5G 네트워크 환경에서 화상 회의에 적용가능한 인증 및 그룹 키 합의 방식의 보안 취약점 분석 및 대응 방안

최화연, 유성진*, 박영호

경북대학교, 한국전자통신연구원

choihy01@knu.ac.kr, *sj.yu@etri.re.kr, parkyh@knu.ac.kr

Cryptanalysis and countermeasures of authentication and group key agreement scheme applicable to video conference in 5G network environments

Choi Hwa Yeon, Yu Sung Jin*, Park Young Ho

Kyungpook National University, *Electronics and Telecommunications Research Institute

요 약

2020년 Luo 등은 5G 네트워크 환경에서 화상 회의에 적용가능한 도메인 간 상호 인증 및 그룹 키 합의 방식을 제안하였다. 본 논문에서는 Luo 등이 제안한 인증 및 키 합의 방식에서 제시한 공격자 모델을 통해 안전성을 분석하여 알려진 임시 키 공격에 취약함을 입증하였다. 또한, 입증한 취약점을 해결하기 위하여 3가지 대응 방안을 제안하여 합법적인 사용자에게 안전하고 효율적인 서비스를 보장하고자 한다.

Ⅰ. 서 론

최근 전 세계적으로 코로나19 팬데믹 사태를 겪으며 비대면 업무 구축의 중요성이 대두되고 있다. 따라서 코로나19로 인해 비대면으로 급격하게 변화된 비즈니스 환경에 신속하게 대응하기 위하여 공공 기관, 연구소, 기업 및 학교 등은 재택근무로 전환하고 실시간 교육 및 회의는 Google Meet, Webex 및 Zoom 등 화상회의 플랫폼을 활용하고 대면 접촉을 최소화하여 비대면 업무 시스템 구축이 활발하게 이루어지고 있다.

화상회의 대표 플랫폼인 Zoom의 경우, 작년 대비 155배 이상 사용자가 증가하면서 화상회의 플랫폼 시장이 급격하게 성장하고 있다. Zoom은 회의 당 최대 100명의 사용자가 참여할 수 있으며 회원가입 절차없이 회의 주소만 있으면 접속할 수 있어 언제 어디서나 서비스를 이용할 수 있는 것이 장점이다[1]. 그러나 화상회의 플랫폼은 악의적인 공격자에 의해 안전하지 않은 그룹 회의가 형성되거나 인가되지 않은 사용자가 회의에 참석하게 된다면 합법적인 사용자의 프라이버시를 보장할 수 없을 뿐만 아니라 다양한 보안 공격에 취약할 수 있다. 또한, 화상회의 플랫폼 서비스를 이용하기 위해 활용되는 스마트폰, 태블릿 등의 스마트 기기는 제한적인 소비 전력, 메모리 및 연산 능력을 가지므로 영상 및 음성 품질 불량, 끊김 현상 등이 발생할 수 있다. 따라서 이러한 문제점들을 해결하기 위하여 5G 네트워크 환경에서 화상회의에 적용 가능한 안전하고 효율적인 인증 및 그룹 키 합의 방식[2-3]에 대한 연구가 필수적이다.

2020년 Luo 등은[4] 5G 네트워크 환경에서 화상회의에 적용가능한 도메인 간 상호 인증 및 그룹 키 합의 방식을 제안하였다. Luo 등이 제안한 방식은 각 도메인에 속한 사용자들이 타원곡선암호 시스템을 사용하여 상호 인증을 수행하고 새로운 도메인 그룹을 만들어 안전한 통신을 보장한다. 본 논문에서는 Luo 등이 제안한 인증 및 그룹 키 합의 방식의 공격자 모델을 기반하여 알려진 임시 키 공격에 대한 보안 취약점을 증명하고 이를 보완하는 대응 방안을 제시한다.

Ⅱ. Luo 등이 제안한 인증 및 키 합의 방식

Luo 등이 제안한 인증 및 그룹 키 합의 방식은 초기화 및 실행 단계로 구성되어있으며, 본 논문에서 사용되는 매개변수는 다음 표 1과 같다.

표 1. 매개변수

기호	의미
μ_i, CG, KGC_k	그룹 사용자, 그룹 컨트롤러, 키 생성 센터
ID_i, ID_0	그룹 사용자, 그룹 컨트롤러의 아이디
sk_i, pk_i	그룹 사용자의 개인키 및 공개키
sk_0, pk_0	그룹 컨트롤러의 개인키 및 공개키
s_k, KC_k	키 생성 센터의 마스터 개인키 및 공개키
x_i, x_0	그룹 사용자 및 그룹 컨트롤러의 비밀 값
TK	그룹 세션 키
$H(\bullet)$	단 방향 해시 함수
$\|$	결합 연산
$\oplus$	XOR 연산

2.1. Luo 등이 제안한 방식의 초기화 단계

다음 그림 1은 Luo 등이 제안한 인증 방식의 그룹 사용자 및 그룹 컨트롤러의 초기화 단계이다.

Key Generation Center (KGC_k)		Group User (μ_i)/Group Controller(GC)
$s_k \in Z_q^*$		$x_i \in Z_q^*$
$\{s_k, P_k\}$		$pk_i = x_i P_k$
$KC_k = s_k P_k$		
$\{q, G, P_k, G_1, KC_k, H_1, H_2, H_3, H_4, H_5\}$		
$r_i \in Z_q^*$		
$R_i = r_i KC_k$	$\xrightarrow{\{usk_i, R_i\}}$	
$h_i = H_1(ID_i, R_i, pk_i)$		
$usk_i = r_i s_k h_i + H_1(ID_i, R_i, s_k pk_i)$		

$sk_i = usk_i - H_1(ID_i, R_i, x_i \cdot KC_k)$
$sk_i P_k = h_i R_i$
$\{sk_i, x_i\}$
$\{pk_i, R_i\}$
$sk_0 = (x_0 + r_0 s_i h_0) \bmod q$
$pk_0 = sk_0 P_0$

그림 1. Luo 등이 제안한 그룹 사용자 및 그룹 컨트롤러 초기화 단계.

2.2. Luo 등이 제안한 방식의 실행 단계

다음 그림 2는 Luo 등이 제안한 인증 방식의 실행 단계이다.

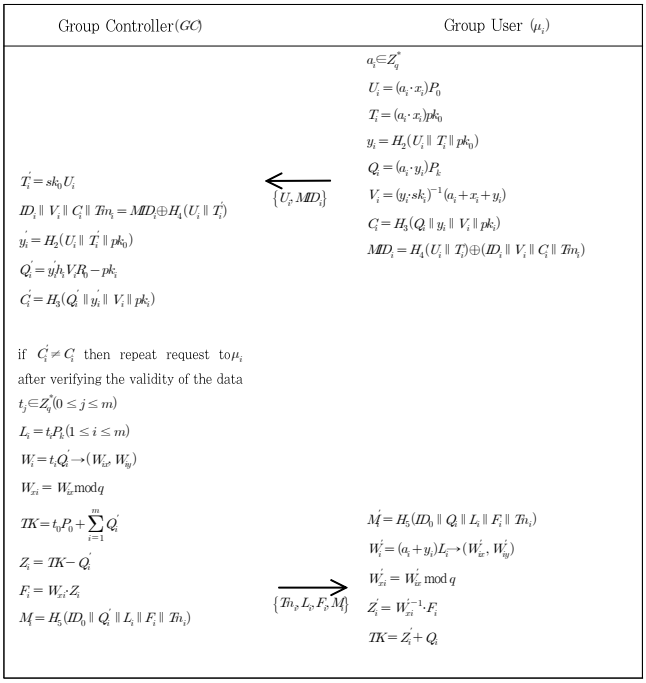

그림 2. Luo 등이 제안한 방식의 실행 단계.

Ⅲ. Luo 등이 제안한 방식의 공격자 모델

3.1. 공격자 모델 타입 A_1

악의적인 공격자는 합법적이지 않은 사용자로 그룹 사용자의 비밀 값 x_i와 그룹 컨트롤러의 비밀 값 x_0를 얻을 수 있다.

3.2. 공격자 모델 타입 A_2

악의적인 공격자는 악의적인 키 생성 센터로서 키 생성 센터의 마스터 개인키 s_k를 얻을 수 있다.

Ⅳ. Luo 등이 제안한 방식의 보안 취약점 및 대응 방안

본 논문에서는 Luo 등이 제안한 방식이 알려진 임시 키 공격에 취약하다는 것을 입증하였으며 이를 개선하기 위한 대응 방안을 제시한다.

4.1 알려진 임시 키 공격

Luo 등은 악의적인 공격자가 그룹 사용자의 랜덤 값 a_i을 얻을 수 있다고 가정했을 때 합법적인 사용자들의 인증 메시지를 성공적으로 생성할 수 없으며 그룹 키 TK 를 계산할 수 없다고 주장하였다. 그러나 본 논문에서는 Luo 등이 제안한 방식의 공격자 모델 타입 A_1을 기반하여 그룹 사용자의 비밀 값 x_i을 얻을 수 있으며 공개 채널로 송·수신되는 메시지 $\{U_i, MID_i\}$을 통해 공격자는 $T_i = (a_i + x_i) pk_0$, $y_i = H_2(U_i \| T_i \| pk_0)$, $Q_i = (a_i + y_i) P_k$을 계산할 수 있다. 또한, 악의적인 공격자는 공개 채널에서 전송되는 $\{Tn_i, L_i, F_i, M_i'\}$ 메시지를 도청하여 $W_i' = (a_i + y_i) L_i$, $Z_i' = W_{xi}'^{-1} \cdot F_i$을 계산할 수 있다. 따라서 악의적인 공격자는 그룹 세션 키 $TK = Z_i' + Q_i$를 성공적으로 계산할 수 있으므로 Luo 등의 방식은 알려진 키 공격에 취약하다.

4.2 대응 방안

Luo 등이 제안한 인증 및 그룹 키 합의 방식은 알려진 임시 키 공격에 취약하여 그룹 세션 키를 얻을 수 있다는 문제점이 있다. 이를 개선하기 위해 3가지 대응 방안을 제시한다.

- 대응 방안 1. 사용자의 패스워드 및 생체 신호를 사용한 three-factor 인증 메커니즘을 제시한다. Three-factor 인증 메커니즘 장점은 랜덤 값 및 패스워드 등 두 가지 요인이 악의적인 공격자에게 노출되더라도, 생체 신호를 얻을 수 없으므로 높은 보안 수준을 보장한다.
- 대응 방안 2. Luo 등의 방식은 사용자의 장기 비밀 키가 안전하게 마스킹되어 있지 않으며 비밀 자격증명 값이 업데이트되지 않기 때문에 심각한 보안 문제가 발생할 수 있다. 따라서 시스템의 보안을 향상시키기 위해 장기 비밀 키를 랜덤 값, 패스워드 및 생체 신호를 사용하여 안전하게 마스킹하고 비밀 자격증명 값을 주기적으로 업데이트하여 높은 안전성을 보장한다.
- 대응 방안 3. 효율적인 시스템을 구축하기 위해 타원곡선암호 시스템과 AES 대칭키 암호 시스템을 함께 사용한 하이브리드 암호 방식을 적용하여 연산량 및 통신량을 측면에서 우수한 성능을 보장한다.

Ⅴ. 결론

본 논문에서 Luo 등이 제안한 5G 네트워크 환경에서 화상 회의에 적용 가능한 인증 및 그룹 키 합의 방식의 안전성을 분석하여 Luo 등의 방식이 알려진 임시 키 공격 등에 취약함을 증명하였다. 이에 악의적인 공격자가 그룹 세션 키를 획득하여 그룹 통신에 참여할 수 있음을 보였다.

이러한 보안 취약점을 해결하기 위하여 사용자의 패스워드 및 생체 정보를 사용하여 높은 보안 수준을 제공하며 타원 곡선 암호화 방식과 대칭키 암호화 방식을 함께 사용한 하이브리드 암호 방식을 적용하여 효율적인 연산량 및 통신량을 보장한다.

향후 제안한 대응 방안을 통해 높은 안전성과 효율성을 보장하는 5G 네트워크 환경에서 화상 회의에 적용가능한 안전하고 효율적인 인증 및 그룹 키 합의 방식을 제안할 계획이다.

참 고 문 헌

[1] Archibald, M. M., Ambagtsheer R. C., Casey M. G., and Lawless M., “Using Zoom Videoconferencing for Qualitative Data Collection: Perceptions and Experiences of Researchers and Participants,” International Journal of Qualitative Methods, vol 18, pp. 1-8, 2019.

[2] Yu S. J., and Park Y. H., “SLUA-WSN: Secure and Lightweight Three-Factor Based User Authentication Protocol for Wireless Sensor Netowrks,” Sensors, vol. 20, no. 15 pp. 4143-4169, 2020.

[3] Yu S. J., Park K. S., and Park Y. H., “A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environment,” Sensors, vol. 19, no. 16, pp. 3598-3618, 2019.

[4] Luo M., Wu J., and Li X., “Cross-domain certificateless authenticated group key agreement protocol for 5G network slicings,” Telecommunication Systems, vol. 74, pp. 437-449, 2020.