Target Privacy Threat Modeling for COVID-19 Exposure Notification Systems

Ananya Gangavarapu
PathCheck Foundation
Cambridge, MA, USA
ananya.gangavarapu@pathcheck.org

Ellie Daw
PathCheck Foundation
Cambridge, MA, USA
elliemdaw@gmail.com

Abhishek Singh
PathCheck Foundation
Cambridge, MA, USA
abhishek.singh@pathcheck.org

Rohan Iyer
PathCheck Foundation
Cambridge, MA, USA
rohan.iyer@pathcheck.org

Gabriel Harp
The MIT Press
Cambridge, MA, USA
gabriel.harp@pathcheck.org

Sam Zimmerman
PathCheck Foundation
Cambridge, MA, USA
sam@pathcheck.org

Ramesh Raskar
PathCheck Foundation
Cambridge, MA, USA
ramesh.raskar@pathcheck.org

Abstract

The adoption of digital contact tracing (DCT) technology during the COVID-19 pandemic has shown multiple benefits, including helping to slow the spread of an infectious disease and to improve the dissemination of accurate information. However, to support both ethical technology deployment and user adoption, privacy must be at the forefront. With the loss of privacy being a critical threat, thorough threat modeling will help us to strategize and protect privacy as digital contact tracing technologies advance.

Various threat modeling frameworks exist today, such as LINDDUN, STRIDE, PASTA, and NIST, which focus on software system privacy, system security, application security, and data-centric risk, respectively. When applied to the exposure notification system (ENS) context, these models provide a thorough view of the software side but fall short in addressing the integrated nature of hardware, humans, regulations, and software involved in such systems. Our approach addresses ENSs as a whole and provides a model that addresses the privacy complexities of a multi-faceted solution. We define privacy principles, privacy threats, attacker capabilities, and a comprehensive threat model. Finally, we outline threat mitigation strategies that address the various threats defined in our model.

1 Introduction

Privacy is one of the most important components when evaluating a digital contact tracing system. Privacy is of paramount importance due to multiple reasons ranging from government policies and regulations to adoption by individuals. Existing threat modeling frameworks and approaches focus mostly on security threats and effectiveness during the software development life-cycle (SDLC). Digital tracking of COVID-19 infections requires leveraging the existing components, such as web server technologies, to build new services such as exposure notification (EN) apps. The repurposing of existing components and the algorithmic nature of DCT leads to radically different privacy concerns not considered while designing or using those components in traditional ways. Hence, an enhanced approach is needed for privacy threat modeling and privacy impact assessment for CT capabilities.

We have started with evaluating existing threat modeling frameworks like LINDDUN [15], STRIDE [14], PASTA [16], and NIST [11] for use in privacy threat modeling. Most of the privacy threat models provide a software-centric approach to threat modeling and fall short when it comes to non-stereotypical privacy attacks like coercion attacks or complying with evolving privacy directives such as ePrivacy directives from European Data Privacy Board (EDPB) [2]. To address the additional privacy requirements, we propose a few enhancements to existing privacy threat models. First, we propose a modeling approach based on target state attacker capabilities and applicable exhaustive threat categories. The target state ensures the minimization of false positives, the minimization of overlooked threats, and a consistent result regardless of who is doing the threat modeling. Another proposed enhancement is to simplify threat models to accommodate many-to-many relationships between threat categories and attacker capabilities. Finally, in order to avoid confusion, we have standardized the terms used across target privacy threat models.

This document first introduces the enhanced framework and then uses the framework to build the Target Privacy Threat Model for Exposure Notification System (ENS).

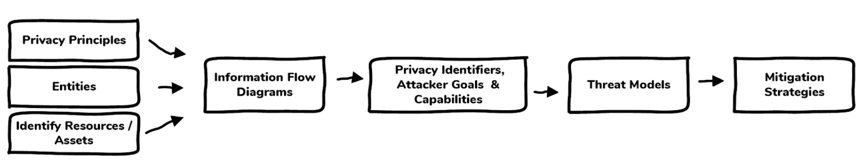
2 Terminology

There are a variety of ways to leverage technology to aid the manual contact tracing process. Traditionally, this process involves a public health official interviewing a person who has been diagnosed with an infectious disease in order to identify who they may have had contact with so that these contacts can be alerted to take proper measures to prevent further spread of the virus. Apps that have been built to help with this process typically alert users who have had a potential virus exposure, rather than performing tracing of contacts. As such, these apps are often referred to as exposure notification (EN) or exposure alerting (EA) apps. The functionality provided works in conjunction with manual contact tracing to scale the efforts of early quarantine and other preventive measures. Some applications provide additional features beyond exposure notification and therefore may not be pure EN apps. In this paper, we use the umbrella term exposure notification systems (ENS) to refer to EN, EA, and apps with functionality to aid in scaling outcomes of manual contact tracing, though it is important to note that privacy-preserving applications under this umbrella do not typically "trace" users and their contacts.

3 Target Privacy Threat Modeling Framework

The Target Privacy Threat Modeling (TPTM) Framework is a privacy-driven threat modeling framework that helps to systematically identify privacy attacker capabilities and mitigate privacy threats in a system or an interconnected platform. The TPTM Framework leverages an attacker-centric threat model that is driven by the attacker's capabilities and motivations to exploit the privacy vulnerabilities. Also, as a privacy threat model framework, the focus is on attacker goals that compromise the privacy of users, rather than their security.

The following diagram shows various steps of the TPTM Framework:



The TPTM Framework starts with privacy principles and identifies the resources and/or assets in the scope. Threat models help to identify attacker goals and capabilities in the context of specific information flow diagrams and develop effective mitigation strategies. The TPTM Framework recommends doing threat modeling at various phases of the development and deployment of the systems.

4 Target Privacy Threat Modeling Framework for Exposure Notification Systems

ENS, which has become an important toolset in mitigating COVID-19, has two principal components:

- **Case management:** Key functions are i) streamlined electronic capture and management of data on patient and contacts and ii) integrated workflows with surveillance systems.
- **Proximity tracing / exposure notification:** Key functions are i) use opt-in digital tools to augment manual contact tracing and ii) use Bluetooth technologies to compute proximity and duration of exposure to patients diagnosed with COVID-19.

4.1 ENS Architectural Approaches

All of the ENS solution implementations fall into one of three categories of architecture:

- **A centralized architecture:** The anonymity of users and confidentiality of contact events is only provided with regard to outside entities, i.e., other users or external actors; the operators and involved authorities can, however, identify all users and connect them to recorded contact histories.
- **A partially decentralized architecture:** Users and contact events are only concealed from other users and third parties; the server can de-anonymize positively tested users. The system also has a data donation function, by which users can choose to share their contact histories for epidemiological research. If done so, positively tested users' contact events would become visible to operators and authorities.
- **A completely decentralized architecture:** Users remain anonymous toward other users and third parties, and their contact events also remain private. Operators and authorities can de-anonymize positively tested users but cannot access their contact history. Epidemiological research is not possible.

Each of the architectures mentioned above results in different threat models and hence different mitigation strategies. Before we get into specifics of threat models, let us first identify privacy principles.

4.2 Privacy Principles

Privacy principles form the base for the scope and key business requirements of ENS approaches. General Data Protection Regulation (GDPR) has been the gold standard for personal data protection, and this document uses GDPR and related privacy directives from EDPB. The following are key privacy principles used as the scope for the target threat modeling:

- **Lawful:** ENS and related components must comply with all applicable laws, rules, and regulations. Any data collection and use must have a lawful basis.
- **Informed consent:** A user must provide informed consent as a prerequisite for the installation and use of ENS. A user should be able to give their consent to each function of an app separately, such as the collection of proximity data, location data, sharing data, or other key separate functions.
- **Purpose binding:** Purpose binding ensures that personal data processing is performed according to predetermined purposes.
- **Identity control:** Users make the determination to release redacted, disconnected, and/or aggregated space-time points from location data, or obfuscated identifiers from e.g., Bluetooth.
- **Transparency:** Consumers should be given notice of an organization's information practices before any personal information is collected from them.

- **Accountability:** In order to ensure that organizations adhere to ENS privacy principles, there must be enforcement measures.
- **Proportionality:** The potential risk that private information may be exposed to or misused as a result of the ENS must be proportional to the public health benefits of that system for combating the epidemic.
- **Data retention:** To minimize risk of improper data use, breach, or loss, ENS must have responsible data retention procedures, e.g., practicing data minimization and destroying data after a set amount of time.

4.3 Entities

The main entities for privacy threat modeling are the data subject, the data controller, and the data processor(s). The following table depicts different actors under each of the entity groups:

Entity Type	Actors and Participants
Data Subject	Users or business entities of ENS or related resources
Controller	Health authorities, government, and other parties determining purposes and means of processing personal data
Processor	Organizations providing resources for data processing, such as cloud computing providers, database providers, app providers, etc.

4.4 Identify resources and assets

Resources are typically software components or tools used in ENS. In addition to privacy principles, the assets and the resources drive the scope of the target threat modeling activities. The following table lists all of the components/services used in each of the architectural approaches.

Architectural Approach	Related Resources/Assets	Example
Centralized Architecture	Web server, browser, mobile app, databases, algorithms, and app stores.	Singapore's TraceTogether [12]
Partially Decentralized Architecture	Web server, browser, mobile app, databases, algorithms, app stores, and support services.	PathCheck Foundation apps [5], Germany's Corona Warn [4], Ireland's Covid Tracker [7]
Decentralized Architecture	Mobile app, app stores, and support services.	TraceCorona [9]

Resources or assets are evolving as time passes and all the vendors, including Google and Apple, are updating the software and other assets continuously. For this paper, we are considering the following versions / frameworks only:

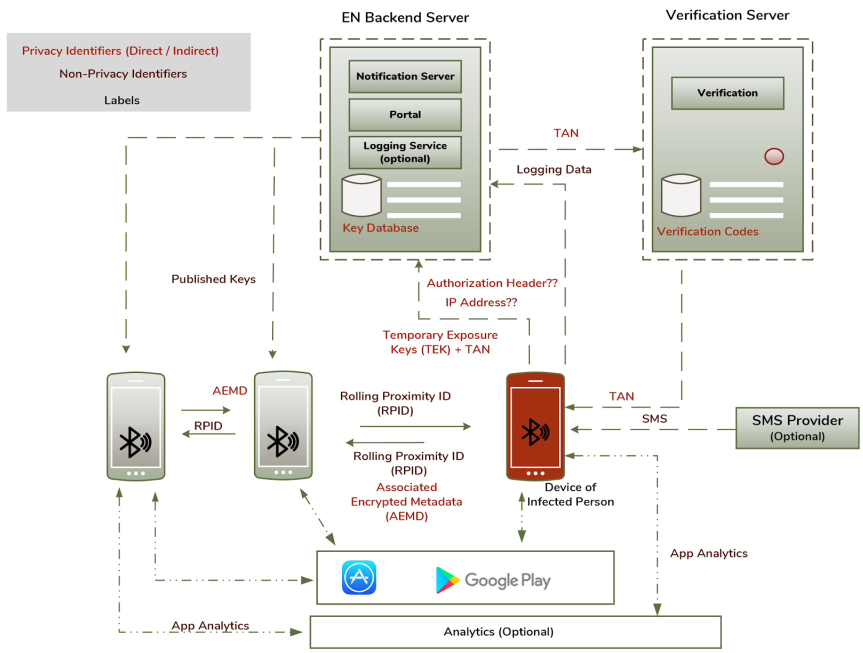
- Google Exposure Notification Server v0.7.0
- GAEN Exposure Notification API v1.5 [8]
- Pan-European Consortium (PEPP-PT)
- DP-3T
- Apple iOS 11 or greater
- Android 8 or greater

For target threat models, we take superset of the resources required for all three architectural approaches.

4.5 Information Flow Diagrams (IFDs)

Data flow diagrams (DFDs) traditionally used to identify privacy threats are not effective for privacy identifiers in ENS. DFD-based threat modeling fundamentally looks at how data is designed to move through a system. The approach cannot, therefore, provide a means to inherently analyze how an application appears to a potential attacker. Instead, we propose information flow diagrams, IFDs, to identify all privacy identifiers in functional and/or business terms.

The figure below depicts an IFD for a partially decentralized architecture (GAEN mobile app / Express Server):



4.6 Privacy Identifiers

Privacy Identifiers are any data, element, or information that can be used, directly or as a proxy, to identify a person or group of persons. The following table lists most of the direct and indirect privacy identifiers in the target state of ENS.

Direct Privacy Identifiers	Indirect Privacy Identifiers
Name, address, user email, phone IMEI, IP address, MAC address	Location data, local public health agency, age of the user, infection status, device model / version, gender, date of interview, temporary encryption key (TEK), associated encrypted metadata (AEMD), pseudonyms

Several non-identifiers are being used in ENS as well, such as transaction logging data, OS versions, Locale, TAN, etc.

4.7 Privacy Threat Categories

Privacy threat categories provide high-level goals of the attacker(s). In traditional privacy threat modeling approaches, threat categories are identified separately from the attacker's goals and we combine both of them for easier reference.

- **Surveillance** is the observation or monitoring of an individual's communications or activities.
- **Stored data compromise** refers to end systems that do not take adequate measures to secure stored data from unauthorized or inappropriate access.
- **Misattribution** occurs when data or communications related to one individual are attributed to another.

- **Secondary use** is the use of collected information about an individual without the individual's consent for a purpose different from that for which the information was collected.
- **Exclusion** is the failure to allow individuals to know about the data that others have about them or to participate in its handling and use.
- **Linkability** is a higher-level goal of a privacy attacker and refers to the ability to identify related items in two (or more) seemingly unrelated datasets. From an attacker's perspective, this is done with the intention of identifying a person or a location. For example: identifying a place of worship based on the times when groups of people gathered there.
- **Identification** is a higher-level goal of a privacy attacker. It uses adversarial tactics to identify or de-anonymize a person or a group of people. This can either be done with the data directly, or by some combination or observation of various types of datasets. It can also occur during any phase of the information flow (or app usage in this case).
- **Detection** is when an attacker is able to detect whether a piece of data exists or not. A common example of this is membership inference, where the attacker is able to tell whether or not a particular individual is present within a dataset.
- **Non-repudiation** occurs when a user is unable to refute that a piece of data belongs to them. In the context of digital exposure notification, imagine a user being unable to deny that a certain anonymous value was transmitted by their device.
- **Integrity compromise** is a higher-level goal of a privacy attacker, as well. These attacks aim to compromise the validity or trustworthiness of infection or location data. This can happen during the broadcast phase, when an attacker may aim to broadcast dishonest values or broadcast values with dishonest metadata/properties. It could happen during the reporting phase, when an attacker may aim to report a dishonest positive infection result. It could also happen during the download phase, when an attacker may aim to block downloads of honest values.

4.8 Attacker Capabilities

These are means by which some attackers may be able to achieve attacker goals. The attacker capabilities are not completely mutually exclusive to each other and may result in overlaps in threat models.

Coercion attacks are especially threatening during COVID-19. Coercion is a unique type of privacy threat that aims to manipulate a user in order to divulge information that compromises privacy. This threat can be particularly difficult to combat because it involves the human aspect of the ecosystem. During a severe pandemic, people are anxious about their health and safety, and attackers have launched fraudulent schemes preying on COVID-19 anxieties. Coercing citizens to divulge information poses a privacy threat that could allow an attacker to identify, detect, or manipulate data.

Data disclosure could pose a serious privacy threat for mobile app users. In the ideal case, a server storing positive infection data does not collect any information that could potentially identify a user. In other words, even the server couldn't learn any information about the users behind the data. However, various aspects could affect this server privacy such as the collection of metadata or the length of time data is stored, among other things. If an attacker is able to gain access to the server and thus to the data stored on the server, these factors could affect what privacy leakage occurs. Data disclosure could occur through any of the nodes where data either stays at rest or in flow.

Eavesdropping can be passive or active but always refers to an attacker observing communication for a malicious purpose. One scenario that could take place in the context of ENS is for an attacker to place Bluetooth devices that observe and collect transmitted contact numbers. With the knowledge of a collection device's location and the positive infection status, an attacker could detect whether an observed device is part of the positive infection set, or could identify other devices that may have gotten an exposure notification due to the positive infection dataset. Finally, with the additional data captured during eavesdropping and the datasets available to a user, capability to combine multiple datasets, an attacker could combine information and perform a linkage attack causing additional privacy leakage. Eavesdropping could be at different layers and different stages of the operation. In addition to the cases discussed for bluetooth signal eavesdropping, an attacker could also eavesdrop on an app's interaction with the operating system and use it to identify privacy sensitive information about the user. Such examples have been explored exhaustively in the side-channel attack literature.

Replay attacks re-transmit legitimate data with the goal of gaining information or disrupting typical functionality. In an ENS, this could take the form of an attacker replaying any anonymous values that were observed while listening on Bluetooth channels. This could cause devices to think they had contact with a device they did not have contact with. An attack of this type could overwhelm manual contact tracing infrastructure, or more generally cause anxiety in citizens.

Spoofing is an adversarial action to impersonate a user in order to either disseminate fraudulent data or collect data that does not belong to the attacker. For ENS, an attacker may attempt to spoof contact events or even positive infection statuses, affecting the integrity of data. Another form of spoofing attack is to tamper with the data.

Tampering with data refers to data being changed, either to another seemingly valid value or to a meaningless value that may compromise the usefulness of a dataset. Because many ENS mobile apps are decentralized, meaning that data is processed on the devices themselves, tampering may be a bigger threat on application servers that may store data for a specific purpose related to the app functionality.

4.9 Privacy Threat Model

There are multiple ways to represent privacy threat models and we choose to use a simplified tabular representation. All of the threat types described below are reproduced using various tools such as mitmproxy [10] and GAEN Explorer [13] or using experiments done by other researchers [1, 8, 6]. Also, we have not included any security or other adversarial attacks, such as Drain Attacks as they don't directly impact privacy of the data subjects.

D - Direct Identifier I - Indirect Identifier

Attacker Capability - Coercion Attacks	
CA001	Infection status or potential exposure of the person revealed in mobile apps
Attacker Goals	Stored data compromise, identification
Attackers	Authorities, organizations, employers, assailants
Privacy Identifiers	Infection status (D), exposure details (I)
Attack Details	Attackers may coerce the user to show, in the mobile app, the infection status or potential exposure to infection.
CA002	Suitable ways of withdrawing consent are not built into mobile apps
Attacker Goals	Secondary use
Attackers	Authorities, organizations
Privacy Identifiers	Infection status (D), exposure details (I)
Attack Details	Consent is used as a legal basis for data processing and the attackers can make the design of the mobile app complicated for the users trying to withdraw their consent.
CA003	A law-enforcement attacker can compromise privacy using a subpoena
Attacker Goals	Stored data compromise, identification
Attackers	Authorities, hackers, assailants
Privacy Identifiers	Infection status (D), exposure details (I)
Attack Details	Authorities can force the users to disclose their private information stored in the mobile app using a legal mechanism such as a subpoena. The attacker then can learn the social interactions of the user of the mobile app.
CA004	Users are not given sufficient information about the app
Attacker Goals	Stored data compromise, identification
Attackers	Authorities, hackers, assailants
Privacy Identifiers	Infection status (D), exposure details (I), and other personal information
Attack Details	Attackers can use misinformation to force users to upload private information to a server and consequently reveal user information.

Attacker Capability - Data Disclosure	
DD001	Users lose control of their mobile device, allowing the people to see personal health data
Attacker Goals	Stored data compromise, identification
Attackers	Hackers, organizers, assailants
Privacy Identifiers	Infection status (D), exposure details (I)
Attack Details	Users lose control of their phone, allowing people to see all the data including infection status, date of infection, and other personal data.
DD002	Privacy leaks while using third-party tools and technologies
Attacker Goals	Stored data compromise, identification, linkability
Attackers	Authorities, hackers, assailants
Privacy Identifiers	Infection status (D), exposure details (I), user details (D)
Attack Details	Third-party tools, used in conjunction with mobile apps or web servers for various purposes like troubleshooting, are likely to disclose private data. For example, when the "Usage and diagnostics" option in Google Play Services is enabled (which it is by default), then telemetry data on GAEN operation is shared with Google.
DD003	Indefinite storage of data and possible later linkage with other personal data
Attacker Goals	Stored data compromise, identification, linkability
Attackers	Authorities, hackers, assailants
Privacy Identifiers	Infection status (D), exposure details (I), user details (D)
Attack Details	Authorities, either deliberately or through misconfigured implementations, retain the data permanently. It would be possible to link the data retroactively with other data to carry out de-anonymization attacks.

Attacker Capability - Eavesdropping	
EV001	Identification of users based on communication data
Attacker Goals	Identification, surveillance, linkability
Attackers	Authorities, organizations, hackers
Privacy Identifiers	TEK (D), IP address (I), Device information (I)
Attack Details	When a user chooses to share TEK with the designated health authorities, the operators can identify personal details of the users by means of communication metadata such as IP address. This results in re-identification of the users and associated healthcare data like TEK.
EV002	Profiling user movement using daily RPID generated
Attacker Goals	Identification, surveillance, linkability
Attackers	Authorities, organizations, hackers
Privacy Identifiers	TEK (D), IP address (I), device information (I), location information (I)
Attack Details	Attackers can build movement profiles of the users using RPIDs captured using Bluetooth LE sniffers and capture RPIDs and TEKs downloaded. Using the movement profiles, especially public locations like train stations or office locations, user de-anonymization is possible.
EV003	Profiling user movement using daily RPID generated
Attacker Goals	Identification, surveillance, linkability
Attackers	Authorities, organizations, hackers
Privacy Identifiers	TEK (D), IP address (I), device information (I), location information (I)
Attack Details	Attackers can build movement profiles of the users using RPIDs captured using Bluetooth LE sniffers and capture RPIDs and TEKs downloaded. Using the movement profiles, especially public locations like train stations or office locations, user de-anonymization is possible.
EV004	Tracing using Bluetooth interface's MAC address

Attacker Goals	Identification, surveillance, linkability
Attackers	Authorities, organizations, hackers
Privacy Identifiers	IP address (I), device information (I), location information (I)
Attack Details	Smartphones with Bluetooth enabled can be traced with the help of the Bluetooth interface's MAC address. An attacker could use this technique to trace users at specific locations.

Attacker Capability - Spoofing, Tracing, and Replay Attacks	
ST001	BLE range extensions can generate false positives
Attacker Goals	Integrity compromise
Attackers	Hackers, authorities, organizations, employers, assailants
Privacy Identifiers	Infection status (D), location (I)
Attack Details	To cause false alarms, an attacker can place BLE range extenders to spoof that a device is "nearby" when it may not be. To complete the attack, the attacker must ensure that the interactions between the attacker's device and other devices are logged as a contact event.
ST002	Generate false alarms though active relays
Attacker Goals	Integrity compromise
Attackers	Hackers, authorities, organizations, employers, assailants
Privacy Identifiers	Infection status (D), location (I)
Attack Details	An attacker can generate a false alarm by real-time relay attacks that lead to the users falsely being alerted that they may have had a positive exposure. One attacker tactic could be via the relay of Bluetooth signals from the people tested at testing centers to other phones in the proximity.
ST003	Generate wormhole attacks
Attacker Goals	Integrity compromise, misattribution, exclusion
Attackers	Hackers, authorities, organizations, employers, assailants
Privacy Identifiers	Infection status (D), location (I)
Attack Details	Using commercially available Bluetooth LE sniffers, attackers can collect RPIDs and pass them onto more distant locations without being noticed. This compromises the contact tracing system as a whole by falsely duplicating information about the presence of infected persons in many locations.
ST004	A verification code used to upload information of another app
Attacker Goals	Stored data compromise, identification
Attackers	Authorities, service provider, employers, hackers
Privacy Identifiers	Infection status (D)
Attack Details	An attacker can use a verification code, generated for an infected person to upload their temporary encryption key (TEK), in another app to upload their information, resulting in compromise of the overall system.

4.10 Threat Mitigation Strategy

We propose Privacy by Design methodology [3], developed by Anne Cavoukian, Ontario's Data Protection Commissioner, because of its applicability in mitigating conventional and non-stereotypical threats. Also, we didn't provide a prescriptive threat mitigation strategy because the mitigation strategy can be applied at various levels, ranging from legal frameworks to technical solutions like differential privacy for data stored in the servers.

The following table lists all mitigation strategies and privacy attacks the respective mitigation strategy addresses:

Mitigation Strategies	Details	Privacy Attacks Addressed
Applying a Privacy-by-Design approach for developing ENS solution components (mobile app, backend server, etc.)	Data Minimization: Identify and use only required attributes. Remove / destroy any data, whether direct identifier or indirect identifiers, when they are no longer required. The cryptographic tokens shared by the apps should be valid for the shortest interval and should be continuously replaced with new tokens, so that an app cannot be tracked using the tokens it shares.	DD02, DD003
	Data Separation: Isolate and distribute processing of personal data. Processing separation to be applied at different components of DCT including separation of verification activities from exposure notifications [13]. Further levels of privacy can be attained by using methods like multi-party computation or secure enclaves in order to ensure privacy of data during computation.	DD002
	Data Abstraction and Perturbation: Aggregate and add noise to the data at source. For example, it is recommended that data is abstracted or perturbed before the data is uploaded from mobile app to the servers. Usage of standard metrics and mechanisms for perturbation like differential privacy should be used.	DD002, DD003
	Inform: Inform users and data subjects about the processing of their personal data in a timely and detailed manner.	CA004
	Control: Put users and data subjects in control over processing of their personal data and provide easy-to-use interfaces to opt-out from data sharing.	CA001*, CA002*, CA003*, DD001*
	Visibility: Provide visibility into how the personal data is processed and what privacy-enhancing techniques used.	
	Regulation: Impose strict data processing and usage regulations at the institutional level and establish role based access control within an organization.	
Securing communication between various components	Enabling SSL certificates for all data-intransit communication.	EV001
	Removing HTTP headers like ‘Authorization’ reduces linkability issues.	EV001
	HMAC enhancements to mitigate relay and replay attacks. [3]	EV002*,EV003*,ST002*, ST001*
Use Reference Architectures for ENS	Follow proven reference architecture recommendations [6] like separation of processing, authentication, etc.	EV002*, EV003*, ST004
	Keep mobile apps and server components current with latest APIs, patches, and OS upgrades.	EV004

	Perform end-to-end security and vulnerability assessment of the DCT components.	ST001*, ST002*, ST004*

*Minimizes the attack and does not fully mitigate the attack

5 Conclusion

Although there are existing threat models which aim to address privacy challenges, the unique ecosystem within exposure notification systems requires a more comprehensive approach. To this end, we introduce an enhanced framework for Target State Privacy Threat Modeling, which simplifies terminology, minimizes overlooked threats, and ensures consistency across instances of the threat model.

Further, we used our newly enhanced framework to build a Target State Privacy Threat Model for ENS. This model reflects the comprehensive privacy concerns faced by exposure notification systems and defines specific privacy threats based on attacker capabilities, including what privacy identifiers are affected and how the attack might take place.

Finally, we provide mitigation strategies that should be taken to address the threats identified in the ENS Target State Privacy Threat Model.

Glossary

Term/Acronym	Description	Reference
Privacy Identifiers	Any data, element, or information that can be used, directly or as a proxy, to identify a person or group of persons.	
LINDDUN	Systematic elicitation and mitigation of privacy threats in software systems	`https://www.linddun.org/`
STRIDE	approach to threat modeling	`https://en.wikipedia.org/wiki/Threat_model`
PASTA	Process for Attack Simulation and Threat Analysis (PASTA) seven-step, risk-centric methodology.	`https://en.wikipedia.org/wiki/Threat_model`
NIST	physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce.	`https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology`
DCT	Digital Contact Tracing	`https://en.wikipedia.org/wiki/Digital_contact_tracing`
GDPR	General Data Protection Regulation (GDPR) has been the gold standard for personal data protection	`https://en.wikipedia.org/wiki/General_Data_Protection_Regulation`
EDPB	European Data Privacy Board	`https://en.wikipedia.org/wiki/European_Data_Protection_Board`
TAN	Acronym for "[Transaction Authentication Number]	`https://en.wikipedia.org/wiki/Transaction_authentication_number`
SMS	Short message service	`https://en.wikipedia.org/wiki/SMS`
DFD	Data Flow Diagrams	`https://en.wikipedia.org/wiki/Data-flow_diagram`

IFD	Information flow diagram	https://en.wikipedia.org/wiki/Information_flow_diagram
TPTM	Target Privacy Threat Modeling Framework	https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html
COVID	A respiratory illness. It is colloquially known as coronavirus.	https://en.wikipedia.org/wiki/Coronavirus_disease_2019
TEK	Temporary Encryption Key - used as part of the anonymous exposure notification protocols.	https://en.wikipedia.org/wiki/Key_(cryptography)

References

[1] Lars Baumgärtner, Alexandra Dmitrienko, Bernd Freisleben, Alexander Gruler, Jonas Höchst, Joshua Kühlberg, Mira Mezini, Markus Miettinen, Anel Muhamedagic, Thien Duc Nguyen, Alvar Penning, Dermot Frederik Pustelnik, Filipp Roos, Ahmad-Reza Sadeghi, Michael Schwarz, and Christian Uhl. Mind the gap: Security & privacy risks of contact tracing apps, 2020.

[2] European Data Protection Board. Statement 3/2019 on an eprivacy regulation. https://edpb.europa.eu/sites/edpb/files/files/file1/201903_edpb_statement_eprivacyregulation_en.pdf.

[3] Ann Cavoukian. Identity in the information society, aug 2010, volume 3, issue 2, pp 247-251. privacy by design: the definitive workshop. a foreword by ann cavoukian, ph.d.

[4] CoronaWarn. Open-source project corona-warn. https://www.coronawarn.app/en/.

[5] PathCheck Foundation. Pathcheck. https://pathcheck.org/.

[6] Yaron Gvili. Security analysis of the covid-19 contact tracing specifications by apple inc. and google inc. https://eprint.iacr.org/2020/428.pdf.

[7] HSE Ireland. Covid tracker app - ireland's covid virus contact tracing. https://covidtracker.gov.ie/.

[8] Douglas J Leigh and Stephen Farrell. Contact tracing app privacy: What data is shared by europe's gaen contact tracing apps. https://www.nachdenkseiten.de/upload/pdf/200731-Leith+farrell-on-contact-tracing-app-privacy-july-2020.pdf.

[9] Author Markus Miettinen. Contact tracing for pandemic response, tracecorona. https://tracecorona.net/.

[10] Mitmproxy. Mitmproxy is a free and open source interactive https proxy. https://mitmproxy.org/.

[11] National Institute of Standards and Technology. A tool for improving privacy through enterprise risk management, version 1.0. nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

[12] OpenTrace. Opentrace community github. github.com/opentrace-community.

[13] Bill Pugh. Gaen explorer github. https://github.com/billpugh/GAEN_Explorer.

[14] Adam Shostack. Experiences threat modeling at microsoft. http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-413/paper12.pdf.

[15] L. Sion, K. Wuyts, K. Yskout, D. Van Landuyt, and W.Joosen. Interaction-based privacy threat elicitation. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pages 79–86, 2018.

[16] Tony Ucedavalez. Real-world threat modeling using the pasta methodology. https://owasp.org/www-pdf-archive/AppSecEU2012_PASTA.pdf.