

2020

한국정보보호학회 하계학술대회

CISC- S'20

Conference on Information Security
and Cryptography - Summer 2020

07.15^{WED}

온라인 컨퍼런스

<http://www.cisc.or.kr/>

주최
주관



후원



과학기술정보통신부



Blockchain-empowered for Secure Data Storage and Sharing in Vehicular Edge Computing Networks	Muhammad Firdaus · Kyung-HyuneRhee / 197
허가형 블록체인을 활용한 자기 주권형 신원의 디지털 공공·민간서비스 플랫폼 융합 방안	조강우 · 정병규 · 신상욱 201

블록체인 2

무결성을 보장하며 보상체계를 갖는 블록체인 기반 커뮤니티 정보교류 Web 환경	윤혜원 · 김원희 · 김다영 · 노혜윤 · 김형종 / 207
블록체인 네트워크 한계 보완을 위한 사이드체인 동향	심민주 · 최승주 · 서화정 / 211
Secure Localized Training in Collaborative Learning Schemes	Sandi Rahmadika · Kyung-Hyune Rhee / 214
블록체인에서 랜덤 비콘 프로토콜을 이용한 PRNG 비교 분석	정병규 · 조강우 · 신상욱 / 218
사물 인터넷 환경에서 수정 가능한 블록체인 기반 접근제어 시스템 설계	임준호 · 천지영 · 노건태 · 정익래 / 222
IoT 환경에서의 블록체인 활용에 대한 연구	김대영 · 이덕규 / 226

어플리케이션보안

암표방지를 위한 모바일 티켓팅 시스템에 관한 연구	송윤민 · 황용운 · 이임영 / 233
하이퍼레저 패브릭 기반 장학금 통합 관리 시스템 개발	김은별 · 송경린 · 최찬미 · 최윤영 · 채기준 / 237
회전에 강한 특징을 이용한 돌로네 기반 대체 가능 지문 템플릿 연구	이민섭 · 이상훈 · 정익래 / 241
암호화 API 오용 탐지에 관한 연구 동향 조사	이민욱 · 조금환 · 김형식 / 245
Zero-Knowledge Proof 기반의 마이데이터 서비스 제공 방안	이민경 · 최슬기 · 곽진 / 249

산업보안

IEC 62443-4-2 기반 HVDC 및 ESS 보안 적용 방안	박원경 / 255
안전한 원격 근무를 위한 그룹키 기반 프로토콜 제안	김익진 · 김득훈 · 곽진 / 259
몬테카를로 시뮬레이션을 통한 기업의 위험표현 및 사이버보험 효과도 분석 연구	김민수 · 김예주 · 왕성진 · 김형종 / 263

해킹 및 방어기술

안드로이드 UI 은닉을 통한 소프트웨어 기반 카메라 프레임 탈취 기법	한수민 · 심현석 · 박정수 · 정수환 / 269
키보드 입력 감지 트리거 구현 및 분석	박연균 · 윤종희 / 273
Python Pickle 모듈을 통한 셸코드 Exploitation과 Mitigation 연구	윤창조 · 김경곤 / 275
N-gram 알고리즘을 이용한 Spectre 공격 바이너리 정적 식별 방법	김문선 · 양희동 · 김광준 · 이만희 / 279
Federated Learning에서 개선된 백도어 공격 방법	임규민 · 김창진 · 서재홍 / 283
안티바이러스의 자가 보호 기법 분석	이성원 · 윤종희 / 287

안전한 원격 근무를 위한 그룹키 기반 프로토콜 제안

김의진¹, 김득훈², 곽진³

^{1,3}아주대학교 사이버보안학과

²아주대학교 컴퓨터공학과 정보보호응용및보증연구실

The Proposal of Group-Key Based Protocol for Secure Remote Work

Eui-Jin Kim¹, Deuk-Hun Kim,² Jin Kwak³

^{1,3}Department of Cyber Security, Ajou University

²ISAA Lab., Department of Computer Engineering, Ajou University

요 약

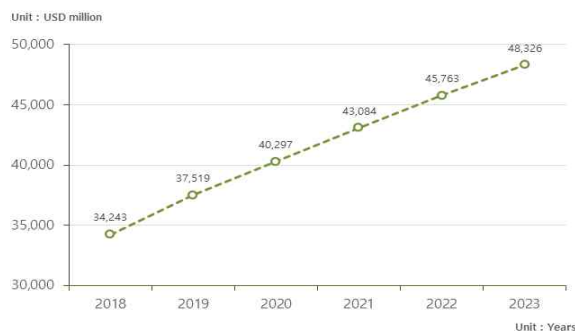
최근 세계적으로 유행하는 질병으로 인해 비대면 서비스인 언택트(Untact) 문화가 확산되고 있다. 원격 근무를 포함한 UC&C(Unified Communication & Collaboration) 시장은 매년 성장하여 2023년에는 약 483억 달러 규모의 시장이 될 것으로 전망된다. 원격 근무 플랫폼의 수요 증가로 인해 시장 규모가 증가하고 있는 한편, 원격 근무 플랫폼의 보안 취약점으로 인한 문제점도 발생하고 있다. 악의적인 공격자에 의한 사용자의 세션키 탈취 및 세션키 노출로 인가되지 않은 사용자의 참여 등과 같은 위협이 발생할 수 있다. 따라서 본 논문에서는 원격 근무에서 발생 가능한 보안 위협을 해결하기 위해 안전한 원격 근무 환경을 위한 그룹키 기반의 프로토콜을 제안한다.

I. 서론

최근 발생한 세계적으로 유행하는 질병의 확산으로 인해 언택트(Untact) 문화가 확산되고 있다. 직장, 학교를 비롯한 단체들은 정부의 지침으로 사회적 거리 두기를 하고 있고, 이로 인해 최근 주목받는 것이 원격 근무이다.

원격 근무를 포함한 글로벌 UC&C(Unified Communication & Collaboration) 시장은 (Fig. 1)과 같이 2019년 기준 연평균 성장률 약 7.1%로 2023년까지 약 483억 달러 규모로 성장할 것으로 전망된다. 국내에서는 정부가 국가적 차원의 대응으로 재택·원격 근무를 확대하고, 원격 근무 솔루션 지원 및 기술개발 촉진에 투자하고 있다. 또한, 미국은 2005년부터 2018년까지 원격 근무자가 약 173%

증가하였고, 최근 질병으로 인해 독일은 재택 근무를 의무화하는 등 원격 근무를 활성화하고 있다[1].



(Fig. 1) Global UC&C Market Forecast

원격 근무의 활성화와 수요 증가로 인해 시장 규모가 증가하고 있는 동시에 보안 취약점을 이용한 문제점도 등장하고 있다[2]. 원격 근무 플랫폼에서 인가되지 않은 사용자가 안전하지 않은 채널로 주고받는 세션키를

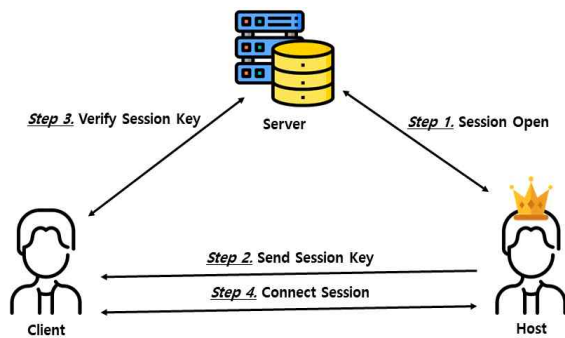
이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2017R1E1A1A01075110).

탈취하거나, 사전에 특정 사용자를 등록하지 않는 경우 특정 플랫폼의 사례와 같이 비인가자가 회의를 무단으로 참여 및 접근하여 회의를 방해하는 등의 위협이 발생할 수 있다[3].

따라서 이와 같은 위협을 방지하기 위해 본 논문에서는 2장에서 원격 근무 플랫폼에서 발생 가능한 보안 위협을 분석하고, 3장에서 이에 대한 대응방안으로 프로토콜을 제시한 뒤, 4장에서 안전성 분석을 하고, 5장으로 결론을 맺는다.

II. 원격 근무 플랫폼 보안 위협 분석

본 장에서는 원격 근무 환경에서 발생 가능한 보안 위협에 대하여 분석한다. (Fig. 2)는 원격 근무 플랫폼 절차에 대한 설명이다.



(Fig. 2) Procedure of Remote Work

Step 1. Session Open

호스트는 서버와 종단 간 암호화 통신을 이용하여 회의를 개설한다.

Step 2. Send Session Key

호스트는 세션키를 클라이언트에게 전달한다.

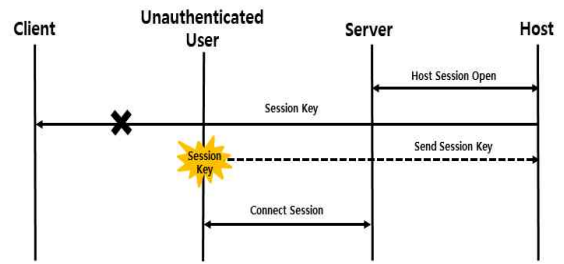
Step 3. Verify Session Key

클라이언트는 호스트로부터 받은 세션키를 서버에 보내 클라이언트를 인증한다.

Step 4. Connect Session

클라이언트가 정당하다면 클라이언트는 호스트가 주최한 회의에 접근할 수 있다.

그러나 위 과정에서 세션키를 안전하지 않은 채널로 전달 시 또는 중간자 공격을 이용할 시 A사의 사례처럼 인가되지 않은 사용자의 세션에 접근이 가능하다[4].



(Fig. 3) Problem in Remote Work

(Fig. 3)은 원격 근무 플랫폼에서의 보안 위협을 나타내며, 호스트가 안전하지 않은 채널로 클라이언트에게 세션키를 전달 시, 인가되지 않은 사용자는 세션키를 탈취하여 호스트가 개설한 회의에 접근할 수 있음을 보여준다[4].

위 과정에서 클라이언트와 호스트 간 민감 정보 통신 시 기밀성 문제, 인가되지 않은 사용자가 세션에 접근할 수 있는 접근 제어 문제, 악의적인 사용자의 세션키 탈취를 위한 중간자 공격 등의 문제가 발생할 수 있다. 따라서 인가된 사용자만 접근할 수 있도록 그룹키 기반의 프로토콜을 제안하고자 한다.

III. 제안 사항

본 장에서는 안전한 원격 근무 환경을 위한 그룹키 기반의 프로토콜에 대해서 제안한다.

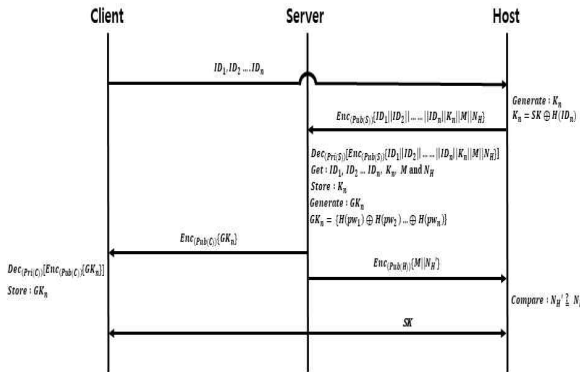
3.1 표기법

제안하는 기법에서 사용하는 파라미터는 다음 <Table 1>과 같다.

<Table 1> Notation

Parameter	Description
ID_x	The ID of x
K_n	The value of verify Client
GK_n	The Client's group key
SK	The Session key
N_x	The Nonce from x
$H(\cdot)$	Hash function
$\oplus$	XOR operation
pw_n	The Nth Client's password
M	Message
$Pub(x)/Pri(x)$	The key pair of x

3.2 호스트 세션 개설 과정



(Fig. 4) Host Session Open

Step 1. 호스트는 클라이언트에게 ID_n 를 받고 통신 과정에서 클라이언트를 확인하기 위한 K_n 과 세션키 SK 를 생성한다. K_n 은 세션키와 클라이언트 아이디를 해시한 값을 XOR 연산하여 생성한다.

$$K_n = SK \oplus H(ID_n) \quad (1)$$

Step 2. 호스트는 클라이언트의 ID_n , K_n , 메시지 M , 호스트의 Nonce 값 N_H 을 서버의 공개키 $Pub(S)$ 로 암호화하여 서버에게 보낸다.

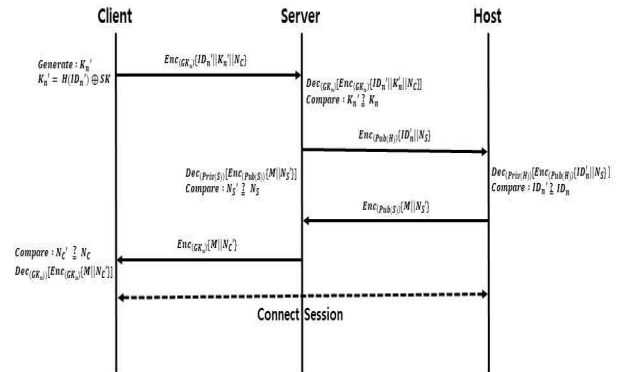
Step 3. 서버는 호스트에게 받은 값을 서버의 개인키 $Pri(S)$ 로 복호화하여 클라이언트 ID_n , K_n , M 그리고 N_H 을 얻는다. 서버는 서버에 등록되어있는 클라이언트들의 $H(pw_n)$ 들을 XOR 연산하여 그룹키 GK_n 을 생성하고 동시에 호스트에게 받은 K_n 을 저장한다.

$$GK_n = H(pw_1) \oplus H(pw_2) \oplus \dots \oplus H(pw_n) \quad (2)$$

Step 4. 서버는 그룹키 GK_n 를 클라이언트의 공개키로 암호화하여 클라이언트에게 보내고, 메시지 M 과 Step 2에서 받은 Nonce 값 N_H' 를 호스트의 공개키로 암호화하여 호스트에게 보낸다.

Step 5. 호스트는 서버에게 받은 Nonce 값 N_H' 과 원래의 Nonce 값 N_H 을 비교한 뒤, 클라이언트에게 세션키 SK 를 보낸다.

3.3 통신 과정



(Fig. 5) Communication Protocol

Step 1. 클라이언트는 호스트에게 받은 세션키 SK 와 ID_n' 를 이용하여 K_n' 을 생성하고, ID_n' , K_n' , 클라이언트의 Nonce 값 N_C 을 그룹키 GK_n 로 암호화하여 서버에게 보낸다.

Step 2. 클라이언트에게 받은 값을 서버는 그룹키 GK_n 로 복호화한 뒤, 클라이언트에게 받은 K_n' 과 호스트로부터 받아 저장한 K_n 을 비교하여 클라이언트를 인증한다.

Step 3. 클라이언트가 정당하다면, 서버는 ID_n' , Nonce 값 N_S 을 호스트의 공개키로 암호화하여 호스트에게 보낸다.

Step 4. 호스트는 서버로부터 받은 값을 호스트의 개인키로 복호화한 뒤, ID_n' 이 사전에 등록된 클라이언트 ID_n 과 맞는지 확인한다.

Step 5. 호스트는 클라이언트가 정당하다면 서버에게 메시지 M , 서버로부터 받은 Nonce 값 N_S' 을 서버의 공개키로 암호화하여 보낸다.

Step 6. 서버는 개인키를 이용하여 복호화하고, N_S' 과 N_S 을 비교한 뒤, 메시지 M 과 클라이언트 Nonce 값 N_C' 을 다시 그룹키로 암호화하여 클라이언트에 보낸다.

Step 7. 클라이언트는 서버로부터 받은 값을 그룹키로 복호화하여 초기에 보낸 Nonce 값 N_C 과 서버로부터 받은 Nonce 값 N_C' 이 같은지 확인한다. 그 후 클라이언트는 호스트와 연결을 진행한다.

IV. 안전성 분석

본 장에서는 3장에서 제안한 프로토콜의 안전성을 분석한다.

4.1 기밀성

원격 근무 환경에서는 호스트와 서버 간, 클라이언트와 서버 간 민감 정보를 전달하기 때문에 암호화 통신을 해야 한다. 본 논문에서 제안하는 프로토콜에서는 통신을 받는 주체의 공개키쌍 $Pub(x)/Pri(x)$ 로 암호·복호화하여 통신하여 통신을 받는 주체만 받을 수 있게 한다. 또한, 그룹키 GK_n 을 이용하여 클라이언트와 서버 간 암호화하여 데이터의 기밀성을 제공한다.

4.2 접근 제어

원격 근무 환경에서는 인가되지 않은 사용자는 회의 세션에 접근할 수 없어야 한다. 본 논문에서 제안하는 프로토콜에서는 서버는 K_n , 호스트는 사전에 등록된 아이디 ID_n 을 이용하여 클라이언트가 정상적인 접근이 가능한 사용자인지를 판단한다. 그러므로 인가되지 않은 사용자는 세션에 접근할 수 없다.

4.3 중간자 공격

원격 근무 환경에서는 악의적인 사용자에 의해 세션키가 탈취되거나, 세션키가 노출될 때 비인가자의 세션 접근이 가능하다. 본 논문에서 제안하는 프로토콜에서 중간자 공격으로 얻을 수 있는 정보는 세션키 SK 와 클라이언트의 아이디 ID_n 이며, 이를 이용하여 K_n 을 계산하여 위장할 수 있다. 제안하는 프로토콜에서는 종단간 암호화 통신을 하고, 각각의 공개키쌍 $Pub(x)/Pri(x)$ 과 그룹키 GK_n 로 암호·복호화하기 때문에 중간자 공격으로 데이터를 탈취하여 K_n 을 생성한다고 하여도 복호화 키를 알 수 없기에, 중간자 공격을 방지할 수 있다.

V. 결론

본 논문에서는 원격 근무 환경에서 세션키 탈취 및 노출로 인한 인가되지 않은 사용자의 접근을 방지하기 위한 프로토콜을 제안하였다.

최근 원격 근무가 주목받으며 비인가자의 접근 및 중간자 공격과 같은 보안 위협이 증가하면서 이와 함께 보안의 중요성이 증가하고 있다. 본 논문의 제안 사항에서는 그룹키를 기반으로 하여 인가되지 않은 사용자의 접근을 막을 수 있는 프로토콜을 제안하였으며, 본 논문을 통해 원격 근무 환경에서 안전성을 향상할 수 있을 것이다.

[참고문헌]

- [1] 권영환, 박태형, 서영희, 송지환, 이중엽, 진희승, “원격 근무 솔루션 기술·시장 동향 및 시사점”, 소프트웨어 정책연구소 이슈리포트 IS-093, Apr. 2020.
- [2] European Network and Information Security Agency, “Security when working remotely”, Train the trainger reference guide, pp. 13-29. Feb. 2020.
- [3] Australian Cyber Security Centre, “Guidelines for Communications Systems”, Australian Government Information Security Manual, pp. 1, Oct. 2019.
- [4] WILTSHIRE POLICE, “THE ‘ZOOM BOMB’ PHENOMENON”, https://www.wiltshire.police.uk/media/4957/Zoom-Security-Guide/pdf/Zoom_Security_Guide.pdf?m=637251405190670000.
- [5] 류호석, 광진, “스마트홈 환경에서의 안전한 디바이스 관리를 위한 그룹키 관리 기법”, 정보보호학회 논문지. Vol. 25, No. 2, Apr. 2015.
- [6] 조정석, “클라우드 환경에서의 지문 및 위치 정보를 활용한 티켓 기반 인증 기법”, 아주대학교 공학 석사학위 논문, Feb. 2020.