채팅 어플리케이션 분석을 통한 새로운 앱 제안

손유진*, 심효은*, 정해빈*, 김명주**
*서울여자대학교 정보보호학과
**서울여자대학교 정보보호학과 교수
s1061001@swu.ac.kr, shy9274@gmail.com, haebin02@gmail.com, mjkim@swu.ac.kr

A New Secure Chatting Application encompassing the Core Functions of the Existing Applications

Yu-Jin Son* , Hyo-Eun Sim*, Hae-Bin Jeong*, Myuhng-Joo Kim**
*Dept of Information Security, Seoul Women's University
**Professor, Dept of Information Security, Seoul Women's University

요 약

기존 채팅 어플리케이션에 대한 감청 논란으로 인해 소비자들은 채팅 어플리케이션에 대한 불신이 커졌다. 따라서 소비자들은 보안 채팅 어플리케이션을 선호하게 되었다. 이에 본 논문에서는 현재 사용하는 보안 채팅 어플리케이션의 기능과 서비스를 비교하여 향후 바람직한 보안 채팅 어플리케이션이 갖추어야 할 기능들을 도출하고 이의 일부 기능을 구현한 결과를 소개한다.

1. 개발 배경

모 정당 간부를 수사하는 과정에서 간부의 사생활과 다수의 지인에 대한 개인정보가 담긴 두 달 분량의 카카오톡 대화록을 수사기관이 들여다본 사실이 불거지면서 채팅 프로그램을 통한 사생활 침해에 대한 논란이 발생했다[1]. 이에 카카오톡 대표는 사실이 아니라고 주장하였지만 계속된 번복으로 인해 수사기관에 의한 채팅 프로그램의 사찰은 사실인 것으로 일반인들에게는 인식되었다. 결국 수사기관이 카카오톡, 네이버 밴드, 네이트온, 마이 피플 등 국내 채팅 어플리케이션을 전반적으로 감청한 것이 밝혀졌다.

이러한 감청 논란으로 인해 많은 이용자들은 일반 채팅 어플리케이션보다는 보안 채팅 어플리케이션을 선호하게 되었으며, 최근까지 많은 보안 채팅 어플리케이션이 출시되고 있다. 하지만 지금까지 공개된 보안 어플리케이션들을 살펴보면 기능, 서비스, 보안 수준이 일정하지 않아 이용자들은 본인에게 적합한 보안 채팅 어플리케이션을 선택하는데 어려움을 겪고 있다. 따라서 이용자들에게 좀더 포괄적이면서도 기존 제품들이 제공하는 서비스, 기능, 보안 수준을 일정 수준 이상 제공하는 새로운 보안 채팅 어플리케이션이 필요하다. 본 논문에서는 지금까지 출시된 보안 채팅 어플리케이션들의 동향을 살펴봄과 동시에 새로운 보안 채팅 어플리케이션이 가져야할 기능에 대한 기본 방향을 설계한다. 아울러 이러한 기능들 중에서 핵심기능을 소프트웨어로 구현한 결과를 제시한다.

2. 기존 채팅 어플리케이션에 대한 분석

2.1 채팅 어플리케이션의 동향

채팅 어플리케이션은 스마트폰의 등장으로 시작되었다. 초기 채팅 어플리케이션은 카카오톡, 라인 등으로 시작했다. 카카오톡 감청 논란 이후 카카오톡을 포함한 채팅 어플리케이션은 보안을 강화했고, 보안 채팅 어플리케이션을 소비자들이 선호하기 시작했다.

카카오톡은 비밀 채팅모드를 추가하여 일반 채팅보다 사용자 정보보호를 한 단계 더 강화한 새로운 형태의 대화방이다. 카카오톡 비밀 채팅 모드는 암호를 풀 수 있는 키를 서버에 저장하지 않고 핸드폰 등 개인 단말기에 저장하는 '종단간 암호화' 기술을 적용한다. 암호화된 대화 내용을 풀 수 있는 암호키가 핸드폰에만 저장되어 서버에서 대화내용을 확인할 방법이 원천적으로 차단된다[2]. 라인 또한 Letter Sealing을 이용하여 보안을 강화하게 했다. Letter Sealing 은

1:1 대화방 메시지에 종단간 암호화 기술을 적용한 서비스로 텍스트메시지, 위치정보, 1:1 통화 음성 및 영상 통화 내용을 암호화한다. 또한 Letter Sealing 에서는 ECDH(Elliptic Curve Diffie-Hellman)를 사용하고 HMAC(Hash-based message authentication code) 방식을 추가하여 메시지 위 변조를 방지한다[3].

카카오톡 감청 사건 이후 Telegram, Wickr, Threema, WhatsApp 과 같은 보안 채팅 어플리케이션이 국내 사용자들에게 각광을 받았다. Telegram 은 Cloud chats 인 일반 채팅 모드와 Secret chats 인 비밀채팅 모드를 제공한다. 여기서 Secret chats 키는 DH(Diffie-Hellman) 프로토콜을 사용하여 생성된다. 메시지 내용과 정보가 담긴 페이로드에 SHA-1 을 사용하여 msg_key 를 생성한다. 데이터는 256 비트의 키를 사용하고 IGE(Infinite Garble Extension)가 적용된 AES 로 암호화한다. 완전 순방향 비밀성을 위해서 100 개의 메시지를 송수신한 경우 또는 키를 사용한지 일주일 이상 된 경우 키를 다시 생성한다. 이는 키가 해킹되어 동일 키가 적용된 모든 메시지가 복호화 되는 것을 방지하기 위한 방법이다[4]. Wickr 는 종단간 암호화, 완전 순방향 비밀성, 보존 메타 데이터를 지원한다. 암호화 기술은 AES256 을 사용하여 데이터를 암호화한다. 중간자 공격을 방지하기 위해 대칭키를 안전하게 분산하는 방법(SSL)을 사용한다. 복호화 키를 배포할 때는 중앙화 되지 않는 보안구조를 사용한다. 사용자 이름, 앱 ID, 디바이스 ID 등은 SHA256 으로 해시 처리된다. ECDH(Elliptic-Curve Diffie-Hellman)암호를 사용하여 메시지 암호키를 생성한다. 메시지는 수신자의 앱과 디바이스에만 한정적으로 사용되며 패스워드와 패스워드 해시를 디바이스에 전혀 남기지 않는다[5]. Threema 는 종단간 암호화와 앱과 서버 간의 연결 도청을 방지하기 위한 계층으로 나뉜다. 모든 암호화 및 암호 해독은 장치에서 직접 수행되며 사용자는 키 교환을 제어할 수 있다. 따라서 서버 운영자뿐만 아니라 타사에서도 메시지 및 통화 내용을 해독할 수 없다. 비대칭 ECC 기반 암호화는 255 비트의 강도를 가진다. Curve25519 의 ECDH 는 해시함수 및 임의의 nonce 와 함께 사용하여 각 메시지에 대해 고유한 256 비트 대칭 키를 도출하고 스트림 암호 XSalsa20 을 사용하여 메시지를 암호화한다. 조작/위조를 탐지하기 위해 각 메시지에는 128 비트 메시지 인증 코드(MAC)가 추가된다. 네트워크 연결에는 순방향 보안을 제공한다. 클라이언트와 서버는 RAM 에만 저장되고 앱이 다시 시작될 때마다 교체되는 임시의 임의 키를 협상한다. 네트워크 트래픽을 캡처한 공격자는 이후에 클라이언트나 서버의 장기 비밀키를 알아내더라도 암호를 해독할 수 없다[6].

마지막으로 같은 프로토콜을 쓰는 앱으로 Facebook messenger 과 WhatsApp 이 있다. 이들은 Open Whisper Systems 이 개발한 Signal Protocol 을 동일하게 사용하고 공개키와 세션키를 생성하는 방법은 같다[7]. 메시지를 교환할 때 세션이 설정되면 클라이언트는 암호화를 위해 CBC 모드에서 AES256 을 사용한다. 인증확인을 위해 HMAC-SHA256 을 사용하여 Message Key 로 보호되는 메시지를 교환한다. Message Key 는 전송된 각 메시지에 대해 변경되고 메시지가 전송되거나 수신된 후에는 세션 상태를 재구성될 수 없다. 또한 전송한 모든 메시지를 “한쪽” 방향으로 보내는 발신인의 Chain Key 에서 파생된다. 새로운 Chain Key 를 만들기 위해 각 메시지 왕복과 함께 새로운 ECDH 승인이 필요하다. 따라서 즉각적인 “hash ratchet”과 왕복 “DH ratchet”의 조합을 통해 순방향 비밀성을 제공한다[8].

2.2 채팅 어플리케이션들의 기능 비교

비교 문항	Threema	Line	Telegram	Facebook Messenger	Wirkr	WhatsApp
종단 간 암호화가 PC에서 가능한가?	O	O	X	X	O	O
@ 소환 기능 가능한가?	O	X	O	X	X	O
메시지 삭제 기능이 있는가?	X	O	O	O	O	O
전화번호 없이 가입이 가능한가?	O	O	O	O	O	X
접속 유무 파악이 가능한가?	X	X	X	O	X	X
멀티 디바이스 지원이 되는가?	X	X	O	O	X	O

(표 1) 채팅 어플리케이션들의 기능 비교

(표 1)에서는 채팅 어플리케이션인 Threema, Line, Telegram, Facebook Messenger, Wickr, WhatsApp 을 조사하였다. (표 1)의 채팅 어플리케이션의 경우 Threema 를 제외한 나머지 채팅 어플리케이션은 모두 메시지 삭제가 가능하다. Threema, Telegram, WhatsApp 은 @소환이 가능하지만 Line, Facebook Messenger, Wickr 는 @소환을 지원하지 않는다. WhatsApp 만 전화번호 없이 가입이 가능하고 Facebook Messenger 만 접속 유무 파악이 가능하다.

2.3 보안 채팅 어플리케이션들의 보안성 비교

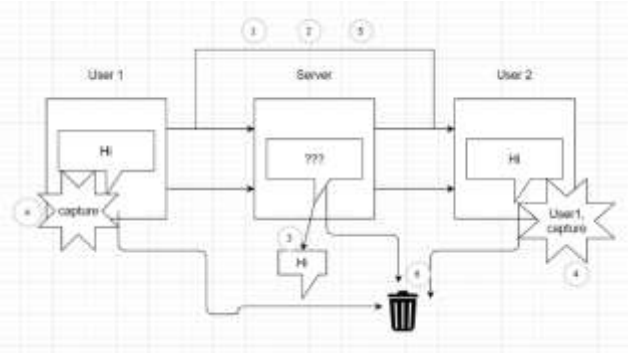
비교 문항	Threema	Line	Telegram
데이터를 암호화해서 전송하는가?	O	O	O
종단 간 암호화가 적용되었는가?	O	O	O
키 유출 시 지난 메시지가 안전하게 보호 되는가?	O	O	△
화면 캡처 방지 또는 알림 기능이 있는가?	O	X	O
그룹채팅에 암호화가 지원되는가?	O	X	X
메시지 자동소멸 기능이 있는가?	X	O	O

(표 2) 보안 채팅 어플리케이션들의 보안성 비교

(표 2)는 보안 채팅 어플리케이션인 Threema, Line, Telegram 에 한정하여 조사한 표이다. Threema, Line, Telegram 의 공통점은 데이터를 암호화해서 전송하고 종단 간 암호화가 적용된다는 것이다. 하지만 Threema, Line 는 키 유출 시 지난 메시지를 안전하게 보호할 수 있지만 Telegram 은 키 유출 시 지난 메시지를 안전하게 보호하는지에 대한 보장이 없다. 또한 Threema, Telegram 은 화면 캡처 방지 또는 알림 기능이 있는 반면에 Line 에서는 화면 캡처 방지 또는 알림 기능을 지원하지 않는다. Threema 는 그룹채팅에 암호화를 지원하지만 Line, Telegram 은 그룹채팅에 암호화를 지원하지 않고 1:1 채팅에서만 암호화를 지원한다. Line 과 Telegram 은 메시지 자동소멸 기능을 지원하는 반면, Threema 는 메시지 자동소멸 기능을 지원하지 않는다[9].

3. 새로운 보안 채팅 어플리케이션

3.1.1 시스템 구성도



(그림 1) 시스템 구성도

새로 제안하는 시스템의 구조도는 (그림 1)과 같이 5 가지 핵심 기능을 중심으로 설명할 수 있다.

① 데이터를 암호화하여 전송
② 종단간 암호화 적용
③ 키 유출 시 지난 메시지 암호화
④ 화면 캡처 방지 기능
⑤ 메시지 삭제 기능

본 논문에서 제시하는 시스템 구조도는 User1 이 “hi” 를 User2 에게 보내는 채팅 흐름에서부터 시작한다고 가정한다. User1 이 “hi 를 User2 에게 전송할 때 데이터를 암호화, 즉 종단간 암호화를 적용한다. 그러므로 키 유출 시 지난 메시지를 안전하게 보호할 수 있다. 또한 메시지 삭제도 가능하며 삭제를 선택할 시 서버에도 남지 않고 사라진다. 이외에도 추가적으로 제시하는 어플 기능으로는 개인정보 유출을 막기 위한 화면 캡쳐 방지 기능을 꼽을 수 있다.

3.1.2 데이터베이스 암호화

모든 채팅 기록은 기본적으로 데이터베이스 내부에 저장되어 있다. 따라서 데이터베이스 자체가 암호화되어 있어야 채팅 기록 등에 대한 정보를 보호할 수 있다.

보안성을 더욱 강화하기 위해 데이터베이스를 복호화 할 수 있는 키의 위치를 다시 한번 더 암호화하는 과정을 수행한다. 애플리케이션 시작 시 사용자가 복호화 키를 입력하게 하고 그 복호화 키를 저장할 때 다시 한번 암호 알고리즘을 통해 암호화를 한 뒤 저장한다.

3.2 사용자 인터페이스(UI)

(그림 2) 사용자 인터페이스 - 채팅 화면

위 (그림 2)는 채팅 어플리케이션의 기본 기능인 텍스트와 이미지가 메시지로 송수신 되는 채팅 화면에 대한 구현 예이다. 해당 화면에서는 메시지를 송신한 시간과 상대방이 그 메시지를 읽었는지 확인할 수 있는 텍스트가 함께 표시되어 있다.

(그림 3) 메시지 삭제 화면

본 논문에서 제안하여 구현한 채팅 시스템의 주요 기능으로는 메시지 삭제와 캡처 금지 기능을 꼽을 수 있다. 위 (그림 3)은 (그림 2)에서 이미지를 삭제한 화면을 보여준다. 메시지를 삭제하는 경우, 시간에 상관없이 메시지 삭제를 하는 사용자뿐만 아니라 그 상대방의 화면에서도 해당 메시지가 삭제된다. 또한 외부로 대화 내용이 노출되지 않도록 채팅 화면에서는 캡처 방지 기능이 적용되어 캡처를 할 수 없다.

4. 결론

본 논문에서는 기존 채팅 어플리케이션의 동향, 보안 채팅 어플리케이션의 서비스와 보안기술을 먼저 살펴보았다. 이를 바탕으로 소비자들에게 새로운 보안 채팅 어플리케이션에 필요한 보안기술과 서비스, 안전하고 편리한 채팅 서비스를 제안하고 주요 기능을 구현하였다. 이를 활용하면 소비자들은 보안 메신저를 보다 편리하면서도 안전하게 사용할 수 있다. 또한 기존 보안 메신저에 있는 보안 기술, 서비스, 기능을 비교 분석하여 이에 대한 일관성을 유지하는 차원에서 설계하고 구현함으로써 소비자들의 새로운 선택에 따른 혼란을 줄이고자 하였다. 본 논문에서 일부 구현한 어플리케이션의 완성도를 높여서 배포할 경우 기존의 특정 보안 채팅 어플리케이션들보다 포괄적이며 일관성 있는 보안 기술과 서비스를 사용자들이 채팅 중에 체험할 수 있을 것으로 기대된다.

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학지원사업의 연구결과로 수행되었음(2016-0-00022)

참고문헌

[1] "카톡 사찰 논란," 경향신문, 2014.10.02 수정, 2021.03.29 접속, https://news.khan.co.kr/kh_news/khan_art_view.html?artid=201410012201225&code=940301
[2] “오늘부터 카카오톡에 프라이버시 모드가 적용됩니다” Kakao 블로그, 2021.03.29 접속 https://blog.kakaocorp.co.kr/254
[3] “Letter Sealing 확대 적용으로 더 안전해진 LINE” Line 블로그, 2021.03.29 접속 https://engineering.linecorp.com/ko/blog/the-next-step-for-even-safer-messaging-letter-sealing/
[4] “Secret chats, end-to-end encryption”, Telegram, 2021.03.29 접속 https://core.telegram.org/api/end-to-end
[5] "Messaging protocol white paper”, Wickr, 2021.03.29 접속 https://wickr.com/wp-content/uploads/2019/12/WhitePaper_WickrMessagingProtocol.pdf
[6] “Cryptography Whitepaper”, Threema, 2021.03.29 접속 https://threema.ch/press-files/2_documentation/cryptography_whitepaper.pdf
[7] “Technical information”, Signal, 2021.03.29 접속, https://signal.org/docs/
[8] “WhatsApp Encryption Overview, Technical white paper”, WhatsApp, 2021.03.29 접속 https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-3&_nc_sid=2fbf2a&_nc_ohc=-m7UJxHJjJsAX8Pf027&_nc_ht=scontent.whatsapp.net&oh=b3fe9f76670d78f50957924f2e32b7d7&oe=60760419
[9] Gyu-Sang Cho, Evaluation of Safeness and Functionality in Applied Technologies for Mobile Messengers, 한국컴퓨터정보학회논문지, 21(8), 29-39, 2016.