Journal of The Korea Society of Computer and Information
Vol. 21 No. 8, pp. 29-39, August 2016

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2016.21.8.029

Evaluation of Safeness and Functionality in Applied Technologies for Mobile Messengers

Gyu-Sang Cho*

Abstract

Recently, KakaoTalk users seek secure messengers with fears of 'possible' censorship over a mobile messenger. Instead German messenger "Telegram" is gaining popularity in South Korea. Are the known as secure messengers actually secure? In this paper, we evaluate secure mobile messengers in terms of private information protection. We establish the fourteen criteria to evaluate the functionality of messenger apps including communication encryption in transit, the possibility of leakage of decrypted messages via server, an encryption algorithm, a key exchange algorithm, an ephemeral message application, etc. Line, Telegram, Snapchat, WhatsApp, Wickr, Facebook Messenger and KakaoTalk, which have many worldwide and domestic users, are to be targeted. Wickr is ranked at the top of the evaluation, followed by Telegram and Line but KakaoTalk and Snapchat are ranked at the bottom of the evaluation list.

▸ Keyword : End-to-End Encryption, Mobile Messenger App, Wickr, Telegram, WhatsApp, Line, Facebook Messnger, KakaoTalk, Snapchat

I. Introduction

지난 2014년 9월 검찰은 '사이버 명예훼손 전담수사팀'을 신설하고 인터넷 공간의 '검열'을 공식화하였다. 사이버 명예훼손을 상시 단속하겠다는 방침을 밝혔을 때와 테러방지법이 국회를 통과했을 때 KakaoTalk 사용자들이 대거 Telegram으로 옮겨갔고 이런 현상을 '사이버 망명'이라고 불렀다. Telegram은 모든 대화를 암호화해 전송하므로 제삼자가 들여다 볼 수 없는 보안성을 갖고 있다고 알려졌기 때문이었다[40].

미국 연방수사국(FBI)은 2015년 12월 캘리포니아 주 샌버너디노 총기 난사사건의 정확한 범행 동기와 공범 여부 등을 조사하기 위해 그의 아이폰을 들여다보는데 실패하자 애플에 협조요청을 했지만 애플이 거절하였다. 공공 안보와 사생활 보호 논란으로 번진 이들의 공방은 세계적인 주목을 받았지만 FBI가 애플의 도움 없이 용의자 아이폰의 잠금장치를 해제하면서 사건이 마무리 되었다. 포렌식 업체 '셀레브라이트'사의 도움을 받은 것으로 추정된다. FBI는 애플만이 아이폰 잠금장치를 해제할 수 있다고 주장해 왔으나 제삼자가 잠금장치를 해제하면서 애플의 보안에 대한 신뢰가 손상되었다[37].

2014년 유럽사법재판소가 이용자의 시효가 지난 채무 관련 기사에 대해 검색사업자의 검색목록 삭제 책임을 인정한 판결이 있은 후에 우리 사회도 잊힐 권리에 대한 관심이 급격히 늘고 있다. 방송통신위원회는 2016년 6월에 "인터넷 자기게시물 접근배제 요청권 가이드라인"을 발표하였다[1]. 자기게시물에 대한 관리권 상실로 인해 발생하는 피해를 줄이기 위해서 본인이 삭제하기 힘들어진 글을 삭제하거나 접근을 배제할 수 있도록 한 것이 핵심이다. 하지만 게시물 작성자가 본인이라는 점을 기술적으로 입증하기 어렵고 제삼자 작성 게시물은 제외되어 있다. 그리고 해외 사업자에게는 적용되지 않는 등의 문제로 인해서 실효성이 떨어진다는 견해가 많다[41].

트위터도 잊힐 권리를 수용하여 사용자의 리트윗을 일괄 삭제하는 기능을 새로이 적용하고 있다. 트위터는 리트윗(RT)라

• First Author: Gyu-Sang Cho, Corresponding Author: Gyu-Sang Cho
*Gyu-Sang Cho(cho@dyu.ac.kr), Dept. of Computer Information, Dongyang University
• Received: 2016. 08. 04, Revised: 2016. 08. 22, Accepted: 2016. 08. 31.

고 하는 기능을 사용하여 글과 사진 등의 게시물을 빠르게 전파할 수 있는 특징을 갖고 있다. 트위터의 원본 게시물이 삭제되면 리트윗된 모든 사본들이 일괄적으로 삭제되도록 기능을 적용한 것이다. 다만 게시물을 복사하여 붙여넣기를 이용한 경우는 이 기능이 적용되지 않는다. 이런 경우는 기술적인 지원은 불가능하고 정보통신망법에 의하여 저작권법 위반이나 명예훼손을 입증하여 블라인드 처리하는 방법을 적용해야 한다[4].

사진과 동영상에 메시지 자기파괴 기능을 구현한 모바일 메신저 Snapchat이 10대와 20대 사이에서 선풍적인 인기를 끌고 있다[17]. 공유한 사진이 몇 초 후에 사라진다는 장점이 부각되어 사용자들이 많아졌고 최근에는 페이스북과 구글에서 높은 금액의 인수제안을 받았다는 소식에 관심도가 더 높아졌다. 그러나 Snapchat의 자기파괴 기능으로 삭제된 줄 알고 있던 사진과 동영상들이 실제로는 지워지지 않은 채 유출되는 해킹사고가 발생한 사례가 있었다[12].

국내의 KakaoTalk 망명사태와 외국의 개인정보 침해사례 등이 계기가 되어서 모바일 메신저 활동을 하는 개인들의 정보가 적절하게 보호되는지 평가해 볼 필요가 있다. 이 연구에서는 그동안 안전하다고 알려진 유명 모바일 메신저들을 포함하여 전 세계적으로 사용자들이 많은 앱을 중심으로 실제로 얼마나 안전한지 그리고 개인정보보호를 위한 기능이 적정한 수준으로 반영되고 있는지 평가하기로 한다.

2장에서는 각 모바일 메신저 앱의 메시지의 안전성을 평가하기 위한 대상을 정하고 그 의미를 기술한다. 3장에서는 Line, Telegram, Snapchat, WhatsApp, Wickr, Facebook Messenger, KakaoTalk 등의 평가대상의 앱들의 기능과 암호화 기술들과 알려진 보안문제점에 대해서 논하기로 한다. 4장에서는 각 모바일 메신저에 대한 평가의 결과를 제시하고 5장에서 결론을 맺기로 한다.

II. Methodology

1. Evaluation Criteria

EFF(Electronic Frontier Foundation)는 “Secure Messaging Scorecard”라는 제목으로 메신저 소프트웨어들에 대해 다음의 7가지 평가항목에 대한 결과를 제시하였다[11].

평가 1: 데이터를 암호화하여 전송하는가?
평가 2: 암호화된 메시지를 중간에서 읽을 수 있는가?
평가 3: 사용자가 개별적으로 상대자의 식별이 가능한가?
평가 4: 키 유출시 지난 메시지가 안전하게 보호되나?
평가 5: 프로그램 코드는 제삼자에 의해 검토되었나?
평가 6: 암호화 설계에 대한 문서화를 잘 하였는가?
평가 7: 제품의 설계 및 구현에 대해서 최근 12개월 동안 독립적인 보안 감사를 수행해왔는가?

평가 1은 메시지를 암호화하였는가에 대한 평가이다.

평가 2는 종단간(End-to-End) 암호화 방식의 적용되는가를 평가하기 위한 것이다.

평가 3은 사용자를 다른 경로를 통해서 신원을 확인할 수 있는 대역 외 인증 지원 여부를 묻는 것이다.

평가 4는 완전 순방향 비밀성(Perfect Forward Secrecy)으로 일회성 소멸키가 적용되는가를 평가하기 위한 것이다.

평가 5는 소스코드를 공개한다는 의미보다는 적용된 알고리즘에 버그, 백도어, 구조적인 결점 등을 찾기 위함이다.

평가 6은 암호화와 인증단계에서 사용되는 알고리즘과 관련 파라미터들, 키 생성, 저장 및 교환 방법, 키 갱신과 변경과 키의 생명주기 등에 대한 문서화 여부를 묻는 것이다.

평가 7은 핵심 개발팀에 독립된 보안팀에 의해 공개적 또는 비공개적으로 제품 설계와 구현과정에 대한 감사를 의미한다.

EFF 공개한 평가 자료는 전통적인 PC용 메신저 프로그램과 모바일 스마트폰용의 메신저 등의 많은 제품에 대하여 평가하고 있다[11]. 2013년에 조사된 내용으로 부분적으로 수정이 반영되었지만 최근에 많이 개선된 모바일 메신저 앱에 대해서 적절히 반영하지 못하는 한계점을 보이고 있다. 그리고 관련 문헌을 제시하지 않은 채로 평가의 결과만 제시하고 있다는 점이 문제점으로 지적된다. 본 연구에서는 평가 항목에 대한 참고문헌을 통하여 출처와 근거를 최대한 반영한다. 그리고 아래의 보안성과 기능성의 평가기준을 추가적으로 반영한다.

평가 8: 메시지 암호를 위한 대칭키 암호 알고리즘은?
평가 9: 서버/P2P방식의 여부?
평가 10: 키 교환에 사용하는 알고리즘은?
평가 11: 화면캡처 방지 또는 알림 기능 있는가?
평가 12: 그룹 채팅에 암호화가 지원되는가?
평가 13: 메시지 자동소멸 기능이 있는가?
평가 14: 평가 대상의 최신 버전?

평가 8은 대칭키 암호 알고리즘의 종류와 비트수를 통해서 암호 수준을 평가한다.

평가 9는 메시지를 서버를 경유하는 방식을 사용하는지 P2P방식으로 클라이언트만 통신하는지를 평가한다.

평가 10은 키교환에 적용된 알고리즘을 평가한다.

평가 11은 화면 캡처를 통해서 상대방에 의한 메시지 유출을 방지하는 기능이 지원되는가를 평가한다.

평가 12: 그룹 채팅에 암호화를 지원하는가를 평가한다.

평가 13은 자동소멸(Self-Destructing)기능을 적용하여 잊힐 권리의 개념이 적용되어 보안성을 더 높이는지 평가한다.

평가 14: 평가 대상의 최신 버전이 지원된 시기를 나타낸다. 기술이 지원되기 시작한 시기를 알아보기 위함이다.

III. Features and Cryptography of the Mobile Messengers

1. Line

1.1 Line의 기능

Line은 최근 보안을 강화한 레터실링(Letter Sealing)이라는 모바일 메신저를 선보였다. 스마트폰과 PC에서 모두 종단간 암호화를 적용한 첫 번째 사례임을 강조하고 있다. 이 기술이 적용됨으로써 기존의 타이머챗(Timer Chat)뿐만 아니라 일반 채팅에도 종단간 암호화가 적용된다. 삭제한 대화 내역에 다른 데이터를 덮어 씌워 기존 데이터를 복구할 수 없도록 하는 True Delete 기능을 새롭게 제공하고 있다[19]. 개인정보보호를 위한 다양한 고도의 기능을 제공하고 있다[18].

1.2 Line의 암호화 기술

Line에서 기존에 사용하던 메시지 암호화 방법은 중간에서 매체를 도청하는 중간자 공격(MITM, Man In The Middle)공격에 의한 메시지 노출을 방지하고 SSL(Secure Socket Layer)보다 가볍고 안전한 채널을 만들기 위해 공개키 방식의 암호화를 적용하였다. 기존의 방식은 서버가 키를 소유하고 있고 메시지를 복호한 상태로 저장한다는 단점이 있어 해커에 공격당하면 메시지가 노출될 수 있다[19].

DH(Diffie-Hellman) 키교환 알고리즘은 제삼자가 중간에 존재하더라도 안전하게 메시지를 교환할 수 있는 방식이다. 기존의 RSA방법에 비하여 키 관리의 편리성이 있다. DH에 타원곡선 알고리즘이 적용된 최신의 방법을 사용한다. 이것은 RSA에 비하여 작은 크기를 사용하며 강한 암호 강도를 가진다. 메시지의 암호화에는 AES256-CBC 방식이 사용된다. 그림 1과 2에서 “Shared Secret”를 주고받으면서 안전하게 키를 공유하여 평문 메시지를 암호화하여 전송하게 되면 서버에 저장된 메시지는 암호화된 상태를 유지하기 때문에 안전한 메시지 송수신이 가능하다. 암호화된 내용에 대한 변조 방지를 위하여 HMAC방식의 메시지 인증코드(MAC, Message Authentication Code)를 사용한다[19].

1.3 Line의 알려진 보안문제

Letter Sealing이 적용되기 이전의 Line에서는 대화내용, 사진, 친구 목록 등의 개인정보가 유출될 가능성이 있다고 알려졌다[20]. 악성코드가 설치된 무선공유기를 사용하여 웹페이지에 접속할 때 라인의 사용자 이름을 선택하면 설치된 자바스크립트에 의해 각종 정보가 유출될 수 있는 취약점이 있다. 이것은 Line 앱을 실행시킬 때 설치된 자바 스크립트를 체크하는 기능을 수행하면 제거되는 취약점이다.

루팅된 Android 폰에서 DB Browser for SQLite라는 툴을 이용하여 ‘DB Name-journal’파일의 내용을 알 수 있다.

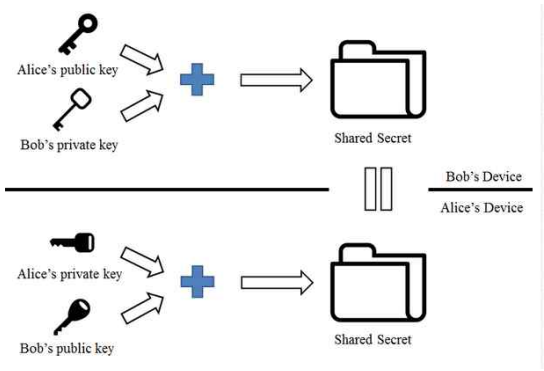

Fig. 1. DH Key Share Method[19]

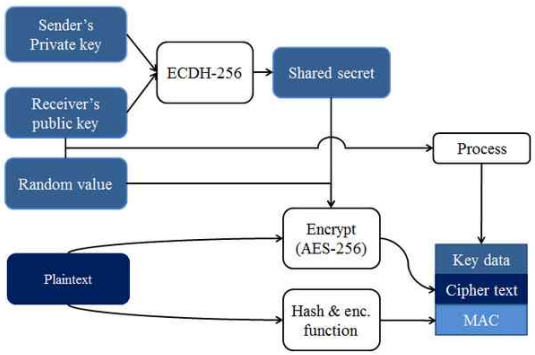

Fig. 2. Letter Sealing Encryption Procedure[19]

타이머 챗 메시지의 경우는 암호화되어 저장되어 있다가 읽기를 위해서 평문으로 복호하는 과정을 거치기 때문에 정보가 유출이 될 가능성이 있다[21]. 이것도 Letter Sealing이 도입되기 전에 존재하던 취약성이다.

Line에서는 보안문제를 공개적으로 대응하기 위하여 ‘LINE Security Bug Bounty Program’을 통해서 취약성 문제를 개선하고 있다[22]. “message/call eavesdropping”과 “SQL Injection” 등의 취약점을 개선한 사례처럼 화이트 해커들의 제보를 통해 LINE의 서비스를 보다 안전하게 제공하려고 노력하고 있다.

2. Telegram

2.1 Telegram의 기능

Telegram의 대화방식은 일반대화와 비밀대화 2가지 방식이 사용된다. 메시지는 클라우드 서버에 저장된다. 일반적인 메신저들이 서버에 메시지를 저장하는 방식과는 다른 것이다. 클라우드 서버 방식은 여러 장치에서 공유할 수 있다는 장점이 있다. 이런 메시지 전달 방식상의 문제로 인해서 Telegram도 메시지가 노출될 가능성이 존재한다. 클라우드 서버에 저장된 메시지를 조사하면 메시지의 내용이 공개될 수 있기 때문이다[6]. Telegram이 안전하다고 알려진 것은 비밀대화(Secret Chat) 기능이 지원되기 때문이다. 종단간 암호화를 방식을 사용하고 있어서 중간에 위치한 서버에서는 내용을 알 수 없고 키를 갖고 있는 두 단말에서만 암복호가 가능한 방식이다.

비밀대화에서는 일정시간이 지난 후에 자신이 보낸 메시지가 자동으로 삭제되는 기능이 사용된다. 설정된 시간 이전이라도 메시지를 지우는 것은 언제나 가능하다. 화면을 캡처하면 상대에게 알리는 기능도 갖추고 있다.

2.2 Telegram의 암호화 기술

Telegram에서는 두 가지 방식의 메시지 전송을 위한 프로토콜이 사용된다. MTProto, part I은 Cloud chats라 한다. 이것은 일반채팅 모드에서 서버와 클라이언트의 암호화를 위한 프로토콜이다. MTProto, part II는 Secret chats라 하고 '비밀채팅' 모드에서 종단간 암호화를 위한 프로토콜이다. MTProto, partII에서 Secret chats 키는 DH(Diffie-Hellman) 프로토콜을 사용하여 생성한다. 메시지의 내용과 정보가 담긴 페이로드를 SHA-1을 사용하여 msg_key를 생성한다. 데이터는 256비트의 키를 사용하고 IGE(Infinite Garble Extension)가 적용된 AES로 암호화된다.

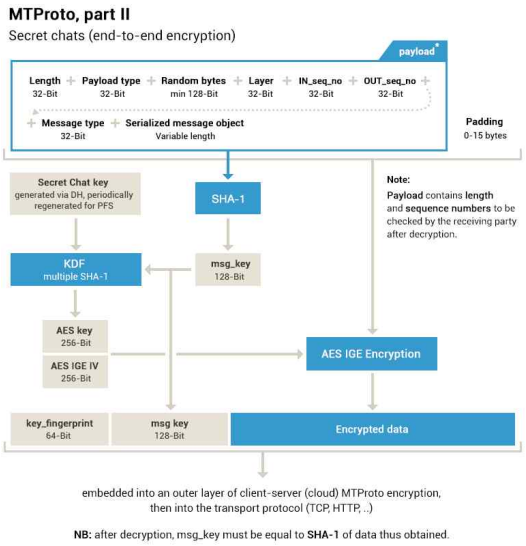

Fig. 3. Schematic diagram of 'Secret chat' [10]

완전 순방향 비밀성을 위해서 Telegram에서는 100개의 메시지를 송수신 한 후나 키를 사용한지 일주일 이상된 경우에 키를 다시 생성한다. 키가 해킹되어 동일 키가 적용된 모든 메시지가 복호되어 노출되는 것을 방지하기 위한 방법이다.

2.3 Telegram의 알려진 보안문제

Telegram은 보안성을 강조하고 있다. 2013년과 2014년에 각각 상금을 걸고 Secret Chat의 암호를 깨는 해킹대회를 열었다. 실제로 해킹에 성공한 사람은 없다고 밝혔다[8]. 그러나 2015년 7월10일~12일 사이에 전 세계적으로 DDoS 공격에 의하여 시스템이 마비된 사건이 발생하였다. 아시안 클러스터에서 공격이 있었다고 Telegram 관계자가 밝혔다[7]. 최근에 Hackers News[8]는 Telegram에는 비밀채팅 기능이 기본설정이 아니라서 사용자들이 선택의 실수를 할 우려가 있다는 점과 사용자 연락처가 서버 DB에 모두 기록하도록 하고 있다는 문제, 서버가 침해된다면 스마트폰의 메타데이터 정보가 유출될 염려가 있다는 문제 등을 제기하였지만 쉽게 일어날 문제는 아닌 것으로 판단된다고 보도하였다.

참고문헌[21]에서 루팅된 안드로이드 폰의 비밀 대화로 전송한 메시지는 cache4.db파일의 enc_chats 테이블에 사용자이름, 데이터, 인증키 등의 다양한 데이터가 들어 있고 data에는 대화내용이 암호화된 상태로 저장되어 있다고 밝혔고 messages 테이블에는 메시지가 평문으로 들어 있다는 분석결과를 내놓았다. 자동 삭제가 설정된 경우는 일정시간 이후에는 기록된 내용이 보이지 않는다고 밝혔다. 비밀 대화의 내용은 서버에서는 암호화된 상태로 저장되지만 클라이언트에서는 복호된 평문으로 기록된다는 것을 확인한 것이다.

Encrypting normal snaps

All standard media (read: picture and video) data sent to Snapchat is:
Padded using PKCS#5.
Encrypted using AES/ECB with a single synchronous key: M02cnQ51Ji97vwT4

Encrypting stories

Stories are:Padded using PKCS#7.
Encrypted using AES/CBC with a unique IV and key per piece of the story (i.e, there isn't a single key/IV you can use).
You can find a media_key and media_iv deep within the return values of a request to /bq/stories.
The server does the AES/CBC encryption - segments are sent to the server using the normal AES/ECB (M02c..) encryption.
StoryEncryptionAlgorithm#encrypt just calls SnapEncryptionAlgorithm#encrypt.

Here's a rough idea of how to decrypt them:

```
# To find `media_key` and `media_iv`, see: /bq/stories documentation
import requests
import base64
import mcrypt

res = requests.post(...)  # POST /bq/stories and ensure res is a dict.
data = requests.get(...)  # GET /bq/story_blob?story_id=XXXXX from result
key = base64.b64decode(res[...]["media_key"])
iv = base64.b64decode(res[...]["media_iv"])

m = mcrypt.MCRYPT("rijndael-128", "cbc")
m.init(key, iv)
dedata = m.decrypt(data)  # Boom.
```

Fig. 4.Procedure of Encryption of Snapchat[16]

3. Snapchat

3.1 Snapchat의 기능

Snapchat은 사진과 영상 메시지를 보내고 난 후 최대 10초 안에 사라진다는 독특한 기능을 선보여 미국의 10대와 20대에게 큰 인기를 얻고 있는 메신저 앱이다.

메시지를 읽거나 유효기간이 지나면 그 메시지는 자동적으로 삭제된다. Snaps는 모든 수신자가 메시지를 읽은 후에 삭제되고 읽지 않은 메시지는 서버에서 30일간 보관된다. Chats서비스는 대화 상대 양쪽이 모두 읽은 후에 서버에서 삭제되고 화면에서도 사라지게 된다. 그러나 어느 한 쪽에서 메시지를 저

장할 수 있는 기능이 있다. My Story는 게시된 후 24시간이 지나면 서버에서 삭제된다. Live Stories의 경우는 스냅을 Live Story나 Local Story로 보내면 이것을 관리하고 다시 볼 수 있는 기능이 있다. Memories는 Snaps와 Story를 Snapchat이 백업하고 관리하여 언제든지 다시 볼 수 있는 기능이다[17].

3.2 Snapchat의 암호화 기술

Snapchat은 공식적으로 기술적인 문서를 발표하지 않고 있다. 어떤 방식으로 메시지를 전송하고 암호화하는지 자세히 알려져 있지 않다. 현재까지 알려진 내용은 Snapchat의 보안 취약성을 밝히려고 시도한 많은 해커와 포렌식 분석가에 의한 것이다. 대표적인 작업으로 Gibsensec.org에서 Snapchat의 인증과 암호화 방법 등에 대한 분석한 내용을 공개하였다[16]. 스냅의 경우는 AES/ECB 방식의 암호알고리즘을 사용하고 PKCS#5을 이용하여 패딩하고 스토리는 AES/CBC 방식의 암호 알고리즘을 사용하고 PKCS#7을 이용하여 패딩한다. 종단간 방식이 적용되지 않고 있고 키 교환은 대칭키 방식을 이용하는 것으로 알려졌다(Fig. 4)[16].

3.3 Snapchat의 알려진 보안문제

이미지 공유 서비스를 시작하면서 보안이 뛰어나다는 것이 이 앱의 주요 특징이지만 취약점이 발견되어 460만 명의 정보가 노출된 사건이 있었다. 2013년 8월에 호주의 Gibson Security의 연구자들이 사용자 이름과 전화번호 조합을 조사하다 이 취약점을 발견한 것이다. 2013년 12월에 처음 공개되었을 때 Snapchat은 이 결점이 크게 문제되지 않는다고 밝혔지만 일주일 후에 사용자들의 정보가 유출되었다. 사용자가 동시에 수천 개의 레코드 찾기가 가능하게 되어 있고 리퀘스트에 제한 수준을 정하지 않아서 생긴 문제이다. 이 후 Snapchat은 이 문제에 대한 수정된 버전을 발표하였다[12].

2014년 10월에 또 다시 20만장 이상의 사진 유출사고가 발생하였다. 이것은 제삼자의 앱이 침해당한 사건이다. 메시지를 받은 사람이 보낸 사람 몰래 Snapchat 사진을 저장할 수 있도록 하는 Snapsave라고 하는 비인가된 제삼자 앱에서 유출된 것이라서 직접적으로 Snapchat의 잘못은 아니라고 해명하였다[13].

Deciper Forensics는 디바이스에 저장된 Snapchat의 메시지가 파일의 확장자의 변경만으로 내용을 복구할 수 있다는 사실을 밝혔다[15]. Galaxy S3에서 AccessData사의 Mobile Phone Examiner+ version 5.2.1.499를 사용하여 분석하였는데 수신된 이미지들은 원래의 이미지파일에 ".nomedia" 확장자를 붙여서 저장된다. 이 파일은 확장자를 변경하기만 하면 간단히 읽을 수 있다[15].

4. Wickr

4.1 Wickr의 기능

Wickr의 통신 기능은 1:1 대화 채널과 그룹 협력을 위한 안전한 대화방을 갖추고 있고 파일과 이미지를 송수신할 수 있다. 사용자가 설정한 메시지 파기를 위한 타이머 설정이 가능하다. 문맥 검색기능도 제공된다. 또한 Role-based Identity 관리, Time-to-Live Setting, Company-wide Security Setting 기능 등이 제공된다.

무엇보다도 Wickr는 안전한 모바일 메신저라는 것이 특징이다. 안전성을 위주로 개발되었으며 전송 및 안전 메시지, 문서, 이미지, 비디오 및 오디오 파일에 종단간 암호화 방식을 적용하여 주고받을 수 있는 기능을 갖고 있다. 모든 메시지에 군사용 등급에 해당하는 암호화를 적용하고 있다. 메시지 전송 시에 타이머를 설정하여 자기 파괴기능을 할 수 있도록 제작되었다. 사진, 오디오 및 콘텐츠는 디스크 장치에서 삭제되고, 메시지에서 모든 기록, 위치정보 및 ID 카드정보를 제거하여 메타데이터가 남지 않도록 하였다. 전화번호부를 안전하게 관리하기 위하여 Wickr의 서버에 저장하지 않는 방식을 사용하였다. 이런 모든 기능은 대화가 감시, 차단, 추적되지 않기 위함이다[42].

4.2 Wickr의 암호화 기술

Wickr은 AES256을 사용하여 데이터를 암호화한다. 송신자와 수신자 간에 MITM공격을 방지하기 위하여 대칭키를 안전하게 분산하는 방법을 사용한다. 복호 키를 배포할 때는 중앙화되지 않는 보안구조를 사용한다. 사용자이름, 앱 ID, 디바이스 ID 등이 SHA256으로 해쉬된다. 메시지가 복호되면 바로 새로운 암호키를 사용하여 완전 순방향 비밀성을 확보한다. ECDH(Elliptic-Curve Diffie-Hellman)암호를 사용하여 메시지 암호키를 생성한다. 메시지는 수신자의 앱과 디바이스에만 한정적으로 사용되고 패스워드나 패스워드 해쉬를 디바이스에 전혀 남기지 않는다. 그리고 모든 사용자 컨텐츠는 유효기간이 지나면 디바이스에서 포렌식적으로 완전하게 지워진다. 안전하게 보관을 위해 UDID(Unique Device Identifier)를 서버에 업로드하지 않는다. Secure Shredder는 완전하게 디바이스에서 모든 데이터를 지우기 때문에 복구가 불가능하다. 어떤 메타 데이터에도 사용자의 통신내용에 관련된 것을 흔적을 남기지 않는다[23].

4.3 Wickr의 알려진 취약성

Wickr은 안드로이드 스마트폰에 어떤 메시지와 관련된 데이터를 남기지 않아서 포렌식 분석이 불가능하다는 연구가 있었다[14]. 이것은 모바일 메신저가 개인정보보호를 위한 가장 좋은 사례의 한 형태일 것이다.

Wickr는 자신들의 코드, 보안, 정책에 대해서 검증을 수행하는 정보보안조직에 의해서 정기적인 감사를 수행해 오면서 투명성을 확보하려는 시도를 하였다. 또한 "Bug Bounty Program" 제도를 통해서 앱의 취약성을 찾은 화이트해커들에게 보상하는 제도를 운영하고 있다.

Asterisk Labs은 iPhone에 설치된 Wickr앱에서 두 가지 취약점이 존재한다는 사실을 밝혔다[25]. 하나는 사용자가 세션

'Auto Lock' 에 설정된 시간이 지난 이후에 백그라운드에 있다가 다시 포어그라운드로 앱이 동작되면 인증을 위한 패스워드 입력 단계가 바이패스 되는 취약점이다. 다른 하나는 사용자가 패스워드를 입력하여 인증절차를 마친 후에도 메모리 영역에 평문으로 저장된 패스워드가 메모리에 그대로 남아 있어서 앱이 백그라운드에 들어가거나 로그오프되어도 이 영역을 덮어쓰거나 지우지 않는 취약점이 존재한다고 밝혔다.

5. WhatsApp

5.1 WhatsApp의 기능

WhatsApp은 2014년에 페이스북에 인수된 후에 사용자가 급격히 더 늘어서 2016년 2월 26일에는 10억 명을 넘어선 세계 최다 사용자를 보유한 모바일 메신저 앱이다[26].

WhatsApp은 실시간으로 문자메시지를 주고받을 수 있고, 그룹 대화가 가능하다. 사진, 동영상, 오디오, 파일, 위치 등도 공유할 수 있는 기능을 제공하고 있다. 간단히 버튼을 누르면 세계 도처에 음성 통화를 할 수 있는 기능이 제공된다. 음성 전화의 내용은 암호화 되어 제삼자가 엿들을 수 없다.

WhatsApp은 2016년 5월 10일자 블로그에 종단간 암호화 기능이 디폴트로 적용된다고 발표하였다. WhatsApp을 업데이트 하는 것으로 전면적인 암호화된 기능을 이용할 수 있는데 대화, 사진, 파일, 그룹채팅 등 WhatsApp의 모든 메시지가 암호화되어 서버에는 평문이 남아있지 않기 때문에 프라이버시가 보호된다는 점을 강조하고 있다[26].

5.2 WhatsApp의 암호화기술

WhatsApp은 그들의 보안백서에 자신들의 앱에 적용하고 있는 메시지의 암호화 기술을 소개하고 있다[2].

WhatsApp의 암호화는 Open Whisper Systems가 설계한 Signal Protocol을 바탕으로 제작되었다. 이것은 종단간 암호화 방식으로 제삼자가 중간에 개입하거나 WhatsApp이 평문으로 접근하는 것을 방지하기 위한 목적으로 설계되었다. 그리고 암호 키가 사용자 장치에서 물리적으로 지속적인 침해를 당했다고 하더라도 이미 전송된 메시지를 시간을 되돌려 복호하지 못하게 하는 완전 순방향 비밀성 기술을 적용하고 있다. 아래의 내용은 백서[2]에 소개된 내용을 바탕으로 작성된 것이다.

공개키와 세션키

Identity Key(IK) Pair –설정 시에 생성되는 장기간 사용되는 키. Curve25519 키 쌍으로 생성.

Signed Pre Key(SPK) – Curve25519 키 쌍으로 생성. 중기간 사용되는 키.

One-Time Pre Keys(OTPK) – 일회용으로 사용하기 위한 Curve25519 키 쌍으로 필요시마다 갱신

Root Key(RK)-Chain Keys의 32바이트 값.

Chain Key(CK)-Message Keys에 의해서 생성하는데 사용하는 32바이트 값.

Message Key(MK)-메시지의 내용을 암호화하는데 사용하는 80바이트 값. 이것은 32바이트 AES-256 키, 32바이트 HMAC-SHA256키, 초기값(IV) 설정을 위한 16바이트로 구성.

메시지의 교환

클라이언트들은 AES256-CBC로 암호화된 메시지를 교환한다. 소멸성 메시지 키가 사용되고 인증을 위해서 HMAC-SHA256이 사용된다. MK와 CK는 각각 다음과 같이 계산된다.

$$MK=HMAC\text{-}SHA256(CK, 0x01) \quad (1)$$

$$CK=HMAC\text{-}SHA256(CK, 0x02) \quad (2)$$

매번 메시지가 전송될 때마다 소멸성 공개키도 함께 보낸다. 응답이 오면 새로운 CK와 RK는 ES(Epemeral Secret)에 의해 다음과 같이 계산된다.

$$ES=ECDH(Esnd, Ercp) \quad (3)$$

$$CK, RK= HKDF(RK, ES) \quad (4)$$

체인은 한 사용자의 메시지 송신에만 사용하기 때문에 재사용되지 않는다.

그룹 메시지

WhatsApp의 그룹 메시지는 server-side fan-out을 하는 방식을 사용하여 그룹에게 메시지를 전달하는 방식을 사용한다. 다음은 그룹에게 첫 메시지(1~4)를 보내는 방법과 후속메시지(5~8)를 보내는 방법이다.

1. 송신자는 랜덤 32바이트 CK를 생성
2. 송신자는 랜덤 Curve25519 서명키(SK)쌍을 생성
3. 송신자는 32바이트 CK와 SK를 묶어서 송신자 키 메시지에 넣음
4. 송신자 키를 각 멤버들마다 암호화
5. 송신자는 CK로부터 MK를 만들어서 CK를 갱신
6. 송신자는 AES256-CBC를 이용해 메시지 암호화
7. 송신자는 SK를 이용하여 암호문에 서명
8. 송신자는 단일 암호 메시지를 서버에 전송. 이 메시지는 모든 그룹 멤버들에게 전달

이 방식에서는 송신자의 메시지마다 키가 변경되는 완전 순방향 비밀성 기능을 제공한다. 그룹 멤버 중 하나가 떠나게 되면 모든 참가자는 송신자 키를 삭제하고 새로 시작하면서 보안성을 유지한다.

5.3 WhatsApp의 알려진 보안취약점

독일의 Der Spigel[28]은 최근 전면적으로 암호화가 적용된 WhatsApp은 생각보다는 안전하지 않을 수 있다는 내용으로 5

가지 보안 취약성을 보도하였다. 첫째로 종단간 암호화는 모든 대화 참여자가 최신버전을 사용하여야 안전하지만 그룹 대화에서 한 명이라도 암호화가 되지 않으면 모두 노출된다는 점을 지적했다. 둘째로 메시지는 암호화되었지만 언제 누구와 대화를 했는지 알 수 있는 메타데이터가 모두 기록으로 남는다는 점을 지적했다. 세 번째는 개방된 Signal 프로토콜을 사용하여 암호화하였지만 개발된 코드는 공개하지 않았다는 점을 지적했다. 네 번째로 암호의 문제가 아닌 키로거(Key logger)나 화면 캡처 등에 의한 문제가 야기될 수 있음을 언급하였다. 다섯 번째로 스마트폰의 도난이나 제삼자가 SIM카드를 소유한 경우에 상대방을 확인하기 어렵기 때문에 그룹채팅의 경우 더욱 대화 내용의 유출가능성이 높다.

그러나 Der Spigel이 언급한 다섯 가지의 취약성은 WhatsApp에만 국한된 문제가 아닌 다른 모든 시큐어 메신저에 공통적으로 적용될 수 있는 취약성 문제라고 이해해야 한다.

6. Facebook Messenger

6.1 Facebook Messenger의 기능

페이스북 메신저는 2016년 7월에 메신저의 월 활동자가 10억명을 돌파하였다고 밝혔다[30]. 최근 페이스북 메신저는 속도가 향상됐으며, 영상통화가 가능해졌고, 다양한 색상, 닉네임, 이모티콘 등이 지원되며, 'Businesses on Messenger'를 통해 비즈니스 기능이 강화되었다. Messenger를 통한 송금 기능이 가능해졌고, 현재 위치를 친구들과 공유할 수 있는 기능도 추가되었다.

이런 변화에 무엇보다도 암호화 기능이 추가된 것이 가장 큰 변화이다. '비밀 대화(Secret Conversations)'라는 이름의 기능은 일대일 메시지를 암호화하는 기능을 수행한다. 그러나 아직 그룹대화의 메시지의 암호화 기능은 갖추지 못하고 있다. 또한 인공지능 챗봇과 같이 페이스북이 메신저에 최근에 도입한 다양한 기능이 종단간 암호화를 설정하면 동작하지 않기 때문에 이 암호화 기능을 수동으로 설정하도록 하였다[31].

6.2 Facebook Messenger의 암호화 기술

페이스북은 암호화가 적용된 최신 메신저의 비밀대화에 대한 내용을 백서로 발간하였다[29]. 공개 프로토콜인 Signal Protocol을 사용하여 적합한 수신자 이외의 제삼자가 평문에 접근할 수 없도록 구현되었다. 아래의 내용은 이 방법에서 사용되는 키들과 메시지의 교환 방법에 관한 설명이다.

공개키와 세션키

모든 공개키는 Curve25519방식을 사용한다. 공개키 쌍은 여러 종류가 사용되는데 장기간 사용되는 식별키 쌍(IK_{pk}, IK_{sk}), 중기간 사용되는 Signed Pre-Key 쌍(SPK_{pk}, SPK_{sk}), 단기간 사용되는 One-Time Pre-Key 쌍($OTPK_{pk}$, $OTPK_{sk}$)이 사용된다. 소멸성 키 쌍 (EK_{pk}, EK_{sk})은 비밀대화에서 매번 순차적으로 생성되며 사용 후 바로 버리는 키이다.

비밀대화를 시작할 때 대화에 참여하는 각 디바이스에는 대칭키가 사용된다. 그리고 다음과 같은 키들이 사용된다. Rook Key(RK)는 256비트의 Chain Key를 구동시키는데 사용하는 키이다. Chain Keys(CK)는 Message Keys를 구동하는데 사용되는 256비트 값이다. Message Keys(MK)는 AES-256용의 256비트, HMAC-SHA256용의 256비트, AES-CBC의 초기벡터(IV)용 128비트 등으로 구성된 640비트 값이다. 메신저가 비밀대화를 시작할 때 영구 IK_{pk}와 현재의 SPK_{pk}를 생성하고 업로드한다. OTPK 키 쌍 묶음을 생성하고 페이스북의 공개 파트에 업로드 한다.

메시지의 교환 방법

비밀대화에서 각 메시지는 AES-CBC로 암호화되고 HMAC-SHA256을 사용하여 인증된다. 유일한 MK는 현재의 CK와 RK로부터 유도되어 첫 번째 값은 다음과 같이 된다.

$$CK=RK \quad (5)$$

$$MK=HKDF(CK) \quad (6)$$

각 메시지를 교환하는데 있어서 송신자는 새로운 소멸키 쌍 (EK_{snd-pk}, EK_{snd-sk})을 생성한다. 송신메시지의 공개부분에 포함시킨다. 수신자는 EK_{snd-pk}를 이용해서 현재 MK값을 계산하면 메시지를 복호할 수 있다. 새로운 소멸키 쌍 (EK_{rcv-pk}, EK_{rcv-sk})를 생성하고 이전 대칭키 값을 아래와 같이 갱신하여 다음 응답에 사용하기 위해서 새로운 RK', CK', MK'을 생성한다.

$$RK',CK'=HKDF(ECDH(EK_{rcv-pk}, EK_{rcv-sk}) \quad (7)$$

$$MK'=HKDF(CK') \quad (8)$$

만일 두 번째 메시지가 상대편에게 응답 전에 보내졌다면 송신자는 새로운 체인키 CK''=HKDF(CK)를 사용하게 되며 응답은 MK''=HKDF(CK'')가 된다.

문서[29]에는 대화의 시작방법, 이미지첨부, 스티커, 대화의 메타데이터, 키 검증, 디바이스 스위치오버 등에 관한 내용이 기술되어 있다.

6.3 Facebook Messenger의 알려진 취약점

보안 전문업체 체크포인트는 페이스북 메신저에서 최근 발견된 악성코드는 악의적으로 대화를 변경하거나 악성코드를 메신저 내에 심어 전파할 수 있는 기능이 있다고 밝혔다[32]. 또 다른 악성 코드는 타임라인 상의 태그된 게시물 또는 친구에 의해 전송된 메시지로 위장하고 무작위로 생성된 문자열 중 하나를 제목으로 사용하며, 피해자의 친구 목록에서 여러 사람을 태그하고 이를 클릭하도록 유도한다[33].

암호화가 적용된 페이스북 메신저가 선보인지 얼마되지 않아서 아직 암호화 기능 자체에 대한 취약점이 보고되지는 않았

다. 암호화 구간에서의 평문 메시지가 노출될 확률은 많지 않지만 암호화 기능이 설치되지 않은 버전과의 대화에서 암호가 사용되지 못하는 문제, 다른 모바일 메신저와 마찬가지로 키로거와 스크린캡처에 의한 메시지의 유출 가능성이 존재한다.

7. KakaoTalk

7.1 KakaoTalk의 기능

KakaoTalk은 2015년 12월 기준 4.8천만 명 가입자 수를 갖고 있는 한국의 대표적인 메신저 앱이다. 전화번호만 있으면 실시간 그룹채팅 및 1:1 채팅기능, 오픈채팅, 사진, 동영상, 연락처 등의 멀티미디어 전송기능, 그룹콜, 페이스톡, 결제, 다양한 이모티콘, 아이템 스토어, 샵 검색, 톡게시판, 채널탭 등의 다양한 기능을 제공하고 있다[43].

2014년에 KakaoTalk 검열논란이 발생하자 다음카카오는 종단간 암호화를 도입하여 메시지가 보호될 수 있는 조치를 취하였다. 제삼자가 대화내용을 확인하는 것을 원천 차단, 비밀대화 지원, 대화내용 저장기간 2~3일로 단축 운영, 수사기관의 KakaoTalk 이용자 정보요청 건수를 공개하는 투명성 보고서 발표 등의 개인정보보호를 위한 조치였다[35,36]. 그 후에 그룹 대화방까지 프라이버시 모드 도입하고 있다[34].

7.2 KakaoTalk의 암호화 기술

KakaoTalk의 '비밀채팅'에서는 종단간 암호화 기술을 적용하고 있다. 인증기술로는 Certificate Pinning[5]을 사용하고 있다. 이것은 MITM 공격을 방어하기 위해서 사용하는 기술이다. 최근에는 그룹 채팅에도 프라이버시 모드를 도입했다고 밝혔는데 최대 50명까지 참여가 가능하고 1:1 비밀채팅과 마찬가지로 종단간 암호화 기술이 적용되었다[34].

KakaoTalk에서 메시지를 서버에 저장하는 방식은 카카오블로그의 공지사항[35]을 통해서 알 수 있다. KakaoTalk의 검열논란에 대해서 언급하면서 실시간 모니터링은 실시간 감청을 위한 장비를 갖추고 있지 않기 때문에 불가능하다고 설명하였다. 또 다른 블로그의 기사에서 KakaoTalk이 대화 내용을 얼마동안, 어떻게, 어떤 정보를 저장하고 있는 것을 언급하였다[36]. 대화의 내용을 서버에 저장하는 이유는 휴대폰을 꺼놓거나 네트워크 연결이 되지 않아서 일정기간 접속을 못하는 경우에 그 동안의 메시지가 유실되지 않도록 하려는 것이고 검열논란 이후에 2~3일로 축소하였다. 사용자가 채팅방에서 메시지를 삭제하거나 채팅방을 나가더라도 서버에 지정된 기간 동안 대화 내용을 보관하고 있다. 3개월 동안 대화의 내용이 아닌 대화의 로그를 관련법에 의하여 보관하고 있다고 한다.

KakaoTalk은 개발의 내용을 공식 문서를 통해서 밝히지 않았다. 완전 순방향 비밀성을 적용할 것이라는 이야기는 있었지만 실제로 적용했는지는 그들이 발표한 보도 자료만으로는 확인할 수 없었다.

7.3 KakaoTalk의 알려진 취약점

KakaoTalk은 검색 품질을 높이기 위해 2016년 1월부터 'URL미리보기'를 위해 수집된 웹주소의 정보를 다음 웹검색에 연동해 왔다. 직접적인 KakaoTalk 대화나 이용자 정보가 포함되지 않은 웹주소만 사용하는 것이지만 개인 사생활이 노출될 수 있다는 논란이 일었다. 5월 27일 언론 보도 이후로 바로 다음과의 검색 연동을 중단했고 사과문을 발표하였다[26].

URL 링크가 첨부된 포함된 '민방위 소집훈련 대상자입니다'라는 문구의 스미싱 문자 메시지를 클릭 할 경우 악성앱이 다운로드 되고 이것에 의하여 스마트폰 카메라, GPS, 마이크 기능이 제어될 수 있다[38].

Table 1. Evaluation of Functionality and Safeness of Mobile Messengers

	Line	Telegram	Snapchat	Wickr	WhatsApp	FB Msg	KakaoTalk
Encrypted in transit	○	○	○	○	○	○	○
Encrypted so the provider can't read it?	○	○	×	○	○	○	○
Verification of contacts' identities	○	○	×	○	○	○	○
Perfect Forward Secrecy	○	△	×	○	○	○	?
Source code open	×	○	×	×	△	△	×
Documentation	○	○	×	○	○	○	×
Code audit	○	○	○	○	○	○	△
Message encryption protocol	AES256-CBC	AES256	AES128-ECB	AES256/GCM	AES256-CBC	AES256-CBC	AES256
Server(○)/P2P(△)	○	○	○	○	○	○	○
Key exchange method	ECDH	DH	대칭키	ECDH	ECDH	ECDH	?
Screen capture protection(○)/Notification(△)	×	△	△	○	×	×	×
Ephemeral message	○	○	○	○	×	×	×
Encryption of Group chat	×	×	×	○	○	×	○
Date of recent version	2015.10	2014.12	2016.3	2015.11	2016.5	2016.7	2015.3

IV. Evaluation

1. Comments on the Evaluation

표 1은 2장에서 제시한 평가 기준을 근거로 각 모바일 메신저 앱의 기능을 평가한 것이다. 표 1에서 Line의 경우는 2015년 10월에 발표한 Letter Sealing 버전[18]에 많은 기능의 향상이 있었다. 기본적인 종단간 암호화를 지원하고 자기 파괴 메시지 기능을 지원하고 있으나 소스코드 공개, 화면캡처 기능방지, 그룹 채팅의 암호화가 지원 되지 않고 있다.

Telegram의 경우는 많은 면에 있어서 충실하게 메시지의 보안성을 지원하고 있다. 완전 순방향 비밀성도 지원하고 있지만 메시지 100개마다 키를 변경하는 방식을 사용하고 있어서 모든 메시지마다 적용하고 있는 다른 앱에 비하여 완벽하다고 볼 수 없다. 화면캡처 방지기능 대신 알림 기능으로 구현되었다[10]. 그룹채팅의 암호화가 아직 지원되지 않고 있다.

Snapchat의 경우는 명성에 비하여 보안성이 취약한 편이다. 지원되는 암호는 128비트이어서 대상 앱 중에서 가장 낮은 수의 비트를 적용하고 있다. 종단간 암호화를 지원하지 않고 있고 키 교환 방식에서 대칭키를 사용하고 있어 키 교환에 취약점이 있다. 메시지를 암호화할 때 스냅의 경우는 AES128-ECB를 사용하고 스토리의 경우는 AES128-CBC를 사용한다[16]. 화면캡처를 할 때 메시지로 상대방에게 알리는 기능이 사용되었다.

Wickr는 2015.11에 최신 기술이 적용된 내용을 백서로 발표하였다[24]. 그 동안 공개 안했던 종단간 암호에 구현 방식에 대한 문서를 공개하였다. 이 부분은 EFF[11]의 평가에는 반영되어 있지 않다. 소스코드 공개 여부를 제외하고는 모든 면에서 가장 우수한 평가를 받았다.

WhatsApp은 2016년 5월에 최신의 기술이 적용된 앱을 공개하였다[2]. 이것의 기본 골격인 Open Signal Protocol은 공개되어 있지만 구현된 프로그램은 아직 공개되지 않았기 때문에 '소스코드 공개부분'은 △으로 평가되었다. 화면캡처 방지기능과 자기 파괴기능이 구현되어 있지 않다[26].

Facebook Messenger은 2016년 7월에 최신판을 공개하였다. WhatsApp과 같은 Open Signal Protocol[29]을 사용하고 있지만 그룹채팅에 암호화가 아직 구현되지 않았고 화면캡처방지 기능과 자기파괴기능이 구현되지 않았다. WhatsApp과 Facebook Messenger는 동일한 공개 프로토콜인 Signal Protocol을 사용하고 있어서 기본적인 동작방식은 같다는 의미이다. 그러나 둘은 서로 달리 구현되어서 같은 프로그램이라고 볼 수 없다.

KakaoTalk은 여러 면에서 부족함을 보인다. 2014년 12월 이후 버전부터는 비밀채팅 기능에 종단간 암호화를 지원한다고 알려져 있다[39]. 그러나 구현된 기술에 대한 문서를 공개하지 않고 있어서 어떻게 만들어졌는지 내용을 파악하기 어렵다. 완전 순방향 비밀성의 기능 평가에서 '?'는 이 기능이 지원될 것이라는 소식이 있었지만 2015년 3월 버전에 적용이 되었다는 자료는 찾을 수 없었기 때문이다[34]. 키교환 방식의 평가 '?'도 ECDH를 사용한 것으로 보이지만 공개되지 않았기에 '?'로 평가하였다. 다른 기능에 비하여 그룹채팅에 암호화를 적용하고 있다는 점이 눈에 띈다.

2. Limitations on the Evaluation

이 연구에서 제안한 모바일 메신저 앱의 개인정보보호를 위한 보안성을 14가지의 평가기준으로 7가지 종류의 모바일 메신저 앱들을 평가하였다.

어떤 기능이 적용되었다는 사실 자체가 기능이 우수하다고 평가할 수는 없을 것이다. 그럼에도 불구하고 기능이 지원되면 지원되지 않는 경우보다 좀 더 안전하다고 말할 수 있을 것이다. 모든 메신저들이 소스코드를 공개하여 객관적으로 평가할 수 있는 상황이 아니기 때문에 평가를 완벽하게 할 수 없는 한계점이 존재한다. 모바일 메신저들이 자신들의 코드를 공개하여 객관적인 평가에 참여한다면 각 기능의 성능, 정확한 코드의 구현, 백도어가 존재하지 않다는 증명 등의 평가 기준을 정할 수 있을 것이다. 그러나 이것은 크게 기대할 수 없는 상황이다.

이 평가에서 반영하지 못한 또 다른 보안 취약점들은 모바일 단말기 OS에서 발생할 수 있는 사례는 1)백도어, RCS등의 멀웨어에 의한 OS의 침해 2)화면사진 찍기에 의한 메시지 유출 3)상대방의 고의적인 키의 유출 등이다.

위에 언급된 사안들은 보안의 관점에서 현실적으로 매우 중요한 문제이지만 이 연구의 평가 항목으로는 다룰 수 없는 문제점들이다. 암호화 방법이나 메신저의 구현과 직접적인 관계가 없기 때문이다. 이런 사안들에 대해서는 다른 방식의 평가 접근법이 고려될 수 있어야 한다.

V. Conclusions

이 연구는 최신의 모바일 메신저 앱의 암호화를 구현하여 개인정보보호의 차원에서 메시지의 보안성을 평가하기 위한 기준과 평가한 결과를 제공하였다.

EFF의 자료[11]에서는 모바일 메신저 앱에 안정성 평가 중 전송중 암호화, 서버단 읽기방지, 대역외 인증, 완전 순방향 비밀성, 소스코드 공개여부, 문서화 여부 등 7가지 항목 평가를 수행하였다. 이 연구에서는 여기에 추가하여 메시지 암호방식, 서버/P2P 방식여부, 키교환 방식, 화면캡처 방지기능, 자기파괴 메시지 적용, 그룹채팅 암호화, 평가대상 버전을 추가하여 최신의 내용이 반영된 결과를 보였다.

평가 대상 중에서 Wickr, Telegram, WhatsApp, Line, Facebook Messnger, KakaoTalk, Snapcht순으로 평가되었다. 기능지원 여부가 완벽성을 입증하는 것은 아니지만 보안성을 높이기 위한 기술이 많이 적용된다는 것이 보안이 좀 더 낫

다는 의미로 해석되길 바란다.

이 연구에서 다룬 메신저 앱들 이외에도 성능과 기능면에서 좋은 앱들이 많이 존재한다. 대표적으로 Bleep는 특이하게 메시지가 서버를 경유하지 않는 P2P방식으로 구현되어 3자 개입의 여지를 없앴다는 점에서 보안성이 뛰어나다고 강조하고 있다. Open Whisper Systems의 Signal Private Messenger의 경우는 소스가 공개되어 있고 좋은 평가를 받고 있다. 또한 Thereema, TextSecure, Off-The-Record 등도 보안성 측면에서 높은 평가를 받고 있지만 한국에서의 지명도와 사용자 수를 근거로 대상을 정하였기에 이 연구에서는 제외되었다. 추후 연구에서 이 모든 메신저 앱들을 평가 대상에 포함시키고 암호화의 기술에 대한 것만이 아닌 사용자의 편의성에 대한 객관적인 평가 척도를 마련하여 개인정보보호를 위한 최적의 모바일 메신저 앱을 평가하는 작업이 수행되기를 바란다.

REFERENCES

[1] Korea Communication Commission, "Guideline for Right to exclude his own Internet postings," *www.kcc.go.kr/download.do?fileSeq=43062*

[2] WhatsApp, "WhatsApp Encryption Overview," Technical white paper, *https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf 2016.*

[3] ZDNet Korea, "Marker Group-Gangwondo, 'Right to be forgotten' Business Agreement," *http://www.zdnet.co.kr/news/news_view.asp?artice_id=20150813172344*

[4] MK News, "Tweeter apply 'Right to be forgotten' for Korea," *http://news.mk.co.kr/newsRead.php?year=2016&no=347663*

[5] Wikipedia, "Transport Layer Security-Dealing with man-in-the- middle attacks," *https://en.wikipedia.org/wiki/Transport_Layer_Security#Certificate_pinning*

[6] Namu Wiki, "Telegram-Security," *https://namu.wiki/w/%ED%85%94%EB%A0%88%EA%B7%B8%EB%9E%A8*

[7] Pavel Durov, "Telegram was kicked out from Play Store for a few hours today due to @naver_line's actions," *https://twitter.com/durov/status/619486763032182784*

[8] Telegram, "$300,000 for Cracking Telegram Encryption," *https:// telegram.org/blog/cryptocontest*

[9] The Hacker News, "Is Telegram Really Secure?-4 Major Privacy Issues Raised by Researcher," *http://thehackernews.com/2015/11/telegram-security-privacy.html*

[10] Telegram, "Secret chats, end-to-end encryption," *https://core.telegram.org/api/end-to-end*

[11] Electronic Frontier Foundation, "Secure Messaging Scorecard," *https://www.eff.org/node/82654, 2014.*

[12] "Target and Sanpchat suffer major data breaches," Computer Fraud and Security, pp. 2-3, Jan. 2014. doi:10.1016/S1361-3723(14)70001-6

[13] BBC Newsbeat, "Hackers threaten to post more Snapchat photos online," *http://www.bbc.co.uk/newsbeat/article/29581386/hackers-threaten-to-post-more-snapchat-photos-online*

[14] Tarun Mehrotra and B. M. Mehtre, "Forensic Analysis of Wickr Application on Android Devices," 2013, IEEE Int. Conf. on Computational Intelligence and Computing Research, 2013. doi:10.1109/ICCIC.2013.6724230

[15] Decipher Forensics, "Snapchat Unveiled: an Examination of Snapchat on Android Devices," *http://www.decipherforensics.com/snapchat*

[16] Gibson Security, "Snapchat - GibSec Full Disclosure," *http://gibsonsec.org/snapchat/fulldisclosure/#encrypting-normal-snaps*

[17] Snapchat Supprot, "When Does Snapchat Delete Snaps and Chats?," *https://support.snapchat.com/en-US/a/when-are-snaps-chats-deleted*

[18] Line, "Line, 'Letter Sealing'-The World First E2EE Technology Through Smart Phone and PC Platform," *https://linecorp.com/en/pr/news/ko/2015/1110*

[19] Line Engineers' Blog, "For more safer dialogue: Letter Sealing," *http://developers.linecorp.com/blog/ko/?p=162*

[20] CNET Korea, "Messenger 'Line' Revealed Security Vulnerability," *http://www.cnet.co.kr/view/129214*

[21] Pioneer of Security Research, "Secure Chat Messenger App Security Check," *http://www.pocsec.com/blog/secure_chat.pdf*

[22] LINE Security Bug Bounty Program, *https://bugbounty.linecorp.com/en/*

[23] Wickr, "How Wickr's Encryption Works," *https://www.wickr.com/security/how-it-works*

[24] Wickr, "Wickr Messaging Protocol-Technical Paper," *https://www.wickr.com/uploads/files/700869603163179165-wickr-whitepaper-final.pdf*

[25] Asterisk Labs, "Making Wickr Weaker," *https://labs.asteriskinfosec.com.au/making-wickr-weaker*
[26] WhatsApp blog, *https://blog.whatsapp.com*
[27] Kakao blog, "Talking about KakaoTalk web address link utilizes in Daum web search," *http://blog.kakaocorp.co.kr/516*
[28] Der Spiegel, "WhatsApp-Update: Gut verschlüsselt, aber nicht komplett sicher," *http://www.spiegel.de/netzwelt/apps/whatsapp-verschluesselung-gut-aber-nicht-komplett-abhoersicher-a-1085726.html*
[29] Facebook, Messenger Secret Conversations-Technical *Whitepaper, http://www.fb.com*
[30] Facebook Newsroom, "Facebook Messenger Celebrates Reaching 1 Billion Monthly Active User," *http://ko.newsroom.fb.com*
[31] The Guardian, "Facebook planning encrypted version of its Messenger bot, sources say," *https://www.theguardian.com/technology/2016/may/31/facebook-messenger-bot-encryption-secure-messaging*
[32] ZDNet Korea, "Facebook Messenger - Malware," *http://www.zdnet.co.kr/news/news_view.asp?artice_id=20160608071232*
[33] Joongangilbo, "New Malware using Facebook," *http://news.joins.com/article/19913438*
[34] DaumKakao, "KakaoTalk serves group chats," *http://stchero.tistory.com/311*
[35] Kakao blog, "The Dispute over Censorship about KakaoTalk," *http://blog.kakaocorp.co.kr/215*
[36] Kakao blog, "Actually, KakaoTalk Messages are," *http://blog.kakaocorp.co.kr/216*
[37] Ohmynews, "FBI Unlocked iPhone without Apple's Assistance," *http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0002194982*
[38] Security News, "Smishing Malware Steals KakaoTalk DB," *http://www.boannews.com/media/view.asp?idx=43794*
[39] Kakao blog, "Privacy Mode Begin Today," *http://blog.kakaocorp.co.kr/254*
[40] Hankookilbo, "Telegram Reveals Korean Version," *http://www.hankookilbo.com/v/016edd62a6c14c6784ff43892e00063d*
[41] Newsis, "Right to be forgotten begins in Korea," *http://www.newsis.com/ar_detail/view.html?ar_id=NISX20160601_0014122124&cID=10401&pID=10400*
[42] Wickr, "Wickr Messenger," *https://www.wickr.com/personal#features*
[43] Wikipedia, "KakaoTalk," *https://ko.wikipedia.org/wiki/%EC%B9%B4%EC%B9%B4%EC%98%A4%ED%86%A1*

Authors

Gyu-Sang Cho received the B.S., M.S. and Ph.D. degrees in Electronic Engineering from Hanyang University, in 1986, 1989 and 1997, respectively.
Dr. Cho joined the faculty of the School of Computer at Dongyang University, Yeongju, Korea, in 1996. He is currently a professor in the Department of Computer Information Warfare, Dongyang University. He is interested in digital forensics, system security, and IoT security.