 담긴 이미지로 주소창을 덮어씀으로써 실제 사이트에 접속한 것처럼 위장한다.

2.2 안티 피싱

지금까지 웹 브라우저의 확장기능이나 툴바를 사용한 여러 안티피싱 솔루션들이 개발되어 왔다[6-8]. 마이크로소프트의 SmartScreen Filter는 인터넷 익스플로러에 탑재된 대표적인 안티피싱 프로그램으로 미리 수집된 피싱 사이트의 URL 정보를 블랙리스트 형태로 DB에 저장하며, 사용자가 방문한 서버의 URL 정보와 비교하여 피싱 사이트 방문 여부를 판단한다. SmartScreen Filter의 가장 큰 장점은 등록된 피싱 사이트로의 사용자 접근을 매우 효과적으로 차단할 수 있지만, DB에 등록되지 않은 신규 피싱 사이트는 탐지가 불가능하기 때문에 피싱 사고로부터 안전할 수 없다.

[1]에서는 피싱 사이트 블랙리스트 생성기를 제안하였는데, 특정 웹 페이지가 피싱 사이트의 웹 페이지인지 판단하기 위한 방법으로 구글 검색엔진을 사용한다. 블랙리스트 생성을 위한 알고리즘에서는 의심되는 웹 페이지의 도메인이 실제 합법적인 사이트의 구글 검색 결과 중 상위 10위 안에 포함되는 페이지의 도메인과 같은지 비교한다. 만일 도메인이 같은 페이지가 없을 경우 이를 피싱 사이트로 판단하여 블랙리스트에 추가한다. 이 연구 결과에 따르면 피싱 사이트 및 합법적 사이트의 탐지율은 각각 100%와 91% 탐지율을 보였다.

[3]에서는 사용자가 피싱 사이트에 접속하는 경우, 피싱 사이트의 URL이 HTTP referer 헤더필드를 통해 합법적인 사이트로 유입되는 특성을 이용한 실시간 피싱 사이트 탐지 시스템을 제안하였다. 이 탐지 시스템을 특정 홈페이지를 가장한 피싱 사이트 탐지에 적용한 결과 6일 동안 40개의 피싱 사이트를 탐지하였다. 하지만 이 연구의 단점은 피싱

사이트에 포함된 웹 페이지가 합법적인 사이트의 링크를 갖지 않는 경우 탐지가 불가능하다는 것이다.

[9]에서는 포털 사이트를 경유하여 금융권 사이트를 접속하게 함으로써 피싱을 방지하는 방안을 제안하였다. 우선 사용자는 포털 사이트에 로그인 한 후 메뉴를 통해 금융권 사이트를 등록한다. 이후 금융권 사이트를 이용하기 위해서는 자신의 계정으로 포털 사이트에 로그인하고 은행 접속 메뉴를 클릭하여 은행에 접속한다. 이 방법을 통한 피싱 방지는 반드시 포털 사이트를 통해서만 가능하다. 즉, 이메일이나 웹 페이지의 링크를 통한 서비스 이용 시에는 안티피싱 기능을 제공할 수 없다.

[10-14]에서는 QR 코드 및 다중채널 인증요소를 이용하여 피싱에 대응하는 프로토콜을 제안하였다. 이들은 QR 코드를 기반으로 하기 때문에 QR 코드 인식을 위한 스마트 장치가 있는 경우에만 인증이 가능하다는 문제가 있다.

[15]에서는 실시간 피싱 방지를 위한 패스워드 기반의 인증 프로토콜을 제안하였다. 하지만 이 프로토콜은 메시지 재생 공격에 취약함이 증명되었다[16]. 메시지 재생 공격에 안전하기 위해서는 패스워드 혹은 인증과정에 사용되는 인증 메시지가 일회용으로 사용되어야 한다. [17]에서는 고정된 패스워드 대신 원타임 패스워드를 이용한 안티 피싱 인증 서비스를 제안하였다. 이 서비스를 이용하기 위해서는 적어도 하나의 메신저를 설치해서 운용해야 한다는 문제가 있다. 그 외에도 피싱 방지를 위한 다양한 프로토콜들이 제안되어 왔지만 메시지 수정 공격, 메시지 재생 공격 등에 취약하며, 인증과정에서 공개키 및 비밀키 발급이 필요하다[18-21].

3. 패스워드 기반의 상호 인증 프로토콜

이 장에서는 실시간으로 피싱 공격의 여부를 판단하고 피싱 공격에 의한 피해를 막을 수 있는 안티 피싱 프로토콜을 제안한다. 제안 프로토콜은 인증 과정에서 별도의 암호키를 요구하지 않는 경량의 인증 프로토콜이다.

3.1 인증 프로토콜 용어 및 계정 등록 과정

현재 인터넷 상의 대부분 서버들은 네트워크 보안을 위해 SSL을 사용하고 있다. 서버는 SSL을 통해 데이터 암호화 기능을 제공하며, 서버 인증서를 통해 클라이언트에게 자신임을 증명한다. 이에 제안 프로토콜은 계정 등록 과정이 시작되기 전에 SSL 프로토콜이 시작된다고 가정한다. SSL 프로토콜의 진행 과정은 다음과 같다.

- 1단계: 클라이언트가 합법적인 서버의 계정 등록 페이지에 접속하면 해당 서버는 클라이언트에게 서버 인증서를 전송한다.
- 2단계: 클라이언트가 서버를 인증하게 되면 상호간에 전달되는 데이터를 암호화하기 위한 세션키를 생성한다.

Table 1. Notation

Notation	Representation
ID	User ID
PC	Password submitted by client
PS	Password registered to the server
RC	Random number generated by the client
RS	Random number generated by the server
H()	One-way hash function
S()	Function that extracts the password hash value of a specific ID from a password file
MC	Authentication message generated by the client
MS	Authentication message generated by the server
MK	Message with session key
MR1	Exclusive-OR operation of RC and PC hash values
MR2	Exclusive-OR operation of RC, RS, and PC hash values
IPC	Client IP address
IPS	Server IP address
IPM	IP address to receive the message
SK	Session key
|	Concatenation operation
⊙	Exclusive-OR operation

- 3단계: 클라이언트는 생성된 세션키를 서버의 공개키로 암호화하여 서버에게 전송한다.
- 4단계: 서버는 개인키로 세션키를 복호화한다.

이제 클라이언트와 서버는 세션키를 통해 안전하게 메시지를 전송할 수 있으며 제안하는 프로토콜의 계정 등록과정이 시작된다. 제안하는 프로토콜에 의한 인증 절차를 설명하기 위해 본 논문에서는 Table 1의 표기법을 사용한다. 먼저 클라이언트는 자신이 서비스를 이용하고자 하는 서버에 Fig. 1과 같이 계정을 등록한다. 패스워드가 해커들에게 노출되는 것을 막기 위해서 사용자가 입력하는 패스워드 P_C는 해시 값 $H(P_C)$로 변환되어 서버에 전달된다. 3.2절에서 인증 프로토콜의 상세한 기술을 위해 사용자가 입력하는 패스워드는 P_C로 표기하고, 서버에 저장된 패스워드는 P_S로 표기하여 서로를 구분하고자 한다.

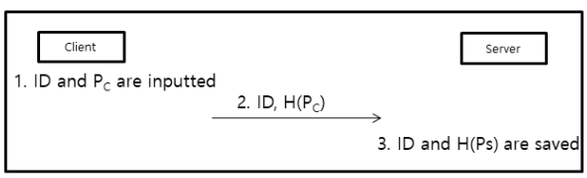

Fig. 1. Registration Phase

3.2 인증 프로토콜

클라이언트가 서버에 계정을 등록한 후 서비스를 이용하기 전에 수행되어야 할 인증 과정은 Fig. 2와 같다.

- 1단계: 사용자는 ID와 패스워드 P_C를 입력한다. 클라이언트 컴퓨터는 R_C를 생성하고 $H(P_C)$를 계산한다. 그리고 R_C와 $H(P_C)$의 배타적 논리합 연산을 수행하여 M_{R1}을 생성한다.
- 2단계: 클라이언트 컴퓨터는 ID와 M_{R1}를 서버로 전송한다.
- 3단계: 서버는 클라이언트로부터 수신한 ID를 S()함수의 입력 값으로 사용하여 패스워드 파일로부터 패스워드 해시 값 $H(P_S)$를 추출한다. 그리고 일회용 인증 메시지에 사용될 R_S와 세션키 SK를 생성한다. R_S는 인증 메시지가 재생 공격에 사용되는 것을 막기 위해 사용되는 난수이다. 세션키 SK는 서버와 클라이언트 간의 데이터 전송 시 사용될 비밀키이며, 일회용으로 사용하기 위해 랜덤 함수로부터 생성된다. 이후 서버는 클라이언트로부터 수신한 M_{R1}에 $H(P_S)$을 수행하여 R_C를 추출한다. 추출된 R_C와 R_S는 $H(P_S)$과 배타적 논리합 연산을 통해 메시지 M_{R2}로 변환된다. 난수 R_S는

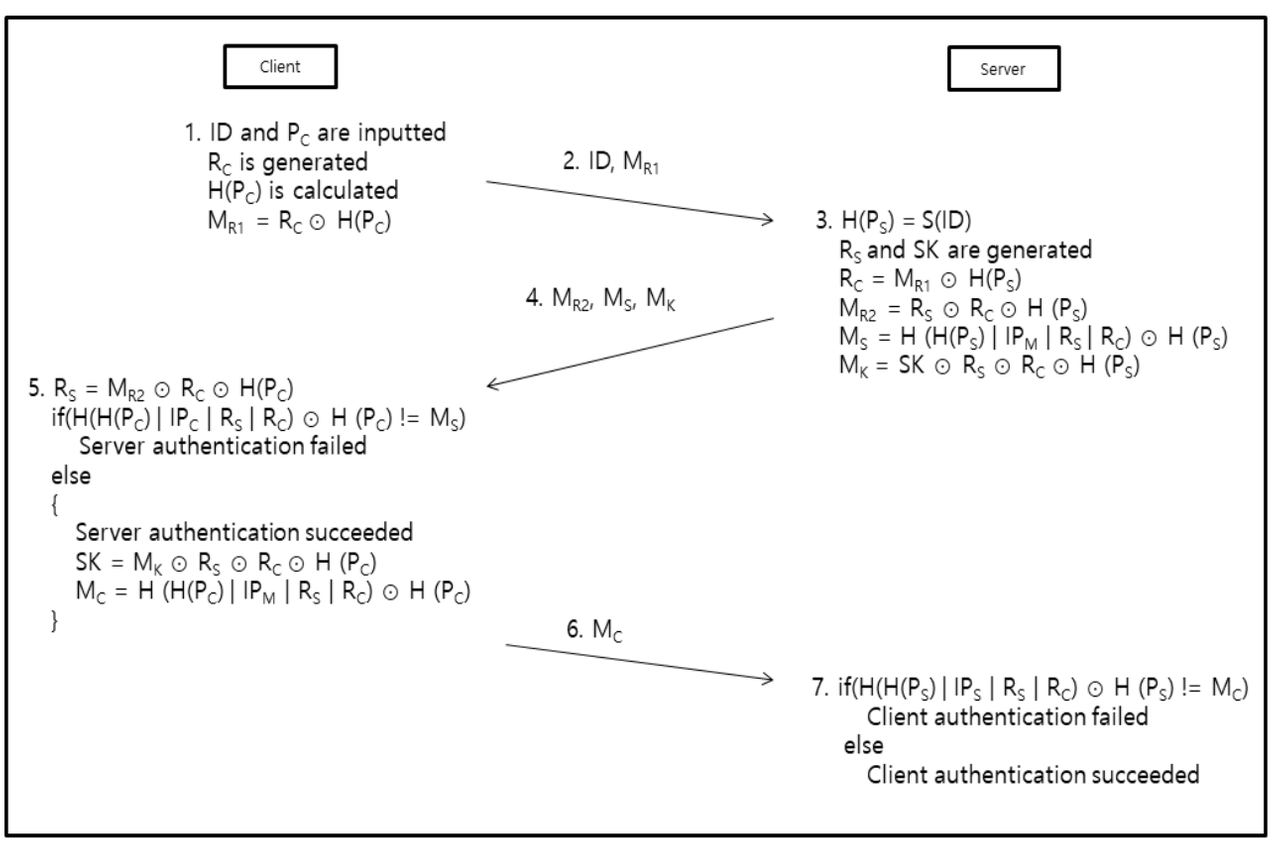

Fig. 2. Authentication Phase

서버에 저장된 패스워드와 R_C를 알고 있는 클라이언트에 의해서만 메시지 M_{R2}로부터 추출될 수 있다. 인증메시지 M_S의 생성은 먼저 서버에 저장된 패스워드의 해시 값, 인증메시지를 받을 클라이언트의 IP 주소(ID를 전송한 클라이언트의 IP 주소), 난수 R_S, R_C를 모두 연접한 후, 해시 연산을 수행한다. 그리고 $H(P_S)$에 대해 배타적 논리합을 수행하여 최종적으로 M_S가 생성된다. 또한 세션키 SK가 도청 및 재생 공격에 사용되는 것을 막기 위해 패스워드의 해시 값 $H(P_S)$와 난수 R_S, R_C를 세션키 SK에 배타적 논리합을 수행하여 메시지 M_K를 생성한다.

- 4단계: 3단계에서 생성된 M_S, M_R, M_K가 클라이언트에게 전송된다.
- 5단계: 클라이언트 컴퓨터는 서버로부터 수신한 M_{R2}과 R_C, $H(P_C)$의 배타적 논리합 연산을 수행하여 난수 R_S를 계산한다. 이후 클라이언트 컴퓨터는 사용자가 입력한 패스워드 해시 값 $H(P_C)$와 자신의 IP 주소, R_C, 서버로부터 수신한 R_S를 연접한 결과에 대한 해시 값을 생성한다. 그리고 이 해시 값에 $H(P_C)$을 배타적 논리합 연산 후 Ms와 비교한다. 만일 두 값이 같으면 클라이언트는 합법적인 서버임을 인증한다. 그리고 M_K 메시지에 R_S와 R_C, $H(P_C)$의 배타적 논리합 연산을 수행하여 세션키 SK를 추출한다. 또한 클라이언트 자신이 타당한 사용자임을 서버로부터 인증받기 위한 인증 메시지 M_C를 생성한다. 인증 메시지 M_C의 생성은 먼저 사용자가 입력한 패스워드의 해시 값 $H(P_C)$, 인증메시지를 받을 서버의 IP 주소, 인증 메시지가 재사용되는 것을 방지하기 위한 난수 R_C, R_S가 연접된 후 해시 연산이 수행된다. 그리고 $H(P_C)$에 대해 배타적 논리합을 수행하여 최종적으로 M_C가 생성된다.
- 6단계: 5단계에서 생성된 M_C가 서버에게 전송된다.
- 7단계: 서버는 자신이 저장하고 있는 클라이언트의 패스워드 해시 값 $H(P_S)$, 자신의 IP주소, R_S, 클라이언트로부터 수신한 난수 R_C의 연접 결과에 해시 연산을 수행한다. 그리고 $H(P_S)$에 대해 배타적 논리합을 수행한 후 이 값을 클라이언트로부터 받은 인증 메시지 M_C의 값과 비교하여 만일 그 값이 같으면 합법적인 클라이언트임을 인증한다.

1단계부터 7단계까지의 상호 인증 절차에 성공한 이후에는 서버와 클라이언트 사이의 데이터 암호화에 사용될 세션키가 공유되었으므로 안전한 데이터 교환이 가능해진다.

4. 안전성 평가

4.1 도청 공격

사용자가 입력한 원본 패스워드 및 패스워드 해시 값이 네트워크를 통해 그대로 서버에 전달될 경우, 해커는 도청 공격을 통해 패스워드나 그에 대한 해시 값을 획득하여 불법적인 로그인이 가능해진다. 제안 프로토콜에서는 인증 과정에서 원본 패스워드와 패스워드 해시 값이 직접 전달되지 않는다.

해커가 도청 공격을 통해 메시지 M_{R1}, M_{R2}, M_S, M_K, M_C를 수집했다고 하자. 해커가 M_{R1}로부터 패스워드 해시 값을 추출하기 위해서는 난수 R_C를 알아야 한다. 하지만 난수 R_C는 클라이언트만이 알고 있으며, 클라이언트 패스워드를 알고 있는 서버만이 M_{R1}로부터 난수 R_C를 추출할 수 있다. 그리고 M_{R2}로부터 패스워드 해시 값을 추출하기 위해서는 난수 R_C와 R_S를 알아야 한다. 하지만 R_C와 R_S는 서버만 알고 있으며, 패스워드를 알고 있는 클라이언트만이 M_{R2}로부터 R_S를 추출하여 패스워드를 추출할 수 있다.그리고 M_S, M_C에는 패스워드 해시 값이 다른 정보들과 연접된 후, 해시 연산이 수행되어 저장된다. 해시 함수는 역함수가 존재하지 않는 단방향 함수이기 때문에 해커가 네트워크상에서 도청하더라도 해시 값으로부터 원본 값을 추출할 수 없다. 마지막으로 M_K로부터 패스워드를 추출하기 위해서는 세션키와 두 난수들을 알아야 하지만 세션키 및 난수는 클라이언트와 서버를 제외한 제 3자는 알 수 없으므로 패스워드 추출이 불가능하다. 따라서 제안 프로토콜은 도청 공격에 안전하다.

4.2 메시지 수정 공격

해커는 불법적인 로그인을 수행하기 위해 클라이언트와 서버 사이에서 송수신되는 인증 메시지를 변조한다. 제안된 인증 프로토콜은 클라이언트와 서버사이에 전송되는 모든 인증 메시지를 단방향 해시 함수와 배타적 논리합 연산을 통해 생성한다. 따라서 해커는 인증 메시지에 포함되어 있는 원문 정보를 읽고 분석하는 것이 불가능하며, 수정을 통해 인증에 성공하기 위한 타당한 인증 메시지를 재생성하는 것이 불가능하다. 그러므로 제안 프로토콜은 메시지 수정 공격에 안전하다.

4.3 메시지 재생 공격

메시지 재생 공격은 해커가 클라이언트와 서버 사이에서 송수신되는 인증 메시지를 도청을 통해 저장한 후, 마치 자신이 타당한 클라이언트 및 서버인 것처럼 가장하고 재전송하는 공격이다. 재생 공격은 클라이언트와 서버가 인증 시에 항상 동일한 메시지를 전송할 때 발생하는 공격으로, 제안 프로토콜에서는 인증 메시지를 생성할 때마다 매번 난수를 생성한 후 이를 포함하기 때문에 인증 메시지의 재사용이 불가능하다.

해커가 도청으로 클라이언트 및 서버 인증 4단계에서 M_{R2}, M_S, M_K 메시지를 획득했다고 가정하자. 이후 클라이언트가 새로운 인증을 요청할 때 해커는 서버를 가장하여 클라이언트에게 미리 획득한 3개의 메시지를 전송한다. 클라이언트는 항상 난수 R_C를 새로 생성하기 때문에 클라이언트가 계산하는 M_S 값은 해커가 전송한 M_S와 다르다. 따라서 인증 과정은 실패하게 된다. 만일 해커가 인증 6단계에서 M_C 메시지를 획득했다고 가정하자. 해커가 클라이언트를 가장하여 메시지 재생 공격에 성공하기 위해서는 M_C 메시지가 생성되었을 때 사용된 R_C와 R_S가 현재 인증과정에서 클라이언트 및 서버에 의해 생성되어야 한다. 하지만 두 난수 값이 이전 인증과정에서와 똑같을 가능성은 매우 낮다.

4.4 중간자 공격

중간자 공격은 해커가 클라이언트와 서버 사이에서 송수신되는 인증 메시지를 중간에서 릴레이하면서 메시지를 변조하여 서버에게는 클라이언트로 위장하고 클라이언트에게는 서버로 위장하는 공격이다. 제안 프로토콜은 인증 메시지 안에 이 메시지를 수신하게 되는 목적지 IP 주소, 패스워드 해시 값, 난수를 연접한 후 해시된 결과를 저장한다. 만일 해커가 중간자 공격을 수행하는 상황이라고 가정하면, 클라이언트는 자신의 IP 주소와 해커로부터 수신한 인증 메시지에 포함된 IP 주소의 동일성을 확인한다. 하지만 인증 메시지에 포함된 IP 주소는 서버가 생성한 인증 메시지를 받아야 할 대상의 IP 주소이며, 이 주소는 중간자 공격에 의해 해커의 IP 주소로 설정되기 때문에 클라이언트 IP 주소와는 서로 다르다. 따라서 클라이언트는 수신된 인증 메시지가 타당하지 않음을 확인하고 인증 과정을 종료한다.

4.5 피싱 공격

피싱 공격에서는 해커가 위조 사이트를 구축하고 임의의 클라이언트에게 대량의 거짓 이메일을 전송한다. 이메일을 수취한 클라이언트가 이메일에 포함된 피싱 유도 링크를 통해 로그인을 시도할 경우 위조 사이트로 연결이 되며, 클라이언트가 입력한 패스워드가 해커에게 그대로 노출된다. 제안된 프로토콜에서는 클라이언트가 ID와 M_{R1}을 전송하며 서버가 인증 메시지를 보냄으로써 서버 인증이 먼저 수행되어야 한다. 하지만 피싱 공격이 수행될 경우 피싱 사이트는 클라이언트의 패스워드를 알지 못하기 때문에 인증 메시지 M_S 생성이 불가능하다. 그러므로 피싱 사이트는 서버 인증에 실패하며 인증 과정은 종료된다.

4.6 파밍 공격

해커는 파밍 공격을 수행하기 위해 DNS 서버를 해킹하여 특정 도메인과 관련된 IP 주소를 변조하기도 한다. DNS 서버가 변조되면 사용자가 웹 브라우저에 올바른 도메인 이름을 입력하더라도 해커가 구축한 피싱 서버로 접속된다. 제안 프로토콜은 이러한 파밍 공격에 안전하다. 합법적인 서버의 도메인 이름을 입력하였지만 파밍 공격에 의해 가짜 서버에 접속하더라도 제안 프로토콜은 처음에 클라이언트가 ID와 M_{R1}을 전송하며 서버가 인증 메시지를 보냄으로써 서버 인증이 먼저 수행되어야 한다. 하지만 파밍 공격이 수행될 경우 가짜 서버는 클라이언트의 패스워드를 알지 못하기 때문에 인증 메시지 생성이 불가능하다. 또한, 가짜 서버가 클라이언트와 실제 서버 사이에서 인증 과정을 중계한다하더라도 제안 프로토콜은 4.4에서도 알 수 있듯이 중간자 공격에 안전하기 때문에 파밍 공격에 안전하다 할 수 있다.

4.7 기존 안티 피싱과 제안 프로토콜 비교

Table 2는 기존 안티피싱 연구들의 단점들을 요약한 것이다. 블랙리스트를 기반으로 피싱에 대응하는 방법들은 신속한 블랙리스트 업데이트가 중요하지만 새로 구축된 피싱 서버를 즉각적으로 발견하여 블랙리스트를 업데이트하는 것은 거의 불가능하다. 블랙리스트를 사용하지 않는 안티피싱 방법들은 포털 사이트 혹은 메신저 계정 가입들을 요구하거나 스마트 디바이스를 구비해야만 하며, 경우에 따라 인증에 필요한 공개키/비밀키 발급 및 관리가 요구된다. 반면, 제안 프로토콜은 사용자가 직접 별도의 공개키/비밀키를 발급받아 관리할 필요가 없으며, 해커의 다양한 공격에도 안전하다.

Table 2. Summary of Previous Countermeasures

Anti-phishing	Drawback
Anti-phishing with web browser extensions or toolbars[6-8]	Cannot detect new phishing sites that are not blacklisted
Blacklist generators[1-3]	Cannot detect phishing sites in real time
Method that uses the portal site[9]	Cannot detect phishing sites when using hyperlinked services
Methods that use QR code[9-13]	Method not available for smart devices without camera
Password-based authentication protocol[15]	Vulnerable to replay attacks
One time password that uses messenger[17]	Does not operate without using messenger
Authentication protocols that use cryptographic keys[18-21]	Need public and private keys

5. 결 론

본 논문에서는 피싱 공격에 안전한 패스워드 기반의 상호 인증 프로토콜을 제안하였으며, 다양한 해커의 공격에도 안전함을 증명하였다. 기존의 인증 프로토콜과는 달리 인증 과정에서 별도의 스마트 디바이스나 자신의 계정 및 공개키/비밀키 발급을 요구하지 않기 때문에 사용자들은 용이하게 서비스를 이용할 수 있다. 특히, 인증 과정에서 소수의 연접과 해시, 배타적 논리합 연산만을 수행하며 암호키 연산이 없기 때문에 모바일 환경에서의 인증에 효과적으로 사용될 수 있다.

References

[1] M. Sharifi and S. H. Siadati, "A phishing sites blacklist generator," *in Proceedings of the 6th ACS/IEEE International Conference on Computer Systems and Applications*, pp.840-843, 2008.

[2] Y. Zhang, J. Hong, and L. Cranor, "CANTINA: A content-based approach to detecting phishing web sites," *in Proceedings of the 16th International Conference on World Wide Web*, Banff, pp.8-12, 2007.

[3] J. H. Sa and S. J. Lee, "Real-time phishing site detection method," *Journal of the KIISC*, Vol.22, No.4, pp.819-825, 2012.

[4] OpenSSL, SSL/TLS MITM vulnerability (CVE-2014-0224) [Internet], https://www.openssl.org/news/secadv/20140605.txt.

[5] T. Li and Y. Wu, "Trust on web browser: attack vs. defense," *in Proceedings of the International Conference on Applied Cryptography and Network Security*, pp.241-253, 2003.

[6] NETCRAFT, Netcraft Extension [Internet], http://toolbar.netcraft.com.

[7] PhishTank, Join the fight against phishing [Internet], http://www.phishtank.com.

[8] Mozilla, FirePhish Anti-Phishing Extension [Internet], https://addons.mozilla.org/en-US/firefox/addon/firephish-anti-phishing-extens.

[9] S. Kim, J. Kang, and Y. Kim, "Countermeasures against phishing/pharming via portal site for general users," *The Journal of KICS*, Vol.40, No.6, pp.1107-1113, 2015.

[10] Y. S. Lee, N. H. Kim, H. T. Lim, H. K. Jo, and H. J. Lee, "Online banking authentication system using mobile-OTP with QR-code," *in Proceedings of 5th International Conference on Computer Sciences and Convergence Information Technology*, pp.644-648, 2010.

[11] A. Gandhi, B. Salunke, S. Ithape, V. Gawade, and S. Chaudhari, "Advanced online banking authentication system using one time passwords embedded in Q-R code," *International Journal of Computer Science and Information Technologies*, Vol.5, No.2, pp.1327-1329, 2014.

[12] 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," *The Journal of KICS*, Vol.37C, No.10, pp.949-964, 2012.

[13] S. Seo, C. Choi, G. Lee, and H. Choi, "QR code based mobile dual transmission OTP system," *The Journal of KICS*, Vol.38B, No.5, pp.377-384, 2013.

[14] J. Park, J. Kim, M. Shin, and N. Kang, "QR-code based mutual authenctication system for web service," *The Journal of KICS*, Vol.39B, No.4, pp.207-215, 2014.

[15] M. Sandirigama, A. Shimizu, and M. T. Noda, "Simple and secure password authentication protocol(SAS)," *IEICE Transactions on Communications*, Vol.E83-B, pp.1363-1365, 2000.

[16] C. L. Lin, H. M. Sun, and T. Hwang, "Attacks and solutions on strong-password authentication," *IEICE Transactions on Communications*, Vol.E84-B, pp.2622-2627, 2001.

[17] C. Y. Huang, S. P. Ma, and K. T. Chen, "Using one-time passwords to prevent password phishing attacks," *Journal of Network and Computer Application*, Vol.34, pp.1292-1301, 2011.

[18] W. C. Kuo and Y. C. Lee, "Attack and improvement on the one-time password authentication protocol against theft attacks," *in Proceedings of the 6th International Conference on Machine Learning and Cybernetics*, pp.1918-1922, 2007.

[19] M. Kim, B. Lee, S. Kim, and D. Won, "Weaknesses and improvements of a one-time password authentication scheme," *International Journal of Future Generation Communication and Networking*, Vol.2, pp.29-38, 2009.

[20] M. Sharifi, A. Saberi, M. Vahidi, and M. Zorufi, "A zero knowledge password proof mutual authentication technique against real-time phishing attacks," *in Proceedings of the 3rd International Conference on Information Systems Security*, pp.254-258, 2007.

[21] M. Saeed and H. S. Shahhoseini, "APPMA: An anti-phishing protocol with mutual authentication," *in Proceedings of the 15th IEEE Symposium on Computers and Communications*, pp.308-313, 2010.

김 익 수

http://orcid.org/0000-0002-4572-5000

e-mail : iksuplorer@ssu.ac.kr

2000년 숭실대학교 컴퓨터학부(학사)

2002년 숭실대학교 컴퓨터학과(석사)

2008년 숭실대학교 컴퓨터학과(박사)

2009년~현 재 숭실대학교 컴퓨터학부 교수

관심분야 : 시스템 보안, 네트워크 보안, 인증 프로토콜

최 종 명

http://orcid.org/0000-0003-3595-1503
e-mail : jmchoi@mokpo.ac.kr
1992년 숭실대학교 컴퓨터학부(학사)
1996년 숭실대학교 컴퓨터학과(석사)
2003년 숭실대학교 컴퓨터학과(박사)
2004년~현 재 목포대학교 컴퓨터공학과 교수
관심분야 : HCI, 소셜 컴퓨팅, 상황인지 시스템, 인증 프로토콜