Summary of Bluetooth Contact Tracing Options

Logan Small, John Harris, Matt Hopkins, Nathaniel de Lautour
Defence Technology Agency
14 May 2020

EXECUTIVE SUMMARY

Bluetooth-augmented contact tracing has emerged as a novel system for health authorities to use during the ongoing COVID-19 pandemic and is recommended for use as part of an audit of contact tracing by infectious disease specialist Dr Ayesha Verrall. Each Bluetooth contact tracing protocol has a trade-off between important factors such as privacy, performance and the health authority's access to interaction data. This paper reviews the rapidly evolving landscape of approaches that have emerged at the time of writing, with a focus on identifying the best candidates for use within New Zealand.

A defining difference between all contact tracing protocols is the concept of centralisation. In general, this refers to the end destination of a user's interaction data and how this is used by a heath authority. Two primary architectures exist:

Centralised – An app user who subsequently tests positive will voluntarily upload their interaction data to a central repository operated by a trusted health authority. The health authority will assess the data for potentially infectious interactions and proactively contact other application users by using information obtained during the installation of the app. The protocols developed using the centralisation approach include *BlueTrace*, *PEPP-PT* and the *NHS* protocol. Current implementations of centralised approaches do not have full functionality on iOS devices as interactions are not always logged when the app is running in the background or the phone is locked.

Decentralised – An app user who subsequently tests positive will voluntarily upload their unique ID to a central repository operated by a trusted health authority. Since the health authority does not have the interaction history of this user, they cannot contact any potentially infected third-party. Instead, they publish a public list of known infectious user IDs which is accessible to all other users. Each user's app will periodically check this public list and match these infected IDs against IDs received by their device. As the matching occurs on the user's phone, it is the responsibility of the user to voluntarily self-isolate and potentially contact the health authority should they receive a notification. Protocols developed using the decentralised approach include *DP-3T*, *TCN*, *PACT*, *Whisper*, and notably the new Apple/Google *Exposure Notification* Application Programming Interface (*API)*.

The two protocols discussed for use in New Zealand have been the *BlueTrace* protocol as used in Singapore and Australia, as well as the Apple/Google *Exposure Notification API*. The *BlueTrace* protocol is a more mature technology that has seen weeks of testing in Singapore, while the *Exposure Notification API* has yet to see a nation-wide rollout. The *Exposure Notification API* fixes a range of technical issues that *BlueTrace* encounters, notably the loss of functionality on iOS devices when running in the background. However, as the health authority does not have immediate access to all interaction data of exposed users, it may be less useful from a contact tracing perspective. Adoption of the *BlueTrace* protocol also enables potential interoperability with the current version of the Australian COVIDSafe app should a trans-Tasman bubble be established. However, the technical limitations may lead to poor uptake among iOS smartphone users, reducing the effectiveness of the system.

I. Introduction

Contact tracing within New Zealand for the ongoing coronavirus disease 2019 (COVID-19) pandemic requires accurate knowledge of an individual's recent social contacts. The contact tracing process can be augmented using communications between personal smartphones as an automated method of logging proximity to other devices. The potential benefits of digital contact tracing have been well studied [1] and is recommended for use by Dr Ayesha Verrall in [2].

Bluetooth Low Energy (BLE) is well suited to assist in digital contact tracing due to its power efficient design and ubiquity in modern smart phones. For a contact tracing app, BLE messages which include an ID unique to each app are continually transmitted between nearby devices. Since Bluetooth has a useful range of less than 10 metres, any device consistently receiving messages is logged as an interaction. App users who are tested positive may inform the health authority of their unique ID and a risk assessment algorithm is run on users who have been in contact with this ID, notifying them if they may have been exposed to the virus. Measures are taken to ensure that the individual privacy of users is maintained during operation.

II. Options

Numerous Bluetooth contact tracing solutions are being rapidly developed, with dozens of feature-complete apps made by high-profile businesses, universities, research institutes and online communities. However, only a select few have been taken into serious consideration by governments worldwide. The first in use was TraceTogether [3] in Singapore, later open-sourced as OpenTrace, utilising the open-source protocol *BlueTrace* [4]. Australia and some Eastern European countries have since released their own apps also based on the *BlueTrace* protocol. Pan-European efforts have led to two distinct approaches, *PEPP-PT* [5] and *DP-3T* [6], in the initial stages of release in a few European countries. The United Kingdom are also trialling a custom protocol which shall be referred to as the *NHS* protocol [7]. Further details on these protocols and many others (*TCN*, *PACT* and *Whisper* to name a few) are provided in Appendix A.

III. Limitations

Each protocol above has been built around Bluetooth Low Energy (BLE) in one of two modes. BLE messages are sent either through one-way non-connectable messages or through a two-way connection where a device can interrogate the other for further information. Android devices request that the user give the app location permission during install despite not actually using GPS data.

iOS and Android devices implement BLE functionality in unique ways and place restrictions on apps to preserve power consumption and reduce security implications. In iOS, when a BLE app is running in the background, the active transmission of advertisements is disabled. The iOS app will continue to listen for other advertisements in a passive scanning mode but contact events between iOS devices would not be logged if two local users had their phones locked because no advertisements are being transmitted. Android devices will also fail to communicate successfully with iOS devices that are passively scanning. These implementation issues occur in all BLE contact tracing protocols and apps mentioned above and cannot be wholly resolved without major changes to the way the operating system works.

These limitations have been addressed by the developers of iOS and Android, Apple and Google respectively. They have released specifications on an *Exposure Notification API* [8][9] inspired by *DP-3T*. Additional power saving techniques are also included. However, Apple and Google have placed extremely restrictive legal constraints [10][11] on its use for security and privacy reasons, limiting the ability for health authorities to extend the Bluetooth capabilities. As a result, *Exposure Notification API* has itself become a competing Bluetooth contact tracing protocol, alongside those detailed in Appendix A. As Apple and Google have control over how this protocol is used, continuing to develop *BlueTrace* means continuing to deal with the technical limitations on iOS.

IV. Comparison Of Key Characteristics

Characteristic	Decentralised: Apple/Google *Exposure Notification API*	Centralised: Singaporean *BlueTrace*
Performance	Human-out-of-the-loop contact tracing. The intent is that users receive automated notifications and trust is placed on them that they will self-isolate, with advice from public health authorities about what to do. Uses transmitted and received signal strength, days since contact event and extensible nation-specific parameters for exposure risk assessment.	Human-in-the-loop contact tracing, allowing for health authorities to perform rapid epidemic surveillance and moderate the contacts during a contact tracing interview. Uses calibrated transmitted signal strength, received signal strength and contact duration for exposure risk assessment.
Privacy	All interaction information is kept on the user's phone. Users are not required to share personal contact details with health authority via the app.	When tested positive, a user's interaction information is voluntarily shared with health authorities. The nation's app may be configured to require users to register their personal contact details (such as phone number) with the health authority.
Data Access	Decentralised approach to contact logging, users who are tested positive voluntarily upload their phone's unique IDs to a central server.	Centralised approach to contact logging, users who are tested positive voluntarily upload both a list of their unique phone IDs, as well as a list of phone IDs that the positive case may have been in contact with.
User Friction	No location permissions required on Android or iOS. Works in the background on iOS. Temporary phone IDs generated without access to internet. Decreased battery usage with connectionless handshakes.	Requires location permissions on Android (despite not using GPS). iOS apps running in background do not communicate with other iOS users running the app in the background. Requires daily access to the internet for temporary phone IDs. Increased battery usage with connections between phones.
Maturity	No nation-level rollout of apps, currently in Beta version. Sample app implementations available to developers.	Rolled out in Singapore, Australia, Alberta (Canada) and some eastern European countries such as Poland and Czechia. Sample app implementation available to developers.

Table 1: Comparison of key characteristics between the centralised BlueTrace *and the decentralised* Exposure Notification API.

V. DISCUSSION

As outlined in [12], the performance and reliability of Bluetooth contact tracing apps has not yet been firmly established. The use of Bluetooth contact metrics based on signal strength and contact duration can result in both false positives and negatives. It is uncertain how serious a problem this will be in practice. Other than its South Pacific neighbours, the need for interoperability between countries has not been communicated as being of immediate concern. In summary, the ideal protocol would:

- Provide contact tracing staff with information about a user's recent social contacts (*BlueTrace*)
- Address the limitations in the iOS and Android Bluetooth implementations (*Exposure Notification API)*
- Use non-connectable BLE for improved security and to minimise battery usage. (*Exposure Notification API*).
- Interoperability with the Australian protocol [13]. (Currently *BlueTrace*, subject to change).

There are significant pros and cons for using either approach. Ideally, the solution would be to use the *Exposure Notification API* in a centralised manner or have the ability to fix some of the technical limitations of *BlueTrace*. However, due to the extremely restrictive legal constraints placed on its use [10][11], it may not possible to use the *Exposure Notification API* in a centralised manner or use it in parallel with protocols such as *BlueTrace*. Such a hybrid approach requires a change in the current state of the *Exposure Notification API* and its terms and conditions for use as set by Apple and Google.

Adopting the current version of *BlueTrace*, New Zealand's app would be limited in that all iOS devices would also have severe limitations, requiring the app to be in the foreground and the phone unlocked for full functionality. Android phones will also require location permissions despite not gathering any GPS data. Using the current version of the *Exposure Notification API*, the limitations are resolved but the ability to moderate potential contacts is removed from the contact tracing process.

VI. CONCLUSION

In their current states, no digital contact tracing approach is without significant limitations. The use of the *BlueTrace* protocol in an app similar to Singapore's TraceTogether has the potential to meet Dr Verrall's digital contact tracing recommendations [2], however the limitations in iOS devices limit the effective number of interactions that are logged for contact tracing purposes. Although the *Exposure Notification API* solves these implementation constraints, it provides health authorities with less interaction information to aid manual contact tracing. The intent of the *Exposure Notification API* is that the exposed users are notified that they have been exposed and receive advice from the public health authority about what to do next.

REFERENCES

[1] L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dörner, M. Parker, D. Bonsall, and C. Fraser, "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing," *Science*, 2020. https://doi.org/10.1126/science.abb6936

[2] A. Verrall, "Rapid Audit of Contact Tracing for Covid-19 in New Zealand" *Ministry of Health*, 2020, Retrieved from https://www.health.govt.nz/system/files/documents/publications/contact_tracing_report_verrall.pdf

[3] "TraceTogether", https://www.tracetogether.gov.sg/

[4] J. Bay, J. Kek, A. Tan, C. S. Hau, L. Yongquan, J. Tan, and T. A. Quy, "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders", April 2020, Retrieved from https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf

[5] "Pan-European Privacy-Preserving Proximity Tracing", https://github.com/pepp-pt/

[6] "Decentralized Privacy-Preserving Proximity Tracing", https://github.com/DP-3T/

[7] "The NHS App" https://www.nhs.uk/using-the-nhs/nhs-services/the-nhs-app/

[8] "Privacy-Preserving Contact Tracing - Apple and Google", https://www.apple.com/covid19/contacttracing/

[9] "Google and Apple partner on COVID-19 Exposure Notifications API" https://www.google.com/covid19/exposurenotifications/

[10] "Exposure Notification APIs Addendum", Retrived from https://developer.apple.com/contact/request/download/Exposure_Notification_Addendum.pdf

[11] "Google COVID-19 Exposure Notifications Service Additional Terms", May 2020, https://blog.google/documents/72/Exposure_Notifications_Service_Additional_Terms.pdf

[12] N. de Lautour, L. Small, J. Harris, and M. Hopkins "Bluetooth Low Energy and Proximity Detection by RSSI", 2020

[13] "COVIDSafe App", https://www.health.gov.au/resources/apps-and-tools/covidsafe-app

[14] J. Harris, L. Small, M. Hopkins, and N. de Lautour, "An Executive Summary of Bluetooth Low Energy", 2020

[15] "Exposure Notification API – Android API Documentation – Preliminary", May 2020, Retrieved from https://www.blog.google/documents/74/Android_Exposure_Notification_API_documentation_v1.3.pdf

[16] "Exposure Notification API - iOS Framework Documentation" https://developer.apple.com/documentation/exposurenotification

[17] "Exposure Notification API – Bluetooth Specification – Preliminary", April 2020, Retrived from https://www.blog.google/documents/70/Exposure_Notification_-_Bluetooth_Specification_v1.2.2.pdf

[18] "Exposure Notification API - Cryptography Specification – Preliminary", April 2020, Retrieved from https://www.blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf

[19] "Exposure Notifications Android Reference Design", https://github.com/google/exposure-notifications-android

[20] "Building an App to Notify Users of COVID-19 Exposure", https://developer.apple.com/documentation/exposurenotification/building_an_app_to_notify_users_of_covid-19_exposure

[21] "OpenTrace" https://github.com/opentrace-community

[22] "PEPP-PT sample Android app" https://github.com/pepp-pt/pepp-pt-ntk-sample-android

[23] "Decentralized Privacy-Preserving Proximity Tracing – White Paper", https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf

[24] "TCN Protocol", https://github.com/TCNCoalition/TCN

[25] "TCN Coalition", https://tcn-coalition.org/

[26] "PACT: Private Automated Contact Tracing", https://pact.mit.edu/

[27] "CovidSafe", https://github.com/covidsafe

[28] L. Loiseau, V. Bellet, T.S. Bento, E. Teissonniere, M. Benoliel, G. Kinsman, P. Milne, "Whisper Tracing – an open and privacy first protocol for contact tracing", https://docsend.com/view/nis3dac

[29] "Coalition Network", https://github.com/nodlecode

[30] "Nodle", https://nodle.io/

[31] "Coalition App" https://www.coalitionnetwork.org/

APPENDIX A: BLUETOOTH PROTOCOLS

The following protocols all rely on Bluetooth Low Energy (BLE), an implementation of Bluetooth that prioritises battery saving techniques. BLE terminology used in this paper are defined in detail in [14]. All protocols considered in this paper are developed with privacy-preservation in mind, only technical issues with privacy implementations will be discussed. Approaches that do not protect the user's privacy will be not be covered.

Note: The information on Bluetooth apps is current at time of writing and rapid changes will make it quickly out of date.

A. *Exposure Notification API*

The two smartphone operating systems being targeted are iOS and Android, developed by Apple and Google respectively. To aid with Bluetooth app development on their platforms, Apple and Google have co-operated [8][9] to provide interoperability between their two operating systems and have published draft publications for API [15][16], Bluetooth [17] and Cryptography [18] specifications. The API performs contact logging in a decentralised method, with initial inspiration from the *DP-3T* protocol. Reference implementations of the iOS and Android have been provided for quick app development [19][20]. The API uses only non-connectable advertisement packets that are transmitted and received between Android and iOS, including in the background and while the phone is locked. Android apps using this API also do not require location permissions.

Current implementations: N/A (Not yet released), Google Sample Implementation, Apple Sample Implementation.

Considering implementations: Many nations, including those listed below as already having existing apps.

B. *BlueTrace*

The Singaporean TraceTogether app [3] was later open-sourced as a protocol called *BlueTrace*, detailed in their white paper [4]. Devices share a cryptographically secure temporary device ID along with the phone model for use in proximity calculations. A confirmed COVID-19 case voluntarily uploads their social contact log to their health provider using a provided authentication code, which then can signal all devices on the network to check for matches against their contact logs. OpenTrace [21] is a reference implementation of the *BlueTrace* protocol that has been open-sourced via GitHub under the GPL-3.0 license. The upload server and cryptographic key generation occur in the cloud on a server owned by the health authority.

Current implementations: Singapore TraceTogether, Australia COVIDSafe, Czechia eRouška, Poland ProteGO, Slovakia Covid World, Alberta (Canada) ABTraceTogether.

C. *Pan-European Privacy-Preserving Proximity Tracing*

The Pan-European Privacy-Preserving Proximity Tracing (*PEPP-PT*) project [5] has researchers from European countries co-operating to build a BLE-based protocol that complies with the strict European GDPR privacy regulations. The protocol supports a centralised approach (such as the Singaporean TraceTogether). With the release of the decentralised-only Apple/Google API, this has led countries such as Germany to opt against using *PEPP-PT*. The protocols are being open-sourced under MPL-2.0 [22], with sample implementations in development also under MPL-2.0. Originally a German-led initiative, only France remains an active proponent of this protocol, with Germany and others moving to *DP-3T*.

Current implementations: Georgia NOVID20.

Considering implementation: France StopCovid, Italy Immuni.

D. *Decentralized Privacy-Preserving Proximity Tracing*

The Decentralised Privacy-Preserving Proximity Tracing (*DP-3T*) [6] project has developed an approach that gives minimal information to the backend servers, unlike the *PEPP-PT* and BlueTrace protocols. *DP-3T* also uses extra methods to protect privacy such as not sending the entire temporary device ID in each packet. The protocol and reference implementation are open-sourced on GitHub under the MPL-2.0 license [23].

Current implementations: Austria STOPP KORONA.

Considering implementation: Switzerland Next Step, Netherlands PrivateTracer, Germany, Estonia, Finland.

E. *TCN, PACT and Whisper*

TCN [24] is a protocol developed by the TCN Coalition [25] that have jointly developed a common protocol between their apps. PACT [26] is a protocol developed by Microsoft volunteers and the University of Washington that has been released as a complete app solution [27]. Whisper [28] is a protocol developed by the Coalition Network [29] and Nodle [30] with an app released on the Google Play store [31]. While all these protocols and apps are promising and well-developed, none have been officially supported by any nation and may become obsolete by the release of the aforementioned protocols.

Current implementations: None.

F. *Other Proprietary or Unknown Protocols*

Some nations have opted to develop custom Bluetooth contact tracing protocols, or not reveal the protocol in use.

Current implementations: UK NHS COVID-19, North Macedonia StopKorona!, Russia Contact Tracer, Norway Smittestopp, Malaysia MyTrace, Indonesia PeduliLindungi, Hungary VirusRadar, Qatar EHTERAZ, India Aarogya Setu, (Many are waiting on Apple to fix issues on iOS).