디지털산업정보학회 논문지 제16권 제4호-2020년 12월
http://dx.doi.org/10.17662/ksdim.2020.16.4.055

줌의 보안 취약점 분석과 보안 업데이트 결과 비교

김 규 형*·최 윤 성**

Comparing Zoom's Security Analysis and Security Update Results

Kyuhyeong Kim·Younsung Choi

〈Abstract〉

As corona began to spread around the world, it had such a big impact on many people's lives that the word "Untact Culture" was born. Among them, non-face-to-face meetings naturally became a daily routine as educational institutions and many domestic and foreign companies used video conferencing service platforms.

Among many video conferencing service platforms, Zoom, the company with the largest number of downloads, caused many security issues and caused many concerns about Zoom's security.

In this paper, Zoom's security problems and vulnerabilities were classified into five categories, and Zoom's latest update to solve those problems and the 90-day security planning project were compared and analyzed. And the problem was solved and classified as unresolved. Three of the five parts have been resolved but are still described as how they should be resolved and improved in the future for the two remaining parts.

Key Words : Zoom Security Analysis, Video Conferencing, End-to-End Encryption, Network Security

Ⅰ. 서론

코로나19 사태가 확산되며 '언택트 문화'라는 말이 생겼으며 많은 사람들에게 큰 영향력을 미치고 있다. 사회적 거리두기가 모든 국민에게 일상화되었으며 외출 시 마스크는 필수 물품이 되었다. 이와 같이 비대면 문화가 발전하면서 교육, 산업 분야에 급격하고 많은 변화가 일어났다. 교육 부분에서는 초등학교, 중학교, 대학교의 재학생들이 기존의 오프라인 수업이 아닌 온라인으로 원격수업을 받고 있으며, 산업적인 면에서는 국내·외의 기업들이 재택근무를 진행하는 등의 비대면 문화가 보편화되고 있다. 비대면 문화를 통해 다양한 클라우드 기반 화상회의 서비스 기업들이 주목을 받고 있는데, 대표적으로 줌(Zoom) 비디오 커뮤니케이션의 줌, 마이크로소프트의 팀즈, 구글 행아웃 미트 등이 있다. 화상회의 서비스의 수요가 증가하면서 서비스 이용량이 증가했지만, 특히 줌은 하루 평균 이용자 수가 작년에 비해 40배 이상 상승했

* 인제대학교 컴퓨터공학과, 영어영문학과 복수전공(제1저자)
** 인제대학교 AI융합대학 산업보안전공 조교수(교신저자)

으며, 앱스토어에서 가장 많은 다운로드 수를 기록하기도 했다.

줌은 중국과 미국 국적을 가지고 있는 에릭 유안이 설립한 회사에서 개발되었다. 에릭 유안은 기업용 메세징 시장의 강자인 슬랙도 개발하였는데, 이는 클라우드 기반 화상회의 솔루션이며 무료와 유료 서비스를 효율적으로 매칭하여 시장을 이끌고 있다. 영국 정부는 줌으로 내각 회의를 진행했고 국내·외 기업들 또한 줌을 통해 화상회의를 개최하기도 했다. 전문가들은 줌이 설치가 간단하며 회원가입 없이 초대 링크를 통해 쉽게 화상회의를 참여할 수 있기 때문에 다른 서비스들 보다 더 많은 이용자가 사용하고 있다고 판단하고 있다. 줌은 코로나의 확산으로 큰 혜택을 받은 기업이라는 말은 과언이 아니다. 하지만 줌에 대한 관심이 늘어나는 만큼 줌의 보안에 대한 다양한 이슈가 발생하고 있다. 줌바밍(Zoom bombing)과 같은 신조어가 만들어질 만큼, 줌의 보안과 사생활 침해에 대한 우려가 세계적으로 퍼졌으며 이로 인해 사용자들이 줌을 신뢰하지 않고 사용을 하지 않은 경우도 발생하고 있다. 본 논문에서는 이처럼 줌의 보안성의 취약성에 대해 여전히 남아있는 문제를 확인해 보고자 한다[1-3].

본 논문에서는 줌에 대한 다양한 문제점과 취약성을 분석하여 '종단 간 암호화', '허약한 알고리즘, '암호화키의 중국 서버 유출', 'ios 앱 개인 정보 유출', '줌 ID 다크 웹 유통&줌바밍'로 대표되는 문제점 5가지를 분석하였다. 해당 문제들을 해결하기 위해 줌은 90일 보안 계획과 그 이후의 계속된 업데이트를 통해 문제들을 해결하기 위해 노력하였다. 이러한 줌의 노력에도 불구하고 5가지 중 3가지는 해결을 하였지만, 나머지 2개에 대해선 완벽히 보완하지 못하였다는 것을 전달하고 있다. 이에 대해 90일 프로젝트와 그 이후의 업데이트 내용들을 정리하여 비교 분석하였다. 보안상의 취약점이 완전히 해결되지 못한 부분에 대해서 보완해야 함을 전달하고자 한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서 줌과 관련된 보안 사례를 분석하고, 3장에서 줌의 보안관 관련된 5가지 문제점을 분석한다. 그리고 4장에서는 줌의 보안관련 업데이트 사항을 비교 및 분석하여 보안 이슈를 해결된 사항과 아직 해결되지 못한 부분으로 분류하여 향후 개선이 필요한 사항을 제시하고자 한다. 5장에서는 본 논문의 결론을 짓는다.

Ⅱ. 줌 보안 사례분석

2.1 줌 회원정보 다크웹 유출

보안업체 인트사이츠는 다크 웹에서 대략 2,300개 정도의 줌 사용자(이름과 비밀번호) 정보들이 포함된 데이터베이스가 공유되고 있다고 발표하였다. 다크웹은 인터넷 주소 추적이 어려운 것으로 알려져 있는데, 이곳에서 화상회의 플랫폼인 Zoom의 해킹 방법 등이 거래되고 있는 상황이다. 기존에 유출되었던 이용자들의 계정 정보를 이용하여 Zoom에 로그인 시도를 한 후, 성공한 계정들을 다크 웹에 다시 유출시키거나 PC에 악성코드를 감염시켜 줌 계정의 정보를 탈취하는 방법들이 자주 사용되고 있는 것으로 알려졌다. 회사 측은 해당 DB를 확보하게 되면 대화 내용을 염탐하거나 채팅방 운영 권한을 뺏길 수 있으니 사용자에게 보안에 대한 주의할 필요가 있다고 했다. 이와 관련해서 한 보안 전문 연구원은 "현재 다크 웹에서 유출된 줌 회원 계정 정보는 수만 건에 달한다"라며 "최근 줌 사용이 늘면서 관련 공격 게시글이 성행하고 있지만 다른 플랫폼 관련해서도 충분히 발생할 수 있는 상황"이라며 강조했다. 또한 "사용자가 줌 클라우드 보안 서비스에 올려 악성인지를 확인하기도 한다"라며 "하지만 해당 링크는 타인이 단순 검색을 통해 볼 수 있으며 이를 클릭해 링크를 타고 접속할 수 있다"라는 말을 통해 사이버 일어날 수 있는

공격 외에도 개인 사용자 단에서 발생할 수 있는 보안 위협도 경고했다. 해당 이유 등으로 인하여 미국, 대만, 독일, 인도 등 해외에서는 줌 사용을 제한하고 나섰다. 해당 사례는 많은 보안 전문가에 의해 보안성을 반드시 강화해야 한다는 지적을 받았다[4, 5].

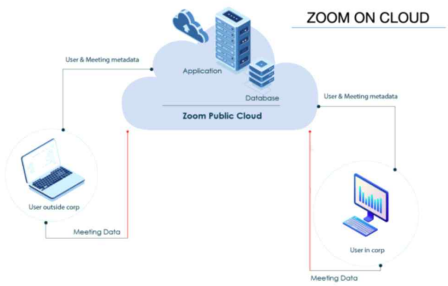
2.2 줌 바밍 & 줌 트롤링

2020년 3월 31일, IT 전문 매체 <더 인포메이션>의 창업자인 제시카 레싱과 미국의 정보기술(IT) 전문 기자 카라 스위셔는 IT 업계 여성 창업자들이 직면한 문제에 관한 대화를 나누기 위해 '줌'을 이용했다. 하지만 그들은 계정을 바꿔가며 대화방에 침입하는 해커의 음란물을 통한 방해로 대화방을 닫을 수밖에 없었다. 줌의 취약한 보안 구조를 이용하여 해커들은 화면을 가로채 음란물을 띄우고 인종차별 메시지와 욕설을 하여 전 세계에서 많은 사건이 발생하고 있다. 이는 '줌 폭격(Zoom Bombing)' 또는 '줌 트롤링(Zoom Trolling)'이라는 단어가 생길 정도로 문제화되고 있다. 그리고 마이크·웹캠 해킹을 통한 개인 privacy 침해 우려가 있어 줌을 이용했던 개인 사용자들과 학교, 기업 등에도 비상이 걸렸다. 뉴욕시는 3월 말부터 뉴욕에 거주하는 학생 110만 명을 대상으로 줌 등 다양한 화상회의 플랫폼을 이용해 원격수업을 진행했다. 하지만 CNN 방송이 4월 5일에 미국 뉴욕시는 줌을 통해 원격수업을 진행 중인 각급 학교의 해당 앱 사용을 중단하라는 지침을 내렸다고 보도되었으며, 뉴욕시 교육부 대변인인 대니얼 필슨은 "각 학교에 가능한 한 빨리 줌 사용을 중단하도록 지시했으며 직원과 학생들이 마이크로소프트의 '팀스' 등 적절한 보안 대책을 갖춘 비슷한 종류의 다른 플랫폼을 이용할 수 있도록 지원하겠다"라고 밝혔다. 이처럼 줌 트롤링의 사생활 침해 문제는 보안상으로 큰 이슈화되었다[6-8].

Ⅲ. 줌의 보안 취약점 분석

3.1 종단간 암호화 문제

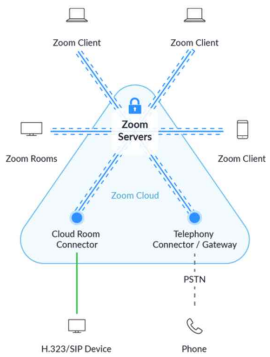
줌은 최대 100명까지 무료로 40분 동안 사용할 도 있는 public(대중) 클라우드 버전과 개인 클라우드 유료 버전으로 나누어 서비스를 제공한다. 유료버전은 사용자 관리를 제외한 Meeting Data(텍스트, 영상, 음성)를 이용자가 서버를 통해 직접 보관할 수 있는 특징이 있다. 줌은 공식적으로 두 개의 버전 모두에게 종단 간 암호화(End-to-End Encryption)를 지원한다고 발표했지만 이에 대해 많은 논란이 있다.



<그림 1> 줌 퍼블릭 클라우드 버전(무료)

대부분의 공교육 시장에서는 <그림 1>와 같은 저렴하고 무료인 퍼블릭 클라우드 버전을 주로 사용한다. <그림 2>는 줌이 공식적으로 제공한 줌의 퍼블릭 클라우드의 네트워크에 대한 개념도이다.

서버의 부하를 줄이기 위해 거의 모든 통신을 P2P(텍스트(peer-to-peer) 방식으로 처리하였던 이전 화상회의 솔루션들은 서비스 공급자의 서버로는 Meeting Data(텍스트, 음성, 화상)가 경유되지 않았다. 이와 같은 방식은 온라인 교육 관련 솔루션 또는 소규모 화상회의에서 여전히 사용되고 있다. 지금은 퍼블릭 클라우드 기반을 통해 모든 데이터를 서버에서 처리하여 대역폭 관리를 통신 사정과 최종 사용자의 단말기에 따라 최적화를 하고 있다. 이는 PC뿐만



<그림 2> 줌 무료 버전 네트워크 통신 개념도

이 아니라 스마트폰으로도 연결할 수 있도록 하였으며 많은 인원이 참여해도 회의 품질을 유지하기 위함이다. 퍼블릭 클라우드 서비스에서 보안성에 대한 중요성은 점차 강조된다. 줌은 공식적으로 E2EE를 지원하고 있다고 표명했다. 공식 자료에도 자물쇠 아이콘을 통해 <그림 3>과 같이 암호화를 제공하고 있다고 보여주고 있다.

<그림 3> HTTPS 웹 보안연결 지원하는 줌 웹사이트

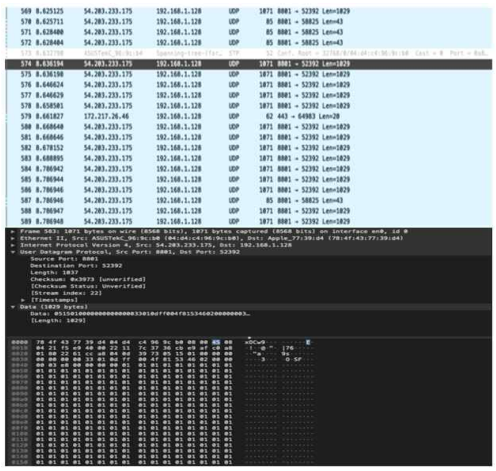
암호화가 실제로 이루어지고 있는지 확인을 해보았다. 우선 줌을 통해 네트워크 패킷 필터링을 활용하여 통신 과정을 확인해 보았다.

UDP(User Datagram Protocol)는 특성상 주로 음성/영상 전송과 같이 빠른 속도가 중요한 스트리밍 서비스에 사용된다. 또한 다중 연결(N:M, 1:N)이 가능하며 TCP보다 연결 속도가 빠른 장점이 있다. 하지만 네트워크의 여러 경로를 지나게 될 수 있는 비연결형 서비스이기 때문에 신뢰성이 TCP에 비하여 떨어진다. SSL, HTTPS를 통해 인증절차와 함께 패킷을 암호화가 가능한 TCP에 비해 UDP의 경우 DNS Spoofing이나 DNS Cache Poisoning을 통하여 암호화되어 있지 않은 데이터 패킷을 가져와서 내용을 들여다볼 수 있다.

웹브라우저를 통해 화상회의에 참여하거나 줌에 가입하고 로그인하여 화상회의를 여는 과정은 네트워크상에서 줌이 말한 종단 간(End-to-End) 암호화가 되어 있다. 회의 정보와 일반 사용자 정보와 같은 Metadata 통신은 암호화되어 있다는 것이다.

일반적으로 회원가입부터 회의 열기까지의 기능들은 모두 웹에서 가능한 기능이고 실제로 온라인 교육이나 화상회의처럼 영상과 음성 및 채팅은 별도의 앱이 실행된다. 하지만 줌의 앱에서 문제를 발견하였다.

실제로 온라인 교육 또는 화상회의 시 음성과 영상 데이터는 <그림 4>와 같이 일반적인 UDP로서 암호화되어 있지 않다는 것이 확인된다.



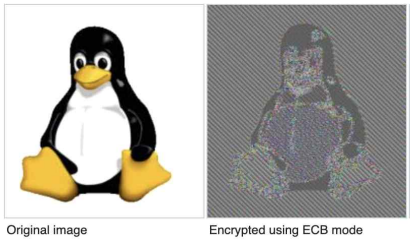
<그림 4> 암호화되지 않은 UDP 패킷 내용

회의 내용에 관련된 Meeting Data인 영상과 음성

은 암호화되어 있지 않고 User & Meeting Meta Data(맥락 데이터)의 부분만 암호화되어 있다. 이러한 영상, 음성을 이용하는 화상회의를 클라우드 상에서 암호화하여 다양한 단말기에 전송하는 것에는 기술적으로 해결하기 어렵다는 것이 현실이다. 즉, 미팅 데이터를 직접 보관하여 관리를 해주는 고가의 On-Premise(프라이빗 클라우드 버전) 버전을 구매하지 않는다면 서버를 관리하는 줌은 전 세계의 모든 회의와 관련된 데이터들을 들여다볼 수 있다. 해당 문제에 대해서 보안회사들과 여러 언론과 연구기관들은 경고를 하며, 줌의 종단 간 암호화에 대한 정확한 입장 표명을 요구했다[9-13].

3.2 허약한 암호화 알고리즘

줌은 AES-256 방식의 암호화 알고리즘을 사용하고 있다고 밝혀왔다. 하지만 캐나다의 비영리 개인 정보 및 보안 연구기관인 시티즌랩에서 줌은 실제로 AES-128 알고리즘 방식을 사용하고 있다는 것을 발견했다. ZOOM의 자체 암호화 체계를 RTP(Real-time Transport Protocol)에 추가하는 전송 프로토콜에 추가되는 특이한 방식으로 Zoom 회의의 모든 참가자의 오디오 및 비디오는 참가자 간에 공유된 단일 AES-128 키로 암호화되고 복호화된다. 그리 줌의 암호화와 복호화는 ECB(Electric CodeBook) 모드에서 AES를 사용된다. AES 키는 Zoom 서버에서 회의 참가자에게 생성되고 배포된 것으로 확인된다. 이러한 암호화 모드가 입력 패턴을 유지하므로, 해당 보안성엔 취약성 발생한다. 그래서 ECB 모드에서 발생하는 보안문제점이 없는, 분할된 정수 카운터 모드 또는 AES in f8-mode 모드에서 AES를 사용하는 것이 스트리밍 미디어 암호화를 위해 필요하다. <그림 5>는 ECB의 위험성의 고전적 그림 예시이다. 펭귄의 전체적인 모양은 여전히 ECB 모드로 암호화된 이미지에서 볼 수 있다. 줌의 대표인 에릭 유안 대표는 해당 사실을 인정하고 "보다 나은 암호화 설계 방식을 찾아 조만간 발표할 것"이라고 밝혔다[11, 14, 15].

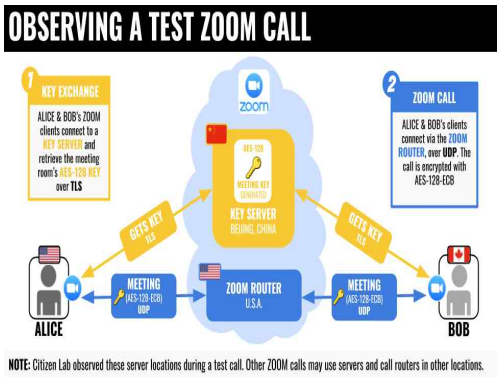


<그림 5> 원본사진과 ECB 모드 사진

3.3 암호화 키의 중국 서버 경유

줌은 높은 서비스 품질과 가용성을 얻기 위해 아마존 AWS를 인프라로 사용한다. 이런 특성상 서버는 전 세계에서 분산처리된다고 볼 수 있다. 이는 어떤 나라에서든 미국 아마존의 줌 메인 서비스에 접속하는 것이 아닌 해당 국가의 아마존 서비스에 복제되어 있는 서비스를 사용할 수 있다. 이처럼 네트워크 부하에 따라서 중국의 아마존 AWS에도 접근할 수도 있다. 그리고 캐나다의 개인 정보 및 보안 연구기관인 CitizenLab(시티즌랩)에 따르면 암호화 및 암호화 키가 중국 서버로 전송이 의심된다는 연구결과가 발표되기도 하였다. 미국과 캐나다에서 여러 번의 테스트 호출 중에 중국 베이징에 있는 서버로 전송된 회의 암호화 및 복호화를 위한 AES-128 키가 TLS를 통해 참가자 중 한 명에게 전송된 것으로 확인되었다. 베이징, 52.81.151.250. 스캔 결과 Zoom 서버 소프트웨어를 실행하는 중국의 총 5개 서버와 미국의 68개 서버 베이징 서버와 동일하다는 것을 확인했다. 이러한 서버를 통해 키가 배포될 수 있는 위험성을 강조했다. 중화 인민 공화국을 포함하여 합리적으로 자원이 풍부한 국가 공격자들은 암호화, 보안 문제 및 회의 키를 처리하는 중국에 위치한 해외 서버에서 쉽게 식별할 수 있는 제한이 있는 앱을 이용하기 용이 할

수 있다. 이에 대해 Zoom은 해당 내용과 관련된 보고서를 90일 이내에 제공할 것이라고 발표했다[10, 11].



<그림 6> 줌 테스트 호출의 토폴러지

3.4 iOS 앱 개인정보 유출

2020년 4월 IT 매체인 마더보드(motherboard)는 줌의 iOS 앱이 사전에 사용자 고지나 동의 없이 사용 정보 및 개인 정보를 광고 목적으로 Facebook(페이스북)에 전송한 것을 지적했다. 이는 사용자가 연결된 페이스북 계정이 없을 시에도 적용되었다. 줌은 페이스북의 소프트웨어 개발키트인 SDK를 사용을 통해 페이스북의 Grapg API에 접속하여 자동으로 Facebook에 데이터를 전송하였다. 이로 인해 페이스북은 광고에 활용되는 타겟 게이터, 접속하고 있는 국가, 이용자의 기기 모델과 이용 시간대 등을 이용자가 줌 앱을 실행 시 마다 전달받았다. 더 큰 문제는, 문제가 거론된 시점까지도 줌은 개인 정보 보호 정책에 대해 이용자에게 정확한 내용을 밝히지 않았다는 것이다. 초기 줌의 개인 정보 보호 정책은 페이스북 계정을 이용하는 사람들에 대한 세부 정보를 수집할 수 있다는 내용이 포함되어 있었지만, 페이스북을 사용하지 않는 이용자들의 데이터까지 페이스북과 공유하고 있었다는 사실을 언급하고 있지 않아 논란이 확산되었다. 이러한 문제가 이슈화되자 에릭 유안은 잘못을 인정하고 공식적으로 사과를 하였으며 이를 수정하였다. 이용자들의 개인 정보 보호를 가장 중요하게 다룰 것이며, 회의를 모니터링하거나 기록을 저장하지 않으며 아용자의 데이터를 판매하지 않을 것임을 명시했지만 서비스를 제공하는 데 필요한 이용자 데이터는 불가피하게 수집할 수밖에 없음을 밝혔다. 하지만 이는 개인정보를 언제든 마케팅에 활용할 수 있다는 우려가 남아있다. 이 사건을 통해 취약한 보안 의식 수준을 보여준 사례가 되었으며, 사용자 개인 정보가 마케팅 목적으로 잘못 쓰일 수 있는 위험성을 통해 보안이 강조되어야 한다는 것을 전 세계에 알리게 되었다[16-20].

3.5 다크웹 유통 및 초대장 유출

앞선 사례에서 언급했듯이 근본적인 보안 취약성 때문에 '줌 폭판' 또는 '줌 트롤링' 행위가 해외에서 큰 문제로 대두되었다. 이는 크게 2가지로 원인을 분석할 수 있다. 첫 번째로는 줌 계정이 다크 웹에 유통됨으로써 줌 폭탄이 자연스럽게 발생하고 있다는 것이다. 이름 및 호스트 키, 미팅 ID, 이메일과 패스워드만 저장된 데이터 등과 같은 데이터들이 유통되었으며 심지어 심지어 의료 소프트웨어, 뱅킹, 컨설팅 등 다양한 분야의 줌 계정 크리덴셜(credential)도 포함돼 있었다고 한다. 또한, 다른 보안업체인 Sixgill에서도 352개의 줌 계정이 해킹되었다고 보도하였다. 두 번째로는 화상회의 초대장은 2020년 3월 중순까지 이중 안전장치가 없이 링크 주소만 있으면 누구나 들어갈 수 있는 비밀번호가 없는 단문 형식 링크 주소였다. 즉 초대장이 유출된다면 모든 화상 대화 내용이 유출될 가능성이 있다는 뜻이다. 이와 같은 시유들은 줌 폭탄 사건을 일으키는 원인들로 분석할 수 있으며 해당 문제들에 대해 조치가 필요하다[10, 16, 21-23].

Ⅳ 줌의 업데이트 내용 비교분석

4.1 줌의 90일 보안계획 & 추후업데이트

줌의 보안에 대한 많은 논란이 발생하자 에릭 유안은 2020년 4월 1일 90일 보안 프로젝트를 통해 모든 문제를 수정하기 위해 필요한 인력을 투입하는 것을 약속하였다. 줌은 주간 웨비나를 통해 진행사항 등을 공식 블로그를 통해 전달하였다. 90일 프로젝트 이후에도 여전히 남아있는 문제점들을 꾸준한 업데이트를 통해 해결하고 있음을 블로그를 통해 전달하고 있다. 본 논문에서 제시한 문제점과 지금까지의 업데이트된 내용(90일 보안계획 업데이트, 추후 업데이트)들을 분석하여 비교하여 분석하였다. 그래서 분석한 내용을 바탕으로 현재 줌 관련 보안 취약점 이슈가 해결된 부분과 해결되지 못하여 현재도 문제가 되고 있거나, 현재 개선이 진행중인 부분으로 나누어 분석하였다.

4.2 해결된 문제점

4.2.1 (3.1.2)해결 : 허약한 암호화 알고리즘

줌은 AES-256 방식의 암호화 알고리즘을 사용하고 있다고 밝혀왔다. 하지만 토론토 대학 시민 연구소에서 줌은 AES-128 알고리즘을 사용하고 있음을 발견했다. 이에 대해 2020년 4월 29일 줌은 공식 블로그를 통해 AES-256 암호화에서 AES-256-GCM으로 전환했다고 한다. GCM은 인증된 암호화 알고리즘으로서 비밀 유지 이외에도 데이터 무결성을 제공하므로 효율성뿐만 아니라 현대의 대부분 기기에서 연동이 가능함을 밝혔다. 이후 2020년 6월 3일에 줌에 GCM 암호화를 5월 30일부터 모든 계정에 활성화하였으며 모든 무료 사용자와 유로 사용자에게 지원된다고 전했다[24, 25].

4.2.2 (3.1.4)해결 : iOS 앱 개인정보 유출

줌 iOS 앱이 사전에 사용자 고지나 동의 없이 개인정보 및 사용 정보를 광고 목적으로 페이스북에 전송한 것이 알려진 후 줌은 2020년 3월 27일 업데이트를 통해 해당 Facebook SDK 이용과 관련한 변경사항을 공식 블로그를 통해 전했다. 당시 줌은 Facebook의 iOS 용 SDK를 이용하여 “Facebook으로 로그인하기” 기능을 통해 줌은 사용자들이 줌 플랫폼에 더 편리하게 접속할 수 있도록 지원했다. 하지만 줌은 Facebook SDK가 모바일 OS 유형, 기기 시간대, 버전, 기기 OS, 화면 크기, 기기 모델과 통신사, 디스크 공간, 프로세서 코어가 같은 기기 관련 정보와 같이 줌 서비스 제공과는 무관한 각 기기의 정보 수집이 확인되어 iOS 클라이언트에서 Facebook SDK를 제거하였다. 줌은 이번 일을 계기로 고객의 개인 정보 보호를 매우 중요하게 생각한다는 것을 강조했다[26].

4.2.3 (3.1.5)해결 : 다크웹 유통 및 초대장 유출

줌은 2020년 9월 10일 공식 블로그를 통해 이중 인증(2FA)을 통해 사용자를 보호하고 보안 위반을 차단할 수 있다고 발표하였다. 이중 인증은 사용자에게 계정 소유권을 인증하는 자격 증명 또는 두 개 이상의 증거를 요구하여 사용자를 식별한다. 예로는 사용자 생체 정보(지문, 음성), 사용자의 소지품(스마트카드 또는 모바일 기기), 사용자가 알고 있는 정보(암호 또는 PIN) 등이 있다. 이는 보안을 한 단계 더 추가된 상태로 불순한 의도를 가진 사용자가 암호를 추측하거나 직원 또는 학생의 기기에 대한 액세스를 얻는 것을 차단하여 ID 절도 및 보안 위반 위험을 감소시킬 수 있다. 이는 다크 웹을 통해 계정을 거래한 이들에게 이중 보안이라는 시스템은 사용에 제한을 주어 해당 문제에 대해 충분히 해결할 수 있는 점을 의미한다고 볼 수 있다[27].

4.3 미해결된 문제점

4.3.1 (3.1.1)미해결 : 종단 간 암호화

줌은 엔드 투 엔드 암호화 구축을 위해 Keybase를 인수하였으며 제이슨 리 CISO 영입을 통해 서비스 모든 영역에 종단 간 암호화를 적용하겠다고 밝혔으며 세계 최대 온라인 코드 공유 사이트 '깃허브'에 공유를 통해 종단간 암호화 설계 업데이트 내용을 전달하고 있다. 전달되고 있는 내용으로는 종단 간 암호 기능을 4단계를 통해 제공하겠다고 발표하였다. 이번에 발표한 것은 Meeting-Key Exchange Protocol만 개선한 4단계 중 1단계에 속한다고 한다.

1단계에서는 웹브라우저만으로 대화방에 참여하는 경우와 Zoom Webinar Product, Zoom Chat Product에서는 종단 간 암호를 지원하지 않으며 Zoom Desktop Client, Zoom Mobile App, Zoom Room에서만 E2EE Meeting을 개설할 수 있고, 또 참석할 수 있다고 한다. "Streaming", "Live Transcription", 등와 같은 특정 기능들은 E2EE Meeting에서는 지원되지 않으므로, E2EE Meeting 시는 반드시 확인하고 사용해야 한다.

줌은 2021년에 better identity management와 E2EE SSO integration을 지원하는 2단계를 발표할 계획이다. "Join Before Host" 기능을 지원하고 Transparency Tree 기능을 구현하여 Meeting에 참여하고자 하는 참석자에 대하여, 미팅에 참석한 모든 자가 주기적으로 검증하는 방식을 구현할 것이라고 한다. 마지막인 4단계에서는 악의적인 Zoom Server를 통하여 Meeting에 참석하는 경우를 차단하기 위해 "Real-Time Security" 기능을 구현한다고 계획하였다. 이와 같이 E2EE 기능 실현의 최종 완성을 위해 줌은 여전히 노력하고 있음을 알 수 있으며 현재에는 기술 프리뷰를 통해 이용자들의 피드백을 받고 있으나 아직은 보안성에 대한 다양한 이슈가 존재하고 있다[28-32].

4.3.2 (3.1.2)미해결 : 암호화 키의 중국 서버 경유

줌은 이용자들의 개인 정보 보호와 보안을 지킬 수 있도록 CISO 자문 위원회를 구성하여 개인 정보와 안전, 포용 분야의 여러 조직과 검토를 진행하였으며 데이터, 기록, 콘텐츠 관련 정보는 투명성 보고서를 통해 제공한다. 하지만 이와 같은 줌의 노력에도 여전히 암호화 및 복호화에 사용되는 키가 중국 서버를 경유하는 문제에 대한 논란은 종식되지 않았다.

국민의 힘 김영식 의원은 정부가 주도적으로 나서서 민간 사용을 자제시켜야 한다고 밝혔다. 김영식 의원은 중국 정부에 의한 정보 유출 우려가 해결되지 않은 상황을 걱정하였으며, 이는 국가 보안 기술연구소에서 발표한 '줌 보안 취약점 현황 분석'을 확인해 보면, 줌은 종단 간 암호화(E2EE)가 아닌 사용자와 서버 사이의 암호화를 사용하고 있기 때문에 보안성에 주의가 필요하다고 한다.

중국은 2017년부터 시행 중인 사이버 보안법에 의거하여 중국 내 모든 서버는 중국 당국이 요구할 시 모든 데이터를 제출해야 한다. 이로 인해 데이터 센터들은 중국 당국에 암호 키를 공개해야 하는 법적 의무가 있어 중국 정부가 필요로 할 시 줌의 사용자 데이터들을 얻을 수 있다. 즉 화상회의와 관련된 모든 데이터가 중국으로 유출될 가능성이 존재하는 것이다. 김영식 의원은 각 기업이 보유하고 있는 핵심 기술과 영업기밀 등이 중국으로 유출될 가능성이 높은 만큼, 당장 민간 부분의 줌 사용 주의보를 발령을 통해 줌의 민간 사용을 자제해야 한다고 전달한다. 이를 통해 중국 서버에 관련된 논란의 여지가 아직 남아있음을 확인할 수 있다[33-35].

4.4 업데이트 내용 비교분석 및 개선

이슈화되었던 보안에 관련된 다양한 문제점과 취약성에 대해 정리해보았으며 줌의 90일 보안 계획과

그 이후 추후 업데이트된 내용들을 비교 및 분석해 보았다.

<표 1> 문제점과 업데이트 내용 비교

문제점&취약성	90일 보안계획	추후 업데이트
종단간 암호	X	E2EE 4단계 중 1단계만 발표되었고 현재 개선 중
허약한 알고리즘	AES128 -> AES-256-GCM	AES128 -> AES-256-GCM
암호화키 중국 서버 경유 논란	△	여전히 종식되지 않은 논란
iOS 앱 개인정보 유출	iOS Facebook SDK 제거	iOS Facebook SDK 제거
다크웹 유출&줌바밍	X	이중 인증(2FA)

90일 보안계획을 통해 가장 논란이 되었던 알고리즘에 관련된 부분이 개선되었다. 또한 ios 관련 개인정보 유출에 대한 문제도 완전히 해결되었다. 남아있던 문제들도 9월 10일과 10월 22일 업데이트를 통해 해결을 위해 노력하고 있음을 확인할 수 있다. 다크웹 유출과 줌바밍과 같은 사생활 침해에 관련된 문제는 이중 인증 기능을 도입함으로써 해결하였다.

하지만 종단 간 암호와 중국 서버에 대한 문제는 여전히 진행 중으로 확인된다. 종단 간 암호화는 4단계 중 1단계를 통해 초기 버전을 제하고 하고 있다. 하지만 최종 단계인 4단계까지는 아직 시간이 더 필요하며, 암호화 키의 중국 서버에 대한 문제는 여전히 이슈 거리로 남아있는 것으로 보아 아직 완벽히 해결하지 못했음을 알 수 있다. 현재 발표된 1단계도 최종 사용자 간의 데이터 암호화가 아닌 사용자와 서버 간의 전송되는 데이터를 암호화하고 있다. 이는 여전히 종단 간 암호화를 완전히 이행하지 못한 상태이다. 또한, Zoom Webinar Product, Web Browser 그리고 Zoom Chat Product를 통해 Meeting에 참여하는 경우와 같이 특정 방법에서는 지원하지 않는다. 줌은 앞으로 보안성을 더욱 높이기 위해 해당 부분들을 업데이트해야 한다. 그러면 중국 서버에 관련된 문제도 종단 간 암호화가 완벽히 해결된다면 자연스럽게 같이 해결될 수 있을 것으로 유추되며 해당 문제를 해결하기 위해 빠른 개선이 필요하다[31].

VI. 결론

본 논문에서는 2020년 코로나가 확산이 되며 신흥 강자로 자리 잡은 줌에 대하여 거론되고 있는 여러 보안상의 문제와 취약성을 다루어 알아보았다. 해당 문제들에 대한 줌이 공식으로 밝힌 업데이트 내용과 비교하여 해결, 미해결로 분류하였고 여전히 보안상의 문제점에 대해선 논란이 있음을 확인할 수 있다. 특히 종단간 암호 기술과 관련된 부분은 아직 완벽하게 해결되지 못하였다. 현시점 종단간 암호의 4단계 중 1단계까지 제공이 되었으나 여전히 보안상의 문제는 거론되고 있으며 추가적으로 새로운 문제점이 발생할 수 있다. 또한 줌에서 사용되는 암호화 키가 중국 서버를 경유될 수 있는 논란은 여전히 남아있는 상황이다. 클라우드 기반 화상회의 솔루션의 보안에 대한 논란을 잠재우기 위해서 줌은 종단간 암호의 모든 기술을 제공하고 추가로 발생하는 문제들에 대응할 수 있는 대응책을 강구할 필요가 있다.

참고문헌

[1] Kandukuri, Balachandra Reddy, and Atanu Rakshit, “Cloud security issues,” IEEE International Conference on Services Computing, 2009, p.p.517-520.

[2] Kalaiprasath · R. Elankavi · Dr. R. Udayakumar, “CLOUD SECURITY AND COMPLIANCE - A SEMANTIC APPROACH IN END TO END

SECURITY," International Journal of Mechanical Engineering and Technology, Vol.8, Issue 5, 2017, pp.987–994.

[3] Thierry Le Pennec, Inter-Network and inter-protocol video ocnference privacy method, apparatus, and computer program product, United States Patent(US 7474326B2), 2009.

[4] 양정모, "클라우드 컴퓨팅의 신뢰성 향상 방안에 관한 연구," 디지털산업정보학회 논문지, 제8권, 제4호, 2012, pp.107-113.

[5] 최은정, 아이뉴스24, 줌 회원정보 수만건 다크웹서 유출 주의, 2020.

[6] Sarah Young, "Zoombombing Your Toddler: User Experience and the Communucation of Zoom's Ptivacy Crisis," Journal of Business and Technical Communication, Vol.35, 2020, pp.147-153.

[7] 양환석, "공격정보 수집을 이용한 클라우드 서비스의 안전성 향상에 관한 연구," 디지털산업정보학회 논문지, 제9권, 제2호, 2013, pp.73-79.

[8] 이정애, 한겨레신문 , 수업 도중 음란물·욕설 '줌폭격' 이뤄질라…뉴욕시 화상회의 플랫폼 '줌' 퇴출, 2020.

[9] 정혜인 · 김성준, "개인정보관리체계계(PIMS)를 이용한 클라우드컴퓨팅 개인정보 보안 개선 방안 연구," 디지털산업정보학회 논문지, 제12권, 제3호, 2016, pp.133-155.

[10] 지윤성, 뉴스톱, 줌(Zoom) 화상회의, 보안상 안전하지 않다 지윤성 팩트체커, 2020.

[11] THECITIZENLAB, Bill Marczak and John Scott-Railton, Move Fast and Roll Your Own Crypto 'A Quick Look at the Confidentiality of Zoom Meetings', 2020.

[12] 이상영 · 이윤현 · 이윤석, 이식성을 위한 메타데이터 기반의 CDSS 구축, 디지털산업정보학회 논문지, 제8권, 제1호, 2012, pp.221-229.

[13] Howard M. Zeidler · Palo Alto, Calif, END-TO-END ENCRYPTION SYSTEM AND METHOD OF OPERATION, United States Patent(US4578530), 1986.

[14] 이정태, AI타임스, Zoom(줌) 개인정보 보호 및 보안 문제 20가지, 2020.

[15] Deshpande, Ashwini M., Mangesh S. Deshpande, and Devendra N. Kayatanavar, "FPGA implementation of AES encryption and decryption," 2009 International Conference on Control, Automation, Communication and Energy Conservation. IEEE, 2009, p.p.1-6.

[16] 애드 테크 101, 줌 보안 이슈:위험성,문제점,대안, https://adtechnow.tistory.com/33, 2020.

[17] Weaver, Jesse, and Paul Tarjan, "Facebook linked data via the graph API," Semantic Web, 4, 2013, pp.1245-250.

[18] Burkhardt, Marcus, et al, "THE EVOLUTION OF FACEBOOK'S GRAPH API," AoIR The 21stAnnual Conference of the Association of Internet Researchers, AoIR2020, 2020.

[19] 유혜정, "프라이버시를 제공하는 저작권 보호 프로토콜," 디지털산업정보학회 논문지, 제4권, 제2호, 2008.

[20] 신문과 방송, 언텍트(Untact, 비대면), 한국진흥재단, 5월호, 2020.

[21] 네이버 개인정보보호, 화상회의 앱 '줌(ZOOM)'의 프라이버시 논란과 보안 이슈, 2020, https://blog.naver.com/n_privacy/221924299386.

[22] Kristin Finklea, Dark Web, Comgressional Research Service, 2017.

[23] Michael Chertoff · Tobby Simon, "The Impact of the Dark Web," Global Com,ission on Internet Governance, NO.6, 2015.

[24] Zoom Official Blog, 90-Day Security Plan Progress

Report: April 29, 2020, https://blog.zoom.us/ko/90-day-security-plan-progress-report-april-29/.
[25] Zoom Official Blog, 90-Day Security Plan Progress Report: June 3, 2020, https://blog.zoom.us/ko/90-day-security-plan-progress-report-june-3/.
[26] Zoom Official Blog, Zoom's Use of Facebook's SDK in iOS Client, 2020, https://blog.zoom.us/ko/zoom-use-of-facebook-sdk-in-ios-client/.
[27] Zoom Official Blog, Secure Your Zoom Account with Two-Factor Authentication, 2020, https://blog.zoom.us/ko/secure-your-zoom-account-with-two-factor-authentication/.
[28] AEP코리아네트 블로그, Zoom에서 지원하는 E2EE(End-to-End Encryption), 2020, https://blog.naver.com/aepkoreanet/222121234397.
[29] Zoom Official Blog, Webinar Recap – Ask Me Anything with Eric Yuan & Zoom Leadership: Oct. 21, 2020, https://blog.zoom.us/webinar-recap-ask-me-anything-with-eric-yuan-oct-21/.
[30] Zoom Official Blog, Zoom Rolling Out End-to-End Encryption Offering, 2020, https://blog.zoom.us/zoom-rolling-out-end-to-end-encryption-offering/.
[31] Blum, Josh, et al. "E2E Encryption for Zoom Meetings," 2020.
[32] Mehmet Balasaygun, Freehold, NJ(US); Jean Meloche, Madison, NJ (US); Heinz Teutsch, Green Brook, NJ (US); stani Yajnik, Berkeley Heights, NJ(US), System and method for end-to-end encryption and security indication at an endpoint, United States Patent, US 9,356,917 B2, 2016.
[33] 최아름, 정보통신신문, '줌' 보안취약점 확인…정부 차원 대책 마련 시급, 2020.
[34] Zoom Official Blog, CEO 보고서: 90일 완료 후 Zoom의 계획, 2020, https://blog.zoom.us/ko/ceo-report-90-days-done-whats-next-for-zoom/.
[35] Erastus Karanja, "The role of the chief information security officer in the management of IT security," Information & Computer Security, Vol.25, No.3, 2017, pp.300-329.

■ 저자소개 ■

김규형
Kyuhyeong Kim

2015년 3월~현재
인제대학교 컴퓨터공학과,
영어영문학과 복수전공 학사과정

관심분야 : 인공지능, 빅데이터, 네트워크 보안
E-mail : rbgud2017@gmail.com

최 윤 성
Younsung Choi

2020년 3월~현재
인제대학교 AI융합대학
산업보안전공 조교수
2016년 3월~2020년 2월
호원대학교 IT소프트웨어보안학과
조교수
2015년 8월 성균관대학교
전자전기컴퓨터공학부 (공학박사)
2010년 3월 ~ 2012년 2월
경북대학교 법학박사수료
2007년 8월 성균관대학교
전자전기컴퓨터공학부 (공학석사)
2006년 2월 성균관대학교 정보통신공학부
(공학학사)

관심분야 : 정보보호, 디지털포렌식, 산업보안
E-mail : cys2020@inje.ac.kr

논문접수일 : 2020년 11월 25일
수 정 일 : 2020년 12월 4일
게재확정일 : 2020년 12월 15일