Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.3, Jun. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.3.291

'애플과 구글의 코로나 접촉 추적 사양'에 대한 보안성 평가 및 검증 가능한 연산을 이용한 개선

김 병 연,[1†] 김 휘 강[2‡]
[1,2]고려대학교 정보보호대학원 (대학원생, 교수)

Security Analysis on 'Privacy-Preserving Contact Tracing Specifications by Apple and Google' and Improvement with Verifiable Computations

Byeong Yeon Kim,[1†] Huy Kang Kim[2‡]
[1,2]Korea University School of Cybersecurity (Graduate student, Professor)

요 약

그동안 COVID-19의 확산을 막고 사회를 정상화하려는 노력이 있었고, 감염 확산 탐지를 위해선 접촉자 추적 기술이 필수적이다. 하지만, 정부에 의한 접촉 추적 과정에서 공개된 감염자의 개인 정보 침해에 대한 우려가 제기되고 있고, 이에 Google과 Apple은 개인 정보 보호와 보안을 고려하여 정부와 보건 기관의 COVID-19 확산 방지에 대한 노력을 도울 수 있도록 블루투스 기술을 사용한 접촉 추적 기술을 발표했다. 그러나 더 나은 접촉 추적 기술을 제시하기 위해서는 체계적으로 보안 위협 및 취약점 도출하는 과정이 필요하다. 본 논문에서는 STRIDE, LINDDUN 위협 모델링을 통해 COVID-19 접촉 추적 기술에 대한 보안성을 분석하고, 이것을 기반으로 Zero-knowledge Succinctness Non-interactive Arguments of Knowledges(zkSNARKs)와 Public Key Infrastructure(PKI)를 이용해 실질적인 데이터 무결성과 개인 정보 보호 보장 방식을 제안한다.

ABSTRACT

There has been global efforts to prevent the further spread of the COVID-19 and get society back to normal. 'Contact tracing' is a crucial way to detect the infected person. However the contact tracing makes another concern about the privacy violation of the personal data of infected people, released by governments. Therefore Google and Apple are announcing a joint effort to enable the use of Bluetooth technology to help governments and health agencies reduce the spread of the virus, with user privacy and security central to the design. However, in order to provide the improved tracing application, it is necessary to identify potential security threats and investigate vulnerabilities for systematically. In this paper, we provide security analysis of Privacy-Preserving COVID-19 Contact Tracing App with STRIDE and LINDDUN threat models. Based on the analysis, we propose to adopt a verifiable computation scheme, Zero-knowledge Succinctness Non-interactive Arguments of Knowledges (zkSNARKs) and Public Key Infrastructure (PKI) to ensure both data integrity and privacy protection in a more practical way.

Keywords: Covid-19, STRIDE, LINDDUN, zkSNARKs, PKI

Received(02. 04. 2021), Modified(04. 19. 2021), Accepted(04. 22. 2021)

† 주저자, securekim@korea.ac.kr
‡ 교신저자, cenda@korea.ac.kr(Corresponding author)

I. 서 론

COVID-19 바이러스의 출현으로 인해 전 세계적으로 발생한 대규모 감염 사태는 정책 · 사회 · 경제 · 보건 등 다양한 측면에서 악영향을 끼치고 있다. 이에 세계보건기구(World Health Organization)에서 국제적 공중보건 비상 사태(PHEIC)를 알리며 COVID-19를 신속하게 식별하고 치료하며 바이러스가 얼마나 널리 퍼졌는지 정확하게 추정할 수 있도록 생명을 구하기 위한 연구의 의무를 요청하였고[1], 이에 많은 연구자가 COVID-19의 확산을 막기 위해 활발한 연구를 수행하고 있다.

본 논문에서 다루고자 하는 구글과 애플의 개인정보 보호 접촉 추적(Privacy Preserving Contact Tracing 이하 PPCT)은 상기 서술한 여러 가지 측면의 국제적 비상사태를 해결하기 위해 COVID-19의 확산율을 낮추겠다는 의지로 시작되었다. 그러나 실세계에서는 UN 인권위원회가 "개인 정보의 과도한 공개"가 인권 침해에 악용될 수 있다는 성명을 발표하였고[2], 한국의 인권위원회는 특히 실시간 위치 추적이 가능한 손목밴드를 착용하도록 하는 방안에 대해 심각한 우려를 표명하기도 하였으며[3], 이러한 한국의 개인정보 공개 문제는 Nature 지에 소개되기도 하였다[4]. 게다가 이러한 개인 정보 공개는 심각한 문제가 되어 인권사무소에 진정이 제기되기도 하는 등 COVID-19로 인한 개인정보 침해 문제가 사회적 문제로 떠오르고 있다[5]. 따라서 본 논문에서는 Privacy 보호 측면에서 PPCT 설계에 대한 보안 위협 모델(STRIDE, LINDDUN)을 선정하고, 이를 통해 체계적이며 객관적인 취약점 점검을 진행한다. 이후 취약점에 대한 분석을 진행하고, 취약점에 대한 PPCT의 보안성을 향상 시킬 방안을 제안한다.

II. 관련 연구

2.1 위협 모델링

위협 모델링은 취약점 감소의 효과를 보여주는 SDL(Security Development Lifecycle)의 핵심 요소로, 소프트웨어 설계자는 이를 활용하여 비교적 쉽고 조기에 잠재적인 보안 문제를 식별하고 완화할 수 있다. 즉, 위협 모델링을 사용하면 예를 들어 공격자가 어떤 식으로 인증 데이터를 변경하는지, 데이터를 읽는다면 어떤 영향을 미치는지, 특정 리소스에 대한 접근이 거부되면 어떤 일이 일어날지에 등에 대해 예측해 볼 수 있으며, 이러한 보안 위협 분석 기법에는 STRIDE[6], PASTA[7], OCTAVE[8], TVRA[9], STPA-sec[10], LINDDUN[11], Attack Tree[12], Security Cards[13], HTMM[14], Trike[15], VAST[16] 등 다양한 기법이 있다. 본 논문에서는 PPCT에 대해 S/W 취약점 및 Privacy 관점에서 위협을 분류를 진행해야 하므로, 상기 모델링 방법들을 비교 분석해 보았을 때 S/W 취약점, 개인정보보호 관점으로 보안 위협을 분류하는 모델인 STRIDE 와 LINDDUN을 바탕으로 모델링 하는 것이 알맞다고 판단된다.

2.1.1 STRIDE

STRIDE 모델은 Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege 등 발생 가능한 6가지 보안 위협을 다룬다. 이 프레임워크는 Shift-left를 위하여 보안 전문가가 아닌 사용자를 염두에 두고 개발되었기 때문에 모든 개발자가 위협 모델링을 수행할 수 있도록 정확한 지침을 제공하고 있다[17]. STRIDE 모델의 속성에 대한 설명은 다음과 같다.

1. Spoofing: 아이디, 비밀번호 등 다른 사용자의 인증 정보를 불법적으로 접근하고 사용하는 경우
2. Tampering:데이터베이스를 무단 변경하거나 네트워크에서 전달되는 데이터를 변경하는 등 데이터를 악의적으로 수정하는 경우
3. Repudiation: 데이터를 읽거나 쓰는 등 리소스에 접근 이후 이를 부인하는 경우
4. Information Disclosure: 사용자에게 권한이 없는 파일을 읽을 능력이 부여되거나, 침입자가 컴퓨터 간에 전송되는 데이터를 읽을 수 있는 등 접근하지 않아야 할 대상에게 정보가 노출되는 경우
5. Denial of Service: 유효한 사용자에 대해 리소스를 사용할 수 없게 만들어 서비스를 거부하는 경우
6. Elevation of Privilege: 권한 없는 사용자가 권한을 얻게 되어 시스템을 조작할 수 있는 경우

2.1.2 LINDDUN

LINDDUN은 Linkability, Identifiability, Non-repudiation, Detectability, Information disclosure, Content unawareness, Policy and consent noncompliance 등 발생 가능한 7가지 보안 위협을 다루므로, 개인정보 관련 위협을 다루기에 적당하다[18].

이 모델은 DFD(Data Flow Diagram)로 표현된 Object, Process, Database, Data Flow에 대해 위협을 식별하는 부분에서 STRIDE와 유사하며, 각각의 위협을 트리로 작성하여 체계화하게 된다. 이후 트리에 대한 상세 설명을 위해 오용 사례 시나리오를 작성하여 위협을 문서화 한 뒤 완화하기 위한 전략을 결정한다. LINDDUN 모델의 속성에 대한 설명은 다음과 같다.

1. Linkability: 획득한 데이터들을 연결하여 데이터 주체를 유추 가능한 경우
2. Identifiability: 획득한 데이터를 통해 데이터 주체를 식별 가능한 경우
3. Non-repudiation: 데이터 주체가 데이터 소유권을 부인하는 것이 불가능한 경우
4. Detectability: 데이터를 통해 주체의 패턴을 구별 가능한 경우
5. information Disclosure: 데이터 주체의 정보가 허가되지 않은 대상에게 노출되는 경우
6. content Unawareness: 데이터 주체가 자신의 데이터 수집, 처리, 저장, 공유를 인식하지 못하는 경우
7. Policy and Consent Non-compliance: 개인정보의 처리, 저장, 취급이 법률을 준수하지 않음.

2.2 COVID-19 접촉 추적 기술 보안 연구 사례

기존 접촉 추적 기술 보안에 관한 연구는 각 추적 기술 방법론에 대해 경험을 기반으로 위협 식별, 분석하는 방향으로 진행되고 있었으나, 최근에는 다양한 접촉자 추적 기술에서 사용되는 공통의 평가 기준을 도출하여 비교 분석하는 연구도 있었다[19].

Pan-European Privacy-Preserving Proximity Tracing(PEPP-PT) 팀에서는 중앙 집중화되지 않은 데이터 관리 개념의 Decentralized Privacy-Preserving Proximity Tracing(DP3T) 라는 기술을 발표 하였다[20]. 이후 DP3T에 대한 보안 평가가 다시금 이루어졌고, 이들은 DP3T의 보안성을 강화시키기 위해 Trusted Platform Module (TPM)의 필수적인 사용을 주장 하였다[21]. 그러나 사실상 TPM은 칩셋마다 구현이 다르고 모든 모바일 기기에 TPM 이 탑재된 것은 아니므로 현실성이 떨어진다.

이후 Google과 Apple에서 COVID-19 접촉 추적 기술과 함께 API가 포함된 구체적인 사양(PPCT)을 내놓았고[22], Yaron Gvili는 PPCT에 대해 Power Drain(전원 및 스토리지 고갈) 공격, Relay and Replay(패킷 중계 및 재전송) 공격, Trolling(감염된 것처럼 속임) 공격, Linking(대상에서 나오는 신호 주기와 파워를 통해 위치를 추정) 공격, Tracking and Deanonymization(신호로 위치를 추정한 뒤 키가 게시되면 대상자의 정보를 추정) 공격 등을 도출하고 그 결과 및 완화 전략을 분석하였다[23]. 상기 나열한 방법론에 대한 보안 분석 및 평가 관련 연구들은 체계적인 방법론에 따라 분석된 것이라고 보기 어렵거나 보완 방향에 대한 구체적인 해결책을 제시하지 못하였다.

반면 Zero Knowledge Proof 관점에서 PPCT에 대해 구체적인 보완책을 제시한 연구도 있다[24]. 그러나 해당 연구에서는 의사의 신분이 밝혀질 수 있고 이 경우 환자의 신분이 간접적으로 노출되는 문제를 막지 못했다.

본 논문은 보안 기법에 따라 체계적으로 분석하여 가능한 보안 문제를 도출해 보고, 해당 문제들을 해결해 보안성을 향상할 수 있는 설계를 제시한다.

III. PPCT에 대한 보안성 평가 기준 도출

3.1 Data Flow Diagram (DFD)

본 논문에서는 취약점, 개인정보보호 관점에서 위협을 식별하기 위해 STRIDE와 LINDDUN을 적용하였다. 이 둘은 DFD로 표현된 Object, Process, Database, Data Flow에 대해 위협을 식별하는 부분에서 유사하므로, PPCT Spec자체에 대한 전반적인 구조를 파악하기 위해 Spec에 대한 DFD를 작성하였다.

사양(Specification)은 각 국가와 플랫폼(Android/iOS)의 구현방식에 따라 코드가 조금씩

달라질 수 있으므로 작성 시 함수 단위의 구현 레벨은 생략하였다. PPCT의 DFD 작성결과는 [Fig.1]이며, 각 부분에 대한 자세한 설명은 다음과 같다.

1. 두 사용자 [E1][E2]는 각자 자신의 스마트폰을 들고 접촉한다.
2. 두 블루투스 프로세스[P1]는 보낼 Payload를 준비한다[P2]. 이때 방송 주기는 200~270ms이다.
3. 사용자들은 각자 임시 키 교체 주기[P4]인 24시간마다 Temporary Exposure Key(TEK)를 랜덤하게[P5] 생성하여[P6] 저장하고 있다[D1].
4. 두 모듈은 주소 순환 시간 주기(10~20분 사이, 약 15분)마다 동시에[P4] AES-128 암호화한 Rolling Proximity Identifier(RPI), Associated Encrypted Metadata(AEM)를 생성해야 한다.
5. TEK로부터 RPI Key를 생성하고, 이 키로 RPI를 생성한다[P7].
6. TEK로부터 AEM Key를 생성하고, 생성했던 RPI와 RPI Key를 사용해 AEM을 생성한다[P8].
7. 두 사용자는 각 RPI, AEM을 기반으로 생성한 Payload를 교환하고 저장한다[D2].
8. 이후 확진자는 Health Authority[E3]에 의해 확진 판정을 받았고, 판정 전 COVID-19 가 접촉자에게 이동했을 가능성이 있다.
9. 따라서 확진자는 이 결과를 진단 서버에게 알리기 위해 데이터베이스[D3]에 저장된 TEK들을 보낸다[P11].
10. 진단 서버[D4]는 확진자의 진단키를 다른 사용자들이 다운로드 받을 수 있도록 게시한다[D5].
11. 각 사용자는 진단 키 다운로드 주기[P3]에 따라 진단키를 다운로드 받는다[P13].
12. 진단 키로부터 다른 키들을 도출하고 이전에 다른 사용자에게 받았던 payload를 복호화하여 위험성을 도출한다[P14].
13. 확진자와 밀접 접촉하여 위험성이 크다고 판단되면[P15], 접촉자에게 알려준다[P16].

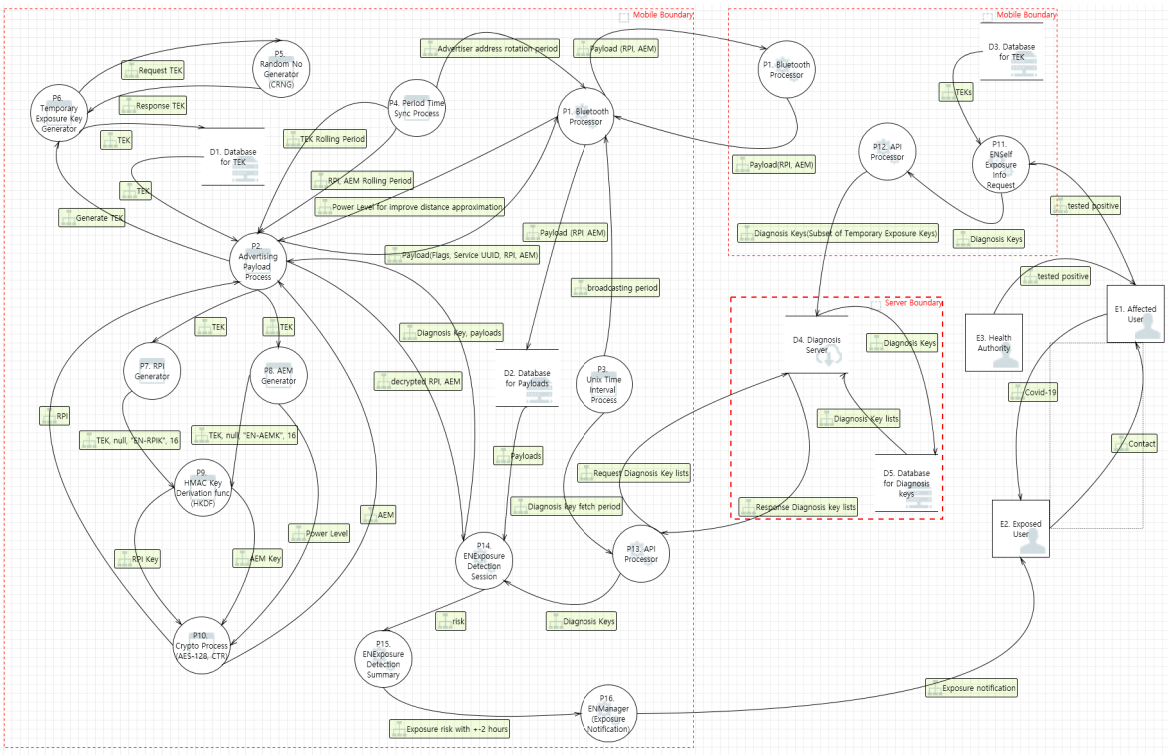


Fig. 1. PPCT Data Flow Diagram

3.2 Attack Library

Attack Library는 분석하는 대상에서 발생할 수 있는 공격들의 리스트로, 본 논문에서는 Attack Library 작성을 위해 Bluetooth, Server, Mobile과 관련된 신뢰 가능한 기관 혹은 기술 보고서, 논문, 표준, 발표, 취약점 데이터베이스를 수집하였다.

수집한 공격 리스트의 타입과 연도, 제목, 출처 및 저자의 일부는 Table 1.과 같다.

이러한 Attack Library를 작성하면 분석 대상의 보안 위협을 구체화할 수 있으며, 알려진 공격 지점 및 방법, 유형을 보안성 평가 지표에 상세히 반영할 수 있다.

추가로, 수집한 공격 리스트 일부의 제목과 카테고리 그리고 상세 설명은 Table 2.와 같다.

Table 1. PPCT Attack Library

No	Type	Year	Title	Ref
1	Vulnerability	2020	CVE-2020-6616	[28]
2		2020	CVE-2020-0022	[29]
3		2020	CVE-2020-9770	[30]
4		2020	CVE-2020-9023	[31]
24	Paper	2020	Security Analysis Of The COVID-19 Contact Tracing Specifications By APPLE INC. And GOOGLE INC.	[23]
25		2020	The pandemic of social media panic travels faster than the COVID-19 outbreak	[32]
26		2019	Tracking Anonymized Bluetooth Devices	[33]
27		2019	SMART HOME PERSONAL ASSISTANTS: A SECURITY AND PRIVACY REVIEW	[34]
28		2018	Testing vulnerabilities in Bluetooth Low Energy	[35]
29		2018	Ransomware Prevention using Application Authentication-Based File Access Control	[36]
30		2018	Implementing Privacy Policy: Who should Do What?	[37]
31		2018	AES Vulnerabilities Study	[38]
34	Conference	2017	Exploiting BlueBorne	[39]
35		2014	MITM on smartphones	[40]
37	Technical Report	2017	Gattacking Bluetooth Smart Devices	[41]
38		2015	Making an SSL Auditing Proxy with a Mac and Burp	[42]
39	Web document	2016	CALLJAM	[43]
40		2008	CRNG Cracked - SSH Vulnerable	[44]

Table 2. PPCT Attack Library with explanation

no	Title	Category	Explanation
1	CVE-2020-6616	Network	The randomness implementation does not meet the requirements of the Bluetooth Core Specification
2	CVE-2020-0022	Network	Remote attacker within proximity can silently execute arbitrary code with the privileges of the Bluetooth daemon as long as Bluetooth is enabled. No user interaction is required and only the Bluetooth MAC address of the target devices has to be known. For some devices, the Bluetooth MAC address can be deduced from the WiFi MAC address.
3	CVE-2020-9770	Network	An attacker in a privileged network position may be able to intercept Bluetooth traffic.
4	CVE-2020-9023	Network	devices have two users that are not documented and are configured with weak passwords
24	Security Analysis of the CCPT	Platform	SECURITY ANALYSIS OF THE COVID-19 CONTACT TRACING SPECIFICATIONS BY APPLE INC. AND GOOGLE INC.
25	The pandemic of social media panic travels faster than the COVID-19 outbreak	Social	Need to unpack the influence of social media on such measures that carry a huge economic loss.
26	Tracking Anonymized Bluetooth Devices	Network	The vulnerability discovered by BU researchers exploits this secondary random MAC address to successfully track a device.
27	SMART HOME PERSONAL ASSISTANTS: A SECURITY AND PRIVACY REVIEW	Platform	review of the security and privacy issues in SPA, categorizing the most important attack vectors and their countermeasures.
28	Testing vulnerabilities in Bluetooth Low Energy	Network	There are known vulnerabilities in the Bluetooth protocol, and that given the right technology, those vulnerabilities can be exploited.
29	Ransomware Prevention using Application Authentication-Based File Access Control	OS	Ransomware may attempt to attack AntiBotics and explain how these attacks can be thwarted.
30	Implementing Privacy Policy: Who should Do What?	Policy	Without substantial upgrades of institutions and infrastructure, privacy law and policy will continue to fall short of what it should achieve.
31	AES Vulnerabilities Study	Crypto	Particular weak values that can be inserted in the data stream by an attacker in order to get the key are found.
34	Exploiting BlueBorne	Network	Exploiting BlueBorne in Linux-based IoT devices
35	MITM on smartphones	Network	Mitigating man-in-the-middle attacks on smartphones
37	Gattacking Bluetooth Smart Devices	Network	Introducing a New BLE Proxy Tool
38	Making an SSL Auditing Proxy with a Mac and Burp	Network	Many mobile apps don't properly implement SSL/TLS.
39	CALLJAM	OS	CallJam malware includes a premium dialer to generate fraudulent phone calls
40	CRNG Cracked - SSH Vulnerable	OS	OpenSSL bug is to reduce the entropy in the seed to only 15 bits

3.3 STRIDE Threat Modeling

3.3.1 STRIDE

앞서 설명한 바와 같이 STRIDE는 보안 전문가가 아닌 사용자를 염두에 두고 개발되었기 때문에, 모든 개발자가 위협 모델링을 수행할 수 있도록 정확한 지침을 제공하고 있어 분석 대상의 전 범위에 대해 누락을 최소화하며 분석하는 것이 가능하다.

다음 Table 3.은 기존에 분석한 DFD 요소에 따라 STRIDE를 이용해 위협을 식별한 결과 일부를 보여주며, Attack library 사용 여부 및 상관관계를 포함하였다.

Table 4. DFD Elements per STRIDE

	S	T	R	I	D	E
Entity	√		√			
Process	√	√	√	√	√	√
Data Flow		√		√	√	
Data Store		√	√	√	√	

Table 4.는 STRIDE를 이용해 적용 가능한 DFD에 따라 √ 표시한 것으로, Table 3.을 만들 때 근거로 사용한 것이다. 이것은 위협 적용 가능성이 있다는 의미이며, 반드시 포함되는 것은 아니다. 일례로 DB에 대한 Repudiation은 log를 포함하

Table 3. STRIDE for PPCT DFD

Type	No	Name	Threat Description		Attack Library	Threat No
Entity	E1	Affected User	S	DoS attacks cause social panic by tricking the Affected User.	25	T1
Entity	E1	Affected User	R	Deny the diagnosis result by Affected User.	3	T2
Entity	E2	Exposed User	S	Social panic by Attacker who creates a large amount of random packets.	25	T3
Entity	E2	Exposed User	R	DoS attacks cause social panic by tricking the Affected User.	3	T4
Process	P1	Bluetooth Processor	S	Linking through random mac address estimation.	40	T8
Process	P2	Advertising Payload Process	I	Extract TEK through system information leakage or sniffing.	10,11	T15
Process	P3	Unix Time Interval Process	D	Editing the time period causes denial of service	7,8,12, 13	T16
Process	P5	Random No Generator(CRNG)	I	Estimates TEK with low randomness	40	T18
Process	P7	RPI Generator	E	RPI creation through elevation of privilege	7,8,12, 13	T20
Process	P8	AEM Generator	E	AEM creation through elevation of privilege	7,8,12, 13	T21
Process	P12	API Processor	S	Illegal access to user's information through sniffing or MiTM.	35,38	T27
Process	P12	API Processor	T	Infected information transmitted by man-in-the-middle attack.	35,38	T28
Process	P15	ENExposure Detection Summary	T	Social media panic due to incorrect risk calculation.	25,36	T37
Datastore	D2	Database for Payloads	T	Malicious modification of payload data through SQL injection.	33	T42
Datastore	D3	Database for TEK	T	Malicious modification of TEK data through SQL injection.	33	T44
Datastore	D4	Diagnosis Server	T	Intercept and editing data through man-in-the-middle attacks	32	T47
Datastore	D5	Database for Diagnosis keys	T	Malicious modification of Diagnosis key through SQL injection.	33	T52

고 있는 경우에만 가능한데, 일반적으로 스마트폰에서는 Datastore에 log를 저장하는 대신 출력한다.

3.3.2 Attack Tree

분석 대상에 대한 모든 보안 위협을 체계화하기 위해 Attack Tree를 작성하였다. STRIDE를 기준으로 작성하였으므로 개인 정보 측면보다는 공격에 의한 Social Panic의 측면에서 작성하였다.

Attack Tree 작성결과 크게 서비스 거부, 감염 정보 오남용에 대한 공격이 있었고 상세하게는 네트워크 공격, 시스템 공격, 물리적 공격, 알고리즘에 대한 공격이 있었다(Fig.2).

지금까지 STRIDE 위협 모델링을 통해 취약점 관점에서 PPCT의 보안 위협을 식별하였고, 다음 장에서는 개인 정보에 대한 위협을 도출하기 위해 LINDDUN을 사용하여 보안 위협을 도출한다.

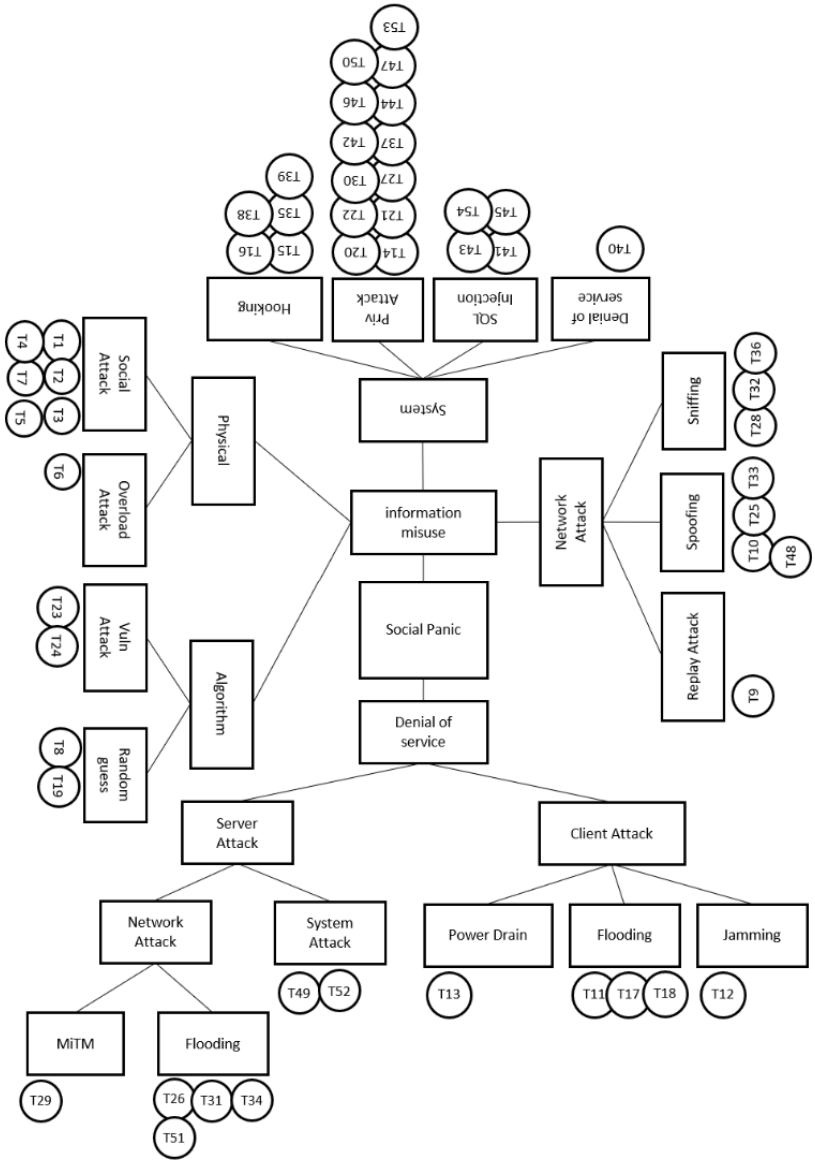


Fig. 2. PPCT Attack Tree

3.4 LINDDUN Threat Modeling

3.4.1 LINDDUN

LINDDUN은 개인정보보호 관점의 위협모델로, DFD를 기반으로 분석한다는 부분에서 STRIDE와 비슷하다. Table 5.는 LINDDUN을 이용해 적용 가능한 DFD에 따라 √ 표시한 것이다.

〔Table 5〕를 바탕으로 DFD에 기반해 PPCT에 대한 LINDDUN 위협을 식별하였으며, 그 결과는 〔Table 6〕 에 LINDDUN 순서대로 L, I, N, D, D2, U, N2 로 Mapping 하여 작성하였다.

Table 5. DFD Elements per LINDDUN

	L	I	N	D	D	U	N
Entity	√	√				√	
Process	√	√	√	√	√		√
Data Store	√	√	√	√	√		√

Table 6. LINDDUN for PPCT DFD

Type	No	Name	LINDDUN
Entity	E1	Affected User	L
Entity	E1	Affected User	U
Entity	E2	Exposed User	L
Entity	E3	Health Authority	I
Entity	E3	Health Authority	N2
Process	P1	Bluetooth Processor	L
Process	P1	Bluetooth Processor	D
Process	P2	Advertising Payload Process	N2
Process	P3	Unix Time Interval Process	L
Process	P4	Period Time Sync Process	L
Process	P5	Random No Generator(CRNG)	L
Process	P6	Temporary Exposure Key Generator	L
Process	P7	RPI Generator	L
Process	P8	AEM Generator	L
Process	P9	HMAC Key Derivation func (HKDF)	L
Process	P10	Crypto Process (AES-128, CTR)	D2
Process	P11	ENSelf Exposure Info Request	I
Process	P11	ENSelf Exposure Info Request	U
Process	P11	ENSelf Exposure Info Request	N2
Process	P12	API Processor	L
Process	P12	API Processor	I
Process	P12	API Processor	U
Process	P12	API Processor	N2
Process	P13	API Processor	N2
Process	P14	ENExposure Detection Session	N2
Process	P15	ENExposure Detection Summary	D2
Process	P16	ENManager(Exposure Notification)	D2
Datastore	D1	Database for TEK	L
Datastore	D1	Database for TEK	U
Datastore	D2	Database for Payloads	L
Datastore	D2	Database for Payloads	U
Datastore	D3	Database for TEK	L
Datastore	D3	Database for TEK	U
Datastore	D4	Diagnosis Server	L
Datastore	D4	Diagnosis Server	U
Datastore	D5	Database for Diagnosis keys	L
Datastore	D5	Database for Diagnosis keys	U
Datastore	D5	Database for Diagnosis keys	N2

3.4.2 Threat Tree

DFD에 대한 위협이 식별되었으므로 LINDDUN 모델에서 도출한 위협을 대상으로 하여 Threat tree를 작성한다.

Table 7. A part of Process of LINDDUN

LINDDUN				Attack Library
Linkability	P1	Data subject identification by inference through signals		2, 3, 9 35,38, 39
		P3	Linking information through broadcasting cycle	
		P4	Linking information through address synchronization cycle	
		P12	Linking information through sniffing and spoofing	
	P5	Inferring MAC address through an weak randomness		1, 2, 31
		P9	Possibility of random key collision using weak hashing algorithm	
	P6	TEK collection through privilege elevation and hooking		7,8, 12,13
		P7	RPI collection through privilege elevation and hooking	
		P8	AEM collection through privilege elevation and hooking	
Non-Compliance	P2	Personal information leakage through payload collection		10, 11, 30
		P11	Affected user information is processed without compliance	
		P12	Information leakage about infection without compliance	
		P13	Cookies does not comply with the law	
		P14	Infection risk information does not comply with the law	

Threat tree는 위협의 범주를 세분화해서 표현하는 것으로, 〔Table 7〕은 문서 형태로 작성한 PPCT에 대한 Threat tree 중 일부를 보여준다. STRIDE와 마찬가지로 Attack library와의 상관관계를 포함하였다.

3.4.3 Misuse Case

Threat tree에 대한 이해도를 높이기 위해 Misuse Case(MUC)를 작성하며, 각 위협이 어떻게 발생할지 식별자, 공격자, 시나리오, 결과 등을 포함하여 작성한다.

〔Table 8〕 은 Threat tree에 관한 MUC의 일부를 보여 준다.

Table 8. A part of Misuse Case

Misuse Case 1	Details	
	Tree	Linkability
	Summary	Attackers can connect information such as MAC, timing, and signal strength.
	Attacker	An attacker who wants information from an Affected user
	Scenario	bf1. Bluetooth MAC address inference through Wifi signal
		bf2. Inferring MAC address through an weak randomness
		bf3. Linking information through address synchronization cycle
		bf4. Linking information through broadcasting cycle
		bf5. Possibility of random key collision using weak hashing algorithm
		bf6. TEK, RPI, AEM collection through privilege elevation and hooking
	Result	User identification through Key, MAC, Cycle timing

Misuse Case 2	Details	
	Tree	Non-Compliance
	Summary	User information is processed without compliance
	Attacker	Theft of sensitive data. Such attacks lead to high financial loss.
	Scenario	bf1. Personal information leakage due to government server
		bf2. Exposed user information is processed without compliance
		bf3. Affected user information is processed without compliance
		bf4. Cookies does not comply with the law
		bf5. Infection risk information does not comply with the law
	Result	Authorities will have the ability to impose fines of up to 20 million euros or 4% of a company's total global annual turnover. (GDPR)

IV. 평 가

4.1 PPCT에 대한 개선안

우리는 3장에서 PPCT Spec에 대한 체계적인 분석을 토대로 크게 개인 정보 노출, 감염 정보 오남용에 대한 공격이 가능하다는 사실을 알게 되었다. 구체적으로는 첫 번째 Misuse Case 1에 의해서 Diagnosis Server에서 User의 정보를 폐기하지 않는 경우 개인을 식별할 수 있다는 것을 알 수 있었고, 두 번째로 Misuse Case 2에 의해 키 정보 등 의사의 정보가 노출되면 Linking 되어 확진자의 정보가 간접적으로 노출될 수 있다는 것을 알 수 있다. 마지막으로 STRIDE의 Attack Tree에서 확인된 T10, T25, T33, T48 등 Spoofing 공격으로 인해 감염자의 감염 사실이 숨겨진다면, 접촉자들은 확산 예방 조치가 어려워져 사회 혼란 및 앱의 존재 이유 자체가 훼손되는 문제가 있다.

따라서 본 논문에서는 zkSNARKs[25]와 PKI[26]를 도입함으로써 위 세 가지 문제인 위변조와 개인 정보 유출 문제를 해결하고 나아가 서비스의 실용성과 확장성을 확보하고자 한다.

zkSNARKs는 증명자와 검증자 간의 상호작용을 통한 증명 시스템인 영지식 증명의 일종으로, 간결성과 비 상호작용성을 특징으로 한다.

여기서 간결성은 검증자로서 연산의 간결함을 의미한다. 한정된 자원을 가진 검증자가 복잡한 연산을 증명자에게 위임하고, 증명자는 연산을 수행한 후, 결괏값과 연산의 무결성을 증명하는 증명을 돌려주면 이를 바탕으로 검증자가 검증을 수행하게 된다. 증명자와 검증자는 사전에 신뢰 설정 단계에서 검증에 필요한 증명 키와 검증키를 나누어 가진다. 이 값은 증명 생성과 검증에 사용한다.

zkSNARKs 에서 우리가 주목한 3가지 핵심 특성은 다음과 같다:

1. Short proof in constant size : 증명 생성 시 입력 치수나 연산의 복잡도와 상관없이 증명의 크기는 항상 288 bytes로 일정해서 서버에서 동시에 많은 peer 노드에게 방송 시 대역폭 비용에 대한 부담이나 데이터 손실에 따른 거짓 양성/음성 발생 확률이 낮다.
2. Independent Verification cost: 증명 비용은 증명 생성 시 입력 크기 또는 연산의 복잡도와는 독립적이기 때문에 본래의 연산 수행 대비 훨씬 경제적이고 빠른 검증이 가능하여서 네트워크 확장성에 이점이 있다.
3. zero-knowledge for data privacy : 증명자는 증명 생성 시 비밀 입력값을 받아 생성할 수 있고, 검증자는 연산과 그 결과에 대한 무결성을 제외하고는 아무런 정보도 알 수 없다.

두 번째로 PKI는 디지털 인증의 관리와 공개키 암호화의 관리에 쓰이는 소프트웨어, 하드웨어, 절차의 집합이다. 여기서 PKI는 의사 협회 등 공개되어도 되는 인증 기관을 통해 영지식 증명에 서명하고 실제 의사의 정보는 기관에 숨겨 의사의 어떠한 정보도 드러나지 않게 하는 역할을 한다.

본 논문에서는 위 성질들을 이용해 확진자와 접촉자, 의사의 개인 정보 유출을 최소화하면서도 실제 구현 가능한 추적 서비스를 제안하고자 한다.

[Fig.3]에서 A와 B는 같은 시간 같은 장소에 있었고, 각각의 장치는 500ms에 한번 BLE 방송을 하는데, 이때 사용되는 BLE 무작위 맥 주소는 15분에 한 번 혹은 호스트가 설정한 시간 주기로 생성

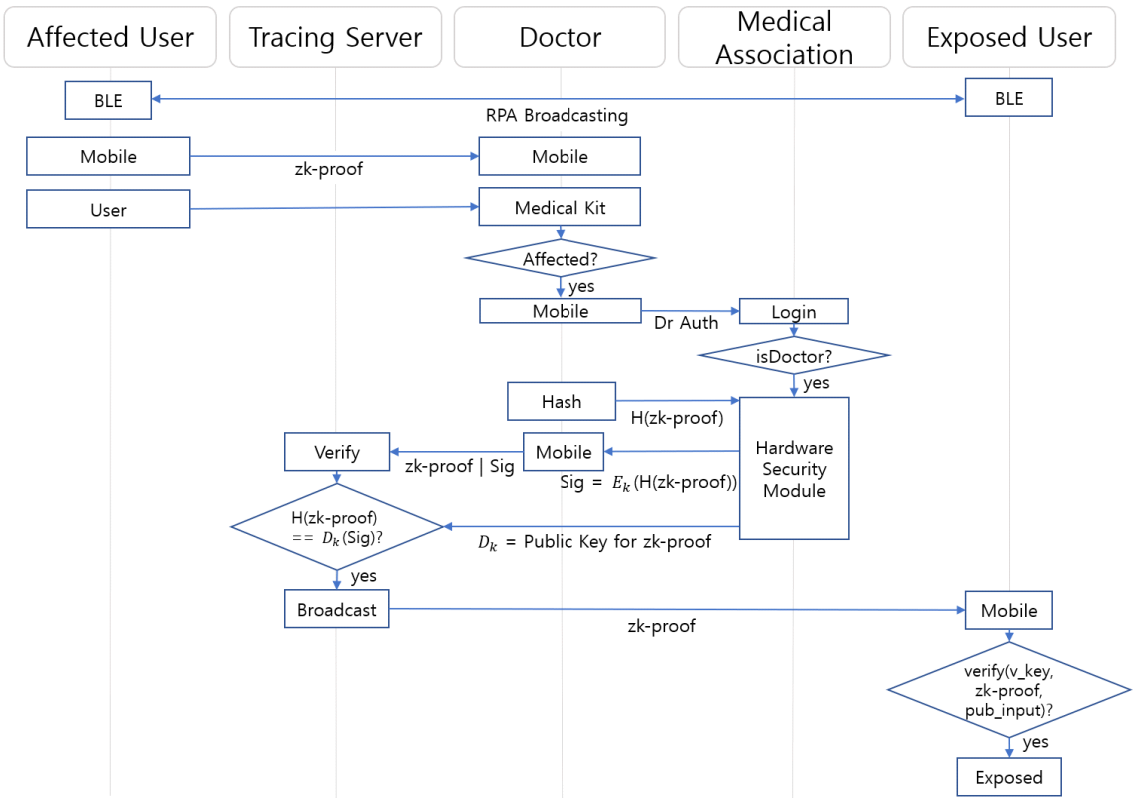


Fig. 3. Data Flow

된다. 여기서 BLE 무작위 맥 주소는 Bluetooth Core Spec[27] 상에 Resolvable Private Address(RPA)를 의미한다. RPA는 BLE bonding 과정에서 형성된 보안 연결 채널을 통해 주고받은 Identity Resolving Key(IRK)를 통해 resolve 가능한 주소를 의미한다. RPA가 생성되는 방식을 보면 명세에 기재된 해시함수를 통해 IRK와 pseudo random seed number를 입력 매개변수로 받아 24bit 해시가 생성되면 해시값 24bit와 random seed number 24bit를 연결해 구성한다. 기존에는 재연결을 위해 IRK가 전달되나, 기기의 고유한 값이고 다른 정보와의 연결을 통해 개인 정보 침해 문제 발생의 우려가 있어서 A는 IRK 대신 자신의 RPA 즉, BLE 무작위 맥을 방송하고 주위에 있던 B는 BLE 무작위 맥을 저장한다.

A는 확진자가 되면 증명자로서 zero knowledge proof(zk-proof)를 생성하게 된다.

zk-proof = prove(pv_key, pub_input, priv_input)

Computation logic은 논리게이트로 구성된 Circuit으로 바뀌고, zkSNARKs를 적용 가능한 문제 형태인 Quadratic Arithmetic Program(QAP)으로 변경된다. 작성된 circuit 로직은 polynomial을 만족하는 witness를 알고 있음을 증명하는 문제로 바뀌게 되는데, witness는 입력값인 공개 입력값, 비공개 입력값과 계산과정에 필요한 중간값들을 의미한다.

```
def circuit(IRK) :
  prand' = BLE random mac'A& 0...0 | 1...1
  localhash=H(IRK, prand')
  h= BLE random mac'A& 1....1 | 0...0
  if(h==localhash) Exposed
```

여기서 증명 생성을 위한 circuit은 모든 노드 즉, 이 서비스를 이용하는 모든 사용자가 확진자와의 접촉 여부를 판단하기 위해 수행해야 하는 연산을 의

미하며, 연산은 LE Core 명세에 기재된 RPA를 resolve 하는 로직에 따라 구성된다.

RPA resolve 로직은 먼저 bit masking을 통해 RPA의 상위 24bit prand 부분을 얻어온 뒤, 해시함수인 H(IRK, prand)를 실행해 로컬 해시를 계산하고 이 값을 다시 RPA의 하위 24bit 해시값과 같은지 비교함으로써 RPA를 생성할 때 사용한 IRK와 동일한지 즉, 동일 디바이스인지 확인할 수 있다.

IRK는 비공개 입력값으로 증명자가 연산을 zk-proof로 구성하는 과정에서 들어가고 검증자에게는 노출되지 않는다. BLE 무작위 주소는 공개된 입력값으로 zk-proof와 함께 전달되어 검증자가 검증 시 대입해야 하는 값이지만, 여기서는 검증자가 자신의 로컬 데이터베이스에 저장되어있는 RPA 목록을 순회하며 직접 대입해 검증을 진행한다.

따라서 A는 IRK, RPA가 아닌 zk-proof 값만을 의사에게 전달하고, 의사는 의사 협회에 로그인한 뒤 A의 zk-proof 해시값만 전달하고, 협회에서는 해당 해시값을 Hardware Security Module(HSM)의 보호된 비공개키로 서명한다. 이후 의사는 이 서명 값을 받아 정부가 운영하는 Tracing Server로 전달한다.

Tracing Server는 의사에게 받은 zk-proof와 서명 값을 의사 협회 공개키로 검증하며, 검증에 성공하는 경우에만 zk-proof를 배포한다.

이후 사용자들은 받은 zk-proof를 검증자로서 검증하게 된다. 검증 시 검증키와 서버로부터 받은 zk-proof와 공개 입력값이 필요한데, 여기서 공개 입력값은 앞서 언급했듯이 로컬 데이터베이스에 저장하고 있는 RPA이다. 따라서 자신이 저장하고 있던 RPA 리스트 중 어느 하나라도 검증 결괏값이 참이 되면 자신이 밀접 접촉자였음을 확인할 수 있다.

하지만 사용자들은 자신이 확진자와 밀접 접촉했다는 사실 외에 확진자와 의사를 특정할 수 있는 개인 정보를 얻을 수 없음은 물론이며, 무선으로 전달해야 하는 데이터양은 최소화함으로써 대역폭 비용과 데이터 손실을 줄여 확장 및 실현 가능한 서비스도 가능하다.

4.2 한계점

먼저 본 연구 결과에 따르면 문제 해결을 위해 정부와 의사 협회 등 국가적 차원의 참여가 필요한데, 한국을 포함한 여러 국가에서 PPCT를 아직 개발 중이거나 개발 시작조차 되지 않은 경우가 많고, 개발되었더라도 Governance 및 Compliance 문제 때문에 실질적인 구현 및 모의 해킹에 대한 참여가 제한되어 있다는 한계점이 있다.

또한 개선안은 24시간 동안 유지되는 TEK 및 15분마다 교체되는 RPI Key, AEM Key 등 키들을 사용하지 않고도 추후 감염자와의 접촉 여부를 알 수 있게 함으로써 키 수집 등 키 관련 취약점으로 인한 개인 정보 유출의 가능성을 완전히 없앴다. 그러나 이 때문에 전파의 세기인 Transmit(Tx) Power 등의 데이터를 AEM Key로 암호화해서 상대방에게 보내는 부분도 함께 사라졌다.

블루투스 기기 간 전파 거리 산정은 다음과 같이 TxPower, Received Signal Strength Indication (RSSI) 값으로 이루어지는데, 상대방의 TxPower값 없이 RSSI 만으로 거리를 추정하면 거리에 대한 정확도가 떨어지게 된다.

distance = 10 ^ ((TxPower - RSSI) / (10 * noise))

따라서 제시한 것처럼 TxPower 값을 보내지 않는 경우, 접촉자에 대한 감염 위험도 산정 또한 정확도가 떨어질 수 있다. 다만 최초 기기에서 AEM을 전달하고, zk-proof와 함께 AEM Key를 제공하면 15분 동안의 추적성만 가지고 접촉 거리 및 감염 위험 정확도를 높이는 구조로 구성하는 것이 가능하다. 이는 개인정보보호와 감염 위험 정확도의 교환 관계가 되므로, 판단에 따라 구현 시 선택이 가능한 부분이다.

그리고 제시된 개선안은 개인뿐만 아니라 의사의 개인 정보에 대해서도 완전한 통제를 다루므로, 확진자 개개인에 대해 상세한 데이터 분석이 필요한 경우 사용하기 어렵다. 하지만 본 설계에 따르면 의사의 군집 데이터는 의사 협회로부터 얻을 수 있게 되므로, 본 개선안을 적용했을 때 통계적 분석은 가능할 것으로 보인다.

V. 결 론

본 논문에서는 COVID-19의 확산을 막기 위해 개발된 PPCT에 대해 보안 평가 기준을 도출하고, STRIDE와 LINDDUN을 활용해 취약점 및 개인

Table 9. Roles and Access permissions

	IRK	Proof	DrID	Diagnosis
Doctor	X	O	X	O
Medical Association	X	X	O	X
Tracing Server	X	O	X	X
Exposed User	O	O	X	X
Affected User	O	O	X	O

정보보호 관점으로 보안성 평가를 수행하였다.

그 결과, 크게 개인 정보 노출, 감염 정보 오남용에 대한 공격이 가능했고 이를 통해 PPCT의 미사용뿐만 아니라 Social Panic과 같은 심각한 문제가 발생할 수 있다는 결과가 도출되었다.

따라서 본 논문에서는 이를 해결하기 위해 PPCT의 Diagnosis Server를 Medical Association과 Tracing Server로 분리하여 zkSNARKs, PKI 사용하는 방안을 제시하였고, 이 설계에 따르면 각 개체에서 획득 가능한 정보(O)와 획득 불가능한 정보(X)의 관계는 〔Table 9〕와 같아진다.

이를 통해서 크게 3가지 문제점을 해결할 수 있다.

첫째로, 기존에는 Diagnosis Server에서 정보를 폐기하지 않으면 정보의 연결이 가능했으나, 제안된 구조에서는 의사와 의사 협회, 정부가 함께 연합하여도 IRK와 Diagnosis를 연결할 수 없으므로 정부는 개인을 식별할 수 없다.

두 번째로, 기존 zero-knowledge 관련 연구〔24〕에서는 의사의 키 정보(소아청소년과 전문의 등)가 노출되면 해당 확진자가 아동이라는 것 등이 간접적으로 노출되는 문제가 있었으나, 제안된 구조에서는 허가된 의사들이 의사 협회의 키를 사용해 서명하므로 의사 개인에 대한 정보가 노출되지 않는다.

마지막으로, 기존에는 확진자가 감염 사실을 알리지 않으면 접촉자들을 속일 수 있었지만, 제안된 구조에서는 확진을 감지한 의사도 접촉자의 RPA 정보를 모르는 상태에서 zk-proof를 전송할 수 있으므로, 감염자가 스스로 감염을 숨길 수 있는 문제를 해결할 수 있다.

다만 본 연구는 개발과 관련한 관계자들의 참여가 제한되어 있으므로, 이후 실제 구현 관련 개발자의 참여와 함께 보안성 평가를 통해 잠재적인 취약점까지 고려하여 평가 기준을 도출하고 해결하는 연구를 진행할 예정이다.

References

〔1〕 WHO, "COVID 19 Public Health Emergency of International Concern," *GLOPID-R*, Feb. 2020.

〔2〕 UN High Commissioner, "The coronavirus outbreak is a test of our systems, values and humanity," *UNHCR*, Mar. 2020.

〔3〕 National Human Rights Chairman, "Corona19 Crisis, a test stand to verify human rights capabilities in our society," *National Human Rights Commission,* Apr. 2020.

〔4〕 Jung Yeon-je, "South korea is reporting intimate details of covid-19 cases: has it helped?," *Nature*, Mar. 2020.

〔5〕 Seo Hangi. "If the public announcement of the movement about Corona 19 is invading privacy? Can be corrected by appealing," *yunhap news*, Mar. 2020.

〔6〕 Lambert S, Ostwald T, Shostack A, Hernan, S. "Threat modeling uncover security design flaws using the stride approach," *MSDN Magazine-Louisville*, pp. 68-75. Nov. 2016.

〔7〕 Marco M, Tony U. "Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis," pp. 1-696. *John Wiley Sons*, May. 2015.

〔8〕 James S, Carol W, Christopher A, Audrey D. "Introduction to the OCTAVE Approach," *SEI,* pp. 1-37. Sep. 2003.

〔9〕 "ETSI TS 102 165-1 v4.2.3 - Telecommunications and Internet converged Services and Protocols for Advanced Networking(TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis," pp. 1-79. Mar. 2011.

[10] James S, Carol W, Christopher A, Audrey D. "Systems thinking for safety and security," *Proceedings of the 29th Annual Computer Security Applications Conference*, pp. 1-8. Dec. 2013.
[11] Joosen W, Wuyts K. "LINDDUN privacy threat modeling: a tutorial," pp. 1-38. Jul. 2015.
[12] Bradley Potteiger, Goncalo Martins, Xenofon Koutsoukos. "Software and attack centric integrated threat modeling for quantitative risk assessment," In Proceedings of the Symposium and Bootcamp on the Science of Security, pp. 99-108. *Potteiger,* Apr. 2016.
[13] Tadayoshi K, Tamara D, Batya F. Poster, "The security cards: a security threat brainstorming toolkit," *University of Washington*, 2013.
[14] Shull F, Vemuru K, Villadsen O, Mead N. "A Hybrid Threat Modeling Method," *Carnegie Mellon University - Software Engineering Institute,* pp. 1-53. Mar. 2018.
[15] Larcom B, Eddington M, Saitta, P. "Trike v1 methodology document," pp. 1-17. Jul. 2005.
[16] A. Agarwal. "Vast methodology: Visual, agile, and simple threat modeling," *Prescott Valley*, 2016.
[17] Microsoft, "Microsoft threat modeling tool threats," *microsoft docs.* Aug. 2017.
[18] Kristian Beckers, "Comparing Privacy Requirements Engineering Approaches," 2012 7th IEEE International Conference on Availability, Reliability and Security(ARES), pp. 574-581, Aug. 2012.
[19] Hojun Lee, Seungjoo Kim, Sangjin Lee. "Evaluation Criteria for COVID-19 Contact Tracing Technology and Security Analysis," Korea Institute Of Information Security & Cryptology, Dec. 2020.
[20] Carmela Troncoso. "Decentralized Privacy-Preserving Proximity Tracing," *Arxiv*, Apr. 2020.
[21] Serge Vaudenay. "Analysis of DP3T Between Scylla and Charybdis," *IACR,* Apr. 2020.
[22] Apple, Google, "Privacy-Preserving Contact Tracing ver 1.2 BY APPLE INC. AND GOOGLE INC," Apr. 2020.
[23] Yaron Gvili. "SECURITY ANALYSIS OF THE COVID-19 CONTACT TRACING SPECIFICATIONS BY APPLE INC. AND GOOGLE INC," *Arxiv,* https://eprint.iacr.org/2020/428 Apr. 2020.
[24] Joseph K. Liu, Man Ho Au, Tsz Hon Yuen, Cong Zuo, Jiawei Wang, Amin Sakzad, Xiapu Luo, and Li Li. "Privacy-Preserving COVID-19 Contact Tracing App: A Zero-Knowledge Proof Approach," *Arxiv*, Jul. 2020.
[25] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct non-interactive zero knowledge for a von neumann architecture." *USENIX Security Symposium,* pp. 781 - 796. 2014.
[26] W. Diffie, E. Hellman, "New Directions in Cryptography," *IEEE Transaction on theory,* Nov. 1976.
[27] Bluetooth SIG. "Core Specification," https://www.bluetooth.com/specifications/bluetooth-core-specification 5.2, Dec. 2019.
[28] Nist, "CVE-2020-6616," https://nvd.nist.gov/vuln/detail/ CVE-2020-6616, Aug. 2020.
[29] Nist, "CVE-2020-0022," https://nvd.nist.gov/vuln/detail/ CVE-2020-0022, Feb. 2020.
[30] Nist, "CVE-2020-9770," https://nvd.nist.gov/vuln/detail/ CVE-2020-9770, Apr. 2020.
[31] Nist, "CVE-2020-9023," https://nvd.nis

t.gov/vuln/detail/ CVE-2020-9023, Feb. 2020.

[32] Depoux A, Martin S, Karafillakis E, Preet R, Wilder-Smith A, Larson H. "The pandemic of social media panic travels faster than the COVID-19 outbreak," *J Travel Med.* May. 2020.

[33] Becker, Johannes & Li, David & Starobinski, David. "Tracking Anonymized Bluetooth Devices," *Proceedings on Privacy Enhancing Technologies.* Jul. 2019.

[34] Jide S. Edu, Jose M. Such, and Guillermo Suarez-Tangil. "Smart Home Personal Assistants: A Security and Privacy Review," *ACM Comput,* Dec. 2020.

[35] Thomas Willingham, Cody Henderson, Blair Kiel, Md Shariful Haque, and Travis Atkison. "Testing vulnerabilities in bluetooth low energy," *ACMSE*, Mar. 2018.

[36] Or Ami, Yuval Elovici, and Danny Hendler. "Ransomware prevention using application authentication-based file access control," *SAC,* Apr. 2018.

[37] Hyman, David A. and Kovacic, William E., "Implementing Privacy Policy: Who Should Do What?," *GWU Legal Studies Research Paper*, Feb. 2018.

[38] L. Scripcariu, F. Diaconu, P. D. Mătăsaru and L. Gafencu, "AES Vulnerabilities Study," *ECAI*, Jun. 2018.

[39] ARMIS, "Exploiting BlueBorne," https://www.armis.com/blueborne/ *Blackhat,* Sep. 2017.

[40] Veelasha Moonsamy, Lynn Batten, "Mitigating man-in-the-middle attacks on smartphones," *Australian Information Security Management Conference,* Jan. 2014.

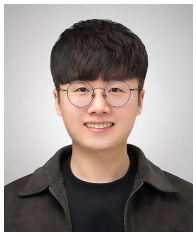
[41] Slawomir Jasek, "GATTacking Bluetooth Smart Devices," *Black hat USA conference,* 2016.

[42] Sam Bowne, "Making an SSL Auditing Proxy with a Mac and Burp," *samsclass*, 2015.

[43] CheckPoint, "CallJam," https://blog.checkpoint.com/2016/09/08/calljam-android-malware-found-on-google-play/, Sep. 2016.

[44] Grant Bugher, "CRNG Cracked," http://perimetergrid.com/wp/2008/05/17/ubuntudebian-crng-cracked-ssh-vulnerable/, May. 2008.

〈저자소개〉



김 병 연 (Byeong Yeon Kim) 학생회원
2015년 2월: 단국대학교 소프트웨어학과 학사
2015년 1월~현재: ㈜삼성전자 소프트웨어 엔지니어
2020년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 자연어처리, 인공지능보안, 비정상행위탐지, 블록체인

김 휘 강 (Huy Kang Kim) 종신회원
1998년 2월 KAIST 산업경학학과 학사
2000년 2월 KAIST 산업공학과 석사
2009년 2월 KAIST 산업및시스템공학과 박사.
2004년 5월~2010년 2월: 엔씨소프트 정보보안실장. Technical Director.
2010년 3월~2014년 12월: 고려대학교 정보보호대학원 조교수.
2015년 1월~2020년 2월: 고려대학교 정보보호대학원 부교수.
2020년 3월~현재: 고려대학교 정보보호대학원 교수
2020년 3월~현재: 고려대학교 정보보호대학원-삼성SDS 보안 공동연구센터장
〈관심분야〉 온라인게임 보안, 자동차 보안, 침입탐지시스템, 네트워크 보안