Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.2, Apr. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.2.255

보안 메시징 프로토콜 MLS에서 관리자에 메시지 노출에 관한 연구*

권 송 희,[1†] 최 형 기[2‡]
[1,2]성균관대학교 (대학원생, 교수)

Study on Message Exposure to Administrator in Secure Messaging Protocol MLS*

Songhui Kwon,[1†] Hyoung-Kee Choi[2‡]
[1,2]Sungkyunkwan University (Graduate student, Professor)

요 약

메신저 애플리케이션은 서버로 메시지 노출을 방지하고자 종단간 암호화를 자체적으로 적용하였다. 안전하고 효율적인 메시지 통신을 위해 종단간 암호화가 적용된 그룹 메시징 프로토콜인 MLS (Message Layer Security)의 표준화가 진행 중이다. 본 논문은 MLS의 동작 과정과 보안 요구사항을 기반으로 안전성 점검을 수행한다. 메신저 통신에서 필수 보안 요구사항인 중앙 서버에 대한 기밀성은 서버 관리자에 의해 쉽게 위반될 수 있다. 그룹의 통신 내용이 궁금한 서버 관리자를 curious admin으로 정의하고 관리자가 MLS에서 그룹키를 획득하는 공격을 제시한다. 메신저 애플리케이션 사용자에게 서버가 언제든 통신 내용을 열람할 수 있다는 점을 상기시킨다. Curious admin 공격을 방지하기 위해 서버를 거치지 않고 사용자 간 인증하는 방안에 대해 논의한다.

ABSTRACT

Messenger applications applied end-to-end encryption on their own to prevent message exposure to servers. Standardization of a group messaging protocol called Message Layer Security (MLS) with end-to-end encryption is being discussed for secure and efficient message communication. This paper performs safety checks based on the operation process and security requirements of MLS. Confidentiality to a middleman server, which is an essential security requirement in messenger communication, can be easily violated by a server administrator. We define a server administrator who is curious about the group's communication content as a curious admin and present an attack in which the admin obtains a group key from MLS. Reminds messenger application users that the server can view your communication content at any time. We discuss ways to authenticate between users without going through the server to prevent curious admin attacks.

Keywords: Messenger application, Secure messaging, Message Layer Security

I. 서 론

메시징 애플리케이션은 전 세계 약 30억 9천만명의 많은 이용자를 보유하고 있다[1]. 메시징 애플리케이션은 업무나 일상 대화 등 다양한 상황에서 사용된다. 클라이언트 그룹과 서버로 구성된다. 클라이언

Received(02. 21. 2022), Modified(03. 23. 2022), Accepted(03. 24. 2022)
* 본 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2020R1A2C1012708).
† 주저자, songhee@o365.skku.edu
‡ 교신저자, meosery@skku.edu(Corresponding author)

트는 서버로 메시지를 전송하고 서버는 메시지 송신자를 포함하여 그룹의 모든 클라이언트에게 메시지를 전달한다.

메신저 애플리케이션은 종단간 암호화 (End-to-End Encryption, E2EE)를 통해 보안을 제공한다. 종단간 암호화는 통신 당사자만 읽고 쓸 수 있고, 서버를 포함한 제삼자는 읽고 쓸 수 없음을 보장한다. 그룹 통신으로 종단간 암호화 범위를 확장하려면 그룹 멤버십 관리에 맞는 보안 요구사항과 키 분배를 위한 별도의 프로토콜이 필요하다.

그룹 통신에서 각 그룹은 메시지의 암복호화에 사용하는 비밀키인 그룹키를 유지한다. 그룹키는 멤버 간에만 공유해야 한다. 안전한 그룹키 분배를 위해 그룹키를 암호화하는 또 다른 키를 사용한다. 그룹키는 그룹 멤버가 변경될 때마다 갱신해야 한다. 새 멤버가 초대되면 그룹키를 갱신하고 새 멤버는 초대되기 이전의 통신 내용을 열람하지 못한다. 멤버가 그룹을 탈퇴할 때도 그룹키를 갱신한다. 탈퇴한 멤버는 탈퇴 이후에 송신된 메시지를 열람하지 못한다.

일부 메신저 서비스는 그룹 통신의 종단간 암호화를 지원하지 않거나 선택사항으로 제공한다[2]. 메신저 서비스는 통신의 종단간 암호화를 필수로 지원해야 한다. 사용자가 그룹 멤버십을 가질 때만 그룹 메시지를 읽을 수 있도록 해야 한다. WhatsApp에서는 탈퇴 후의 그룹키 보안을 만족하지 않아 탈퇴한 멤버에게 메시지가 노출된다[3].

수백 명 이상 규모의 그룹 운영은 확장성과 성능에 한계가 있다. 그룹 통신 보안의 이러한 문제를 해결하기 위해 Internet Engineering Task Force (IETF)에서 그룹 메시징 프로토콜 MLS (Messaging Layer Security)를 설계하고 있다[4]. MLS는 최대 50,000개의 클라이언트를 지원하고, 웹 브라우저 지원을 포함한 여러 산업 활용 사례를 다루며, 공식적인 보안 보장을 제공하는 것을 목표로 한다. MLS는 2명에서 약 50,000명의 사용자들로 구성된 그룹 통신을 위한 보안 표준이다.

많은 Enterprise 제품은 클라이언트와 서버간 암호화를 사용하지만 메시지 내용은 서버에서 암호화되지 않는다. 메시지는 대부분 제삼자의 접근에 취약한 데이터베이스에 보관된다. 서버에서 메시지를 평문으로 획득하지 않도록 암호화가 필요하다.

II. 배경 지식

메신저 통신은 그룹원 수가 두 명인 일대일 통신과 두 명을 초과하는 그룹 통신으로 구분한다. 이 두 가지 통신은 전송자가 한 명이라는 공통점이 있지만, 수신자가 그룹 통신은 두 명 이상이고 일대일 통신은 한 명이다.

메신저 통신은 그룹 멤버, 중앙 서버, 단말로 구성이 된다. 메시지를 생산하는 멤버는 그룹 통신 프로토콜을 운용하는 단말로 상대방 멤버와 메시지를 주고받는다. 서버는 각 멤버들의 주소와 상태를 관리하고 안전하게 비밀키 관리를 담당한다. 멤버들은 여러 기기로 다양한 장소에서 서비스를 이용한다. 멤버들 현재 물리적 위치는 중앙 서버가 관리하고 멤버들은 서로의 물리적 위치를 알지 못하므로 메시지는 반드시 서버를 통해서 멤버들에게 전달된다.

서버에게 TLS (Transport Layer Security)로 보호된 안전한 통신 채널로 메시지를 작성해서 전송되면, 중앙 서버는 메시지 헤더에서 그룹을 파악하고 해당 그룹에 속한 멤버들에게 각각 TLS로 보호된 일대일 통신으로 메시지를 전송한다. 이외 중앙 서버는 메시지 내용을 변경 조작하지 않는다.

그룹 멤버들만 메시지 작성과 열람을 하기 위해 메시지는 각 그룹에 고유한 비밀 그룹키로 암호화하여 전송한다. 반드시 그룹 멤버들만 알아야 하는 그룹키는 멤버가 변경 시 또는 일정한 유효기간 후에 바로 갱신한다. 신입 멤버가 그룹에 가입하면 이 신입 멤버가 가입 이전에 메세지를 열람하지 못하게 그룹키를 갱신한다. 기존 멤버가 그룹을 탈퇴하면 이 멤버가 탈퇴 후에 열람하지 못하도록 그룹키를 갱신한다.

그룹키를 멤버 간에 효율적으로 관리하는 비밀키 생성과 분배 알고리즘은 메신저 그룹 통신에서 필수적이다. 다양한 키 분배 알고리즘들이 사용되고 있다. 그중 대표적으로 널리 사용되는 알고리즘을 소개한다. 또한, 그룹키 관리를 안전하게 하기 위해서는 다음의 보안 요구사항들을 만족해야 한다.

2.1 효율적인 종단간 암호화 방식

그룹 통신에서 종단간 암호화 방식의 종류는 암호화 키와 분배 방식에 따라 세 가지로 나뉜다[6].

Pairwise. 그룹 멤버들 대상으로 멤버들 간에 비밀키를 생성해서 안전한 일대일 통신을 구축한 후 송

Table 1. Classification according to group key type and distribution. The table shows the number of keys and the number of encryption required when there are N group members.

		Pairwise	SendersKey	Tree
Number of keys to need	One-to-One key	N(N-1)/2	N(N-1)/2	-
	Asymetric key pair	-	-	2N-2
	Group key	-	N	1
Group key distribution		$O(N^2)$	O(N)	$O(\log_2 N)$
Group key message encryption		O(N)	O(1)	O(1)

Table 2. Two asymmetric key pairs used in MLS.

	For distribution	For signing
Purpose	Encrypt the group key with the public key	Sign the message with the private key Validate signature with public key
Usage	Group key update message	Group message, Invitation and removal message, Group key update message
Symbol	{PRdistⓘ, PUdistⓘ}	{PRsignⓘ, PUsignⓘ}

신자는 자신을 제외한 다른 그룹 멤버들에게 메시지를 각각 전송한다. 그룹 멤버 N명을 대상으로 비밀키의 개수는 N(N-1)/2이고 메시지 전송은 N-1의 암호화가 필요하므로 O(N)의 복잡도를 갖는다. 그룹 메시지 전송 시 Table 1에서 멤버 A는 각 멤버와 공유하는 일대일키로 각각 암호화하여 전송한다. 멤버가 가입 또는 탈퇴 시 안전을 위해 비밀키를 갱신하면, 비밀키의 개수만큼 $O(N^2)$가 소요된다.

SendersKey. 그룹 메시지 전송 시 모든 그룹멤버와 공유하는 하나의 키로 암호화하면 효율적이다. SendersKey 방식은 멤버 고유의 그룹키를 사용하여 그룹 메시지 전송 시 암호화 횟수를 그룹원 수에 관계없이 한 번으로 감소시켜서 O(1)의 복잡도를 갖는다. 그룹키는 그룹원이 각자 랜덤으로 선택한 비밀키를 사용하고, 송신자는 자신의 sender key로 메시지를 암호화한 후 그룹 멤버들에게 전송한다. 그룹원이 N명일 때 N개의 sender key를 사용한다. 메시지를 수신한 멤버는 송신자의 sender key로 메시지를 복호화한다.

멤버 고유의 그룹키인 Sender Key를 그룹 멤버들과 공유하기 위하여 멤버는 그룹키를 생성해서 다른 멤버들에게 일대일키로 각각 암호화하여 전달한다. Sender key 분배 시 암호화 횟수는 각 멤버당 N-1번이다. 멤버들의 가입 또는 탈퇴로 그룹키 업데이트로 소요되는 복잡도는 O(N)이다. 그룹 메시지 전송은 그룹키 갱신보다 빈번히 일어나므로 pairwise 방식보다 효율적이다.

Tree. SendersKey 방식에서 그룹 메시지 전송 시 암호화 횟수는 유지하고 그룹키 분배 시 암호화 횟수를 감소시켰다. 이를 위해 트리구조를 사용하여 그룹키 관리를 한다. Tree 최하단 노드들에는 각 멤버들을 대표하는 비대칭키를 위치시키고, 최상단 루트 노드에 이르기까지 조상 노드들의 값을 일련의 공식으로 계산해서 tree를 완성한다. Tree 구조의 장점을 활용해서 그룹키를 업데이트 시에 복잡도를 O(N)에서 $O(\log_2 N)$으로 대폭 낮추었다.

Table 1의 tree에서 CD의 개인키는 멤버 C, D가 공유한다. 그룹키 분배 시 공유 개인키에 대응하는 공개키로 암호화하여 암호화 횟수가 감소한다. A는 멤버 C, D에게 CD의 공개키로 암호화된 그룹키를 전달한다.

2.2 보안 요구사항

메신저 그룹 통신과 그룹키 분배 방식에서 반드시 필요한 보안 요구사항들은 첫 번째, 메시지는 해당 그룹에 속한 멤버들만 작성하고 열람해야 한다. 두 번째, 전송되는 메시지 위변조 방지를 보장해야 한다. 세 번째, 복제된 메시지를 구분해서 중복된 메시지는 수신을 방지한다. 이상, 네트워크 통신 프로토콜들에 공통적인 세 가지 보안 요구사항들 외에 메시지 그룹 통신에서 필요한 요구사항들이 네 가지 있다.

- 중앙 서버에 대한 기밀성 (Confidentiality to a middleman server)

: 그룹키 분배를 담당하는 중앙 서버는 비그룹원

이므로 그룹키 접근이 불가하다. 서버에 노출되지 않은 키로 그룹 메시지를 암호화해야 한다. 그룹키 분배과정에서 서버에 그룹키가 노출되지 않도록 한다.

• 권한 검증 (Verification of Permissions)

: 권한이 없는 사용자로부터 메시지의 위변조 방지를 보장해야 한다. 그룹 메시지는 그룹 멤버십을 소유한 그룹원이 작성해야 한다. 송신자 인증을 통해 그룹원 간 송신자 사칭을 방지해야 한다. 그룹원 모두가 공유하는 그룹키는 그룹원 증명이 가능하지만 송신자 인증은 수행하지 못한다. 각 멤버는 그룹키 외에 서명용 키를 보유해야 한다.

초대 및 탈퇴 메시지 수신 시 송신자의 작성 권한 검증 후 수락해야 한다. 메신저 서비스는 그룹장을 선택하여 구현한다. 최초의 그룹장은 그룹을 만든 사용자이다. 그룹장이 다른 그룹원을 그룹장으로 지정하여 권한을 부여한다. 그룹장은 그룹원 초대, 강제 탈퇴 권한을 가진다. 초대 또는 강제 탈퇴 메시지의 수신자는 송신자가 그룹장인지 검증해야 한다. 그룹장이 없는 서비스의 경우 초대 메시지 작성 권한은 그룹원이 가지고 강제 탈퇴 메시지는 작성하지 못한다. 자진 탈퇴 메시지는 송신자가 탈퇴 당사자인지 검증해야 한다.

• 전방향 보안 (Forward secrecy)

: 현재의 세션이 침해되더라도 과거의 세션은 비밀 유지되어야 한다. 새로 초대된 멤버는 현재 세션의 그룹키를 알고 있지만 그룹에 초대되기 전의 그룹 메시지의 열람 및 작성이 불가해야 한다. 새로 초대된 멤버는 새로 갱신한 그룹키로 이전 그룹키를 유추하지 못해야 한다.

• 후방향 보안 (Post-compromise security)

: 현재의 세션이 침해되더라도 미래 세션의 비밀 유지를 보장해야 한다. 탈퇴한 멤버는 그룹 탈퇴 이후에 그룹 메시지의 열람 및 작성이 불가해야 한다. 탈퇴한 멤버가 알고 있는 세션의 그룹키로 이후의 그룹키를 알아내지 못해야 한다.

• 송신 및 수신 부인 방지 (Non-repudiation of delivery and receipt)

: 수신자는 메시지 수신 후 송신자가 전송 사실을 부인하지 못하도록 인증할 수 있어야 한다. 송신자는 수신자가 메시지 열람 후 수신 사실을 부인하지 못하도록 인증하는 수신 부인 방지를 만족해야 한다. 통신 당사자 중 누구도 부정행위를 하지 못하도록 공정성을 제공해야 한다.

III. MLS 동작 과정

MLS는 그룹통신에서 종단간 보안을 제공하는 프로토콜이다. 그룹통신의 보안 요구사항들을 만족하기 위하여 메시지들 그룹키로 암호화해서 전송하여 중계서버가 그 메시지 열람이 불가한다. 더불어 메시지는 송신자의 개인키로 서명을 해서 인증과 부인방지를 제공한다. 다음은 MLS의 주요 기능인 멤버 초대 및 탈퇴에 따른 그룹키 관리 과정을 서술한다.

3.1 서비스 가입

사용자는 최초 사용 시 일 회 서비스에 가입한다. 신규 사용자는 ID를 할당받은 후 서명용 비대칭키 쌍을 생성해서 공개키는 서버에 등록하고 개인키는 보관한다.

3.2 그룹 생성

한 사용자가 그룹을 생성하고 대화상대들을 그룹에 초대해서 그룹 멤버를 구성한다. 멤버들은 그룹에 고유한 자신의 그룹키 분배용 비대칭 키 쌍을 생성한다. 이로서 멤버들은 서명용 그리고 분배용 비대칭키 두 쌍을 소유한다.

MLS에서 그룹키는 Tree 방식으로 관리되고 그룹 멤버들은 동일한 하나의 분배용 트리를 보유한다. 분배용 트리는 왼쪽균형이진트리 (left-balanced binary tree)의 일종으로, 초대 멤버들은 빈 말단 노드들 중 가장 왼쪽부터 채워진다. Fig. 1-I의 예시와 같이, 분배용 tree에는 그룹 멤버들이 말단 노드에 위치하고 말단 노드를 제외한 기타 노드들은 그룹키 관리를 위한 가상의 노드들이다.

두 종류 노드들의 또 다른 차이점은 각 노드가 보유한 비대칭키 쌍의 갯수와 종류이다. 말단 노드는 그룹키 분배용 비대칭키 쌍{$PR_{dist①}$, $PU_{dist①}$}과 서명용 비대칭키 쌍을 {$PR_{sign①}$, $PU_{sign①}$} 보유하는 반면, 비말단 노드는 그룹키 분배용 비대칭키 한 쌍을 가진다. 그룹키 분배용 비대칭키 쌍은 갱신된 그룹키를 암호화하여 멤버들 간에 전송하는 용도로 사용된다. 서명용 비대칭키 쌍은 그룹키 관리에 필요한 메시지를 전달할 때 서명용으로 송신자를 인증한다.

루트 노드가 소유한 분배용 개인키로 (PR_{distGK}) 그룹키를 결정한다. 동일한 분배용 트리를 보유한 멤버들은 동일한 그룹키를 공유한다. 말단 노드는 자신

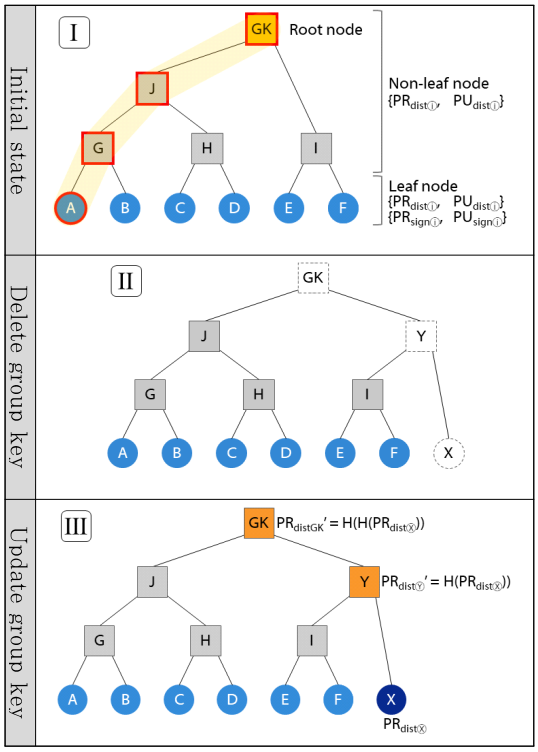

Fig. 1. Tree structures while A invites member X. Leaf nodes where members are placed are circled, and non-leaf nodes are marked with rectangles. Members performing updates are shown in dark blue, and updated non-leaf nodes are shown in orange. The updated key is marked with prime (′). Nodes that do not have key are indicated by dotted borders.

에서 루트 노드까지 최단 경로에 위치한 중간 노드들의 분배용 개인키를 소유한다. 예를 들어 Fig. 1-Ⅰ의 멤버 A는 노란색 하이라이트 된 경로에 있는 노드 A, G, J, GK의 분배용 개인키를 소유한다. 모든 노드의 공개키는 전체 그룹원에 공유된다.

멤버는 자의 또는 타의에 의해 그룹을 탈퇴할 수 있다. 초대 또는 탈퇴로 그룹 멤버에 구성이 변하면 그룹키를 반드시 갱신해야 한다. 초대 시에는 새 멤버가 이전의 대화 내용을 열람하지 못하기 위함이다. 탈퇴 후에 대화 내용을 열람하지 못하도록 탈퇴 멤버를 제하고 그룹키를 갱신한다.

3.3 그룹 초대

신입 멤버를 초대하는 과정의 이해를 돕기 위하여 Fig. 1의 분배용 트리와 Fig. 2의 메시지들로 예를

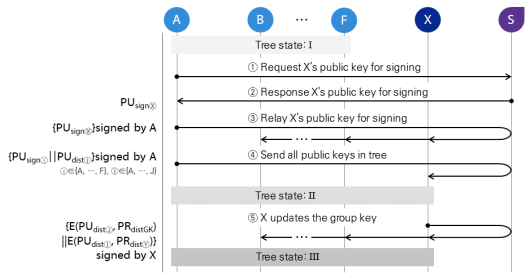

Fig. 2. The process by which A invites X. Invited member X performs group key update. S is the server and the ree state corresponds to Ⅰ, Ⅱ, Ⅲ in Fig. 1, respectively.

들어 설명한다. 그룹에는 A에서 F까지 총 6명의 멤버가 있고, 멤버 A가 새 멤버 X를 초대하는 예시이다. 멤버들은 공통으로 그룹 멤버 전원의 서명용 공개키와 Fig. 1-Ⅰ의 분배용 트리를 보유한다. 각 멤버는 자신이 위치한 말단 노드에서 루트 노드를 연결하는 최단 경로에 위치한 중간 노드의 분배용 개인키들도 보유한다.

Fig. 2의 메시지 ①에서 메시지 ④는 멤버 초대에 필요한 4개의 메시지들이다. 초대자 멤버 A는 초대받은 X의 서명용 공개키를 Fig. 2의 메시지 ①로 서버에 요청해서 메시지 ②로 받는다.

멤버 A는 Fig. 2의 메시지 ③과 같이 X의 ID와 X의 서명용 공개키를 포함한 메시지를 작성하여 그룹원에 X를 초대하였음을 알리고, 신입 멤버 X에게는 그룹에 초대되었음을 알린다. 초대 메시지를 수신한 멤버들은 그룹키 업데이트를 위해 현 그룹키를 삭제하고 각자 분배용 트리에 새 멤버 X를 왼쪽균형이진트리 구조에 맞추어 추가한다. 그룹의 분배용 트리는 Fig. 1-Ⅱ와 같다.

초대자 A는 신입 멤버 X에게 분배용 트리 구조와 트리에서 공유된 키 등, 그룹정보 메시지를 Fig. 2의 메시지 ④로 전달한다. 그룹정보 메시지는 1) 현재 그룹 멤버 전원의 서명용 공개키, 2) Fig. 1-Ⅰ의 분배용 트리에서 그룹키를 삭제한 분배용 트리, 3) 모든 노드들의 분배용 공개키이다. 신입 멤버 X는 A로부터 수신한 분배용 트리에 자신을 추가하고 왼쪽균형이진트리를 완성하기 위해 중간 노드 Y를 추가하면 다른 멤버들과 동일한 Fig. 1-Ⅱ과 같은 분배용 트리를 가지게 된다.

마지막으로 공석의 루트 노드를 생성해서 그룹키를 갱신한다. 그룹키 갱신은 새 멤버가 초대된 이후 최초 메시지를 전송하는 멤버가 수행한다.

3.4 그룹 탈퇴

멤버는 자진 탈퇴하거나 강제 탈퇴 될 수 있다. 멤버가 그룹을 탈퇴하면 그 사실을 그룹 멤버들에게 전달한다. 자진 탈퇴의 경우는 탈퇴 멤버 자신이 메시지를 전달하고, 강제 탈퇴의 경우는 탈퇴시키는 멤버가 그룹 멤버들에게 메시지를 전달한다. 탈퇴 메시지 전달 이후 과정은 자진 또는 강제의 경우 모두 동일한다.

Fig. 3-Ⅰ V는 7명으로 구성된 그룹의 분배용 트리이다. 이 그룹에서 멤버 A가 탈퇴하는 예시를 들어 설명한다. A의 탈퇴 메시지가 전송되면 그룹 멤버들은 분배용 트리를 갱신한다. 멤버 A가 개인키를 소유한 말단 노드, 루트 노드 (GK), 중간 노드들 (G와 J)의 분배용 비대칭키를 분배용 트리에서 삭제한다 (Fig. 3-V 참조). 이후 최초 메시지를 전송

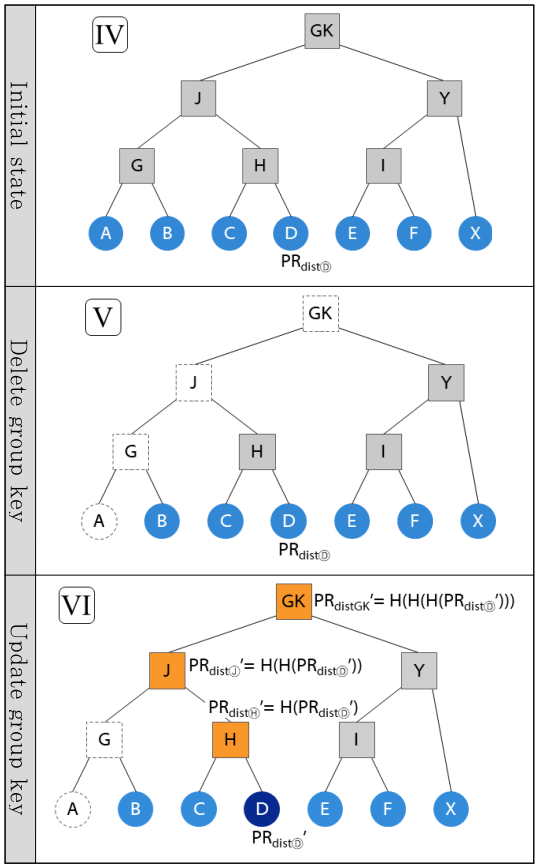

Fig. 3. The figure shows the tree structure during A was leaving. In Ⅳ, member D updates the group key.

하는 멤버에 의해 그룹키가 갱신이 되면 탈퇴 멤버A는 더 이상 메시지를 열람할 수 없다.

3.5 그룹키 갱신

그룹키 유효기간 만료 시 그리고 그룹원 변동 시에 그룹키가 갱신된다. 그룹키 갱신 조건 발생 이후 최초 메시지를 보내는 멤버가 그룹키 갱신을 주도한다.

그룹키 갱신은 Fig. 1-Ⅲ에서 X가 그룹키를 업데이트하는 경우를 예시로 설명한다. Fig. 1-Ⅲ은 새 멤버 X가 그룹에 초대된 직후의 분배용 트리 구조를 나타낸다. 멤버 X는 이 그룹에서 자신이 사용할 분배용 비대칭키 쌍을 생성한다. X의 조상 노드 Y와 GK의 분배용 비대칭키 쌍도 X가 생성해서 다른 멤버들에게 전달한다. 부모 노드의 개인키는 자식 노드의 분배용 개인키를 해시하여 생성한다. 노드 Y의 개인키는 노드 X의 개인키를 ($PR_{distⓍ}$) 해시한 값 $Hash(PR_{distⓍ})$ 이고, 루트 노드 GK의 개인키는 $Hash(Hash(PR_{distⓍ}))$이다. 루트 노드의 분배용 개인키를 그룹키로 사용한다.

그룹키를 포함하여 갱신된 정보를 다른 그룹 멤버들과 공유한다. X는 갱신된 그룹키를 Fig. 2의 메시지 ⑤에 그룹원들의 분배용 공개키들로 암호화해서 공유한다. 복호화는 멤버들이 소유하고 있는 자신에서 루트 노드 사이에 위치한 중간 노드들의 분배용 개인키로 한다. 멤버들 각각의 공개키로 암호화해서 전송하면 복잡도는 O(N)이 된다. 멤버들이 공유하는 최상위 노드의 공개키로 암호화해서 전송을 하면 복잡도는 $O(\log_2 N)$으로 감소한다.

Fig. 1-Ⅲ에 나타난 것처럼, 멤버 A, B, C, D는 노드 J의 분배용 개인키를 공유한다. 멤버 X는 갱신된 그룹키를 멤버 A, B, C, D 각각의 공개키로 암호화해서 전송하는 대신 멤버 A, B, C, D의 공통 조상인 멤버 J의 공개키로 암호화해서 한번 전송한다. 이때 전송하는 메시지를 $E(PU_{distⒿ}, PR_{distGK})$로 표시한다. 즉, 그룹키 (GK)인 루트 노드의 개인키 PR_{distGK}를 노드 J의 분배용 공개키 $PU_{distⒿ}$로 암호화한다는 의미이다.

멤버 E,F에게는 루트 노드의 분배용 개인키와 중간 노드 Y의 분배용 개인키를 전달해야 한다. 멤버 E,F의 공통 조상 노드 I의 분배용 공개키로 암호화한 노드 Y의 분배용 개인키를 전달하고 $E(PU_{distⒾ}, PR_{distⓎ})$로 표시한다. 멤버 E,F는 노드 Y의 분배용

개인키를 복호화하고 이를 해시해서 루트 노드의 분배용 개인키를 도출한다.

Fig. 1-VI은 멤버 A의 탈퇴 이후 멤버 D가 그룹키를 갱신하는 과정이다. 멤버 D는 자신과 조상 노드 H, J, GK의 비대칭키 쌍을 갱신한다. 멤버 A가 탈퇴한 말단 노드와 상위 중간 노드는 left-balanced tree 정의에 위배되더라도 공석으로 남겨둔다 (Fig. 1-VI의 노드 A와 G). 이 노드는 새 멤버 초대 시 우선적으로 채워진다.

3.6 그룹 메시지 전송

멤버는 메시지를 비밀키로 암호화하고 서명용 개인키로 서명한 후 전송한다. 비밀키는 그룹키와 각 멤버의 ID에서 파생된다. 비밀키를 멤버의 ID값을 포함시켜 계산해서 멤버마다 다른 비밀키를 갖는다. 그룹키도 메시지마다 변경이 되는데, 다음 메시지에 사용할 그룹키는 현재 그룹키를 해시해서 생성한다. 사용한 비밀키는 폐기한다. 메시지를 재전송하여도 그 메시지에 사용한 비밀키는 폐기되었으며 현재 순번의 키로는 복호화되지 않으므로 재전송을 방지한다.

송신자는 그룹 멤버들의 물리적 위치를 알지 못하여 직접 멤버들과 종단간 연결을 맺지 못한다. 멤버들의 위치를 알고 있는 중계 서버에게 TLS연결을 맺어서 메시지를 보내면, 서버는 멤버들과 각각 TLS연결을 맺어서 메시지를 중계한다. 메시지는 일차적으로 그룹키를 암호화되어 있고 이차적으로 TLS로 암호화되어 멤버들에게 전달된다.

IV. 보안 분석

메신저 그룹 통신의 7가지의 보안 요구사항을 MLS가 어떻게 준수하고 있는지 검토한다.

재전송 방지는 메시지를 암호화에 사용하는 비밀키를 메시지 전송 시간별로 그리고 멤버별로 변경을 해서 준수한다. 이전에 수락된 메시지를 재전송하여도 이미 비밀키가 변경되어 수신하는 멤버들이 수락하지 않는다. 또한, 그룹원 외에 메시지 열람을 방지하기 위해 MLS는 그룹 멤버만 소유한 그룹키로 그룹 통신을 1차로 종단간 암호화한다. 2차로는 TLS 연결로 그룹 통신을 보호한다. 2중의 암호화 연결로 그룹원 외에 메시지 열람은 거의 불가하다.

4.1 중앙 서버에 대한 기밀성

일반적으로 메신저 그룹 통신은 중계 서버를 맹목적으로 신뢰한다. 그룹 통신 종단간 암호화 적용에도 서버에서 메시지 열람 또는 국가기관에서의 감청의 목적에 의해 그룹 메시지를 열람할 수 있다. 또한, 일탈한 서버 관리자에 의해서도 메시지는 열람될 수 있다.

중계 서버에서 그룹 메시지를 열람하는 공격자 curious admin을 가정한다. Admin은 서버의 TLS 개인키에 접근할 수 있고, 이 키로 사용자와 서버 간 TLS를 해제한다. Curious admin은 멤버들의 공개키를 위조해서 공개키로 암호화된 그룹키를 열람한다. 본 논문은 curious admin attack 가능성을 제시하고 MLS에서 공격 과정을 5장에서 설명한다.

4.2 권한 검증 및 송수신 부인방지

송신자는 메시지에 서명용 개인키로 서명해서 전송한다. 수신자는 인증을 검증해서 송신자를 인증하고 송신자가 메시지 작성 권한 여부를 확인한다. 이 서명으로 추후 송신자는 송신 사실을 부인하지 못한다. 그렇지만, 수신자의 메시지 열람을 인증하지는 못한다. 수신 부인방지 프로토콜을 MLS에 적용 시 수신 증명을 위한 추가 오버헤드 발생과 신뢰할 수 있는 제삼자에 의존하는 문제점 해결이 선행되어야 한다[7].

4.3 전방향 보안

신입 멤버가 초대 이전의 그룹 메시지를 열람하지 못하도록 이전 그룹키를 폐기한다. 폐기하는 그룹키를 도출할 때 사용되었던 분배용 비대칭키도 함께 폐기한다. MLS는 새로 초대된 멤버에게 이전 그룹키를 노출하지 않는 전방향 보안을 만족한다.

4.4 후방향 보안

탈퇴한 멤버가 메시지를 열람하지 못하도록 그룹키와 탈퇴 멤버의 조상 노드의 분배용 비대칭키들을 폐기한다. 새 그룹키로 업데이트 시 그룹키를 암호화하는 분배용 비대칭키를 모르는 탈퇴 멤버는 그룹키 업데이트 메시지를 수신해도 그룹키를 복호화하지 못

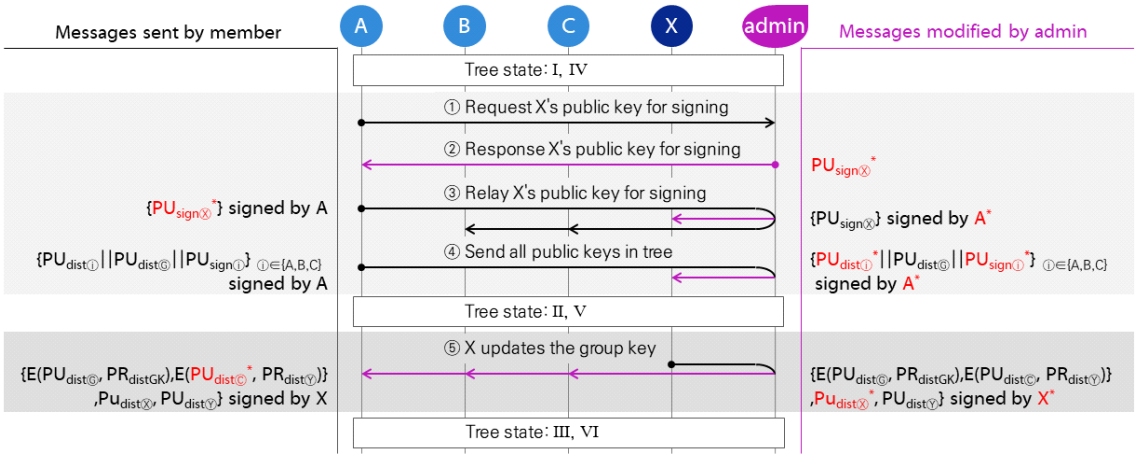

Fig. 4. The process is represented in which the Curious admin obtains a public key during the invitation and group key update. The left side is the message sent by the member, and is marked with a black arrow. The purple arrow is a modified message by the admin, and its content is on right side.

한다. 탈퇴한 멤버는 이후 그룹키를 획득할 수 없어 후방향 보안을 만족한다.

V. 중앙 서버에서 Curious Admin 공격

MLS는 보안 요구사항들은 서버를 신뢰한다는 가정을 전제로 한다. 서버의 신뢰가 담보되지 않는 특별한 경우에는 서버를 통제할 수 있는 관리자에 의해 메시지 열람이 가능한 것을 확인하였다.

Curious administrator는 본인이 관리하는 서버가 중계하는 그룹에 통화 내용이 궁금한 서버 관리자이다. Curious admin이 특정 그룹에 메시지 열람을 위해서는, 그룹 통신에 적용된 2중의 암호를 해제해야 한다. 겉의 암호는 TLS연결로 서버의 개인키로 해제할 수 있다. TLS연결에 사용하는 서버의 개인키와 멤버들이 가입시 서버에 보관하는 서명용 공개키 등에 접근이 가능하다. 속의 암호는 그룹키를 알아야 해제할 수 있는데, 이는 그룹키 갱신 시 서버에 보관된 멤버들의 서명용 공개키를 조작해서 그룹키를 획득할 수 있다.

Curious admin 공격은 신입 멤버의 비대칭키 쌍을 관리자가 위조해서 기존 멤버들에게 전달하고 또한 기존 멤버들의 비대칭키 쌍을 위조해서 신입 멤버에게 전달한다. 멤버 중 한 명이 그룹키를 갱신 시에 관리자가 그룹키를 열람할 수 있는 일종의 중간자 공격이다. MLS에서 공개키 쌍을 전달할 때 송신자를 별도로 인증하지 않기 때문에 중간자 공격이 가능하다.

Fig. 5는 멤버 A, B, C가 참여한 그룹에 새 멤버 X가 초대되어 멤버 A가 그룹키가 갱신되는 과정의 총 5개의 메시지를 도식화한 그림이다. Fig. 4는 그룹키가 갱신되면서 멤버들의 분배용 트리가 변경되는 과정을 보여준다. 좌측 열은 기존 멤버들의 분배용 트리이고 우측 열은 신입 멤버의 분배용 트리이다. 신입과 기존 멤버들 간에 분배용 트리가 다른 이유는 curious admin의 조작에 기인한다. 사용한 기호 및 수식은 Table 3에 정리하였다.

Table 3. Description of formulas and symbols

Symbol	Description
$PU_{dist\ⓘ}$	Public key for distribution owned by node ⓘ
$PR_{dist\ⓘ}$	Private key for distribution owned by node ⓘ
$PU_{dist\ⓘ}^{*}$	Public key for distribution of node ⓘ manipulated by admin
$E(PU_{dist\ⓘ}, Msg)$	Encrypt the message Msg with the public key for distribution of node ⓘ
{Msg}signed by ⓘ	Sign the message Msg with the private key for signing of node ⓘ

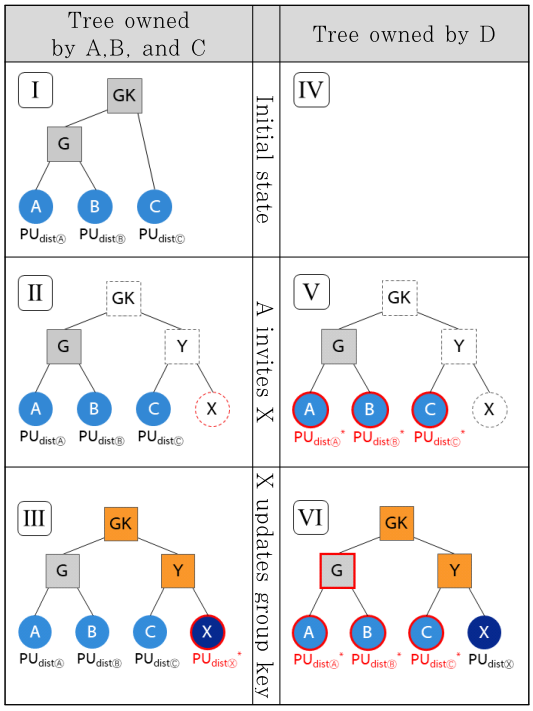

Fig. 5. When member A invites D, the tree structure during the curious admin attack is shown. Forged nodes are indicated by a red border, and forged keys are marked with a star sign (*) and red.

5.1 공격 과정

공격은 그룹에 신입 멤버가 가입 시 개시한다. 개시 직전에 기존 멤버 A, B, C의 분배용 트리는 Fig. 5-I과 같다. 신입 멤버 X가 가입한 후 최초 메시지 전송자 멤버 A는 그룹키를 갱신하기 위해 X의 서명용 공개키를 서버에 요청한다. 관리자는 추후 X가 송신할 메시지를 변조하기 위해 위조한 X의 서명용 공개키 $PU_{sign\text{Ⓧ}}{}^{*}$를 Fig. 4의 ②번 메시지로 A에게 응답한다.

멤버 A는 위조된 X의 서명용 공개키 $PU_{sign\text{Ⓧ}}{}^{*}$를 그룹 멤버에게 Fig. 4의 ③번 초대 메시지와 같이 전달한다. 멤버 A는 자신의 서명용 개인키로 ③번 메시지를 서명한다. 이 메시지 안에 포함된 위조된 공개키가 멤버 X에게 전달되면 공격이 실패한다. 관리자는 ③번 메시지 내 X의 위조된 공개키를 X의 정상 서명용 공개키로 수정하고 관리자가 위조한 A의 서명용 개인키 $PR_{sign\text{Ⓐ}}{}^{*}$로 ③번 메시지를 서명한다.

멤버 A는 X에게 Fig. 4의 ④번과 같이 분배용 트리, 그룹 멤버 A, B, C의 분배용 및 서명용 공개키, 가상 노드 G의 분배용 공개키를 포함한 그룹 정보 메시지를 전달한다. 중간자 공격을 위해서 관리자는 분배용과 서명용 공개키를 위조하여 X에게 전달한다. ④번 메시지도 ③번 메시지와 같이 위조한 A의 서명용 개인키 $PR_{sign\text{Ⓐ}}{}^{*}$로 서명한다. 이후 멤버 X는 Fig. 5-V를 트리로 소유한다. 기존 멤버들은 관리자가 위조한 신입 멤버의 분배용 공개키를 가지고 있고 신입 멤버는 관리자가 위조한 기존 멤버들의 공개키를 가지고 있다.

이후 최초 메시지 송신자가 그룹키를 갱신하는데 신입 멤버 X가 갱신을 실행하는 예로 다음에 설명한다. 그룹키 갱신을 위해 멤버 X는 자신의 분배용 비대칭키 쌍을 생성하고 조상 노드 Y, GK의 분배용 개인키를 자신의 개인키로부터 각각 계산한다.

멤버 X는 새 그룹키를 멤버 A, B와 공유하기 위해 루트 노드 GK의 개인키를 G의 공개키 $PU_{dist\text{Ⓖ}}{}^{*}$로 암호화하여 Fig. 4의 메시지 ⑤로 전달한다. 멤버 C에게는 노드 Y의 개인키를 C의 분배용 공개키 $PU_{dist\text{Ⓒ}}{}^{*}$로 암호화하여 메시지 ⑤로 전달한다. 그룹키를 갱신하는 Fig. 4의 ⑤번 메시지는 X의 서명용 개인키로 서명하여 전달한다.

관리자는 ⑤번 메시지를 $PR_{dist\text{Ⓖ}}{}^{*}$로 복호화 해서 멤버 Y의 분배용 개인키와 그룹키인 GK의 개인키를 획득한다. 기존 멤버 A와 B는 가상 노드 G의 공개키를 $PU_{dist\text{Ⓖ}}$로 알고 있으므로 관리자는 X가 A와 B에게 보낸 메시지를 $PR_{dist\text{Ⓖ}}{}^{*}$로 복호화 한 후 $PU_{dist\text{Ⓖ}}$로 다시 암호화해서 중계한다. 멤버 C로 보내는 메시지도 동일하게 적용한다.

메시지 ⑤에 포함되어야 하는 또 다른 값이 멤버 X의 공개키 $PU_{dist\text{Ⓧ}}$이다. 그룹키를 갱신한 멤버가 새로운 그룹키를 멤버들의 공개키로 암호화해서 전송하기 때문이다. 자주 변하는 그룹키를 지속적으로 알려면 관리자는 신입 멤버의 개인키를 알아야만 한다. 관리자는 멤버 X가 랜덤하게 생성한 개인키 $PR_{dist\text{Ⓧ}}$를 알 수 없다. 대신, 관리자 본인이 알고 있는 개인키로 변경해서 기존 멤버들에게 보내야 한다. 그룹키 갱신을 마치면 기존 멤버들과 신입 멤버의 분배용 트리 구조는 각각 Fig. 5-III, Fig. 5-VI과 같다. 결과적으로, 멤버 X는 그룹 내 다른 멤버들의 공개키를 관리자가 조작한 것으로 알고 있고, 기존 멤버들도 멤버 X의 공개키를 관리자가 조작한 것으로 알고 있다. 루트 노드 GK와 중간 노드 Y의 공개키는 기

존과 신입 멤버가 동일한 값을 지닌다.

5.2 공격의 복잡도

Curious admin 공격을 통해 관리자는 그룹 업데이트를 수행한 멤버가 생성한 그룹키를 획득한다. Curious admin 공격 이전의 기존 멤버 수를 N, 공격 이후 초대된 멤버의 수를 M명이고 tree가 full인 상태라고 하자. 공격 이전에 그룹에 있던 멤버 간에 같은 종류의 트리를 소유한다. 공격 이후 초대된 멤버는 자신 외 말단 노드의 키가 위조된 것으로 구성된 트리를 보유하여 각각 다른 종류의 트리를 소유한다. 전체 트리 종류는 M+1개이다. 관리자가 유지해야 하는 위조한 키 쌍은 말단 노드의 서명용과 분배용 비대칭키 쌍으로 각각 N+M개이다.

관리자가 갱신된 그룹키 획득을 위해 그룹키가 갱신될 때마다 재서명하여야 하는 횟수는 초대된 멤버가 증가할수록 그룹원이 많을수록 늘어난다. 재암호화가 필요한 횟수는 최대 1번, 재서명 횟수는 최대 2log2(N+M)-1이다.

VI. 논 의

Curious admin 공격은 각 그룹원의 공개키 전달 시 소유자 인증이 없고 서버를 통해 전달하기 때문에 발생한다. 공격은 다음 세 가지 방법으로 관리자에 대한 신뢰 가정을 완화하여 해결할 수 있다.

- 문자, 이메일 등의 제2의 채널을 사용하여 서버를 통하지 않고 공개키 직접 전달
- 블록체인 (block chain), Web of trust 등으로 공개키에 대한 신뢰 생성
- 신원기반 암호 (Identity-Based Encryption, IBE)와 같이 신원에 고정적인 공개키의 사용

제2의 채널을 사용하여 공개키를 전달하는 방식은 서버의 개입을 제외하여 서버에 의한 위조를 방지한다. 이 방법을 사용할 시 그룹 멤버 A가 신입 멤버 X를 초대하려면 반드시 X가 공개키를 직접 전달해 주어야 한다. X가 오프라인일 경우 X가 응답할 때까지 기다려야 하는 단점이 있다. 그러나 서버가 추가로 운영해야 하는 시스템에 대한 부담이 적다.

블록체인, Web of trust 등을 통해 공개키의 유효성을 증명하는 방식이 있다. 초대자 A는 신입 멤버 X의 공개키를 서버에서 전달받고 공개키가 유효한 것인지 확인한다. [8]은 공개키의 등록 정보를 블록체인을 통해 공개적으로 관리하고 변조 여부를 주기적으로 확인하여 공개키 무결성을 보장한다. 무결성 확인을 위한 추가적인 오버헤드가 발생하지만, 신입 멤버가 오프라인에 있어도 초대할 수 있다.

공개키를 지정된 신원으로 사용하는 방식인 신원기반 암호[9]를 사용하면 공개키로 휴대폰 번호나 이메일 주소를 사용하면 그룹 초대 시 공개키 요청과정이 생략된다. 초기 IBE 연구는 중앙 기관에서 개인키를 분배하는 방식으로 운용되었다. 중앙 기관이 키를 생성하는 방식은 종단간 암호화의 목적에 위배된다. 중앙 기관에 의존하지 않는 개인키를 생성하는 기법이 연구되고 있다.

VII. 결 론

MLS는 그룹 통신의 종단간 암호화를 위한 새로운 표준이다. MLS는 비대칭키 쌍으로 이루어진 Tree 구조를 사용하여 키 분배를 효율적으로 수행한다. 그룹키 관리에 필요한 시간 및 자원 절약으로 확장성을 제공한다.

그룹 통신에 필요한 보안 요구사항을 식별하고 MLS의 보안점검을 수행하였다. MLS는 주요 보안 요구사항인 전방향 보안과 후방향 보안을 그룹 멤버가 변경될 시 그룹키 갱신으로 만족시킨다. 새로 초대된 멤버는 이전의 그룹키를 알 수 없다. 멤버 탈퇴 시에 탈퇴한 멤버가 알고 있는 키를 모두 삭제하여 이후 통신을 열람하지 못하게 한다.

MLS는 서버를 포함하여 그룹 통신 당사자가 아닌 제삼자의 열람을 방지하고자 종단간 암호화를 적용한다. 서버가 curious admin으로 동작하는 경우에 관리자가 각 멤버의 서명용 비대칭키 위조 및 그룹키 분배 메시지 변조로 그룹키를 획득한다. 관리자는 그룹 통신을 열람한다.

MLS는 표준화 진행에 따라 추후 메신저 서비스에서 사용될 것이다. 메신저 서비스가 MLS를 통해 종단간 암호화를 제공하여도 서버의 동작에 따라 통신이 노출될 수 있으므로 서비스 사용에 주의가 필요하다. Curious admin 공격은 서버의 개입 없이 직접 공개키를 전달 또는 공개키에 대한 제삼자의 신뢰 보증을 제공으로 공개키가 위조되지 않음을 증명하거나 고정된 공개키의 사용으로 예방할 수 있다.

References

[1] Statista, "Global number of mobile messaging users 2018-2025," Nov. 2021, https://www.statista.com/statistics/483255/number-of-mobile-messaging-users-worldwide/.

[2] M.R. Albrecht, J. Blasco, and R.B. Jensen, "Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong," Proceedings of *30th USENIX Security Symposium*, pp. 3363-3380, Aug. 2021.

[3] M. Weidner, M. Kleppmann, and D. Hugenroth, "Key Agreement for Decentralized Secure Group Messaging with Strong Security Guarantees," Proceedings of *2021 ACM SIGSAC Conference on Computer and Communications Security*, pp.2024-2045, Nov. 2021.

[4] R. Barnes, B. Beurdouche and R. Robert, "The Messaging Layer Security (MLS) Protocol draft-ietf-mls-protocol-12," Internet Engineering Task Force, Oct. 2021

[5] K. Cohn-Gordon, C. Cremers, and L. Garratt, "On Ends-to-Ends Encryption Asynchronous Group Messaging with Strong Security Guarantees," Proceedings of *2018 ACM SIGSAC Conference on Computer and Communications Security*, pp.1802-1819, Oct. 2018.

[6] P. Rösler, C. Mainka, and J. Schwenk, "More is less: On the end-to-end security of group chats in Signal, WhatsApp, and Threema," Proceedings of *2018 IEEE European Symposium on Security and Privacy*, pp. 415-429, Apr. 2018.

[7] K. Elmaghraby, and T. Dimitriou, "Blockchain-Based Fair and Secure Certified Electronic Mail Without a TTP," *IEEE Access*, Vol. 9, pp.100708-100724, Jul. 2021.

[8] M. Chase, A. Deshpande, and E. Ghosh, "SEEMless: Secure End-to-End Encrypted Messaging with less Trust," Proceedings of *2019 ACM SIGSAC Conference on Computer and Communications Security*, pp.1639-1656, Nov. 2019.

[9] V. Goyal, "Reducing Trust in the PKG in Identity Based Cryptosystems," Proceedings of *Annual International Cryptology Conference*, pp.430-447, Aug. 2007.

〈저자소개〉

권 송 희 (Songhui Kwon) 학생회원
2019년 8월: 성균관대학교 수학과 졸업
2019년 9월~현재: 성균관대학교 전자전기컴퓨터공학과 석사과정
〈관심분야〉 리버싱 엔지니어링, 인증 프로토콜 보안

최 형 기 (Hyoung-Kee Choi) 정회원
1992년 2월: 성균관대학교 전자공학과 졸업
1996년 2월: Polytechnic University in Brooklyn, NY 석사
2001년 2월: Georgia Institute of Technology in Atlanta, GA 박사
2001년 1월~2004년 12월: Cisco 근무
2004년 3월~현재: 성균관대학교 소프트웨어대학 교수
〈관심분야〉 네트워크 보안, 리버스 엔지니어링