Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.5, Oct. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.5.929

COVID-19 동선 추적에서의 프라이버시 보호를 위한 Exposure Notification 기술에 대한 보안성 평가 및 대응 방안 연구

이 호 준,[1†] 이 상 진[2‡]
[1,2]고려대학교 정보보호대학원(대학원생, 교수)

A Study on the Security Evaluations and Countermeasure of Exposure Notification Technology for Privacy-Preserving COVID-19 Contact Tracing

Hojun Lee,[1†] Sangjin Lee[2‡]
[1,2]Korea University School of Cybersecurity(Graduate student, Professor)

요 약

COVID-19 감염자의 동선을 파악함과 동시에 개인의 프라이버시를 보호하기 위한 방법들이 다양하게 제시되고 있다. 그 중에서 애플과 구글에서 발표한 'Exposure Notification'은 블루투스를 사용한 탈중앙화 방식을 따르고 있다. 하지만 이 기술을 사용하려면 항상 블루투스 기능을 켜 놓아야 하며 이를 통해 다양한 보안 위협이 발생할 수 있다. 본 논문에서는 보안 위협 모델링 기법 중 'STRIDE'와 'LINDDUN'을 적용하여 Exposure Notification 기술의 보안성을 평가하여 발생 가능한 모든 위협을 도출하였다. 또한 보안성 평가 결과를 가지고 대응 방안을 도출하고 이를 바탕으로 보안성을 향상시킨 새로운 모델을 제시한다.

ABSTRACT

Various methods are being presented to identify the movements of COVID-19 infected persons and to protect personal privacy at the same time. Among them, 'Exposure Notification' released by Apple and Google follows a decentralized approach using Bluetooth. However, the technology must always turn on Bluetooth for use, which can create a variety of security threats. Thus, in this paper, the security assessment of 'Exposure Notification' was performed by applying 'STRIDE' and 'LINDDUN' among the security threat modeling techniques to derive all possible threats. It also presented a new Dell that derived response measures with security assessment results and improved security based on them.

Keywords: COVID-19, Contact Tracing, Threat Modeling, STRIDE, LINDDUN

I. 서 론

현재 우리나라는 COVID-19 사태에 효과적으로 대응하기 위해 감염자의 동선을 공개하고 있다. 하지만 이 과정에서 개인의 프라이버시가 침해되고 있다. 여러 나라에서 이러한 문제를 해결하기 위해 감염자 동선 추적 시스템 개발을 앞 다퉈 추진하고 있다. 필요한 정보보호 서비스가 수반되지 않는 상태에서 지식정보화 사회의 발전은 많은 사회적 부작용을 동반할 수밖에 없으며, 이것은 여러 사례를 통해 이미 입증되고 있다.

동선 추적 시스템은 감염자와의 접촉 위험도를 평

Received(07. 08. 2020), Modified(09. 08. 2020), Accepted(09. 14. 2020)
† 주저자, dlghwns817@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

가하는 주체에 따라 크게 중앙 집중형과 탈중앙화 방식으로 나뉜다. 중앙 집중형 방식은 국가 질병 관리 본부 등 신뢰받는 중앙 주체에서 위험도를 평가한 뒤 해당 사실을 사용자에게 알려준다. 반면 탈중앙화 방식은 각 사용자의 장치에서 위험도 평가가 수행된다는 점에서 차이가 있다. 중앙 집중형 방식의 대표적인 기술은 ROBERT(ROBust and privacy-presERving proximity Tracing)[1]가 있으며 탈중앙화 방식의 대표적인 기술로는 구글과 애플에서 발표한 Exposure Notification[2]이 있다.

본 논문에서는 Exposure Notification의 보안성을 평가하고 대응방안을 도출한다. 이를 위해 Exposure Notification에 대해 DFD(Data Flow Diagram)를 작성하고 이를 기반으로 보안위협모델링을 수행한다. 식별된 보안 위협에 대한 대응방안을 제시하고 더 나아가 보안성을 향상시킨 새로운 모델을 제시한다.

II. 관련 연구

2.1 Exposure Notification

Exposure Notification 기술은 Fig 1과 같이 동작한다. 우선 사용자는 자신만의 키를 생성하여 장치에 저장한다. 이를 사용하여 RPI(Rolling Proximity Identifier)라는 식별자를 생성하는데 RPI는 사용자를 식별할 수 없는 임의의 값이며 일정 시간이 지나면 새롭게 생성된다. RPI는 BLE(Bluetooth Low Energy)의 Advertise 모드를 통해 브로드캐스트로 전송되며 일정 거리 내에 존재하는 모든 블루투스 장치는 패킷을 수신하고 RPI 값을 장치에 저장한다. RPI 값을 주고받기 위해서는 장치 간의 거리가 충분히 가까워야 하기 때문에 특정 RPI를 저장하고 있다면 해당 RPI 값을 소유한 사람과 접촉했음을 의미한다. COVID-19 검사 결과가 양성인 사용자는 자신의 키를 서비스 서버에 업로드 한다. 서버에 업로드 된 키는 각각의 사용자에게 전달되고 사용자의 장치는 키를 사용하여 RPI 값을 생성한 뒤 생성된 값이 장치에 저장되어 있는지 확인하여 감염자 접촉 여부를 판단한다.

2.2 보안위협모델링

보안위협모델링은 시스템의 구조를 체계화하고 이를 바탕으로 시스템 전반에 대한 보안 위협을 식별하는 방법이다. 보안위협모델링을 사용하면 보안 개발 수명 주기(SDL)의 설계 단계에서 우선적으로 발생 가능한 취약점을 식별하고 이를 해결할 수 있기 때문에 보안을 강화할 수 있다[3].

우선 시스템의 구조를 체계적으로 분석하기 위해 DFD를 작성한다. DFD를 통해 시스템을 구성하고 있는 모든 구성 요소와 데이터의 흐름을 파악할 수 있다. 다음으로 시스템에서 발생할 수 있는 보안 위협을 식별하기 위해 STRIDE[4], LINDDUN[5] 등을 적용한다. 본 논문에서는 클라이언트-서버 서비스를 분석하기에 적합한 STRIDE와 프라이버시 관점에서 분석이 가능한 LINDDUN을 사용하였다.

STRIDE는 시스템에서 발생할 수 있는 6가지 보안 위협을 다루며 각 글자는 위장(Spoofing), 변조(Tampering), 부인(Repudiation), 정보 유출(Information Disclosure), 서비스 거부(Denial of Service), 권한 상승(Elevation of Privilege)을 의미한다.

LINDDUN은 프라이버시와 관련된 위협을 다루는 모델로 각 글자는 연결(Linkability), 식별(Identifiability), 부인 방지(Non-repudiation), 검출(Detectability), 정보 유출(Information Disclosure), 내용 몰인식(content Unawareness), 정책 및 동의 불이행(policy and consent Non compliance) 관점에서 위협을 분석한다.

Fig. 1. Principle of Exposure Notification Works

Table 1. Detailed Description by Element of Exposure Notification DFD

Group	Component	Explanation
External Entity	E1. Advertisement/Positive User	Service Packet Sender/Infectious Person
	E2. Scanning User	Service Packet Receiver
Storage	D1. Storage	Storage for service keys and incoming information
	D2. Timer	Storage for storing time information to determine service key expiration time
Process	P1. ENApplication	The service application process is associated with users, ENFramework, and servers.
	P2. Request Exposure Info	Exposure Information Request
	P3. ENStateRequest	Service enable/disable request
	P4. Request Permission	Request User Permissions
	P5. Upload Diagnosis Key	Upload Diagnosis Key
	P6. Update Diagnosis Key	Update Diagnosis Key

..... omit

Data Flow	DF77. Data(Scan Data)	Scan Data
	DF78. Data(Scan Data)	
	DF79. System Time Request	Data Flow that Request System Time
	DF80. System Time	System Time

Table 2. Attack Library for Exposure Notification

No	Type	Year	Title	Author	Ref
1	Technical Report	2020	SECURITY ANALYSIS OF THE COVID-19 CONTACT TRACING SPECIFICATIONS BY APPLE INC. AND GOOGLE INC.	Yaron Gvili	[6]
2		2020	Analysis of DP3T Between Scylla and Charybdis	Serge Vaudenay	[7]
3		2018	BLEEDING BIT - The hidden attack surface within BLE chips	armis	[8]
4		2018	OTA Vulnerability on User Equipment in Cloud Services	Myoungsu Kim etc.	[9]
5		2018	Analysis of cheat detection and prevention techniques in mobile games	Oskari Teittinen	[10]
6		2018	Security Vulnerabilities in Bluetooth Technology as Used in IoT	Angela M. Lonzetta etc.	[11]
7		2017	BlueBorne - Exploiting BlueBorne in Linux-based IoT devices	Ben Seri etc.	[12]
8	Conference/ Paper	2014	Mitigating man-in-the-middle attacks on smartphones - a discussion of SSL pinning and DNSSec	Veelasha Moonsamy etc.	[13]

..... omit

14	CVE (Bluetooth)	2017	CVE-2018-9560(LPE)	MITRE
15			CVE-2018-10825(Replay Attack)	
19		2019	CVE-2019-9365(RCE)	
20			CVE-2019-9426(LPE)	
21		2020	CVE-2020-0022(BlueFrag, RCE)	
22	CVE (Server)	2014	CVE-2014-4449(MITM : iOS)	
23		2019	CVE-2019-5215(MITM : Android)	

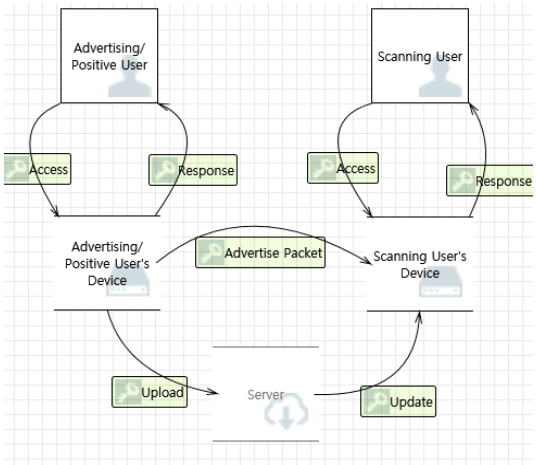

Fig. 2. Exposure Notification Data Flow Diagram Level 0

DFD를 통해 파악한 시스템의 모든 구성 요소에 대해 STRIDE와 LINDDUN에서 다루는 위협이 발생 가능한지 파악한다. 이를 통해 클라이언트-서버 관점 및 프라이버시 관점에서 발생 가능한 모든 위협을 확인할 수 있다.

III. Exposure Notification 기술에 대한 보안성 평가

3.1 Data Flow Diagram 도출

Exposure Notification 기술에서 발생 가능한 보안 위협을 식별하기 위해 DFD를 사용하여 기술의 전체적인 구조를 파악한다. Microsoft 사의 'Threat Modeling Tool'이라는 도구를 사용하여 DFD를 작성하였으며 Level 0에 해당하는 것은 Fig 2, Level 3에 해당하는 것은 Fig 3, Fig 4이다. Level 0의 DFD는 Context Diagram이라고도 하며 분석 대상 시스템과 외부와의 관계를 식별하기 위한 것으로 분석 범위를 결정한다. Level 3의 DFD는 DFD 내의 모든 프로세스가 더 이상 나눠지지 않는 기본 단위이다.

DFD를 작성하기에 앞서 Exposure Notification 기술을 사용하는 사용자를 구분하였다. ① 서비스 패킷을 보내거나 양성 판정을 받은 사용자와 ② 서비스 패킷을 받는 사용자로 구분하였는데 이는 서비스 패킷을 주고받는 관계를 좀 더 명확하고 이해하기 쉽게 하기 위한 것이다. 실제로는 한 명의 사용자가 서비스 패킷을 송수신하며 양성 판정을 받기 때문에 전체적으로는 하나의 시스템에서 동작하고 있음을 이해하는 것이 중요하다. 예를 들어 Fig 4에서 서비스 패킷을 받던 사용자가 양성 판정을 받게 되면 그 순간 Fig 3의 양성 판정을 받은 사용자로 바뀌어 관련 프로세스를 처리하게 된다. Table 1은 DFD Level 3의 구성 요소들을 정리한 것 중 일부이다.

3.2 Attack Library

DFD 구성 요소에서 발생 가능한 보안 위협을 식별하기 위해 Attack Library를 사용한다. Attack Library는 논문, 기술 문서, 취약점 데이터베이스 등 현재까지 알려져 있는 모든 공격 정보를 포함하고 있어 위협 모델링의 정확도를 높일 수 있다.

우선 Exposure Notification 기술과 관련한 기술 자료, 컨퍼런스 발표 자료, 논문 등을 수집하였다. 기술 자료에는 Exposure Notification 기술에서 사용되는 다양한 기술과 관련해서 발생 가능한 전반적인 보안 위협에 대한 정보가 포함되어 있다. 마지막으로 DFD의 각 요소에서 발생 가능한 위협을 실제 공격으로 발전시킬 수 있는 CVE(Common Vulnerabilities and Exposures)를 수집하였다. Table 2는 수집한 Attack Library 중 일부를 정리한 것이다. Exposure Notification 기술은 블루투스 기능을 기반으로 하고 있기 때문에 수집된 Attack Library는 주로 블루투스 취약점과 관련된 것들로 블루투스 취약점에 대한 기술 문서나 논문, CVE 등이다.

3.3 STRIDE 위협 모델링

3.3.1 STRIDE

DFD의 요소별 STRIDE의 적용 범위는 Table 3과 같다.

Table 3. STRIDE by DFD Elements

	S	T	R	I	D	E
Entity	x		x			
Process	x	x	x	x	x	x
Data Store		x	?	x	x	
Data Flow		x		x	x	

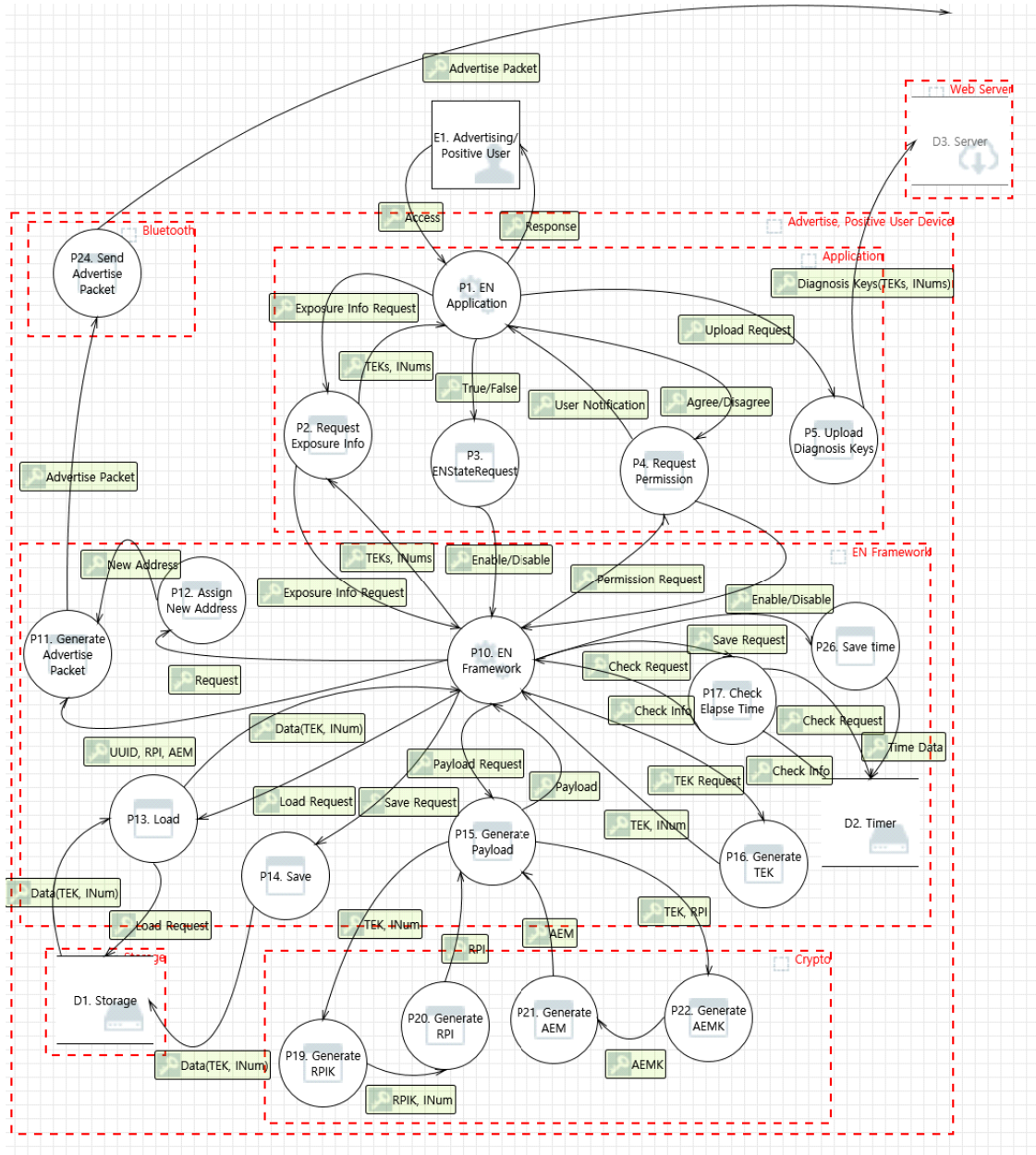

Fig. 3. Exposure Notification Data Flow Diagram Level 3 - Advertising/Positive User

Table 4는 STRIDE를 통해 식별한 36개의 위협 중 일부를 보여주며 각 요소별 발생 가능한 위협과 해당 위협을 발생시키기 위한 Attack Library를 확인할 수 있다. Exposure Notification 기술에서 외부와의 통신은 사용자의 장치 간에 서비스 패킷을 주고받는 과정과 사용자의 장치와 서비스 서버 사이의 키 업로드/업데이트 과정이 존재한다. 따라서 STRIDE 적용 결과, 대부분의 위협은 두 가지 통신 과정에서 발생하는 위협과 그것에 파생되어 발생하는 것이 주를 이룬다. 사용자의 장치 간 통신에서는 블루투스가 사용되기 때문에 블루투스는 항상 활성화되어 있어야 하며 이로 인해 블루투스와 관련된 공개 취약점에 노출되어 있다.

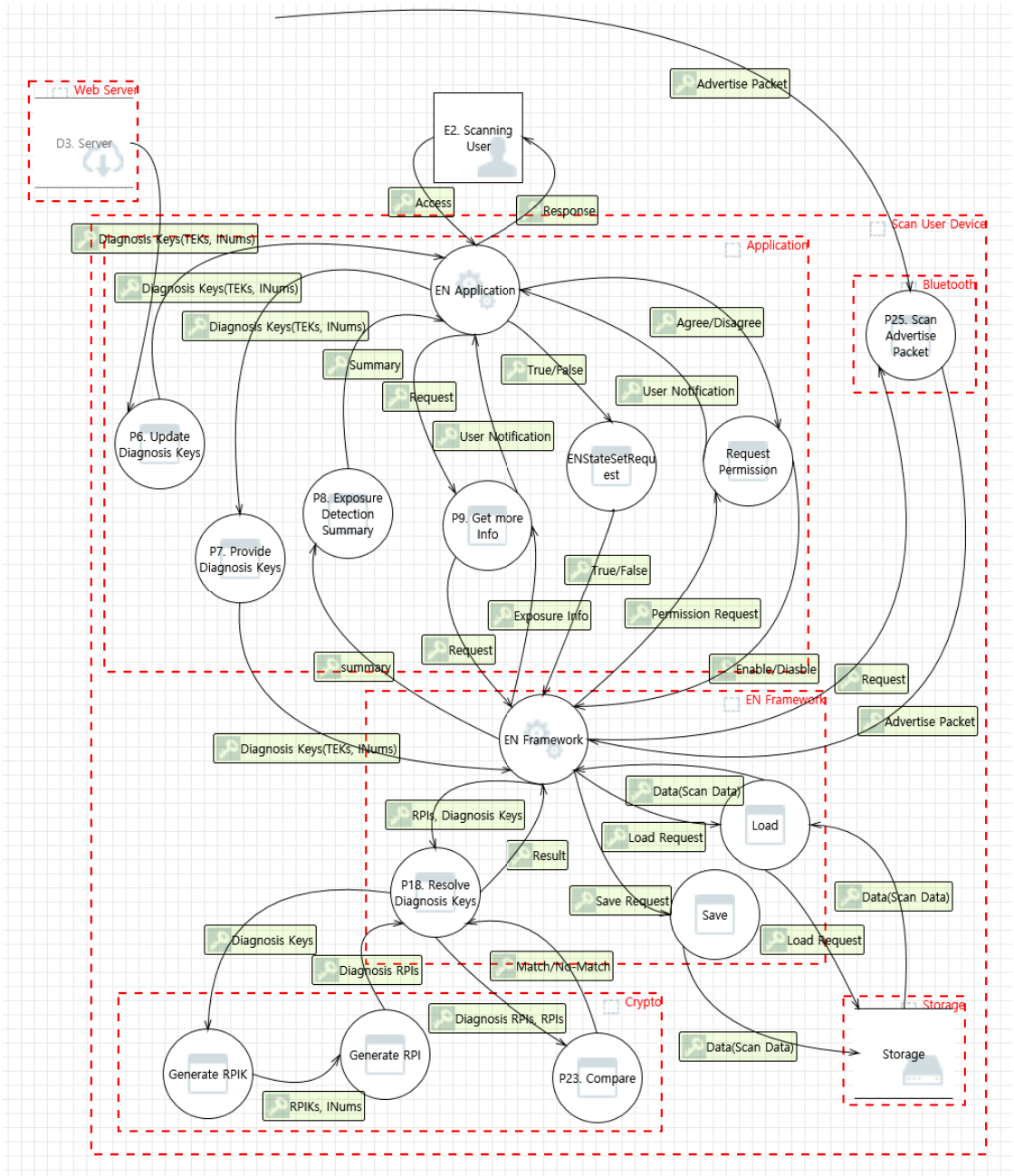

Fig. 4. Exposure Notification Data Flow Diagram Level 3 - Scanning User

Table 4. STRIDE for Exposure Notification

Type No	Name	Description		Attack Library	Threat No
E1	Advertising /Positive User	S	Spoofing due to absence of user authentication procedure	1, 10, 11, 12, 17	T1
		R	Malicious users can randomly change their smartphone system time. This can lead to denial of service use.	5	T2
..... omit					
P1	ENApplication	S	Attacker can create similar applications and impersonate them as normal ones.	18	T5
		I	Service information may be exposed by unauthorized attackers.	3, 6, 7, 19, 21, 22, 23, 24, 25, 26, 27	T6
		D	Attacker who has become able to control a smartphone can interfere with service behavior.	3, 6, 7, 19, 21, 22, 23, 24, 25, 26, 27	T7
		E	Unauthorized attackers can use the service application.	10	T8
		E	Attacker who has acquired a (root) shell on the device may use the service application.	3, 6, 7, 19, 21, 22, 23, 24, 25, 26, 27	T9
P5	Upload Diagnosis Key	S	Attacker could intercept a diagnostic key that is uploaded under the guise of a server.	4, 8, 28, 29	T10
		I	Diagnosis key information may be leaked to the attacker.	4, 8, 28, 29	T11
		D	Upload diagnosis keys may fail by attacker.	4, 8, 9, 28, 29	T12
..... omit					
P25	Scan Advertise Packet	T	Attacker's Relay/Replay Attack could receive malicious packets.	1, 2, 16, 17, 20	T16
		T	Bluetooth packets modulated by an attacker can be received.	3, 6, 7, 19, 21, 22, 23, 24, 25, 26, 27	T17
		R	Receiving can be denied through system time modulation of malicious users.	5	T18
		D	Because it does not validate input values, an attacker can generate and transmit abnormal service packets so that Crash occurs or the process ends.	6	T19
..... omit					
DF80	System Time	T	Time data can be modulated by malicious users.	5	T36

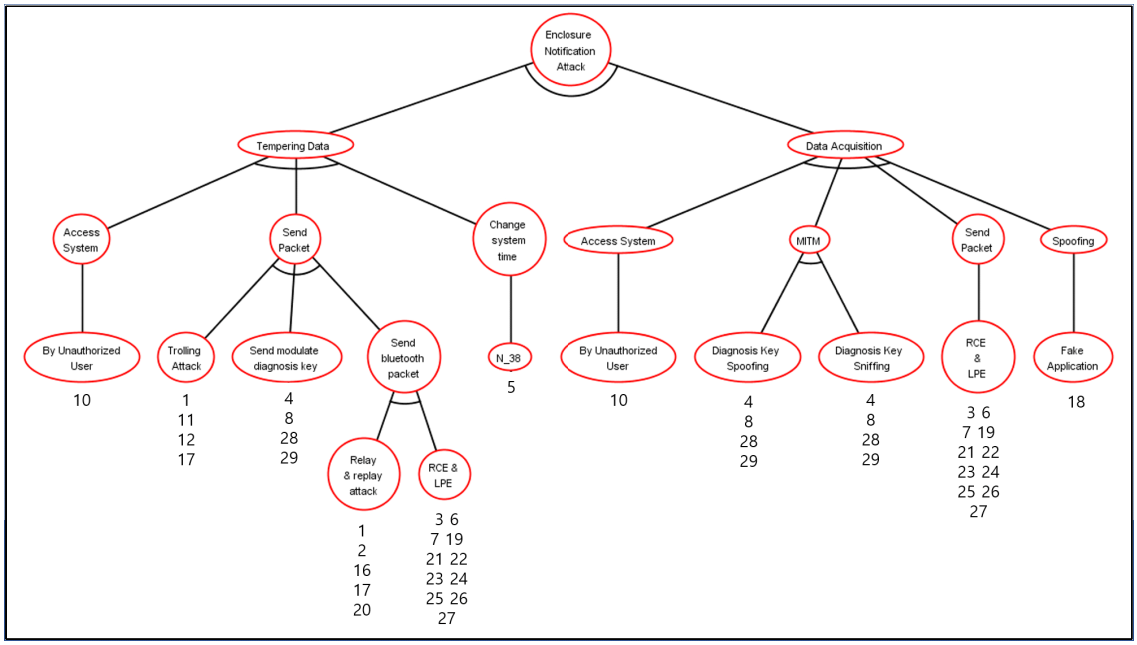

Fig. 5. Attack Tree of Exposure Notification

또한 Exposure Notification 기술에서는 키를 업로드/업데이트 하는 과정에서 별도의 보안 정책이 부재하여 공격자에 의한 중간자 공격 등에 취약하며 기술을 사용하는 사용자가 정상적인 사용자인지 인증하는 절차가 없어 Trolling Attack 등의 비정상적인 사용자에 의한 공격이 가능하다.

3.3.2 Attack Tree

Attack Tree를 사용하여 발생할 수 있는 모든 보안 위협을 체계화할 수 있다. Attack Tree는 DFD 작성 및 STRIDE 적용을 통해 확인한 보안 위협을 가지고 공격 시나리오를 작성하는 것이다. Fig 5는 Exposure Notification 기술에 대한 Attack Tree이며 Exposure Notification 기술에 대한 공격은 크게 데이터 변조, 데이터 획득, DoS, 서비스 제어로 분류할 수 있다. Leaf 노드는 최종적인 공격 방법이며 그 아래는 해당 공격에 사용되는 Attack Library의 번호이다.

Table 5. LINDDUN by DFD Elements

	L	I	N	D	D	U	N
Entity	x	x				x	
Process	x	x	x	x	x		x
Data Store	x	x	x	x	x		x
Data Flow	x	x	x	x	x		x

3.4 LINDDUN 위협 모델링

3.4.1 LINDDUN

요소별 적용 가능한 LINDDUN의 적용 범위는 Table 5와 같다. 3.1에서 작성한 DFD를 기반으로 LINDDUN을 적용하여 보안 위협을 식별할 수 있으며 그 결과는 Table 6과 같다.

Exposure Notification 기술은 기본적으로 프라이버시 보호를 위해 서비스 전체에서 익명 데이터를 사용하기 때문에 식별 위협이 발생하지 않는다. 하지만 특정 상황의 경우 연결 위협이 다수 발생할 수 있음을 확인하였다. 또한 서비스 어플리케이션에서 사용자 인증 절차가 없어 보안 정책을 위반하여 정책 및 동의 불이행 위협이 발생한다.

LINDDUN 기법의 경우, 각 위협에 대해 개별적으로 Threat Tree를 작성하기 때문에 Table 6에 열거한 위협과 관련된 설명은 제외하였으며 Threat Tree로 이를 대체한다.

Table 6. LINDDUN for Exposure Notification

Type	Type No	Threat Target	L	I	N	D	D	U	N
Entity	E1	Advertisement/Positive User	X					X	
	E2	Scanning User						X	
Data Store	D1	Storage	X				X		X
	D2	Timer	X				X		X
Process	P1	ENApplication				X	X		X
	P2	Request Exposure Info							X
	P3	ENStateRequest							X
	P4	Request Permission							X
	P5	Upload Diagnosis Key	X			X	X		X

..... omit

Data Flow	DF77	Data(Scan Data)							X
	DF78	Data(Scan Data)							X
	DF79	System Time Request							X
	DF80	System Time							X

Table 7. Threat Tree for Exposure Notification

Linkability of Entity				
1	L_e			
	1.1	*Linkability of contextual data at Linkability of Data Flow		
Unawareness of Entity				
1	U			
	1.1	U_2 : Unaware of stored data		
*Linkability of Data Flow				
1	L_df			
	1.1	L_df2 : Linkability of contextual data (metadata)		
		1.1.1	L_df : Insecure anonymity system deployed	
			1.1.1.1	L_df14 : Passive attack possible
Linkability of Process				
1	L_p			
	1.1	L_p1 : Different actions can be linked to the same user		
		1.1.1	*Disclosure of Information	
Detectability				
1	D_p			
	1.1	*Disclosure of Information		
*Disclosure of Information				
1	ID_p			
OR	1.1	**Spoofing external entity		
Non-Compliance				
1	NC			
	1.1	NC_2 : Incorrect of insufficient privacy policies		
		1.1.1	NC_3 : Inconsistent / insufficient policy management	
**Spoofing external entities				
1	S			
OR	1.2	S_4 : No Authentication		

Table 8. MUC of Threat Tree

MUC	Details
MUC 01	Threat Tree : L_e(Linkability_entity) Summary : User actions are associated with the user's infection Scenario : Bf1. Attackers use an over-the-shoulder attack to determine if the user enters the COVID-19 inspection results Result: If the user enters the COVID-19 test results in the service application, it only occurs when positive, so the attacker can see that the user has COVID-19.
MUC 02	Threat Tree : U (Unawareness) Summary : The data subject is not aware of the situation where personal information is stored Scenario : Bf1. Attackers attempt rolling attack using drones, etc. Bf2. Abnormal service data stored on your device Bf3. Users cannot determine what service information has been saved Result: Users cannot recognize abnormal service data even if it is stored and cannot identify it even if damage (false positive) occurs Related Attack Library : 1, 11, 12, 17
..... omit	
MUC 05	Threat Tree : L_p (Linkability_process) Summary : Process is associated with your infection Scenario : Bf1. Attackers impersonate servers Bf2. Attacker checks for diagnostic keys uploaded to server Result: An attacker may know that the user has corona-19 because the diagnostic key is uploaded to the server in the service application only when the user is positive Related Attack Library : 4, 8, 28, 29

3.4.2 Threat Tree & MUC(Misuse Case)

도출된 위협 별 상세 정보를 보여주기 위해 Threat Tree를 작성한다. Threat Tree의 노드들을 통해 위협이 발생되는 원인을 파악할 수 있다. Threat Tree에서 노드 별 식별자는 '〔적용항목의 머리글자〕_〔구성요소의 이니셜〕'로 표시한다.

* 표시가 된 항목은 해당 위협을 달성하기 위한 조건을 표 아래에 따로 빼서 설명한다. Table 7은 Threat Tree 중 Entity와 Process와 관련된 것이다. 추가로 Threat Tree에 대한 이해를 높이기 위해 Misuse Case를 작성하였고 그 결과 중 일부는 Table 8과 같다. Misuse Case는 시나리오 및 결과 등을 통해 각 위협이 어떻게 발생할 수 있는지 보여준다.

3.5 위협 우선순위 선정

3.3.2와 3.4.2에서 식별한 위협을 대상으로 체크리스트를 작성하기 위해 DREAD 모델[14]을 사용하여 위협별 위험도를 측정하였다. DREAD 모델은 피해 가능성(Damage potential), 공격 재현성(Reproducibility), 악용 가능성(Exploitability), 영향 받는 사용자(Affected users), 취약점의 발견 가능성(Discoverability)을 기준으로 1~3의 점수를 부여하며 총점을 계산하여 점수가 클수록 높은 우선순위를 부여 받는다. Table 9를 통해 공격 시나리오 별 위험도를 알 수 있다. Trolling Attack 및 사용자 인증 절차 부재에 따른 보안 위협은 쉽게 공격이 재현 가능하며 다수가 피해를 입을 수 있기 때문에 높은 우선순위로 평가되었으며 반대로 블루투스

Table 9. DREAD for Exposure Notification

STRIDE						
Threat	D	R	E	A	D	Sum
RCE & LPE for tempering	1	3	1	1	1	7
Unauthorized user tempering	1	3	3	1	3	11
Trolling Attack	3	3	3	3	3	15
Send modulated diagnosis key	3	3	2	3	2	13
Relay & Replay Attack	3	3	2	3	2	13
Change system time	1	3	3	1	3	11
RCE & LPE for data acquisition	2	3	1	2	1	9
Unauthorized user get data	1	2	3	1	3	10

omit

LINDDUN						
Threat	D	R	E	A	D	Sum
MUC 01	1	1	3	1	3	9
MUC 02	3	3	3	3	3	15
MUC 03	2	2	1	2	1	8
MUC 04	2	3	3	2	3	13
MUC 05	2	2	2	2	2	10
MUC 06	2	2	2	2	2	10
MUC 07	1	3	3	1	3	11
MUC 08	3	2	2	3	2	12
MUC 09	2	2	2	2	2	10
MUC 10	1	2	2	1	2	8
MUC 11	3	3	2	3	2	13
MUC 12	2	2	2	2	2	10
MUC 13	3	2	2	3	2	12
MUC 14	2	3	3	2	3	13

취약점을 이용한 원격 코드 실행(RCE) 및 권한 상승(LPE)으로 인한 위협은 취약점 분야에 대해 잘 알고 있는 일부 전문가만이 공격을 재현할 수 있으며 소수의 인원만이 피해를 입기 때문에 낮은 우선순위로 평가되었다.

3.6 취약점 점검을 위한 체크리스트

STRIDE, LINDDUN을 사용하여 도출한 위협 목록과 DREAD 적용 결과를 바탕으로 취약점 점검을 위한 체크리스트를 작성하였으며 Table 10과 같다. Table 10의 요소들을 점검함으로써 Exposure Notification 기술의 안전성을 평가할 수 있다.

Table 10. Check List for Exposure Notification

No	Detail
C1	Is there a user authentication procedure?
C2	Is the generated TEK, RPI safe for Relay/Replay attacks?
C3	Is there a verification procedure for the diagnostic key?
C4	Don't expose the user's diagnostic results?
C5	Does not expose a user's identity through a service packet?
C6	Can't the user manipulate time data arbitrarily?
C7	Is obfuscation of application applied?
C8	Is the device using the latest OS version?
C9	Is the storage space managed?
C10	Is there a countermeasure against DoS attack?

IV. 보안 위협 대응방안

4.1 대응방안

Exposure Notification 기술에 대해 STRIDE와 LINDDUN을 적용하여 발생 가능한 위협들을 식별하였고 DREAD를 사용하여 위협 간의 우선순위를 선정하였다. 우선순위를 기준으로 총 12개의 대응 방안을 고안하였고 그 중 일부를 Table 11에서 확인할 수 있다.

기본적으로 Exposure Notification 기술은 외부와 데이터를 주고받는 과정이 서비스 패킷을 전송하기 위한 블루투스 기능과 진단키를 업로드 및 업데이트하기 위한 서버와의 통신, 두 가지 경우로 이와 관련된 문제가 주를 이룬다.

블루투스와 관련된 문제를 해결하기 위해서는 최신 OS 버전으로 업데이트 하는 것이 중요하며 서버와의 통신에서는 전자서명을 통한 사용자 인증 절차를 추가함으로써 비인가 사용자에 의한 위협을 없앨 수 있다. 또한 사용자 인증 체계의 부재로 인한 개인정보 유출을 막기 위해 FIDO를 사용하여 사용자

Table 11. Countermeasures of Threat

No	Countermeasure	Description		Related Threat
1	Add User Authentication Procedure	Before	Absence of user authentication procedures	
		After	Using FIDO • Registration 1) The device starts registration through the FIDO authentication module. 2) Input PIN, fingerprint, etc. to FIDO authentication module 3) Create user verification key/sign key pair on device 4) The verification key is sent with the account to the service server (the service server stores it together, securely stores it on the secret device) • Certification 1) Send nonce value to sign device from service server 2) FIDO authentication module unlocking in the same way as the registration process 3) Sign the nonce value using the key that matches the user ID on the device. 4) The server that received the signature value is verified using the verification key that is stored. • Electronic signature algorithm: RSA-PSS [15]	T1, T3 T6, T8 MUC02 MUC04 MUC07 MUC14

omit

3	Add Diagnostic Key Certification Procedure	Before	• Absence of diagnostic key authentication procedure	T10, T11 T13, T14 T30, T31 T34, T35 MUC05 MUC08 MUC09 MUC13
		After	• Upload Diagnostic Key (Device → Server) 1) Server → Device : $\{Nonce\}_{DevicePubKey}$ 2) Device acquires nonce value 3) Device → Server : $\{Nonce \| \{DiagnosisKey\}_{ServerPubKey}\}_{DevicePriKey}$ 4) The server checks the nonce value and obtains the diagnostic key. • Update diagnostic key (server → device) 1) Device → Server : $\{Nonce\}_{ServerPubKey}$ 2) Server acquires nonce value 3) Server → Device : $\{Nonce \| \{DiagnosisKey\}_{DevicePubKey}\}_{ServerPriKey}$ 4) Device checks Nonce value and obtains diagnostic key • The device's public and secret keys utilize key pairs used by FIDO • The server's public key is stored in the application in advance • Electronic signature algorithm: RSA-PSS [15]	

omit

12	Diagnosis key DoS attack response	Before	• No security measures against diagnosis key DoS attacks	T32
		After	• Load Balancing[16] • IDS & IPS	

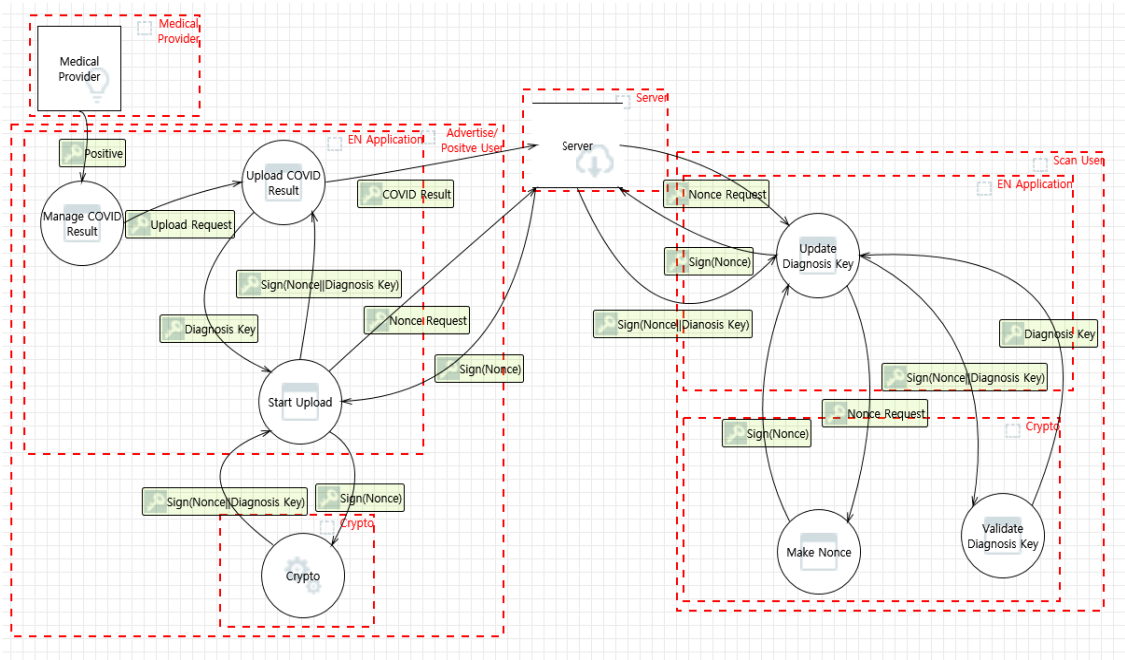

Fig. 6. Improved Exposure Notification DFD - Update & Upload Process

인증을 수행할 수 있다.

4.2 Improved Exposure Notification

4.1에서 제시한 대응 방안을 기반으로 보안성이 향상된 Exposure Notification 기술을 제안한다. Fig 6부터 Fig 8은 보안성을 향상시키기 위해 기존의 Exposure Notification 기술에 추가되거나 변경된 부분을 보여주는 DFD이다.

Fig 6은 진단키를 업로드 및 업데이트 하는 과정으로 전자서명을 통한 사용자 인증 과정을 추가하여 정상적인 진단키가 업로드 및 다운로드 되는지를 확인할 수 있다. 또한 모든 사용자가 주기적으로 업로드를 하게 함으로써 해당 절차만으로 사용자가 감염자인지에 대한 여부를 파악할 수 없게 한다. Fig 7은 사용자 인증 절차로 FIDO 모듈을 통해 실제 서비스에 등록되어 있는 정상적인 사용자임을 인증할 수 있다. Fig 8은 RPI 생성 과정을 나타내는데 이때 RPI 생성에 사용되는 시간 데이터는 서버와 동기화된 값을 사용하여 악의적인 사용자가 임의로 시간을 변경할 수 없으며 RPI 생성에 암호화된 GPS 데이터를 사용하여 Relay 공격 등을 방지할 수 있다. 또한 서비스 패킷을 주고받는 과정에서 전송 세기를 무작위로 변경하는 방법으로 사용자 추적을 어렵게 할 수 있다.

4.3 기존 방안과의 비교

4.2에서 제시한 Improved Exposure Notification과 기존의 Exposure Notification에 대해 Table 10의 체크리스트를 적용한 결과는 Table 12와 같다.

Improved Exposure Notification에서는 사용자 인증 과정이 추가되었기 때문에 C1 및 C3을

Table 12. Comparison of Improved Exposure Notification and Exposure Notification

No	Improved Exposure Notification	Exposure Notification
C1	O	X
C2	O	X
C3	O	X
C4	O	X
C5	O	X
C6	O	X
C7	-	-
C8	-	-
C9	-	-
C10	-	-

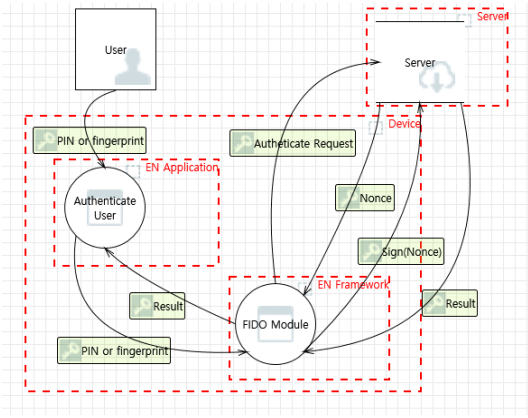

Fig. 7. Improved Exposure Notification DFD - User Authentication Process

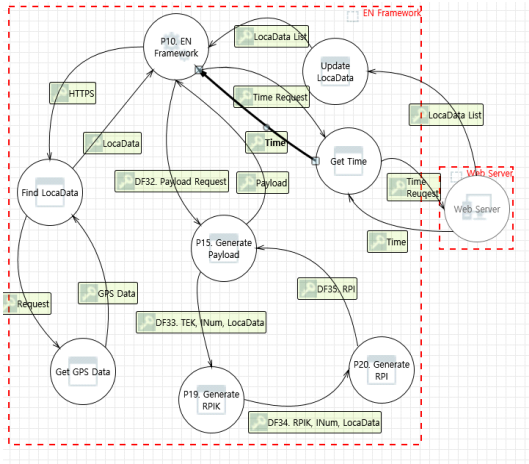

Fig. 8. Improved Exposure Notification DFD - RPI Generation Process

준수하며 GPS 데이터 활용 및 서버와 동기화 된 시간 데이터를 사용함으로써 C2와 C6을 만족한다. C7에서 C10의 내용은 프로토콜을 사용하여 개발자가 어떻게 개발을 하느냐에 따라 위협 발생 여부가 결정되기 때문에 판단이 불가능하다.

V. 결 론

본 논문에서는 STRIDE와 LINDDUN 위협모델링을 적용하여 Exposure Notification 기술의 보안성 평가를 수행하여 발생 가능한 보안 위협을 도출하였다. 확인된 보안 위협을 기반으로 기술을 점검하기 위한 체크리스트를 작성하였고 위협 별 우선순위를 선정하여 주요 위협을 식별하였다. 마지막으로는 보안 위협을 해결하기 위한 대응 방안과 이를 반영하여 보안성이 향상된 새로운 기법을 제안하였다. 향후 연구에서는 새로 제시한 기법에 대한 Design Assurance를 통해 보안 위협이 완벽하게 제거되었는지를 평가할 것이다.

References

[1] Claude Castelluccia, Nataliia Bielova, Antoine Boutet, Mathieu Cunche, Cedric Lauradoux, Daniel Le Metayer, and Vincent Roca, "ROBERT:ROBust and privacy-presERving proximity Tracing," HAL-Inria hal-02611265, May. 2020.

[2] Privacy-Preserving Contact Tracing - Apple and Google, "Exposure Notification - Bluetooth Specification" https://covid19.apple.com/contacttracing, Apr. 2020.

[3] Adam Shostack, Threat Modeling: Designing for Security, WILEY, pp. 109-160, Feb. 2014.

[4] Michael Howard and Steve Lipner, The security development lifecycle, Microsoft Press, Jun. 2006.

[5] LINDDUN, "Threat Tree Catalog" https://linddun.org/linddun-threat-catalog, Apr. 2020.

[6] Yaron Gvili, "SECURITY ANALYSIS OF THE COVID-19 CONTACT TRACING SPECIFICATIONS BY APPLE INC. AND GOOGLE INC.," IACR ePrint 2020-428, Apr. 2020.

[7] Serge Vaudenay, "Analysis of DP3T Between Scylla and Charybdis," IACR ePrint 2020-399, Apr. 2020.

[8] Ben Seri, Gregory Vishnepolsky and Dor Zusman, "BleedingBit: The hidden attack surface within ble chips," Armis, Apr. 2020.

[9] Myoungsu Kim, Junyoung Park, Eunseon Jeong, Insu Oh and Kangbin

Yim, "OTA Vulnerability on User Equipment in Cloud Services," 2018 International Conference on Information Technology Systems and Innovation(ICITSI), pp. 425-428, Oct. 2018.
[10] Oskari Teittinen, "Analysis of cheat detection and prevention techniques in mobile games," Master's Thesis, Aalto University, May. 2018.
[11] Angela M. Lonzetta, Peter Cope, Joseph Campbell and Bassam J, Mohd, "Security vulnerabilities in Bluetooth technology as used in IoT," Journal of Sensor and Actuator Networks 7(3), Jul. 2018.
[12] Ben Seri and Gregory Vishnepolsky, ARMIS, "BlueBorne Technical White Paper," Armis, Apr. 2020.
[13] Veelasha Moonsamy and Lynn Batten, "Mitigating man-in-the-middle attacks on smartphones - a discussion of SSL pinning and DNSSec," Proceedings of the 12th Australian Information Security Management Conference, pp. 5-13, Jan. 2014.
[14] Adam Shostack, "Experiences Threat Modeling at Microsoft" https://adam.shostack.org/modsec08/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf, Apr. 2020.
[15] KISA, "Cryptographic Algorithm and Key Length User Guide," KISA-GD-2018-0034, Dec. 2018.
[16] Sheikh Tahir Bakhsh, Halabi Hasbullah, Sabeen Tahir, Fazli Subhan and Aamir Saeed, "Dynamic load balancing through backup relay in Bluetooth scatternet," Proceedings of the 8th International Conference on Frontiers of Information Technology, pp. 1-6, Dec. 2010.

〈저자소개〉

이 호 준(Hojun Lee) 정회원
2018년 2월: 고려대학교 사이버국방학과 학사
2019년 9월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 디지털포렌식, 보안성평가

이 상 진(Sang-jin Lee) 종신회원
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~현재: 고려대학교 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
〈관심분야〉 디지털포렌식