*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.30, NO.6, Dec. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.6.1151

# COVID-19 접촉자 추적 기술에 대한 평가 기준 마련 및 보안성 비교·분석

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

# Evaluation Criteria for COVID-19 Contact Tracing Technology and Security Analysis

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

요 약

COVID-19 감염 확산을 효과적으로 막기 위해 최근 ICT 기술을 기반으로 하는 접촉자 추적 기술이 사용되고 있으며, 이 기술들에는 추적 방식에 따라 다양한 유형이 존재한다. 하지만 이러한 기술들은 항상 보안 위협에 노출되어 있으며 각각의 유형에 따라 발생 가능한 위협도 다양하다. 본 논문에서는 다양한 유형의 접촉자 추적 기술에서 공통적으로 발생하는 프로세스들을 확인하고 이 과정에서 발생할 수 있는 위협을 식별하였다. 이를 통해 다양한 유형의 접촉자 추적 기술 모두에 적용 가능한 공통된 평가 기준을 도출하였으며, 이를 실제 공개된 접촉자 추적 기술에 적용하여 유형 별 비교 분석을 수행하였다. 이러한 연구는 여러 유형 간의 비교를 통해 안전하고 효과적인 접촉자 추적 기술을 선택하는데 도움이 될 수 있을 것이다.

ABSTRACT

To effectively prevent the spread of COVID-19 infections, contact tracing technology based on ICT technology is used and various types exist depending on the way they are tracked. However, these technologies are always exposed to security threats and each type of threat varies. In this paper, we identified processes that occur in common in various types of contact tracing technology and identified possible threats in this process. This resulted in a common evaluation criteria applicable to all types of contact tracing technologies and applied to actual published contact tracing technologies to perform comparative analysis by type. These studies can help select safe and effective contact tracing technologies through comparisons between different types.

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

## I. 서 론

COVID-19는 다른 전염병에 비해 전파 속도가 빨라 수많은 감염자를 발생시키고 있다. 치료제 및 백신이 개발되지 않은 상황에서 COVID-19에 대처하기 위한 효과적인 방법은 빠른 시간 내에 감염자들을 파악하여 이들과 접촉한 사람들을 빨리 격리하는 것뿐이다. 이러한 이유로 여러 국가에서는 ICT 기술을 활용해 COVID-19 감염자와 접촉한 자들을 신속하게 추적하려 하고 있다.

이러한 접근은 빠르게 접촉자를 파악해 추가 감염으로 인한 피해를 막을 수 있다는 점에서 긍정적이

Received(08. 24. 2020), Modified(10. 23. 2020), Accepted(10. 26. 2020)
† 주저자, dlghwns817@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

다. 하지만 추적의 기반이 되는 ICT 기술은 항상 보안 위협에 노출되어 있으며, 자칫 접촉자 추적 기술이 오용되면 추적 과정에서 사용된 개인 정보가 유출되는 피해가 발생할 수 있으므로 정보보호에 각별히 신경 써야만 한다.

이러한 이유로 최근 접촉자 추적 기술에서 발생할 수 있는 다양한 보안 위협들을 분석한 논문들이 활발하게 발표되고 있다. 그러나 이러한 연구들은 주로 개별 기술을 대상으로 분석을 수행하고 있기 때문에 통합적인 분석을 통해 각 기술 간의 장·단점을 객관적으로 상호 비교하는 연구는 아직 이루어지지 않고 있다.

이에 본 논문에서는 접촉자 추적 기술을 크게 '블루투스 기반 중앙집중형 방식', '블루투스 기반 탈중앙형 방식', '위치정보 기반 방식'으로 나누고, 각각을 대표하는 기술들을 DFD(Data Flow Diagram)로 일반화한다. 이어 보안 위협 모델링(Threat Modeling) 기법 중 STRIDE와 LINDDUN을 사용하여 각각의 접촉자 추적 기술에서 발생할 수 있는 위협들을 식별하고 이를 종합함으로써 객관적인 보안성 평가 기준을 도출한다. 끝으로 도출된 기준을 바탕으로 기존에 발표된 다양한 접촉자 추적 기술들을 비교·분석한다.

본 논문에서 도출된 연구결과들은 향후 보다 효과적인 접촉자 추적 기술을 개발하는데 도움이 될 수 있을 것이다.

## II. 접촉자 추적 기술

본 논문에서 사용하는 접촉자 추적 기술의 구성요소들에 대한 정의는 Table 1과 같다. 접촉자 추적 기술은 전파력이 강한 COVID-19 감염자와 접촉한 사람들을 빠르게 조사하여 감염 위험성이 있는 사람을 파악하기 위한 것으로 크게 블루투스 방식과 비 블루투스 방식으로 나눌 수 있다(QR코드 방식도 있으나, 이는 본 논문에서는 다루지 않는다).

블루투스를 사용한 접촉자 추적 기술은 각각의 사용자마다 추적 데이터(DUCT: Data Used for Contact Tracing)를 부여하고 이를 블루투스로 송·수신한다. 이후 COVID-19 감염자가 발생하였을 때, 감염자의 추적 데이터 또는 감염자가 보유하고 있는 타인의 추적 데이터를 활용하여 감염 위험성이 높은 밀접 접촉자들을 찾아낸다. 이러한 블루투스 기반 접촉자 추적 기술은 또다시 블루투스 기반 중앙집중형 방식과 탈중앙형 방식으로 구분할 수 있다.

블루투스 기반 중앙집중형 방식은 Service Server가 접촉자 추적을 위한 주요 프로세스를 대부분 수행한다. 좀 더 자세히 설명하면 우선

Table 1. Contact Tracing Technology Components

| Entity | Description |
|---|---|
| E1. Sender(Infected User) | Person who sends DUCT(or can be infected user at the same time) |
| E2. Receiver(Infected User) | Person who receive DUCT(or can be infected user at the same time) |
| E3. Hospital | Certified hospital for COVID-19 diagnosis |
| D1. Smartphone | Smartphones used by Sender and Receiver |
| D2. Service Server | Server for contact tracing systems |
| D3. Web Service | Web services used by contact tracing systems |
| P1. Access | Sender or Receiver use their smartphones |
| P2. Generate Account | Creating an account for contact tracing system |
| P3. Generate DUCT | Generating DUCT used by the contact tracing system |
| P4. Provide DUCT | Provides DUCT for tracing contactors on smartphones |
| P5. Send DUCT | Send DUCT |
| P6. Receive DUCT | Receive DUCT |
| P7. Notice Positive | Hospital notifies infected user of positive condition |
| P8. Announce Positive | Infected person enters positive facts on smartphone |
| P9. Upload DUCT | Upload DUCT of infected user |
| P10. Share DUCT | Share DUCT of infected user |
| P11. Calculate Risk | Calculate the probability of contact |

Service Server는 사용자별로 DUCT를 생성해 사용자에게 발급한다(정확히는 사용자의 스마트폰 내에 저장됨). 이후 블루투스 통신 반경 내에 있는 사용자들은 자신이 부여받은 DUCT를 다른 사람과 서로 주고받게 되는데, 이때 수신한 타인의 DUCT는 일정 기간 자신의 스마트폰에 저장된다.

만일 본인이 감염자로 판명되면, 해당 사용자는 자신의 스마트폰에 저장되어 있는 타인의 DUCT 목록을 Service Server에 업로드 하고, Service Server는 이 DUCT 목록을 해독하여 접촉자들의 실명을 알아낸 후 당사자들에게 감염자에 노출됐다는 사실을 통보한다. 블루투스 기반 중앙집중형 방식은 감염 위험성을 서버에서 판단하기 때문에 추적 결과의 정확도가 높다는 장점이 있다. 이러한 중앙집중형 접촉자 추적 기술에는 'ROBERT'[1], 'NTK'[2], 'BlueTrace'[3] 등이 있다.

블루투스 기반 탈중앙형 방식은 블루투스 기반 중앙집중형 방식과 달리 사용자의 장치에서 접촉자 추적을 위한 프로세스가 수행된다. 접촉자 추적을 위해 사용되는 DUCT는 Service Server로부터 발급되는 것이 아니라 사용자의 스마트폰에서 직접 생성되며 이를 블루투스 신호를 통해 주고받는다. 감염자가 발생하였을 경우, 감염자 본인의 DUCT가 Service Server에 업로드 되고 Service Server는 이를 다시 다른 사용자에게 전달한다. 감염자의 DUCT를 받은 사용자들은 자신의 스마트폰에 해당 DUCT와 일치하는 데이터가 존재하는지 파악함으로써 감염 위험성을 판단한다.

블루투스 기반 탈중앙형 방식은 Service Server의 역할이 제한적이기 때문에 개인 정보 유출 위험이 상대적으로 낮다는 장점이 있다. 이러한 블루투스 기반 탈중앙형 방식에는 'DP-3T'[4], 'Google/Apple Exposure Notification'[5] 등이 있다.

위치정보 기반 방식은 국가가 주체가 되어 GPS, 스마트폰 통신 기록 등의 개인 식별이 가능한 DUCT를 활용하여 감염자의 동선을 추적한다[6]. DUCT를 활용하여 감염자의 동선을 파악하고 이를 공개하여 각자가 감염 위험성을 판단할 수 있도록 한다. 위치정보 기반 방식은 다른 접촉자 추적 기술보다 접촉자 추적 결과의 정확도가 월등하다는 장점이 있다. 현재 한국과 중국 등에서 위치정보 기반 방식을 활용하여 감염자의 동선을 파악하고 있다.

## III. 보안 위협 모델링 기법 선정

COVID-19 접촉자 추적 기술에 대한 평가 기준을 도출하기 위해 보안 위협 모델링 기법을 사용하여 접촉자를 추적하는 과정에서 발생할 수 있는 모든 보안 위협을 식별하였다. 보안 위협 모델링은 시스템의 구조를 체계적으로 분석하여 시스템에서 발생할 수 있는 모든 보안 위협을 식별하는 방법이다[7]. 보안 위협 모델링에서 널리 사용되는 방법에는 STRIDE[8], LINDDUN[9] 등이 있다.

접촉자 추적 기술은 사용자와 서버 사이의 통신 과정에서 발생하는 프라이버시 문제가 중요하다. 따라서 본 논문에서는 사용자와 서버 간의 보안 위협 모델링에 적합한 STRIDE와 프라이버시에 초점을 맞춘 LINDDUN만을 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), 탐지(Detectability), 정보 유출(Information Disclosure), 내용 몰인식(content Unawareness), 정책 및 동의 불이행(policy and consent Non compliance) 관점에서 위협을 분석한다.

접촉자 추적 기술의 모든 구성 요소 별로 STRIDE와 LINDDUN에서 다루는 보안 위협이 발생 가능한지 확인함으로써 접촉자 추적 기술에서 발생할 수 있는 모든 보안 위협을 식별할 수 있다. 이를 통해 각각의 위협이 사용자에게 어떠한 위험 요소로 작용하는지 파악할 수 있어 평가 기준을 도출하는데 활용할 수 있다.

## IV. Attack Library 구축

COVID-19 접촉자 추적 기술에 대한 보안 위협 모델링에서 위협을 식별하기 위해 Attack Library를 구축하였다. COVID-19 접촉자 추적 기술과 관련하여 알려진 모든 공격 정보를 Attack Library로 구축하면 정확한 보안 위협 모델링이 가능하다.

Attack Library는 크게 내부자 위협, 외부자 위협,

사용자 위협으로 구분된다. 내부자 위협은 접촉자 추적 기술 중 Service Server에 대한 관리 주체나 접근 권한이 있는 사람에 의한 위협을 의미한다. 외부자 위협은 접촉자 추적 기술 동작 과정에는 포함되어 있지 않은 외부의 제3자에 의해 발생할 수 있는 위협으로 한 명의 개인이 될 수도 있으며 크게는 기업이나 국가가 외부자로서 위협을 발생시킬 수 있다. 사용자 위협은 접촉자 추적 기술에 속해 있지만 악의적인 목적을 가지고 접촉자 추적을 방해하는 행위를 하는 사용자에 의해 발생할 수 있는 위협을 말한다,

## 4.1 내부자 위협

### 4.1.1 DUCT 무결성 위배

접촉자 추적을 위해 감염자의 DUCT가 Service Server에 업로드 되는데 Service Server에 접근 권한이 있는 공격자는 자유롭게 감염자의 DUCT를 수정할 수 있다[10]. 이러한 공격을 수행할 수 있는 주체가 내부 공격자 등으로 한정적이지만 공격을 수행하는 것이 수월하고, 또 공격으로 인해 거짓 추적 결과를 발생시킴으로써 피해를 확산시킬 수 있다.

### 4.1.2 DUCT 기밀성 위배

접촉자 추적 기술에서 Service Server에는 사용자의 DUCT가 업로드 되기 때문에 Service Server에 접근할 수 있다면 DUCT 정보를 획득할 수 있고 이를 바탕으로 사용자 관련 정보를 확인할 수 있다. 블루투스 기반 중앙집중형 방식의 경우, Service Server는 모든 사용자의 DUCT에 접근할 수 있으며 위치정보 기반 방식의 경우에도 Service Server에서 사용자와 관련한 위치 정보 등에 접근할 수 있다. 이러한 점에서 Service Server에 접근 가능한 내부자는 DUCT를 활용하여 사용자 및 감염자에 대한 정보를 유추할 수 있는 Linking attack[10]을 할 수 있다.

## 4.2 외부자 위협

### 4.2.1 Relay/Replay Attack

Relay/Replay Attack[10, 11, 12, 14, 15]은 다른 사람의 DUCT를 수집·복사하여 다른 시간대나 다른 장소에서 이를 재전송하는 공격을 말한다. 블루투스 기반 접촉자 추적 방식은 브로드캐스트로 DUCT를 보내기 때문에 주변에 있는 사람은 모두 DUCT를 수신할 수가 있다. 이렇게 수집된 DUCT를 시간이 지난 뒤, 또는 다른 장소에서 재전송하게 되면 그 주변의 사용자들은 잘못된 DUCT를 수신하게 된다. 만약 수집된 DUCT의 소유자가 COVID-19 확진 판정을 받게 된다면 피해자들은 거짓으로 밀접 접촉자 판정을 받게 된다.

Relay/Replay Attack은 Trolling Attack과 마찬가지로 접촉자 추적 과정에서 오류를 확산시킬 수 있다는 점에서 위험성이 크다.

### 4.2.2 Storage/Power Drain Attack

Storage/Power Drain Attack[11]은 한정되어 있는 스마트폰의 자원을 고갈시켜 스마트폰이 정상적인 기능을 못 하도록 하는 공격이다. 공격자는 많은 양의 정상 DUCT를 만들어 피해자 주변에서 송신한다. 정상 DUCT이기 때문에 피해자의 스마트폰은 모든 데이터를 수신하여 처리하게 되며 이로 인해 스마트폰의 전력, 저장 공간 등의 자원을 고갈시키게 된다. 또한 공격자가 비정상적인 DUCT를 생성하여 송신하더라도 스마트폰은 이를 수신한 뒤 처리하게 된다. 따라서 이 경우에도 스마트폰의 전력 자원이 고갈된다는 문제가 발생한다.

Storage/Power Drain Attack이 수행될 경우, 스마트폰이 정상적으로 작동하지 않아 실제 수신해야 할 정상 DUCT를 받지 못 하게 되며 결과적으로 거짓 음성(False Negative)을 일으킬 수 있다.

### 4.2.3 Service Server DoS

블루투스 기반 탈중앙형 방식에서는 사용자 등록 과정이 부재해 Service Server가 정상 사용자인지 비정상 사용자인지 구분하지 못한다. 따라서 공격자는 사용자로 가장하여 Service Server에 많은 양의 DUCT를 업로드 할 수 있으며 이로 인해 Service Server는 정상적인 서비스 동작을 방해받을 수 있다.

### 4.2.4 False Report Attack by an Outsider

접촉자 추적 방식에는 COVID-19 감염자와의 접

촉 여부를 판단하기 위해 감염자의 DUCT를 Service Server에 업로드 하는 과정이 존재한다. 외부자에 의한 False Report Attack[10, 12, 13, 15]은 외부 공격자가 비감염자의 DUCT를 Service Server에 업로드 하여 잘못된 감염자 데이터가 공유되게끔 하는 공격이다. 외부자에 의한 False Report Attack은 접촉 여부를 판단하기 위해 사용되는 감염자의 DUCT에 문제가 발생하고 이로 인해 수많은 사람이 잘못된 추적 결과를 받기 때문에 위험성이 높다.

#### 4.2.5 Server Impersonation

접촉자 추적 기술에서 접촉 여부를 판단하기 위해 감염자는 Service Server에 자신의 DUCT를 업로드 하고 Service Server는 이를 다른 사용자들에게 공유한다. Server Impersonation 공격[12]은 공격자가 Service Server로 가장하여 발생하는 위협이다. 이러한 공격을 통해 공격자는 감염자의 DUCT를 획득하여 Replay Attack을 수행할 수 있으며, 또는 비정상적인 DUCT를 사용자들에게 공유하는 False Report Attack을 수행할 수도 있다.

이러한 Server Impersonation 공격을 통해 사용자 간의 소셜 그래프를 확인할 수도 있다[13]. 예를 들어, 악의적인 Service Server는 A가 감염자와 접촉하였다는 가짜 사실을 알린다. 만약 B가 A와 접촉이 있었다면 B 역시도 A로 인해 감염자와 접촉했다는 사실을 받게 될 것이다. 이를 통해 악의적인 Service Server는 A와 B 간의 관계를 확인할 수 있다. 이처럼 Server Impersonation 공격에 의한 비정상적인 DUCT로 인해 감염 위험성 계산 결과에 오류가 발생하게 되고 이는 부정확한 추적 결과로 이어질 수 있으며 사용자의 프라이버시가 노출될 수 있다는 점에서 매우 위험하다.

#### 4.2.6 Bluetooth MITM Attack

블루투스 기반 접촉자 추적 기술은 블루투스를 사용하여 DUCT를 주고받는다. 따라서 블루투스에 대한 중간자 공격(MITM: Man in the Middle Attack)을 수행하여 DUCT를 가로채 데이터를 수정할 수도 있으며 사용자의 DUCT를 확인하는 것이 가능하다.

공격자는 블루투스 MITM 공격을 통해 획득한 DUCT를 사용하여 Relay/Replay Attack, False Report Attack을 수행할 수도 있다.

#### 4.2.7 Bluetooth Vulnerability Attack

블루투스 기반 접촉자 추적 기술은 DUCT를 주고받기 위해 블루투스를 사용하기 때문에 항상 스마트폰의 블루투스 기능을 활성화 시켜 놓아야 한다. 따라서 업데이트가 되지 않은 오래된 OS를 사용하는 스마트폰은 'BlueBorne[16]'과 같은 블루투스 취약점을 사용한 공격에 노출될 수 있다.

이러한 공격은 스마트폰 권한 탈취까지 이어질 수 있으며, OS 업데이트 역시 노후 된 기기의 경우에는 불가능하기 때문에 큰 피해를 낳을 수 있다.

#### 4.2.8 Linking Attack by an Outsider

외부자에 의한 Linking Attack[10, 11, 13, 14, 15]은 사용되는 DUCT 간의 연결성을 파악하여 사용자의 개인 정보를 알아내는 공격 기법이다. 스마트폰에서 DUCT 송신이 일정한 주기로 이루어진다면 공격자는 DUCT를 수집한 뒤, 일정한 주기로 오는 DUCT를 통해 해당 DUCT가 동일한 사용자로부터 왔음을 추측할 수 있다. 블루투스 기반 접촉자 추적 방식은 블루투스를 사용한다는 점에서 블루투스 장치 검색을 통해 얻을 수 있는 장치 이름과 사용자의 DUCT를 연결 지어 개인 정보를 확인할 수도 있다.

#### 4.2.9 Tracking Attack

Tracking Attack[11]은 목표가 되는 사용자를 지정하여 수행된다. 공격자는 해당 사용자를 지속적으로 쫓아다니면서 해당 사용자의 DUCT만을 수집한다. 만약 목표가 된 사용자가 COVID-19 확진 판정을 받을 경우, 공격자에게 감염 위험 결과가 전달될 것이고 이를 통해 공격자는 피해자가 COVID-19에 감염되었음을 알아 낼 수 있다.

#### 4.2.10 Shoulder surfing attack

블루투스 기반 접촉자 추적 기술에서 사용자는 병원으로부터 COVID-19 확진 판정을 받게 되면 해당 사실을 스마트폰에 직접 입력해야 한다. 이때, 이 과정은 COVID-19 확진 판정을 받은 경우에만 발생하기 때문에 공격자는 어깨너머공격을 수행함으로써 사용자의 감염 여부를 파악할 수 있다.

또한 블루투스 기반 탈중앙형 방식에서 Service

Server는 접촉자 추적을 통해 감염자와 접촉한 사용자에게는 위험 사실을 알린다. 이때, 위험 사실을 접촉한 사용자에게만 알린다면 공격자는 이러한 알림이 전송되는 것을 확인하여 알림을 받는 사용자가 감염자와 접촉했다는 사실을 알 수 있게 된다.

### 4.3 사용자 위협

#### 4.3.1 Trolling Attack

Trolling Attack[11-15]은 스마트폰 사용자를 검증하지 않아 발생하는 위협이다. 접촉자 추적 기술은 스마트폰의 사용자는 사람이라는 전제 조건이 있다. 악의적인 감염자나 감염이 의심되는 사람이 자신의 스마트폰을 드론 등에 장착한 뒤, 방대한 범위의 지역을 돌아다니게끔 하여 가짜 접촉을 유도할 수 있다. 그 결과, 실제 감염 위험이 없는 사람들이 잘못된 추적 결과를 받게 되며, 이러한 결과를 바탕으로 이루어지는 추가적인 접촉자 추적 결과 역시 문제가 발생하게 된다. Trolling Attack은 공격에 따른 영향이 한 사람에 그치지 않고 추적 기술 전반에 영향을 미치기 때문에 매우 위험하다.

#### 4.3.2 GPS Manipulation

위치정보 기반 방식에서는 스마트폰의 GPS 정보가 사용되는데 사용자에 의해 GPS 정보가 조작될 경우, 접촉자 추적 결과에 대해 사용자가 부인하는 것이 가능하며 잘못된 DUCT 정보가 Service Server에 전송되게 된다. GPS 정보 조작의 경우, 이를 가능하게 하는 다양한 어플리케이션이 공개되어 있어 공격을 수행하기 쉽기 때문에 위험도가 높다.

#### 4.3.3 System Time Manipulation

접촉자 추적 기술은 사용자가 스마트폰을 소지하고 있음을 전제로 하고 수행되는데 사용자는 자신의 스마트폰 시스템 시간을 임의로 수정하는 것이 가능하다[17]. 악의적인 사용자는 이러한 점을 이용하여 자신의 행위를 부인할 수 있다. 블루투스 기반 접촉자 추적 기술에서는 DUCT를 생성할 때 시간 정보가 사용되는데 이러한 시간 정보를 조작함으로써 비정상적인 DUCT를 만들고 이를 전파하는 것이 가능해지기 때문이다.

#### 4.3.4 Ignore the possibility of contact

접촉자 추적 기술에서 접촉 가능성이 있다는 결과를 받아 본 사용자는 이러한 사실을 병원, 스마트폰 등에 알림으로써 추가적인 접촉자 추적이 이루어져야 한다. 하지만 사용자가 접촉 가능성을 알고도 이를 부인하고 알리지 않을 경우, 추가적인 접촉자 추적이 불가능하며 접촉자 추적 과정에 오류가 발생할 수 있다.

#### 4.3.5 False Report Attack by an User

외부자에 의한 False Report Attack과 비슷하게 사용자에 의한 False Report Attack[10, 12, 13, 15]은 감염자 혹은 감염이 의심되는 사람이 자신의 DUCT를 Service Server에 업로드 하는 것이 아니라 다른 사람의 DUCT를 업로드 함으로써 발생하는 위협이다. 사용자에 의한 False Report Attack은 접촉 여부를 판단하기 위해 사용되는 감염자의 DUCT에 문제가 발생하기 때문에 수많은 사람이 잘못된 추적 결과를 받게 된다는 점에서 위험성이 높다.

## V. 접촉자 추적 기술에 대한 보안 위협 모델링

블루투스 기반 중앙집중형 방식, 블루투스 기반 탈중앙형 방식, 위치정보 기반 방식 각각에 대해 보안 위협 모델링을 수행하였다. 보안 위협 모델링에 앞서 각 방식의 DFD를 작성하였다. DFD를 작성하여 보안 위협 모델링을 적용할 경우, 분석 대상의 모든 요소 및 정보의 흐름을 파악할 수 있어 정확한 분석을 수행할 수 있다. 작성된 DFD를 기반으로 STRIDE 및 LINDDUN을 적용하면 접촉자 추적 기술에서 발생할 수 있는 모든 보안 위협을 식별할 수 있다.

### 5.1 블루투스 기반 중앙집중형 방식

블루투스 기반 중앙집중형 방식은 공통적으로 등록 과정, 데이터 교환 과정, 진단 과정으로 구성된다. 과도한 계정 생성을 통한 서비스 과부하를 막기 위해 등록 과정이 진행되며 계정 생성이 완료되면 각 개인에게 DUCT가 할당된다. 사용자는 블루투스를 사용하여 DUCT를 주고받으며 이를 개인이 소유한 장치에 저장한다. COVID-19 검사 결과, 양성 진단을 받은 사용자는 자신의 장치에 저장된 DUCT를

Service Server에 업로드하고 Service Server는 이를 통해 감염 위험 가능성이 있는 사용자에게 결과를 알려준다.

#### 5.1.1 DFD

블루투스 기반 중앙집중형 방식의 동작 과정에서 발생할 수 있는 보안 위협 및 개인 정보 위협 요소를 확인하기 위해 블루투스 기반 중앙집중형 방식을 정규화 하여 DFD를 작성하면 Fig 1과 같다.

#### 5.1.2 STRIDE 보안 위협 분석

블루투스 기반 중앙집중형 방식에 대해 작성한 DFD를 기반으로 STRIDE를 적용하여 발생 가능한 보안 위협을 확인한 결과는 Table 2와 같다.

블루투스 기반 중앙집중형 방식에서 위협은 크게 사용자-사용자 간의 DUCT 교환 과정과 Service Server-사용자 간에 DUCT를 주고받는 과정에서 발생한다. 블루투스 기반 중앙집중형 방식에서는 감염자의 DUCT를 업로드 받아 Service Server에서 접촉 가능성이 있는 사용자를 계산한 뒤 접촉자로 의심이 되는 사용자에게만 해당 사실을 알린다는 점에서 감염 위험에 대한 정보가 유출될 수 있다.

또한 사용자 간 DUCT 교환을 위해서는 장치의 블루투스 기능을 항상 활성화 해놓아야 한다는 점에서 다양한 블루투스 취약점에 의한 공격 위협에 노출되어 있다.

블루투스 기반 중앙집중형 방식에서는 모든 사용자의 DUCT를 Service Server에서 생성하기 때문에 Servie Server에 악의적인 내부자가 있을 경우, 모든 사용자에 대한 DUCT가 유출, 변조될 수 있다는 문제가 있다.

#### 5.1.3 LINDDUN 보안위협 분석

블루투스 기반 중앙집중형 방식에 대해 작성한 DFD를 기반으로 LINDDUN을 적용하여 발생 가능한 보안 위협을 확인하였으며 그 결과는 Table 3과 같다. 블루투스 기반 중앙집중형 방식에서는 기본적으로 DUCT로 직접적인 사용자 식별이 불가능한 데이터를 사용하기 때문에 식별 위협은 거의 발생하지 않는다.

다만 STRIDE 분석 결과를 통해 확인된 위협들과 연계되어 연결 위협이나 정보 유출 위협이 다수 발생한다.

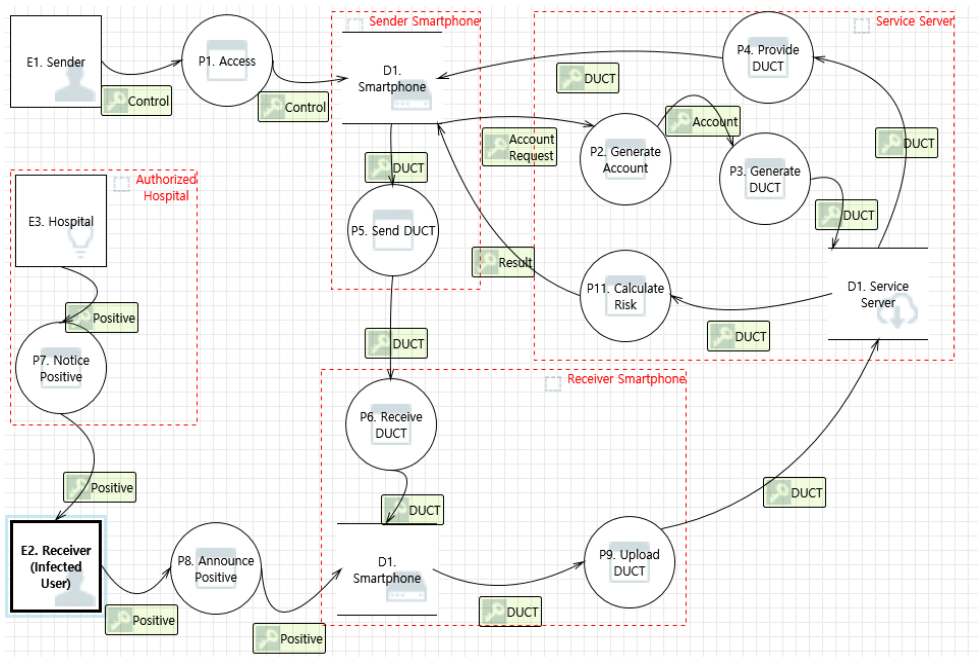


Fig. 1. DFD of centralized contact tracing architecture based on bluetooth

Table 2. STRIDE analysis for centralized contact tracing architecture based on bluetooth

| Entity | Description | |
|---|---|---|
| E1. Sender | S | Spoofing by trolling attack |
| | R | Repudiation by system time manipulation |
| | R | Repudiation by ignore the possibility of contact |
| | R | Repudiation by false report attack |
| E2. Receiver | S | Spoofing by trolling attack |
| | R | Repudiation by system time manipulation |
| | R | Repudiation by ignore the possibility of contact |
| | R | Repudiation by false report attack |
| D1. Smartphone | I | Information disclosure by bluetooth vulnerability attack |
| | D | Denial of Service by bluetooth vulnerability attack |
| | D | Denial of Service by storage/power drain attack |
| | E | Elevation of Privilege by bluetooth vulnerability attack |
| D2. Service Server | S | Spoofing by server impersonation attack |
| | T | Receiving tampered DUCT by false report attack |
| | T | Violation of integrity on user's DUCT by malicious insider |
| | I | Violation of confidentiality on user's DUCT by malicious insider |
| P5. Send DUCT | R | Repudiation by system time modulation |
| P6. Receive DUCT | T | Receiving tampered DUCT by relay/replay attack |
| | T | Receiving tampered bluetooth packet by bluetooth MITM attack |
| | R | Repudiation by system time modulation |
| | D | Denial of Service by power drain attack |
| | E | Elevation of Privilege by bluetooth vulnerability attack |
| P8. Announce Positive | I | Information disclosure by shoulder surfing attack |
| P9. Upload DUCT | S | Spoofing by false report attack |
| | I | DUCT disclosure by server impersonation |
| | D | Denial of Service by server impersonation |
| P11. Calculate Risk | T | Risk result tampering by server impersonation |
| | I | Information disclosure by shoulder surfing attack |

Table 3. LINDDUN analysis for centralized contact tracing architecture based on bluetooth

| Entity | Description | |
|---|---|---|
| E2. Receiver | U | The data subject is not aware if the situation in which personal information is stored |
| D1. Smartphone | D | Disclosure of information by bluetooth vulnerability attack |
| D2. Service Server | L | Linking attack allow an malicious insider to know that who was infected |
| | D | Disclosure of information by malicious insider |
| P5. Send DUCT | L | Linking attack allows an attacker to know that two DUCT came from same user |
| | I | Tracking attack allows an attacker to identify user |
| P8. Announce Positive | L | User's actions are associated with infection by shoulder surfing attack |
| | D | Disclosure of information by shoulder surfing attack |
| P9. Upload DUCT | L | Process asscoiated with a user is infected |
| | D | Process inferred whether a user is infected |
| | D | Disclosure of information by server impersonation |
| P11. Calculate Risk | L | Transfer risk result is associated with the fact that a user is in danger |
| | D | Transfer risk result inferred whether a user is in danger |
| | D | Disclosure of information by shoulder surfing attack |

### 5.2 블루투스 기반 탈중앙형 방식

블루투스 기반 탈중앙형 방식은 공통적으로 DUCT 생성 과정, 데이터 교환 과정, 진단 과정으로 구성된다. DUCT는 사용자의 장치에서 일정 주기로 생성되며 블루투스를 통해 다른 사용자에게 전달되어 저장된다. 감염자 발생 시, 해당 사용자의 DUCT가 Service Server에 업로드 되며 이는 다른 사용자들에게 배포된다. 각 사용자들의 장치에 감염자 데이터와 일치하는 데이터가 저장되어 있는지 여부를 파악함으로써 감염 위험성을 사용자에게 알려준다.

#### 5.2.1 DFD

블루투스 기반 탈중앙형 방식의 동작 과정에서 발생할 수 있는 보안 위협 및 개인 정보 위협 요소를 확인하기 위해 블루투스 기반 탈중앙형 방식을 정규화 하여 DFD를 작성하면 Fig 2와 같다.

#### 5.2.2 STRIDE 보안위협 분석

블루투스 기반 탈중앙형 방식에 대해 작성한 DFD를 기반으로 STRIDE를 적용하여 발생 가능한 보안 위협을 확인하였으며 그 결과는 Table 4와 같다. 블루투스 기반 탈중앙형 방식 역시 중앙집중형 방식과 마찬가지로 사용자 간의 DUCT 교환 과정과 Service Server-사용자 간에 DUCT를 주고받는 과정에서 위협이 주로 발생한다. 블루투스 기반 중앙집중형 방식과는 다르게 계정 등록 절차가 없기 때문에 공격자는 비정상적인 DUCT를 생성하여 이를 업로드 하여 Service Server가 감염자 DUCT로 인지하게끔 할 수 있다. 사용자 간 DUCT 교환을 위해 장치의 블루투스 기능이 항상 활성화되어 있어야 하므로 다양한 블루투스 취약점에 의한 공격에 노출되어 있다.

#### 5.2.3 LINDDUN 보안위협 분석

블루투스 기반 탈중앙형 방식에 대해 작성한 DFD를 기반으로 LINDDUN을 적용하여 발생 가

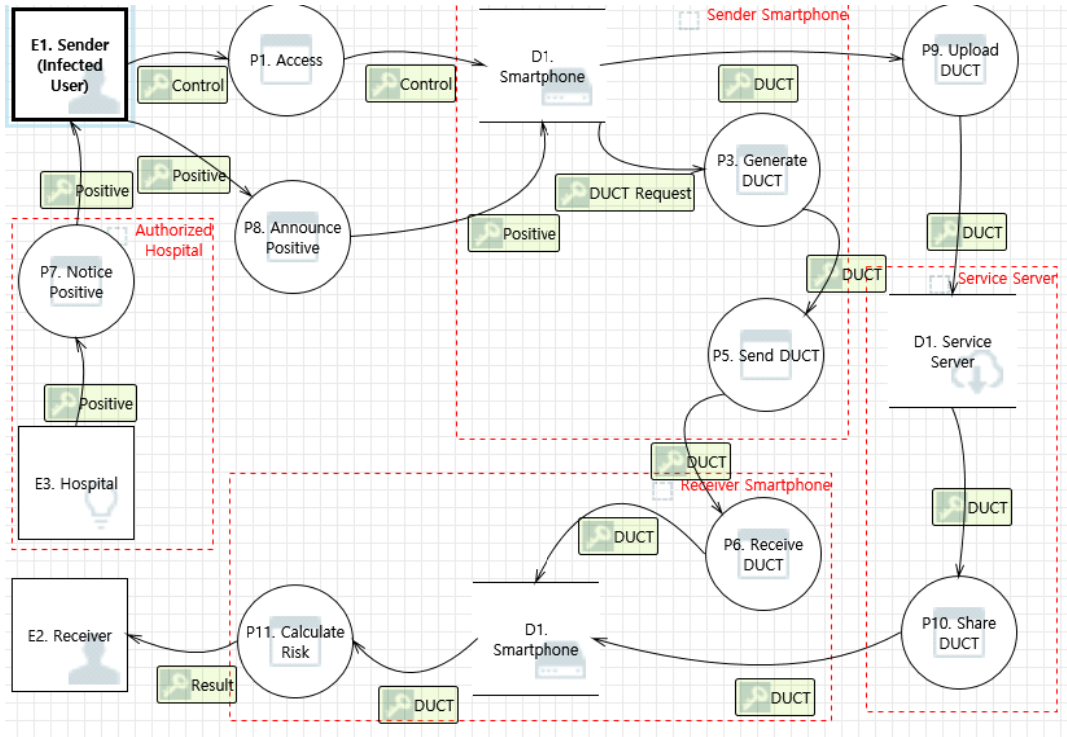


Fig. 2. DFD of decentralized contact tracing architecture based on bluetooth

Table 4. STRIDE analysis for decentralized contact tracing architecture based on bluetooth

| Entity | Description | |
|---|---|---|
| E1. Sender | S | Spoofing by trolling attack |
| | R | Repudiation by system time manipulation |
| | R | Repudiation by ignore the possibility of contact |
| | R | Repudiation by false report attack |
| E2. Receiver | S | Spoofing by trolling attack |
| | R | Repudiation by system time manipulation |
| | R | Repudiation by ignore the possibility of contact |
| | R | Repudiation by false report attack |
| D1. Smartphone | I | Information disclosure by bluetooth vulnerability attack |
| | D | Denial of Service by bluetooth vulnerability attack |
| | D | Denial of Service by storage/power drain attack |
| | E | Elevation of Privilege by bluetooth vulnerability attack |
| D2. Service Server | S | Spoofing by server impersonation attack |
| | T | Receiving tampered DUCT by false report attack |
| | T | Violation of integrity on infected user's DUCT by malicious insider |
| | I | Infected user's DUCT can leak by malicious insider |
| | D | Denial of Service by uploading large amounts of DUCT |
| P5. Send DUCT | R | Repudiation by system time modulation |
| P6. Receive DUCT | T | Receiving tampered DUCT by relay/replay attack |
| | T | Receiving tampered bluetooth packet by bluetooth MITM attack |
| | R | Repudiation by system time modulation |
| | D | Denial of Service by power drain attack |
| | E | Elevation of Privilege by bluetooth vulnerability attack |
| P8. Announce Positive | I | Information disclosure by shoulder surfing attack |
| P9. Upload DUCT | S | Spoofing by false report attack |
| | I | DUCT disclosure by server impersonation |
| | D | Denial of Service by server impersonation |
| P10. Share DUCT | S | Providing abnormal DUCT pretending to be a server |
| | D | Denial of Service by server impersonation |

Table 5. LINDDUN analysis for decentralized contact tracing architecture based on bluetooth

| Entity | Description | |
|---|---|---|
| E2. Receiver | U | The data subject is not aware if the situation in which personal information is stored |
| D1. Smartphone | D | Disclosure of information by bluetooth vulnerability attack |
| D2. Service Server | D | Disclosure of information by malicious insider |
| P5. Send DUCT | L | Linking attack allows an attacker to know that two DUCT came from same user |
| | I | Tracking attack allows an attacker to identify user |
| P8. Announce Positive | L | User's actions are associated with infection by shoulder surfing attack |
| | D | Disclosure of information by shoulder surfing attack |
| P9. Upload DUCT | L | Process associated with a user is infected |
| | D | Process inferred whether a user is infected |
| | D | Disclosure of information by server impersonation |

능한 보안 위협을 확인하였으며 그 결과는 Table 5와 같다. 블루투스 기반 중앙집중형 방식과 마찬가지로 블루투스 기반 탈중앙형 방식 역시 사용자를 식별할 수 있는 위협은 거의 발생하지 않으며 STRIDE 분석 결과를 통해 도출된 위협들과 관련한 연결 위협 및 정보 유출 위협이 다수 발생한다.

### 5.3 위치정보 기반 방식

위치정보 기반 방식에서 Sender가 휴대폰을 사용할 경우, 위치정보를 담고 있는 DUCT가 Service Server에 저장된다. Service Server는 인증된 병원에서 감염 사실을 통보 받은 경우, 감염자의 DUCT를 확인하여 동선을 추적하고 그 결과를 웹 사이트 등에 공개한다. 이 때 공개된 동선을 확인한 사용자는 직접 감염 위험성을 판단해야 한다.

#### 5.3.1 DFD

위치정보 기반 방식의 동작 과정에서 발생할 수 있는 보안 위협 및 개인 정보 위협 요소를 확인하기 위해 위치정보 기반 방식을 정규화 하여 DFD를 작성하면 Fig 3과 같다.

#### 5.3.2 STRIDE 보안위협 분석

위치정보 기반 방식에 대해 작성한 DFD를 기반으로 STRIDE를 적용하여 발생 가능한 보안 위협을 확인하였으며 그 결과는 Table 6과 같다.

위치정보 기반 방식은 DUCT로 위치 데이터가 활용되는데 이러한 DUCT는 사용자가 스마트폰을 사용하면서 GPS, 네트워크 통신 과정에서 필수적으로 생성되는 정보이다. 특히 네트워크 통신 과정에서 생성되는 위치 기록은 외부에서 공격하는 것이 쉽지 않다. 하지만 Service Server의 내부자가 악의적인 행위 시 감염자의 개인 정보가 직접적으로 유출될 수 있고 이는 큰 피해로 직결된다는 위험이 존재한다. 또한 감염자 정보를 제공하는 웹 서비스의 관리자 권한이 탈취되면, 감염자 식별 또는 잘못된 정보 전달이 일어날 수 있다. 무엇보다 감염 위험성 판단을 사용자가 자율적으로 판단할 수 있도록 한다는 점에서 악의적인 사용자가 거짓 감염 위험성 판단 결과를 도출할 수 있다는 문제점이 존재한다.

#### 5.3.3 LINDDUN 보안위협 분석

위치정보 기반 방식에 대해 작성한 DFD를 기반으로 LINDDUN을 적용하여 발생 가능한 보안 위협을 확인하였으며 그 결과는 Table 7과 같다.

STRIDE 적용 결과와 마찬가지로 감염자를 식별할 수 있는 위치 데이터가 활용되기 때문에 내부자에 의한 공격 시 감염자의 개인 정보가 유출될 수 있다는 위험이 존재한다. 또한 웹 서비스에는 감염자의 동선 데이터가 공개되기 때문에 공격자는 자유롭게 웹 서비스에 접근하여 감염자 정보를 확인하고 이를 실제 감염자와 연결 지을 수 있다.

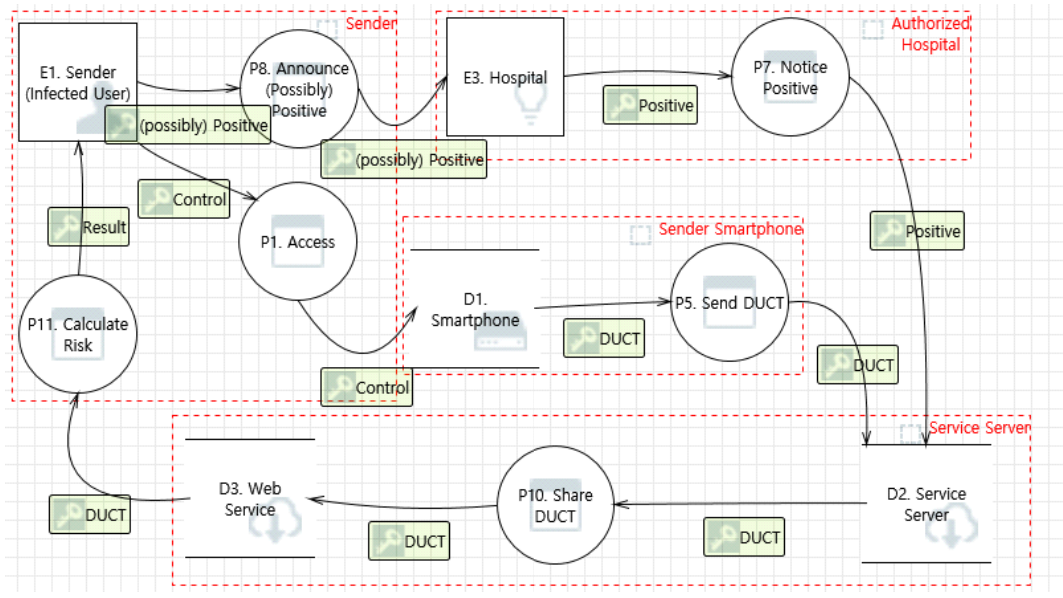


Fig. 3. DFD of contact tracing architecture based on location information

Table 6. STRIDE analysis for contact tracing architecture based on location information

| Entity | Description | |
|---|---|---|
| E1. Sender | S | Spoofing by trolling attack |
| | R | Repudiation by ignore the possibility of contact |
| | R | Repudiation by GPS manipulation |
| D2. Service Server | T | Violation of integrity on infected user's DUCT by malicious insider |
| | I | Infected user's DUCT can leak by malicious insider |
| D3. Web Service | S | It can be impersonated as a similar web service |
| | T | Infected user's DUCT(real location data) can be tempered through obtaining administrator privileges |
| | D | DoS attack on a web service may cause the service to fail |
| | E | Vulnerabilities in the web service may result in the exploitation of administrator privileges on the web service |
| P8. Announce Positive | I | Information disclosure by shoulder surfing attack |
| P10. Share DUCT | T | Infected user's DUCT(real location data) can be tempered by malicous insider |
| | I | Infected user's DUCT(real location data) leakage by malicious insider |

Table 7. LINDDUN analysis for contact tracing architecture based on location information

| Entity | Description | |
|---|---|---|
| D2. Service Server | I | Internal attacker can identify infected user |
| | D | Disclosure of information by internal attacker |
| D3. Web Service | I | Tracking attack allows an attacker to identify user |
| P8. Announce Positive | L | User's actions are associated with infection by shoulder surfing attack |
| | D | Disclosure of information by shoulder surfing attack |
| P10. Share DUCT | D | Disclosure of information by internal attacker |

## VI. 접촉자 추적 기술에 대한 평가 기준 제안

블루투스 기반 중앙집중형 방식, 블루투스 기반 탈중앙형 방식, 위치정보 기반 방식에 대한 STRIDE 및 LINDDUN 분석을 통해 식별된 위협들을 종합하여 전반적인 접촉자 추적 기술을 평가할 수 있는 공통 평가 기준을 만들었으며 Table 8과 같다. 제안된 기준을 사용하면 다양한 유형의 접촉자 추적 기술에 대한 통합적인 비교·분석이 가능하며 효과적인 접촉자 추적 기술을 파악할 수 있다.

## VII. 기존 접촉자 추적 기술들에 대한 비교

앞서 제안한 접촉자 추적 기술에 대한 평가 기준을 적용하여 기존 접촉자 추적 기술들에 대한 비교를 수행하였다. 분석 대상은 BlueTrace, Exposure Notification (EN), 한국 접촉자 추적 기술(KOR)이며 그 결과는 Table 9와 같다.

세 가지 접촉자 추적 기술 모두 충족하지 못 하는 평가 기준은 C1과 C25로 세 가지 접촉자 추적 기술 모두 현재 스마트폰을 사용 중인 사람이 해당 스마트폰의 소유주임을 검증하지 않기 때문에 비정상적인 사용자에 의한 Trolling attack 등에 노출되어 있다. 또한 COVID-19 감염자만이 Announce Positive 프로세스를 수행한다는 점에서 해당 프로세스가 COVID-19 감염 사실을 유출한다는 문제가 있다.

C2와 C18은 접촉자 추적 중 사용되는 시간 데이터와 관련된 것으로 BlueTrace은 DUCT 데이터를 Service Server에서 생성하고 KOR의 경우 통신 기록을 DUCT로 활용한다는 점에서 시간 데이터는 Service Server와 동기화된다고 볼 수 있다. 반면 EN의 경우, DUCT를 스마트폰에서 생성하기 때문에 악의적인 사용자에 의해 시스템 시간 변경을 통한 행위 부인이 가능하다.

C10과 관련하여 BlueTrace와 EN은 Drain attack에 노출되어 있다. BlueTrace의 경우, BLE handshake 과정이 있어 Storage Drain

Table 8. Evaluation criteria for contact tracing technology

| Entity | Criterion | | Related Attack |
|---|---|---|---|
| E1. Sender | C1 | Ensure that sender is a normal user | 4.3.1<br>4.3.2<br>4.3.3<br>4.3.4 |
| | C2 | Time data manipulation by sender should not be possible, such as using server-synchronized time information | |
| | C3 | If there is a possibility of user contact, the system must always be informed of that fact | |
| | C4 | GPS manipulation by sender should be prohibited | |
| E2. Receiver | C5 | Ensure that receiver is a normal user | 4.3.1<br>4.3.2<br>4.3.3<br>4.3.4 |
| | C6 | Time data manipulation by receiver should not be possible, such as using server-synchronized time information | |
| | C7 | If there is a possibility of user contact, the system must always be informed of that fact | |
| | C8 | Receiver should be able to see information stored on their smartphone | |
| D1. Smartphone | C9 | Must be safe from published bluetooth vulnerabilities | 4.2.2<br>4.2.7 |
| | C10 | Resources must be managed against drain attack | |
| | C11 | Abnormal bluetooth packets need to be filtered properly | |
| D2. Service Server | C12 | Validated servers must be verified through authentication between smartphone and service server | 4.1.1<br>4.1.2<br>4.2.3<br>4.2.5 |
| | C13 | Access management to the service server should be done properly | |
| | C14 | Only normal users should upload DUCT through user registration, etc. | |
| D3. Web Service | C15 | Need to take action on the creation of similar websites | |
| | C16 | No vulnerabilities should exist for web services | |
| | C17 | Need to respond appropriately to DoS attacks on Web services | |
| P5. Send DUCT | C18 | Time data manipulation by user should not be possible, such as using server-synchronized time information | 4.2.8<br>4.2.9<br>4.3.3 |
| | C19 | There should be a defense against the linking attack and tracking attack, such as random bluetooth signal strength | |
| P6. Receive DUCT | C20 | Do not allow DUCT reuse | 4.2.1<br>4.2.2<br>4.2.6<br>4.2.7<br>4.3.3 |
| | C21 | Must be safe from published Bluetooth vulnerabilities | |
| | C22 | Abnormal bluetooth packets need to be filtered properly | |
| | C23 | Time data manipulation by user should not be possible, such as using server-synchronized time information | |
| | C24 | Resources must be managed against drain attack | |
| P8. Announce Positive | C25 | The process should not be able to distinguish the infected from the non-infectious | 4.2.10 |
| P9. Upload DUCT | C26 | Only verified users with authentication between smartphone and service server must upload DUCT | 4.2.4<br>4.2.5<br>4.3.5 |
| | C27 | Make sure that the infected person's DUCT is always uploaded | |
| | C28 | Ensure that DUCT is uploaded to validated servers through authentication between smartphone and service server | |
| | C29 | The process should not be able to distinguish the infected from the non-infectious | |
| P10. Share DUCT | C30 | Ensure that DUCT is delivered from validated servers through authentication between smartphone and service server | 4.1.1<br>4.1.2<br>4.2.5 |
| | C31 | Ensure that infected person's DUCT is always shared | |
| | C32 | Access management to the service server should be done properly | |
| P11. Calculate Risk | C33 | Be sure to receive contact from verified servers through authentication between smartphone and service server | 4.2.5<br>4.2.10 |
| | C34 | The process should not be able to distinguish the infected from the non-infectious | |

Table 9. Integrated comparison and analysis of existing contact tracing technology(O : Sufficient, X : Insufficient, - : Not applicable)

| Criterion | BlueTrace | EN | KOR |
|---|---|---|---|
| C1 | X | X | X |
| C2 | O | X | O |
| C3 | O | - | X |
| C4 | - | - | - |
| C5 | X | X | - |
| C6 | O | X | - |
| C7 | - | X | - |
| C8 | X | X | - |
| C9 | X | X | - |
| C10 | X | X | O |
| C11 | O | X | - |
| C12 | X | X | O |
| C13 | △ | △ | △ |
| C14 | O | X | - |
| C15 | - | - | X |
| C16 | - | - | X |
| C17 | - | - | X |
| C18 | X | X | O |
| C19 | X | X | - |
| C20 | X | X | - |
| C21 | X | X | - |
| C22 | O | X | - |
| C23 | X | X | - |
| C24 | X | X | - |
| C25 | X | X | X |
| C26 | O | X | - |
| C27 | X | X | - |
| C28 | X | X | - |
| C29 | X | X | - |
| C30 | - | X | O |
| C31 | - | X | O |
| C32 | - | △ | △ |
| C33 | X | X | O |
| C34 | X | O | O |

Attack은 막을 수 있지만 Power Drain Attack에 노출되어 있으며, EN에 대해서는 Storage Drain Attack과 Power Drain Attack을 모두 수행할 수 있다. 반면, KOR의 경우 사용자의 스마트폰 사용 중 발생하는 통신 기록이 DUCT로 사용되고 DUCT가 다른 사용자에게 전송되는 것이 아닌 Service Server로 전송된다는 점에서 Drain Attack에 안전하다.

C12와 C33의 경우, BlueTrace와 EN에서는 Service Server에 대한 인증 절차가 별도로 존재하지 않아 Server Impersonation이 가능하지만 KOR의 경우, 스마트폰 통신에 앞서 Server(통신사)와 사용자 간의 인증 절차가 수행되기 때문에 안전하다.

C13과 C32의 경우는 Service Server에서의 내부자 관리와 관련된 내용으로 세 가지 유형 모두 공격 가능성이 존재한다는 수준까지만 확인이 가능하다. EN은 프로토콜이라는 점에서 이를 구현한 방식에 따라 내부자 공격 여부가 달라질 것이며 BlueTrace와 KOR의 경우, 관련 자료가 공개되어 있지 않아 확인이 불가능하다.

C34는 접촉 여부를 계산하는 과정으로 BlueTrace는 Service Server에서 접촉 여부를 계산하여 접촉자에게만 해당 사실을 알리기 때문에 이 과정을 통해 접촉자임을 유출할 수 있다는 문제가 존재한다. 반면 EN과 KOR의 경우, 접촉 여부 판단을 사용자나 사용자의 스마트폰에서 수행하기 때문에 프로세스로 인한 정보 유출이 존재하지 않는다.

## VIII. 결 론

COVID-19 확산을 막기 위한 다양한 접촉자 추적 기술들이 공개되고 있으며 기술의 유형에 따라 각기 다른 보안 위협들이 발생할 수 있다. 각각의 기술이나 각 유형별로 발생할 수 있는 보안 위협에 대해서는 기존에 다양한 연구가 진행되었다. 하지만 통합적인 비교 및 분석은 이루어지지 않아 효과적이면서도 안전한 접촉자 추적 기술을 선택하는데 어려움이 존재하였다.

이에 본 논문에서는 접촉자 추적 기술을 블루투스 기반 중앙집중형 방식, 블루투스 기반 탈중앙형 방식, 위치정보 기반 방식으로 나누고 이러한 세 가지 유형의 접촉자 추적 기술을 통합적으로 비교·분석할 수 있는 공통된 평가 기준을 작성하였다. 이를 위해 각 유형별로 STRIDE 및 LINDDUN 분석을 통해 발생가능한 모든 위협을 식별하였다.

작성된 공통 평가 기준을 사용하여 각 유형별로 대표되는 기존의 접촉자 추적 기술을 비교·분석하였다. 이를 통해 보안 위협에 안전하고 개인 정보 보호를 효과적으로 할 수 있는 접촉자 추적 기술이 무엇인지 확인할 수 있었다. 이러한 공통 평가 기준을 활용한다면 COVID-19의 확산을 막기 위한 접촉자 추적 기술 선택 시 도움이 될 것이다.

## References


[1] Claude Castelluccia, Nataliia Bielova, Antoine Boutet, Mathieu Cunche, C´edric Lauradoux, Daniel Le M´etayer, and Vincent Roca, "ROBERT: ROBust and privacy-presERving proximity Tracing," hal-02611265, May. 2020.

[2] Fraunhofer AISEC, "Pandemic Contact Tracing Apps: DP-3T, PEPP-PT NTK, and ROBERT From A Privacy Perspective," IACR ePrint 2020-489, Apr. 2020.

[3] Jason Bay, Joel Kek, Alvin Tan, Chai Sheng Hau, Lai Yongquan, Janice Tan and Tang Anh Quy, "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders," Government Technology Agency-Singapore, Apr. 2020.

[4] Carmela Troncoso, Mathias Payer, Jean-Pierre, et al, "Decentralized privacy-preserving proximity tracing," arXiv preprint arXiv:2005.12273, May. 2020.

[5] Google & Apple, "Exposure Notification v1.2," https://covid19.apple.com/contacttracing, Apr. 2020.

[6] Adam Shostack, "Threat Modeling", WILEY, pp. 109-160, 2014.

[7] NIA, "Korean ICT services against COVID-19 pandemic", Apr. 2020.

[8] Michael Howard, Steve Lipner, "The security development lifecycle", Microsoft Press, 2006.

[9] DistriNet, https://linddun.org/linddun.php, Aug. 2018.

[10] Ruoxi Sun, Wei Wang, Minhui Xue, Gareth Tyson, Seyit Camtepe, Damith Ranasinghe, "Vetting Security and Privacy of Global COVID-19 Contact Tracing Applications," arXiv preprint arXiv:2006.10933, Jun, 2020.

[11] Yaron Gvili, "Security Analysis of The COVID-19 Contact Tracing Specifications by Apple Inc. and Google Inc.," Cryptology ePrint Archive: Report 2020/428, Apr. 2020.

[12] Serge Vaudenay, "Analysis of DP3T Between Scylla and Charybdis", Cryptology ePrint Archive: Report 2020/399, Apr. 2020.

[13] Serge Vaudenay, "Centralized or Decentralized? The Contact Tracing Dilemma," Cryptology ePrint Archive: Report 2020/531, May. 2020.

[14] Archanaa S. Krishnan, Yaling Yang, Patrick Schaumont, "Risk and Architecture factors in Digital Exposure Notification," Cryptology ePrint Archive: Report 2020/582, May. 2020.

[15] Ellie Daw, "Component-Based Compariosn of Privacy-First Exposure Notification Protocols," Cryptology ePrint Archive: Report 2020/586, May. 2020.

[16] Ben Seri, Alon Livne, "BlueBorne - Exploiting BlueBorne in Linux-based IoT devices', Armis, 2017.

[17] Oskari Teittinen, "Analysis of cheat detection and prevention techniques in mobile games," Aalto University, May. 2018.

## 〈저 자 소 개〉

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

김 승 주(Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년: 한국인터넷진흥원(KISA) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2004년~현재: 한국정보보호학회 이사
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2010년: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2011년~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2012년: 선관위 디도스 특별검사팀 자문위원
2014년~2015년: 육군사관학교 초빙교수
2014년~2016년: 다음카카오 프라이버시 정책 자문위원회 위원
2015년~현재: 방위사업청 방산기술보호 자문관
2016년~2018년: 개인정보분쟁조정위원회 위원
2016년~현재: 산업통상자원부 전략물자기술 자문위원
2016년~현재: 한국카카오뱅크 정보보호부문 자문교수
2017년~현재: 고려대학교 국방RMF연구센터(AR2C) 센터장
2018년~2020년: 4차산업혁명위원회 위원: 대통령직속 4차산업혁명위원회 위원
2018년~현재: 고신뢰 보안운영체제 연구센터(CHAOS) 센터장
2020년~현재: 합동참모본부 정책자문위원회 자문위원
〈관심분야〉 보안공학 및 보안내재화 방법론, 보안성 평가/인증, RMF A&A, 암호학 및 블록체인

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