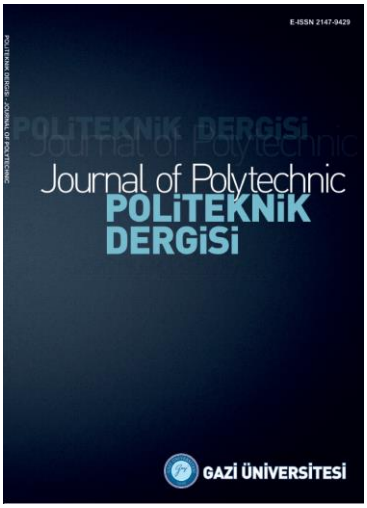

POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)
URL: http://dergipark.org.tr/politeknik

Turkey's contact tracing infrastructure from security and privacy perspective

Güvenlik ve mahremiyet perspektifinden türkiye'nin temaslı takip uygulaması

***Yazar(lar) (Author(s))**: Ayşe SAYIN[1], Mehmet Tahir SANDIKKAYA[2]*

ORCID[1]: 0000-0002-6120-626X

ORCID[2]: 0000-0002-9756-603X

To cite to this article: Sayın A., Sandıkkaya M., "Turkey's contact tracing ınfrastructure from security and privacy perspective", ***Journal of Polytechnic***, *(*): *, (*).

Bu makaleye şu şekilde atıfta bulunabilirsiniz: Sayın A., Sandıkkaya M., "Turkey's contact tracing ınfrastructure from security and privacy perspective", ***Politeknik Dergisi***, *(*): *, (*).

Erişim linki (To link to this article): http://dergipark.org.tr/politeknik/archive

DOI: 10.2339/politeknik.1118577

Turkey's Contact Tracing Infrastructure from Security and Privacy Perspective

Highlights

- *Digital contact tracing strategies*
- *Comparison of contact tracing applicaitons architectures*
- *Privacy preserve contact tracing*
- *Determination of HES specific attack vectors*
- *HES specific mitigation suggestions*

Graphical Abstract

Contact tracing application used in Turkey during the Covid 19 is examined. The application is evaluated by taken into account the security and privacy aspects while comparing it with other contact tracing applications in the world.

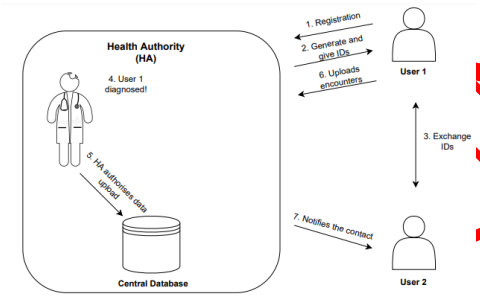

Figure. Centralized contact tracing apporach.

Aim

Evaluate the security and privacy features of Turkey's contact tracing application.

Design & Methodology

Possible vulnerable scenarios for HES are discussed after foreseen behaviour of HES is examined and narrowed since HES is a close-sourced application.

Originality

Many studies examine vaious contact tracing applications around the world but HES is not included. The study anaylzes HES considering security, privacy and data protection concerns.

Findings

The last version of HES found to be vulnerable to common attack scenarios.

Conclusion

Each attack scenarios for HES with relevant mitigation techniques for security breaches and possible privacy violations are concluded.

Etik Standartların Beyanı (*Declaration of Ethical Standards*)

The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

Güvenlik ve Mahremiyet Perspektifinden Türkiye'nin Temaslı Takip Uygulaması

Araştırma Makalesi / Research Article

Ayşe SAYIN*, Mehmet Tahir SANDIKKAYA

İstanbul Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü, Türkiye

(Geliş/Received : 25.05.2022 ; Kabul/Accepted : 21.06.2023 ; Erken Görünüm/Early View : 03.09.2023)

ÖZ

Temas takip uygulamaları güvenlik ve kişisel bilgilerin kötüye kullanımı endişelerine yol açabilir. Türkiye'nin COVID-19 pandemisi sırasında kullanıma sunduğu temas takip uygulaması Hayat Eve Sığar (kısaltılmış hâli ile HES), güvenlik ve kişisel bilgilerin gizliliği gözetilerek henüz ele alınmamıştır. HES'in özellikleri kamuya duyurulmadığından bunların belirlenmesi için var olan temas takip yaklaşımları ile HES karşılaştırılarak uygulamanın çözümlenmesine çalışılmıştır. Bu karşılaştırma, HES'in güvenlik ve kişisel bilgilerin kötüye kullanılabilirliği açılarından özelliklerini göstermiş böylece HES'in dikkate alınması gereken açıklarını da ortaya çıkarmıştır. Bu çalışmada, HES'in güvenlik açıklarını azaltabilecek çözüm ve teknikler önerilmiştir. Bununla birlikte, kullanımdaki son HES uygulamasının tasarımından kaynaklı veri yetkilisinden ya da çevreden kaynaklanabilecek ihlaller içermektedir. Bu çözümleme ile önümüzdeki yıllarda ortaya çıkacak benzer uygulamaların tasarımında dikkat edilmesi gereken konulara dikkat çekilmiştir.

Anahtar Kelimeler: Temaslı takip, güvenlik ve mahremiyet, hes, hayat eve sığar.

Turkey's Contact Tracing Infrastructure From Security and Privacy Perspective

ABSTRACT

Contact tracing applications may lead to security and privacy concerns. Turkey's contact tracing application (Hayat Eve Sığar, abbreviated as HES), which is introduced during COVID-19 pandemic, have not been covered yet for its security and privacy features. Comparison of HES with the existing cutting-edge contact tracing approaches could be used to analyse and determine the features of HES. Comparison indicated the undocumented security and privacy features of HES and revealed a set of vulnerabilities that could cause serious attacks. Mitigation techniques against vulnerabilities are proposed but current HES application includes serious attacks that could be performed by an insider or an outsider. The analysis emphasized to be considered in the design of similar applications that will emerge in the future.

Keywords: Contact tracing, security and privact, hes, hayat eve sığar.

1. INTRODUCTION

Timely identification and isolation of contacts can prevent the spread of epidemics [2]. Especially with the COVID-19 pandemic, efforts are being made to identify and isolate contacts, and thus lag the spread of the disease [3]. The trade off between controlling the spread of the disease and mitigation of the privacy problems introduced by contact tracing applications (CTAs) must be managed. The advantage of being able to control the spread of the disease brought by contact tracing creates problems for preserving the privacy and security of the individuals. Turkey also has a CTA, named Hayat Eve Sığar (abbreviated as HES, Life Fits Into Home in English), that is created by the Ministry of Health of Turkey. The concerns about security and privacy of the individuals that contact tracing exposed also valid for Turkey's CTA.

*Sorumlu yazar (Corresponding Author)
e-posta : sayinays@itu.edu.tr

CTAs can use people's identity information, health report, health status and location due to their existence. Carelessly prepared privacy policies and applications without security design could damage the privacy of individuals seriously. In fact, these applications may involuntarily turn into surveillance tools [3]. On the other hand, the benefit of contact tracing in reducing the spread of infectious diseases is obvious [4]. This study is conducted in order to provide a requirement analysis to protect individual's security and privacy while benefiting from CTAs. Existing contact tracing approaches are compared to be able to investigate Turkey's contact tracing.

In this study, existing contact tracing approaches are compared with Turkey's. Existing CTA models have been evaluated in order to develop a CTA requirements analysis, where individuals can remain anonymous as long as identification is not necessary. It has been examined whether HES meets the developed CTA requirement analysis or not. Effectiveness of the security and privacy features of Turkey's CTA, HES, is evaluated by comparing them with other existing

contact tracing approaches. The evaluation process revealed common vulnerabilities and attack scenarios that a CTA might have with their mitigation strategies. The suggested mitigation strategies can be used in similar applications.

1.1. Contribution

Many contact tracing approaches are already studied with respect to security and privacy properties [5], [6], [7], [8]. Turkish CTA, HES, is not investigated enough except rare publications. This study provides an introduction to risks at common for CTAs, then focuses on the last version of HES. Measures against known vulnerabilities to HES are stated to avoid from having the same threats on future CTAs.

- Workflow of a CTA, CTA's architectures and contact tracing approaches are detailed and a background for CTAs is provided in Section 2.
- Possible behavior of HES are discussed in Section 3.
- An adversarial model is defined over the possible scenarios of HES application in Section 4.
- The foreseen mechanism of HES is described in Section 5, over the security and privacy goals and assumptions that are stated in Section 4.

2. BACKGROUND

Digital contact tracing is based on identifying each person that have been contacted with an infected person. Many applications that have been developed by industry, academia or governments for tracing contacts. Open-souce and closed-sources CTAs exist [9]. In this section, the flow, deployment, proximity, data type approaches of CTAs are examined for later comparison with HES.

2.1. Workflow of a contact tracing solution

Sudden encounter with the pandemic enforced the engineer to design rapid CTA solutions that have not long-term challenged. Therefore, distinctive features of existing CTAs are classified without advertising any of them. Workflow of a digital contact tracing application can be generalized and summarized in four phases [5] which are *initialization*, *sensing*, *reporting* and *tracing*.

Initialization phase: Set and initialize the contact tracing infrastructure. After this phase each user is assumed to have a mobile application.

Sensing phase: Proximity or location data of each user is collected in this phase.

Reporting phase: If a user is infected then that user should be able to inform related parties. In most applications this report is produced voluntarily.

Tracing phase: The authority use traced person's location or proximity data to inform contacted people.

It is possible to categorize digital contact tracing by considering (a) location data type and (b) where the contact tracing is conducted. There are *centralized* and *decentralized* contact tracing approaches exposed from where the contact tracing is conducted (Section 2.2, Section 2.3). Location data can be used with two different techniques in CTAs. One of the techniques is based on *absolute location data* that saves geographic position (Section 2.4). The other one is based *on relative location data* that saves proximity of devices (Section 2.5).

2.1. Centralized approaches in contact tracing

Architecture of CTAs is based on where proximity detection is performed. In centralized approach, a trusted third party is required since contact detection is accomplished in a central server [10]. Therefore, individuals need to register to the central server to subscribe contact tracing service.

The central server deals with encounter records of diagnosed users to determine at-risk users [11]. Each user is required to keep records of their encounters in their device. The applications of users have each encounter's ID. When a user is infected, their accumulated encounters are sent to the central server. The server performs the contact tracing operation then notifies the encountered contacts [12] (Figure 1).

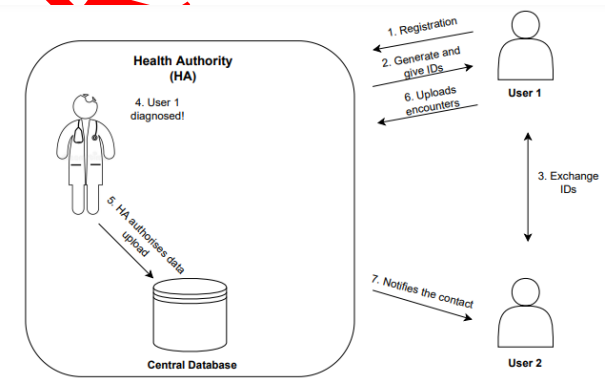

Figure 1. Centralized contact tracing apporach.

2.3. Decentralized approaches in contact tracing

Contact detection is conducted at devices of each individual in decentralized approach [13]. Still, a centralized server could exist to exchange the data. Contact tracing could be done right after the user install the application. The user does not have to register. CTA generates non-persistant IDs for each user. These Ids are exchanged whenever a device founds another device in its proximity. A benefit of decentralized approach is preventing track of a specific user by using temporary IDs. Temporary IDs are generated from a seed, chirp or previous temporary IDs. Server does not process any data, it is just like a database center that stores temporary IDs of the infected users' encounters. Therefore, server is worked as a bulletin board in decentralized contact tracing architecture. If a user learns that he or she is infected he/she sends the list of encountered devices to the information exchange server.

Applications notify their users if they are close to an infected person by polling to the server regularly [14] (Figure 2).

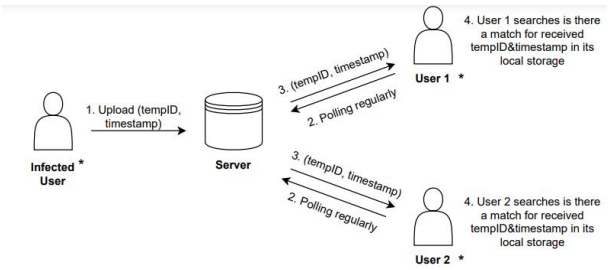

Figure 2. Steps of contact awareness in decentralized approach.

2.4. Contact tracing with absolute location data

Contact tracing with absolute location relies on binding the time and the absloute location one has visited. The geographic position data can be gathered from GPS, base stations or WiFi access points. The bound spatio-temporal data are accumulated to trace a contact [15].

Someone can be tracked continously or discretely depending on the collection of the location data. An exact location that someone visited can be collected by looking GPS coordinates or recording regularly the discrete places that her/him visited. Collected discrete or continuous spatio-temporal data can be used to trace the contacts of users.

On the other hand, localization could be manage by using various techniques such as triangulation. This paper only considers localization techniques that are done by the application not the infrastructure.

2.5. Contact tracing with relative location data

Contact tracing with relative location relies on connecting two nearby communication enabled (e.g. Bluetooth) devices. Devices broadcast their advertisement packets to initiate a connection with devices nearby. Connected devices build a secure communication channel. This secure channel is used to exchange users' IDs (proximity). Contact tracing could be done by the collected proximity data [16].

3. ANALYSIS AND COMPARISON METHODOLOGY

Many studies examine CTAs [17], [18], [19], [20] but HES is not included. Therefore, the scope of the study is analyzing HES considering security, privacy and data protection concerns. In this study, possible operational improvements in HES are omitted since HES is closed-sourced. Any operational detection capability or improvement cannot be fairly discussed. Therefore, solely the design related issues of HES are inspected in this study.

3.1. Foreseen Behaviour of Hayat Eve Sigar application

Foreseen behavior of HES is narrowed during the behaviour discussion by considering limited number of studies on HES [1], [21]. Determining HES behaviour is helpful to examine weaknesses and vulnerabilities of HES.

Wen et al. [1], stated that the most of the CTAs lack functionality transparency. In addition to that, many of the applications declared that they are strict with the General Data Protection Regulation. Wen et al. tried to expose the features of the applications using reverse engineering. They stated that the lack of the transparency of the CTAs, especially released by governments and related authorities, pushed them to investigate privacy aspects of these CTAs. Wen et al. [1] examine close-sourced digital contact tracing application by focusing on:

- collected privacy-critical data types
- privacy leakage measures
- confidentiality features
- platform independence

Each disassembled application, including HES, is checked whether the contact tracing is done by GPS or BLE. According the results of their study [1], HES

- has a centralized architecture
- uses both Bluetooth and GPS

techniques to track contacts.

Analysis of spatial data helps to determine the used localization or proximity techniques. HES uses both GPS and Bluetooth techniques to track contacts. Security and privacy issues are actually exposed from the data in use. Therefore, it is important to describe which and how data is used in HES application.

The list below shows results of the important BLE broadcasting configuration parameters in HES. The list is created by evaluating and eliminating results for HES from Wen's et al. study [1]:

- **Broadcasting Timeout** is set without limiting broadcast time. Therefore, there is no timeout for BLE advertisement packets.
- **Device Connectable** is set as activated. The nearby devices can access and build connections.
- **TxPower** is used for calculating the distance between devices.

Peculiar features in BLE can be used to identify a specific device. A specific device can be identified by keeping these values, such as *Manufacture ID*, *Characteristic UUID* and *Service UUID* [22].

According to Wen et al. [1], HES uses a static *ServiceUUID* value when advertising BLE packets.

The techniques that are used to trace contacts, data storage and process architecture, information broadcasting configurations and parameters, device identifiable values usage of HES are explained so far in this section. The unexpressed and unknown sections of HES's behaviour is evaluated by considering possible existing structures in Section 5.

4. THE ADVERSARIAL MODEL

Particular threats can adversely impact the contact tracing mechanism. Defining an adversary model assists auditing possible risks of HES application. An adversarial model is explained by pointing out adversary's capacity. The security and privacy goals are stated. Security and privacy aspects of HES are specified (4.1).

Adversary is who puts effort to compromise the contact tracing operation. The adversary model considers both an outsider and an insider. The adversary model consists of an honest-but-curious insider and an outsider.

An honest-but-curious insider adversary is capable of gathering all possible information without breaking the protocol.

An outsider adversary is capable of impersonate a user and interrupt, intercept, replay, eavesdrop or change messages that are sent in the public channel. Further, an outsider adversary is considered as who can launch a similar application to trick individuals (similar to phishing attack).

4.1. The security and privacy goals

Scope of the assets of an digital contact tracing process is declared in order to mention security and privacy goals.

Machines along all process are considered as assets such as devices of the individuals or servers. Any information that is stored in these devices are also assets. Likewise, data that is transmitted through wireless communication channels can be described as asset since another information can be derived from transmitted data.

List of assests:

- Location of the individuals
- Past/current health condition of the individuals
- Social relationships of the individuals
- Any privacy-sensitive data stored in the device (PII)
- Individuals' daily routine (Spatio-temporal data)

Overall, the aim is transmitting and processing data with keeping confidentiality and integrity of them to track contacts. Privacy concept includes preventing any leakage of confidential data to protect individuals privacy from unwanted breachs such as de-anonymization or tracking.

4.2. Assumptions on adversarial model

Assumptions about the adversary model are listed below:

- The information that the user provides to the application voluntarily can be stored and used by application
- The devices are tamper-resistant
- A secure channel can be built between parties

5. ATTACK SCENARIOS

Functionality of HES is estimated since source code of HES is not publicly available. Possible threats and risks of HES are discussed by foreseen behaviour of HES. Vulnerabilities and possible attacks against HES are discussed here.

5.1. De-anonymization of the users

De-anonymization attack: concludes exposing a user's identity by equating the broadcasting data of the user with user's identity.

Generic Attack Vector:

- In centralized digital contact tracing architectures,
  - **a)** Proximity are stored in individuals' devices. Encounters uploaded to the server from the individual's devices when a user gets infected. At she same time, a passive adversary can eavesdrop the network traffic since user to server communication only occurs on infected case.
  - **b)** A diagnosed person can be identified if the user is in isolation and only met with a single person (the unique suspect) [6].
  - **c)** An attacker can create dummy users and use multiple devices to perform a sybil attack [23] to de-anonymize users. The attacker can switch usage of devices in short period of times to narrow captured broadcasting data space to equate with real identity of users. The narrowed space is scanned in case of one of the attacker's devices get a notification with a close contact [7].
- In decentralized digital contact tracing architectures,
  - **a)** An adversary that keep a log of their proximity with recording proximity time, duration, location, gender. If one of proximity of the adversary has diagnosed then the adversary gets a notification and then the adversary will be able to compare the log records with the notification to de-anonymize the infected user. Malicious recording could automatically done by using a modified application.

HES-specific Attack Vector: *HES stores user IDs in legible characters (Section 3).* HES stores user IDs in legible characters in the inspected version of the application (Section 3). Anyone could read the static readable user IDs since the Bluetooth broadcast packets could read by nearby devices. If a static user ID come out again, in the same or different location and time, an attacker could bound the static ID with the specific person.

HES has a centralized contact tracing architecture. Users have to register to central server with their identities or at least with their phone numbers. HES

demands identity number, users' father name, birthday, phone number, health status and information, profession, location, telephone book, accessing to camera and phone memory from its users.

An honest-butcurious adversary model is considered in this section, although HES seems suspicious about having the aim of keeping users anonymous on the server side. An-honest-but-curious server could map the static user IDs with the users' identities (at least infected user's and their contacts' identities) since static IDs are stored in legible characters. Therefore, a static ID is personal data w.r.t. Personal Data Protection Authority.

Mitigation: A privacy preserving CTA should demand only contact tracing related information from its users. Irrelevant and personally identifiable information (PII) should not be demanded and should not be stored. PIIs should be deleted after creating unlinkable temporary IDs in registration phase since centralized contact tracing architectures need register their users to the central server. IDs of the users' should not be static and should not be broadcasted/stored in legible alphanumeric characters to protect a specific user from revealing their identity. Additionally, the central server should not store any side information about the user which yields identifying a specific user.

5.2. Video-surveillance of the users

Video-surveillance: the act of observing a scene or scenes of users.

Generic Attack Vector: The video-surveillance attack could perform both centralized and decentralized architectures [14].

a) An adversary can create a local surveillance center using Bluetooth receivers in different places by pairing captured IDs and a pointer to the recorded video. The paired data could store in a database [24].

b) A honest-but curios insider attacker could store scenes from the camera of users' devices by matching them with the user's ID, if the application have access to use camera.

HES-specific Attack Vector: HES demands to access to cameras of devices. Health Minister of Turkey stated that they want to access camera to make users be able to claim a rule violation notification through HES [25]. Arbitrary access of camera could turn into video surveillance of users.

Mitigation: Video-surveillance sensor could be distant from the device. A secret sharing mechanism can be used to mitigate video surveillance since secret sharing prevents pairing captured IDs with recorded videos [26]. Also, the application should not be allowed to access camera or unrelated features of devices.

5.3. Device tracking

Device tracking: an adversary tracks a specific device which means tracking an individual.

Generic Attack Vector:

- In centralized digital contact tracing architectures,
  - **a)** Temporary IDs of users mapped with the users in the central server. A honest-but-curious insider attacker could link the temporary IDs with the device then track the individual.
- In both centralized and decentralized digital contact tracing architectures,
  - **a)** General activity patterns of users can be extracted by deploying Bluetooth nodes in specific places such as a shopping mall. A separate central tracking server could used to track individuals. Bluetooth broadcast packets of users could passively listening and stored with pairing timestamps [27].
  - **b)** A particular device can be distinguished from other devices if Bluetooth advertisement packets include device identifiable values.

HES-specific Attack Vector: A particular device can easily identified in since user IDs does not change with time in HES. Especially in centralized architectures, MAC addresses or other data that could leak device fingerprints can be used to identify a device. An attacker could track a specific device by tracing a specific static broadcast ID. Additionally, HES directly stores user IDs in legible characters that makes tracking a particular user easier.

An-honest-but-curios insider attacker could track a device by looking its ID.

Mitigation: Privacy preserving contact tracing allowed randomisation of broadcasting values [28]. Randomisation of broadcasting value with short periods mitigates tracking of an individual by tracing the individual's static ID. A smarter attacker can link these changed values and keep track of the individual, (see section 5.6 for this case). The leakage from a central server could be limited by a distributed multiparty computation (MPC) [14]. On the other hand, there is no technique to prevent a malicious insider from tracking individuals in the last version of HES. Bluetooth advertisement packets should not contain any device identifiable value.

5.4. Extracting a social interaction graph

Extracting a social interaction graph: is distraction and representation of interactions and proximity between individuals as graphs [29].

Generic Attack Vector:

- In both centralized and decentralized digital contact tracing architectures,
  - **a)** Infected users uploads their encounters to the server. Therefore, an-honest-but-curious adversary in the server disclose the social graph, at least different parts of the social graph, and see the interactions between the individuals including non infected individuals.

HES-specific Attack Vector: An insider attacker could easily extract the social graph since HES uses a centralized architecture.

Mitigation: Disclosing the social graph can be prevented by including additional features in a centralized contact tracing application. IDs of the proximities can be uploaded random and self-reliantly to break the bound between the individuals but the computation would be harder [14]. Also, asymmetric cryptographic accumulator and greatest common divisor function can be used to prevent enumeration and social graph disclosure [30]. Anyway, there is no technical solution to prevent from an insider attacker to extract the social graph in the last version of HES. Extracting a social graph is not an easy attack for an outsider.

5.5. Injection of false-positive and false-negative cases

Injection of false-positive and false-negative cases: is affecting the integrity of contact tracing by injecting false alerts.

Generic Attack Vector:

- In both centralized and decentralized digital contact tracing architectures,
  - **a)** A Bluetooth signal amplifier can be used to range the broadcasting area. Especially, extending the broadcast area in targeted places such as a hospital or test clinic could create lots of falsepositive cases.
  - **b)** A jammer can be used in a targeted area, such as hospitals or public transportation vehicles, to create false-negative cases. The reliability of contact tracing application can be decreased if it has lots of false-positive and false-negative cases.

HES-specific Attack Vector: False-positive and false-negative case injection attack can be performed all kind of digital contact tracing applications. Distinctly, HES broadcasts static IDs which leads to replaying a broadcast message anywhere and anytime.

Mitigation: A hybrid contact tracing architecture can be used to mitigate false status injections. In hybrid type contact tracing, each user has its secret and they use a discrete logarithm scheme to create a shared secret between them [12]. Public-key cryptography algorithms proves that the shared secret cannot be known anyone except encounters [31]. Moreover, HES uses both GPS and BLE techniques. Therefore, the absolute location values may used for checking whether encounters are at the same location or not. However, this solution may bring also privacy issues about tracking a user.

5.6. Linkability

Linkability: is the ability of an adversary to determine the difference whether two broadcast IDs are related or not.

Generic Attack Vector:

- In centralized digital contact tracing architectures,
  - **a)** Temporary IDs of users mapped to a long term pseudonym of a user. The authority is able to link temporary IDs with a unique pseudonym of a user [13]. Corruption of a server or disclosing the linkage secret could create a large scale linkage attack.
- In decentralized digital contact tracing architectures,
  - **a)** Device identifiable values and IDs are ramdomised for avoiding to trace an individual (Section 5.3). An attacker may want to track a device even the device changed its broadcast values regularly. Even though device identifiable values are changed regularly, it is possible to track a specific device if the temporary ID does not change at the same time [7].
  - **b)** A persistent attacker may observe the broadcast packets and may link the disappeared packet by the new created packet.

HES-specific Attack Vector: HES broadcasts a static user ID in legible alphanumeric characters [1]. An attacker does not even need to link broadcast IDs since they are already fixed.

Mitigation: HES should broadcast regularly changing randomized nonces. The broadcast IDs should not be in legible alphanumeric characters. After that, randomisation processes synchronisation of temporary ID and device identifiable values are required to prevent linking different BLE broadcast packets.

5.7. Location and mobilization tracking

Location and mobilization tracking: is an adversary knows presence of a specific user at a location and tracking a specific person's mobility.

Generic Attack Vector:

- In centralized digital contact tracing architectures,
  - **a)** If users share their absolute location data with central server, anhonest-but-curious insider could be able to see the movements of a user.
- In decentralized digital contact tracing architectures,
  - **a)** Temporary IDs of a diagnosed user can be accessed by anyone if the user report herself/himself. Bluetooth nodes could be replaced to distinct areas. Infected users' movements could be observed since temporary IDs of an infected user is a public information. Collected location data could be sorted in chronological order to track the mobility of the user [20].

HES-specific Attack Vector: HES uses both absolute and relative location data for contact tracing. Even though, one of the techniques is enough for tracing a contact both of them can be used to calculate more accurate proximity. HES application uses centralized architecture. A central server can keep track of all real

time location changes of a specific user. An outsider attacker could track mobilization of a user since HES uses static broadcast IDs.

Mitigation: There is no technical solution to protect users from a malicious server but privacy preserving protection mechanisms can be applied. Stored data of users should be deleted after a particular period of time. At least, static IDs should not be used to prevent tracing all movements of a specific user by anyone.

5.8. Replay/Relay attack

Replay/Relay attack: is performed by advertising a message that is received from an honest user.

Generic Attack Vector:

- In both centralized and decentralized digital contact tracing architectures,
  - **a)** The adversary can store the message and spoof the stored message to targeted or another destination [32]. The attack vectors or replay/relay attacks are minimized by changing the IDs in short period of time regularly. Moreover, an attacker still could be able to perform a relay/replay attack in the limited interval.
  - **b)** An attacker can create false positive cases by replaying broadcasted message from a positive tested device. More intense false positive cases can be created by performing replay/relay attacks near by a test clinic or hospital.

HES-specific Attack Vector: If the broadcast message that is sent from a device is not sent with a timestamp in HES, then a malicious user can store the broadcast message and *replay* or *relay* the message at any other time to another device. Broadcast message can be used to deceive another device since HES uses static user IDs. An honest user can be falsely labeled as contact if the honest user has received the replayed/relayed test positive message.

Mitigation: Temporary IDs can be created with an expiration time and broadcast with a timestamp to mitigate the replay/relay attack. Receiver also can take the broadcast messages with a timestamp to compare timestamps if needed to decrease a replay/relay attack risk. However, a replay/relay attack could perform before expiration time of temporary IDs but it would be harder to perform. Expiration time of an temporary ID can be kept as soon as shorter to make performing replay/relay attack harder.

Vaudenay stated a mitigation technique for replay/relay attacks by using a bidirectional communication between advertiser and receiving devices to create a challenge response mechanisms [6].

A hybrid contact tracing architecture could be used to prevent replay/relay attacks. Hybrid contact tracing architectures uses public key infrastructure when sharing the user IDs. Users calculates a Private Encounter Tokens (PET) value when they are broadcast their IDs. The calculated PET value only exists in receiver even though an attacker replay a message to an honest user.

6. COMPARISON OF HES WITH TWO DISTINCT PRACTICAL DESIGN APPROACHES

The attack surface and the impact of an attack can be secreased on the design process of a CTA.

Comparison of following design approaches clarify that HES could benefit from the privacy friendly features of worldwide CTA applications without sacrificing its effectiveness.

6.1. Hamagen vs. HES

Hamagen is an open-source CTA that is developed by Ministery of Health of Israel [33]. Each instance of the application keeps spatio-temporal history of the device. Upon positive Covid-19 diagnosis, the Ministry of Health fetches this data within the consent of the patient and publishes it. Each instance of the application periodically polls the published data and checks for an encounter. The location data of devices are acquired by GPS, GSM base stations and WiFi access points.

The contact tracing operation is performed as follows:

- The application periodically downloads a file that is provided from the Ministry of Health. This files includes the locations of the diagnosed users in the last 14 days.
- Then, the application checks any spatio-temporal overlap.
- If the application finds an overlap, then it notifies the user with the possible overlap place and time information.
- The user reviews the overlap and has right to falsify this claim in this step.
- If the user approves the overlap, then user's location history (last 14 days) is sent to the Ministry of Health.

In this design, the location history is only shared when a user is diagnosed. Additionally, no user identifier is shared but just the spatio-temporal data. Contact tracing is performed locally on each device based on the Ministry's data. Therefore, direct user identification is not possible for other users. This approach decreases the attack surfaces in comparison to HES. Resulting that, replay/relay, device tracking, de-anonymization of the users, false case injections and localization tracking attacks are much more difficult in decentralized Hamagen compared to centralized HES.

6.2. DESIRE vs. HES

Another take in design is DESIRE, which is an hybrid approach [34]. DESIRE uses *Private Encounter Tokens* (PET). PETs are cryptologically generated during encounters and kept secret in each device. DESIRE generates temporary IDs on the user devices. Risk computation is operated centrally.

The contact tracing operation is done as follows:

- Each registered user generates periodic temporary IDs.
- Users exchange their IDs upon encounters.
- Exchanged IDs are used to form/generate PETs.
- Diagnosed user uploads PETs that she/he has in her/his device to the central server.
- Whenever a user would like to calculate risk of contact, he/she could send his/her set of PETs to the server.
- The server notifies the risky user.

Compared to HES, PETs prevent social graph extraction. Additionally, they help to keep user data in encrypted form at the server. This decreases the impact of a possible data breach. Therefore, replay, localization tracking, deanonymization of the users, false case injections and extracting the social graph attacks are much more difficult in hybrid DESIRE compared to centralized HES.

7. RELATED WORK

Tang's study [5] states contact tracing solutions that can notify users who have been in contacted with infected people and, in the meantime, give health authorities the opportunity to take appropriate action. The study examine existing contact tracing solutions and discuss their benefits while outlining several key observations for more efficient and comprehensive privacy-aware contact tracing solutions [5].

Ahmed et al. declared that many of CTAs are created after COVID19 outbreak [12]. They said, the CTAs have different attributes and architectures, they manage data differently. Therefore, they explain these various contact tracing techniques and architectures with their advantages and vulnerabilities. They also examine some of the CTAs in different architectures.

On the other hand, Decentralized Privacy-Preserving Proximity Tracing (DP3T) system helps tracking the contacts. It is argued that some of DP3T's privacy practices may have the opposite effect to what was intended [6]. Therefore, Vaudenay [6] analyze the security and privacy of DP3T with showing that it can pose serious risks to society.

Wen et al. [1] mentioned security and privacy risks of specific cases while they examine the applications. The study [1] audits close-sourced CTAs especially the ones that are developed by governments and health authorities. They disassemble and decompile the application's source code and analyze their architecture, contact tracing techniques as well as how they store and use data.

Xu et al. [35] stated the existence of contact tracing and they emphasized privacy issues has been a bottleneck for existing contact tracking solutions around the world. They present a blockchain-enabled scheme for contact tracing that preserves privacy which named as BeepTrace. They propose to introduce a chain of blocks that links the user and the authorized solver to desensitize the identification of the user and the information of location. The study intend to increase security and privacy of the CTAs with the added benefits of being battery friendly and globally accessible.

8. CONCLUSION

Contact tracing approaches in the various CTAs are examined to be able to create a requirement analysis for a secure and privacy-preserving contact tracing procedure. After that, likely behaviour of Turkey's CTA, HES, is narrowed down to apply requirement analysis.

Based on the analysis, the last version of HES found to be vulnerable to many common attack scenarios. Each attack scenario with relevant mitigation techniques for security breaches and possible privacy violations are discussed. The current status of HES, where the mitigation techniques are not applied, includes many attacks. These attack scenarios could be performed by an insider or an outsider.

HES uses a centralized contact tracing architecture and it necessitates registration to be used. In addition, HES requests many irrelevant information and requires unnecessary access to the devices. Collected information are stored in a central server. Therefore, it is concluded that there is no effective technical solution to protect a user from an honest-but-curious insider in the last version of Turkey's CTA. Even though the central authority is trustworthy, serious attacks could be performed by an outsider.

Overall, the comparison of many CTAs and the analysis that are conducted specific on HES brought out a direction for similar applications that will emerge coming years.

DECLARATION OF ETHICAL STANDARDS

The author(s) of this article declare that the materials and methods used in their studies do not require ethical committee approval and/or legal-specific permission.

AUTHORS' CONTRIBUTIONS

Ayşe SAYIN: Performed the experiments, analyse the results and wrote the manuscript.

Mehmet Tahir SANDIKKAYA: Performed the experiments, analyse the results and wrote the manuscript.

CONFLICT OF INTEREST

There is no conflict of interest in this study.

REFERENCES

[1] H. Wen, Q. Zhao, Z. Lin, D. Xuan, and N. Shroff, "A study of the privacy of covid-19 contact tracing apps," ***International Conference on Security and Privacy in Communication Systems***, 297–317, (2020).

[2] Çakan, "Salgın hastalıkların yayılmasında yüksek riskli bireylerin dikkate alındığı bir matematiksel modelin analizi," ***Politeknik Dergisi***, 24: 1205–1211, (2021).

[3] Z. Yilmazoglu and A. Demircan, "Covid-19 sürecinde mevcut hastanelerde mekanik sistemlerinde alınması gereken Önlemler ve tecrübeler," ***Politeknik Dergisi***, 26: 93–106, (2023).

[4] M. Zastrow, "South Korea is reporting intimate details of COVID-19 cases: has it helped?," ***Nature***, (2020).

[5] C. Lefévre, "Optimal control of a birth and death epidemic process," ***Operations Research***, 29: 971–982, (1981).

[6] Q. Tang, "Privacy-preserving contact tracing: current solutions and open questions," ***Cryptology ePrint Archive***, (2020).

[7] S. Vaudenay, "Analysis of DP3T." ***Cryptology ePrint Archive***, (2020).

[8] T. Martin, G. Karopoulos, J. L. Hernández-Ramos, G. Kambourakis, and I. N. Fovino, "Demystifying COVID-19 Digital Contact Tracing: A Survey on Frameworks and Mobile Apps," ***Wireless Communications and Mobile Computing***, 2020: 1–29, (2020).

[9] M. Shukla, R. M. A, S. Lodha, G. Shroff, and R. Raskar, "Privacy guidelines for contact tracing applications." ***arXiv preprint arXiv:2004.13328***, (2020).

[10] J. Bay, J. Kek, A. Tan, C. S. Hau, L. Yongquan, J. Tan, and T. A. Quy, "BlueTrace: A privacy-preserving protocol for communitydriven contact tracing across borders." ***Government Technology Agency-Singapure, Tech. Rep 18***, (2020).

[11] J. Chan, D. Foster, S. Gollakota, E. Horvitz, J. Jaeger, S. Kakade, T. Kohno, J. Langford, J. Larson, P. Sharma, et al., "PACT: Privacy Sensitive Protocols and Mechanisms for Mobile Contact Tracing." ***arXiv preprint arXiv:2004.03544***, (2020).

[12] R. Sun, W. Wang, M. Xue, G. Tyson, S. Camtepe, and D. Ranasinghe, "An Empirical Assessment of Global COVID-19 Contact Tracing Applications." ***2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE)***, (2021).

[13] N. Ahmed, R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere, A. Seneviratne, W. Hu, H. Janicke, and S. K. Jha, "A survey of covid-19 contact tracing apps," ***IEEE access***, 8: 134577–134601, (2020).

[14] S. Vaudenay, "Centralized or Decentralized? The Contact Tracing Dilemma." ***Cryptology ePrint Archive***, (2020).

[15] Fraunhofer AISEC, "Pandemic Contact Tracing Apps: DP-3T, PEPPPT NTK, and ROBERT from a Privacy Perspective." ***Cryptology ePrint Archive***, (2020).

[16] J. Li and X. Guo, "Global deployment mappings and challenges of contacttracing apps for covid-19," ***Available at SSRN 3609516***, (2020).

[17] J. Bell, D. Butler, C. Hicks, and J. Crowcroft, "TraceSecure: Towards Privacy Preserving Contact Tracing." ***arXiv preprint arXiv:2004.04059***, (2020).

[18] M. Veale, "Analysis of the nhsx contact tracing app 'isle of wight'data protection impact assessment." (2020).

[19] H. Cho, D. Ippolito, and Y. W. Yu, "Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs."***arXiv preprint arXiv:2003.11511***, (2020).

[20] D. J. Leith and S. Farrell, "Coronavirus Contact Tracing App Privacy: What Data Is Shared by the Singapore OpenTrace App?," ***Security and Privacy in Communication Networks: 16th EAI International Conference*** , 80–96, (2020).

[21] L. Baumgärtner, A. Dmitrienko, B. Freisleben, A. Gruler, J. Höchst, J. Kühlberg, M. Mezini, R. Mitev, M. Miettinen, A. Muhamedagic, et al., "Mind the GAP: Security & privacy risks of contact tracing apps," ***IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications***, 458–467, (2020).

[22] P. H. O'Neill, T. Ryan-Mosley, and B. Johnson, "A flood of coronavirus apps are tracking us. Now it's time to keep track of them.." https://www.technologyreview.com/2020/05/07/1000961/ launching-mittr-covid-tracing-tracker, (2020).

[23] C. Zuo, H. Wen, Z. Lin, and Y. Zhang, "Automatic fingerprinting of vulnerable ble iot devices with static uuids from mobile apps," ***Conference on Computer and Communications Security***, 1469–1483, (2019).

[24] W. Beskorovajnov, F. Dörre, G. Hartung, A. Koch, J. Müller-Quade, and T. Strufe, "ConTra Corona: Contact Tracing against the Coronavirus by Bridging the Centralized–Decentralized Divide for Stronger Privacy," ***Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security***, Singapore, (2021).

[25] S. Vaudenay, "Video surveillance + DP-3T ISSUE #121." https://web.archive.org/web/20220323142550/https://github.com/DP-3T/documents/issues/121.

[26] Republic of Turkey Ministry Of Health, "Hes." https://web.archive.org/web/20220323143858/https://hayatevesigar.saglik.gov.tr/ gizlilik_politikasi_eng_index_V2.html.

[27] M. P. Jhanwar and S. Sarkar, "PHyCT: Privacy preserving Hybrid Contact Tracing." ***Cryptology ePrint Archive***, (2020).

[28] O. Seiskari, "corona-sniffer: Contact Tracing BLE sniffer PoC." https://web.archive.org/web/20220323143722/https://github. com/oseiskar/corona-sniffer.

[29] A. K. Mishra, A. C. Viana, and N. Achir, "SimBle: Generating privacy preserving real-world BLE traces with ground truth." ***arXiv preprint arXiv:2101.11728***, (2021).

[30] G. Kambourakis, "Anonymity and closely related terms in the cyberspace: An analysis by example," ***Journal of information security and applications***, 19: 2–17, (2014).

[31] I. Ozcelik, "Capen: Cryptographic accumulator based privacy preserving exposure notification," ***9th International Symposium on Digital Forensics and Security***, 1–6, (2021).

[32] F. Brandt, "Efficient cryptographic protocol design based on distributed el gamal encryption," ***International***

Conference on Information Security and Cryptology, 32–47, (2005).

[33] K. Pietrzak, "Delayed authentication: Preventing replay and relay attacks in private contact tracing," ***International Conference on Cryptology***, India, 3–15, (2020).

[34] "Hamagen, israel's ministry of health's covid-19 exposure prevention app.." https://web.archive.org/web/20230323113357/https://github.com/MohGovIL/hamagen-react-native, (2020).

[35] C. Castelluccia, N. Bielova, A. Boutet, M. Cunche, C. Lauradoux, D. L. Métayer, and V. Roca, "Desire: A third way for a european exposure notification system leveraging the best of centralized and decentralized systems," ***arXiv preprint arXiv:2008.01621***, (2020).

[36] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan, and M. A. Imran, "BeepTrace: Blockchain-Enabled Privacy-Preserving Contact Tracing for COVID-19 Pandemic and Beyond," ***IEEE Internet of Things Journal***, 8: 3915–3929, (2020).