스마트폰 피싱에 안전한 메신저 인증 프로토콜 설계 및 구현

유병석, 윤성현*
백석대학교 정보통신학부

The Design and Implementation of Messenger Authentication Protocol to Prevent Smart Phone Phishing

Byung-Seok Yu, Sung-Hyun Yun*
Div. of Information & Communication Engineering, Baekseok University

요 약 피싱(Phishing)은 사용자 또는 기기를 가장하여 사용자 신분을 도용하는 공격이다. 최근 스마트폰 및 메신저 프로그램 보급에 따라 그 피해가 급증하고 있다. 스마트폰은 음성 통화, SMS와 같은 고유 기능 외에 무선 네트워크 기반의 다양한 응용 프로그램을 구동할 수 있다. 일반적으로 카카오톡, 네이트온과 같은 메신저 프로그램은 클라이언트-서버 구조로 구성되며 안전한 통신을 위해서 상호 인증이 필수적이다. 본 논문에서는 스마트폰 피싱 공격에 안전한 메신저 인증 프로토콜을 제안한다. 제안한 기법은 사용자들 간의 대화를 보호하기 위하여 메시지 암호화 기능과 인증 기능을 제공한다.

• **주제어** : 스마트폰, 보안, 피싱, 프록시 인증, 상호인증

Abstract Phishing is an attack to theft an user's identity by masquerading the user or the device. The number of phishing victims are sharply increased due to wide spread use of smart phones and messenger programs. Smart phones can operate various wi-fi based apps besides typical voice call and SMS functions. Generally, the messenger program such as Kakao Talk or Nate On is consisted of client and server functions. Thus, the authentication between the client and the server is essential to communicate securely. In this paper, we propose the messenger authentication protocol safe against smart phone phishing. To protect communications among clients, the proposed method provides message encryption and authentication functions.

• **Key Words** : Smart Phone, Security, Phishing, Proxy Authentication, Mutual Authentication

1. 서론

최근 모바일 운영체제 기반의 스마트폰이 보급되면서 기존에 PC에서 가능하던 소셜 네트워크 서비스가 모바일 환경에서도 가능하게 되었다. 스마트폰은 그 특성상 항상 휴대할 수 있기 때문에 활용성이 매우 높고 이에 기반을 둔 모바일 서비스가 사용 장소에 제한을 받는 PC 기반의 서비스보다 급속히 성장하고 있다 [1].

소셜 네트워크 서비스는 트위터, 페이스북, 카카오톡과 같이 사람과 사람 간의 정보 교환을 통하여 사회적 관

이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2011-0014589)
*교신저자 : 윤성현(shcrpt@gmail.com)
접수일 2011년 9월 28일 수정일 2011년 10월 20일 게재확정일 2011년 11월 25일

계를 형성 및 유지해 준다. 특히 스마트폰의 보급으로 Wi-Fi나 3G 네트워크를 이용하는 카카오톡과 같은 메신저 앱에 대한 수요가 급증하고 있다 [2].

메신저 앱은 스마트폰 사용자 간에 메시지를 주고받는 메신저 기능을 제공한다. 일반적으로 스마트폰을 기반으로 하는 모바일 메신저는 사용자간 통신 기능과 인증 기능으로 구성된다.

통신 기능은 네트워크를 이용하여 대화 메시지를 서로 주고받는 것을 의미한다. 스마트폰과 기지국(AP) 간은 무선 네트워크 구간이므로 전송 중인 메시지가 스니핑 될 위험이 유선 네트워크 구간보다 높다 [3]. 대화 내용의 기밀성 유지를 위하여 암호 기법의 적용이 필수적이다.

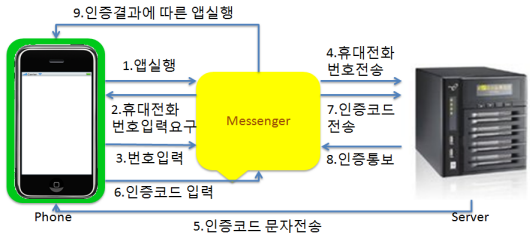
메신저 앱의 인증 기능은 일반적으로 사용자 전화로 전송되는 인증번호를 이용하여 기기 소유자 임을 확인하고 프로그램 사용 가능 여부를 확인하는 절차로 구성된다. 이 경우 SMS로 전송되는 인증번호를 이용하여 다른 기기에 설치된 메신저를 인증할 수 있다. 따라서, 스마트폰 피싱에 대응하기 위해서는 사용자 인증뿐만 아니라 스마트폰 기기에 대한 인증이 추가적으로 요구된다.

본 논문에서는 스마트폰 메신저 앱의 인증 절차를 분석하고 피싱에 안전한 인증 프로토콜을 제안한다. 2 장에서는 피싱 공격에 대한 기존의 메신저 인증 기법의 취약점을 분석한다. 3 장에서는 피싱에 안전한 스마트폰 기기 인증 프로토콜을 제안한다. 4 장에서 BU 메신저의 기능 및 구현 결과를 설명하고 5장에서 결론 및 향후 연구 과제를 제시한다.

2. 피싱 취약점 분석

피싱은 사회 공학적 공격으로 분류되며 가장 공격(Masquerade Attack)의 한 종류이다. 신뢰할 수 있는 대상으로 위장하여 사용자 신분 도용, 인터넷을 이용한 사기 등의 피해를 유발한다. 주요 기관을 가장하기 위해서 일반적으로 유사 URL 또는 이메일을 이용한다 [4]. 사용자 가장은 카카오 톡, 네이트온과 같은 대화형 프로그램에서 지인으로 가장하여 로그인 하는 것을 의미한다.

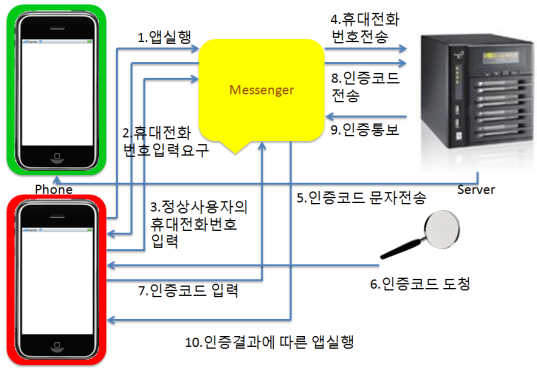
스마트폰은 컴퓨터 기능과 전화기 기능이 융합된 장비이다. PC용 대화형 프로그램인 메신저가 제공하는 다양한 메시지 기반의 대화가 스마트폰 에서도 가능하다. 스마트폰 용 메신저는 앱스토어, 안드로이드 마켓 등에 등록되어 무료로 배포되고 있으며 사용자 수가 급격히 증가하고 있다. 국내 모바일 메신저는 중복 사용 포함하여 2,200만 명 이상이 사용하고 있는 것으로 보고되고 있다 [5].



[Fig. 1] smartphone messenger certification process

스마트폰 메신저를 사용하기 위해서는 일반적으로 그림 1과 같은 인증 절차를 따른다. 사용자가 메신저를 실행하면 서버로 보낼 사용자 전화 번호를 입력 또는 확인하도록 한다. 메신저는 입력된 전화번호를 서버로 전송한다. 서버는 인증코드를 생성하고 사용자 스마트폰에 SMS(문자 메시지)로 이 코드를 전송한다. 사용자는 수신한 인증코드를 메신저에 입력하고 이를 서버로 전송한다. 사용자가 보낸 인증코드가 적합하면 올바른 사용자 및 기기로 서버에 등록하고 인증통보 메시지를 사용자에게 보낸다. 인증코드가 적합하지 않으면 메신저 등록을 취소한다.

그림 1과 같이 기존의 메신저 인증 프로토콜에서는 서버가 사용자 스마트폰으로 인증코드를 보내고 사용자는 수신한 코드를 직접 입력하여 서버로 보낸다. 서버는 인증코드를 확인함으로써 메신저가 설치되어 있는 스마트폰을 인증한다. 단점은 그림 2와 같이 사용자 본인의 스마트폰이 아닌 다른 기기를 이용한 메신저 대리 등록이 가능하다는 것이다.



[Fig. 2] Proxy Registration for mobile devices

그림 2는 사용자 본인의 스마트폰이 아닌 다른 모바일 기기에 메신저를 대리 등록하는 절차를 보여준다. 그림 2의 하단은 공격자의 스마트폰을 상단은 도용하려는 스마트폰을 보여준다. 공격자는 본인의 스마트폰에 설치한 메신저를 실행하고 도용하려고 하는 사용자의 전화번호를 입력한다. 공격자의 메신저는 입력된 전화번호를 서버로 전송한다. 서버는 인증 코드를 생성하고 이를 문자 메시지에 담아 공격자가 보낸 전화번호로 보낸다. 공격자는 서버가 보낸 인증코드를 도청하여 본인의 스마트폰에 있는 메신저에 입력하고 이를 다시 서버로 전송한다. 서버는 공격자가 보낸 인증코드가 적합하면 올바른 사용자 및 기기로 등록하고 인증통보 메시지를 공격자에게 보낸다.

3. 메신저 인증 프로토콜

스마트폰 피싱은 다른 모바일 기기를 마치 사용자의 스마트폰인 것처럼 위장하여 메신저 프로그램을 인증 받는 것을 의미한다. 인증코드 기반의 기존의 인증 기법에서는 공격자가 다른 사용자의 스마트폰으로 전송된 인증코드를 도청하여 본인의 기기에 설치되어 있는 메신저를 인증할 수 있다. 인증코드 기반의 사용자 및 기기 인증은 모바일 기기의 대리 등록이 가능하며 피싱에 이용될 가능성이 높다. 따라서 안전한 모바일 메신저를 설계하기 위해서는 사용자 인증과 더불어 스마트폰 자체에 대한 인증도 고려해야 한다.

본 논문에서 제안한 메신저 인증 기법은 스마트폰 인증 프로토콜과 메시지 보안 프로토콜로 구성된다.

3.1 스마트폰 인증 프로토콜

스마트폰 인증 프로토콜은 메신저가 설치된 사용자 스마트폰을 인증하여 메신저 프로그램의 사용 여부를 결정하는데 사용된다. 스마트폰 인증은 장치 인증서의 서명을 검증함으로써 이루어진다. 또한, 제 3자 공격에 대처하기 위하여 스마트폰과 메신저 서버 간의 상호 증명이 요구된다.

(가정 1) 스마트폰 제조업체는 기기마다 공개키와 개인키를 생성하고 인증기관은 스마트폰의 공개키를 서명하여 장치 인증서를 발급한다.

인증기관, 스마트폰, 서버의 공개키 및 개인키는 다음과 같이 정의한다.

종류	공개키	개인키
인증기관 CA	PK-CA	SK-CA
스마트폰 P	PK-P	SK-P
서버 S	PK-S	SK-S

사용자 스마트폰과 메신저 서버 간의 장치 인증 단계는 다음과 같다.

단계 1: 사용자는 난수 값 R, 기기 일련번호 SN를 스마트폰의 개인키로 서명하여 SIG_P를 만든다. 메신저 서버로 (R, SN, SIG_P, $CERT_P$)를 전송한다. $CERT_P$는 장치 인증서이고 EP는 공개키 암호 알고리즘이다.

$$SIG_p = EP_{SK-P}(R \parallel SN)$$
$$CERT_p = (PK-P, EP_{SK-CA}(PK-P))$$

단계 2: 서버는 인증기관의 공개키 PK-CA로 장치 인증서 $CERT_P$의 서명을 검증하고 사용자 스마트폰의 공개키 PK-P를 추출한다. DP는 공개키 복호 알고리즘이다.

$$PK-P = DP_{PK-CA}(EP_{SK-CA}(PK-P))$$

단계 3: 서버는 단계 1에서 보낸 난수 값 R과 기기 일련번호 SN으로 구성된 메시지의 서명을 다음과 같이 검증한다.

$$(R \parallel SN) = DP_{PK-P}(SIG_p)$$

올바른 서명이면 서버의 개인키 SK-CA로 SIG_P에 대한 서명 SIG_S를 다음과 같이 생성하여 서버 인증서 $CERT_S$와 함께 사용자 스마트폰으로 전송한다.

$$SIG_s = EP_{SK-S}(SIG_p)$$
$$CERT_s = (PK-S, EP_{SK-CA}(PK-S))$$

단계 4: 사용자는 서버 인증서 $CERT_s$를 검증하고 서버의 공개키 PK-S로 수신한 메시지 SIG_s를 다음과 같이 검증한다.

$$PK-S = DP_{PK-CA}(EP_{SK-CA}(PK-S))$$
$$(R \parallel SN) = DP_{PK-P}(DP_{PK-S}(SIG_s))$$

사용자 스마트폰과 메신저 서버 간에 장치 인증서를 이용한 PKI 기반의 상호 인증을 함으로써 스마트폰 대리

등록의 피해를 최소화 할 수 있다. 또한 인증 단계에 사용자 난수 값을 입력하여 제 3자에 의한 재전송 공격을 방지할 수 있다.

3.2 메시지 보안 프로토콜

메시지 보안은 키 교환 기능과 암호화 기능으로 구성되며 제 3자에게 사용자들 간의 대화 내용이 노출되지 않도록 한다.

1) 세션키 공유

서버는 메시지 암호화에 사용될 세션키를 생성하여 대화에 참여하는 사용자 그룹에게 분배한다. 스마트폰 사용자 A, B와 서버의 공개키, 개인키는 다음과 같이 정의한다. 사용자 A, B는 대화에 참여하는 사용자 그룹에 속해 있다고 가정한다.

종류	공개키	개인키
사용자 A	PK-A	SK-A
사용자 B	PK-B	SK-B
서버	PK-S	SK-S

단계 1: 서버는 사용자 그룹의 구성원들 간의 대화를 암호화하는데 사용될 세션키 K-G를 생성한다. (K-G || R-G)를 서버의 개인키 SK-S로 서명하고 사용자 A와 B의 공개키로 각각 다음과 같이 암호화 한다. R-G는 서버가 생성한 난수 값이다.

$$SIG\text{-}KEYS = EP_{SK\text{-}S}(K\text{-}G \parallel R\text{-}G)$$
$$PKG\text{-}KEYA = EP_{PK\text{-}A}(SIG\text{-}KEYS)$$
$$PKG\text{-}KEYB = EP_{PK\text{-}B}(SIG\text{-}KEYS)$$

서버는 PKG-KEYA를 사용자 A에게 PKG-KEYB를 사용자 B에게 전송한다.

단계 2: 사용자 A와 B는 각각 수신한 PKG-KEYA와 PKG-KEYB를 다음과 같이 복호화 한다.

$$SIG\text{-}KEYS = EP_{SK\text{-}A}(PKG\text{-}KEYA)$$
$$SIG\text{-}KEYS = EP_{SK\text{-}B}(PKG\text{-}KEYB)$$

사용자 A와 B는 서버의 공개키 PK-S로 서버의 서명 SIG-KEYS를 검증하고 대칭키 K-G와 난수 값 R-G를 다음과 같이 추출한다.

$$(K\text{-}G \parallel R\text{-}G) = DP_{PK\text{-}S}(SIG\text{-}KEYS)$$

단계 3: 사용자 A와 B는 각각 난수 값 R-G를 해쉬하여 서명하고 이를 K-G로 암호화하여 서버로 전송한다. ES는 대칭키 암호 알고리즘이고 H는 해쉬 함수이다.

$$ES_{K\text{-}G}(SIGA),\ SIGA = EP_{SK\text{-}A}(H(R\text{-}G))$$
$$ES_{K\text{-}G}(SIGB),\ SIGB = EP_{SK\text{-}B}(H(R\text{-}G))$$

단계 4: 서버는 세션키 K-G로 사용자 A와 B가 보낸 메시지를 복호한다. 사용자 A와 B의 공개키로 서명을 검증하고 H(R-G)를 추출한다. 이 값과 R-G를 직접 해쉬한 값이 일치하는 지 확인한다. 일치하면 사용자 A와 B가 K-G를 공유하고 있음을 확인한다.

2) 메시지 암호화 및 복호화

메시지 암호화 및 복호화는 다음과 같은 절차로 수행된다.

단계 1 : 사용자 A는 세션키 K-G로 메시지를 암호화하여 서버로 전송한다.

단계 2 : 서버는 세션키 K-G를 공유하고 있는 사용자들에게 사용자 A의 메시지를 동보 전송한다.

단계 3 : A의 메시지를 수신한 사용자들은 세션키 K-G를 이용하여 암호화 된 메시지를 복호화한다.

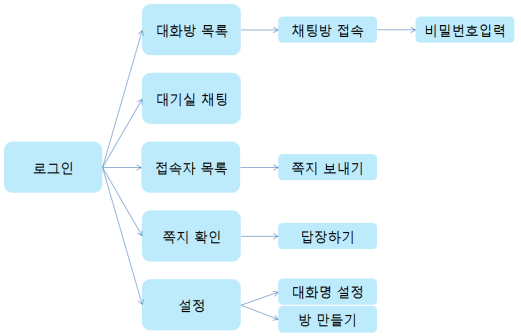
4. 구현 결과

본 논문에서 구현한 메신저 프로그램의 개발 환경, 구성 및 구현 결과에 대해서 기술한다.

4.1 개발 환경 및 메뉴 구성

BU-메신저는 클라이언트 앱과 메신저 서버로 구성된다. 클라이언트 앱은 iOS 4.3 기반의 아이폰용 앱으로 Xcode 통합 개발 툴을 이용하여 Objective-C로 구현하였고 메신저 서버는 Apache Tomcat Server를 이용하였다. 서버는 메신저간의 메시지 전송, 사용자 등록 및 대화방 관리 기능으로 구성되며 키 생성, 메시지 암호화 및 인증서 모듈은 OpenSSL 라이브러리를 이용하여 구현하였다.

4.2 구현 결과



[Fig. 3] The menu structure

BU 메신저는 그림 3과 같이 대화방 목록, 채팅, 접속 목록, 쪽지 보내기, 설정 메뉴로 구성된다. 대화방 메뉴는 사용자가 참여할 수 있는 대화 그룹을 보여주고 원하는 그룹을 선택할 수 있다. 채팅은 그룹의 구성원들과 메시지를 주고받는 대화 창, 접속 목록 메뉴는 현재 메신저 서버에 접속되어 있는 접속자 리스트를 보여준다.

[Fig. 4] User and device authentication screen

그림 4는 메신저 앱이 처음 구동되었을 때 실행되는 사용자 및 기기 인증 화면을 보여준다.

메신저 앱을 처음 실행하게 되면 사용자의 동의를 통해 휴대전화번호, IMEI(International Mobile Equipment Identity: 휴대폰 식별을 위한 시리얼 번호), 장치 인증서를 전송한다. 서버는 전송받은 IMEI와 휴대전화번호를 확인하고 장치 인증서를 발급한 인증기관의 서명을 검증한다. 장치 인증서가 유효하지 않거나 서버에 기록된 IMEI가 일치하지 않는 경우에 메신저 등록을 거부한다.

[Fig. 5] the chat screen

그림 5는 사용자 및 기기 인증을 완료한 사용자 간에 메시지를 주고받는 채팅 화면을 보여준다.

메신저 앱과 서버 간에 주고받는 메시지는 3.2 절의 메시지 보안 프로토콜을 이용하여 보호된다. 메시지 암호화를 위해서 3-DES 알고리즘을 키 교환 및 인증서 모듈 구현을 위하여 RSA 알고리즘을 사용하였다.

5. 결론

본 논문에서는 스마트폰 피싱의 위험에 대해서 분석하고 피싱에 안전한 모바일 메신저를 설계 및 구현하였다.

스마트폰 피싱은 다른 모바일 기기를 마치 사용자의 스마트폰인 것처럼 위장하여 메신저 프로그램을 인증 받는 것으로 기존의 인증코드 기반의 사용자 및 기기 인증은 모바일 기기의 대리 등록이 가능하며 피싱에 이용될 가능성이 높다.

제안한 메신저 인증 기법은 스마트폰 인증과 메시지 보안 프로토콜로 구성된다. 장치 인증서를 이용하여 스마트폰을 인증함으로써 스마트폰 피싱 위협을 최소화 하였으며, 사용자들 간의 대화 내용이 제 3자에게 노출되지 않도록 키 공유 및 메시지 암호화 기법을 설계 및 구현하였다.

REFERENCES

[1] Roy Want, “iPhone: Smarter Than the Average Phone”, Pervasive Computing, IEEE, Volume: 9, Issue: 3, pp. 6-9. 2010.

[2] http://www.kbench.com/digital/?no=105468&sc=1

[3] Welch, D., Lathrop, S., “Wireless security threat taxonomy”, Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society, pp. 76-83, 2003.

[4] Eung Yong Lee, Yun Jeong Kim, Gyumin Cho, "Phishing threats and for Response measures", Information and Communication Industry Development, [IITA] Information and Communications Technology Academic Information Agency, Technical Trends in week No. 1237, 2006.

[5] http://www.ytn.co.kr/_ln/0102_201106050946592111

[6] Yang Seo Choi, Dongil Seo, "personal information through social engineering attacks Flux Beam Technology and Countermeasures Analysis ", Institute of Information Security, Vol. 16, No. 1, 2006.

[7] Joo-Hyun Kim, Youngjae Mang, Kyunghee Lee, etc., "Anti-Phishing and Pharming For cogni-tive-based approach", Information Security and Cryptology papers, Vol. 19, No. 1, 2009.

[8] In Tae Kim Jun Young Jang, Ju Hyeong Lee, Sung Woon Hwang, "Cancer for anti-phishing Implementation of the algorithm and Messenger", Security Engineering Research Institute, Vol. 6, Issue 5, 2009.

저자소개

유 병 석(Byung-Seok Yu) **[학생회원]**

- 2007 3월 ~ 현재 : 백석대학교 정보통신학부 재학중

<관심분야> : 정보보호, 정보통신, 모바일 보안

윤 성 현(Sung-Hyun Yun) **[종신회원]**

- 1992년 2월 : 고려대학교 컴퓨터학과 (이학학사)
- 1994년 2월 : 고려대학교 컴퓨터학과 일반대학원 (이학석사)
- 1997년 2월 : 고려대학교 컴퓨터학과 일반대학원 (이학박사)
- 1998년 3월 ~ 2002년 2월 : LG 전자 중앙연구소 선임연구원
- 2002년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수

<관심분야> : 모바일 상거래 보안, DRM, 프라이버시 보호, 정보통신