# Poster: Trace Yourself - It Could Be Easy

Patrick Rathje
Kiel University, Kiel, Germany
pra@informatik.uni-kiel.de

Olaf Landsiedel
Kiel University, Kiel, Germany
Chalmers University of Technology, Gothenburg,
Sweden
ol@informatik.uni-kiel.de

## Abstract

Contact tracing helps to predict and prevent the spread of viruses. This work proposes Tracey for decentralized, privacy-preserving tracing. Unlike automated tracing solutions that operate in the background, such as the widespread governmental Corona Tracing Apps, our system builds on manual contact exchanges to ensure reliable contact tracing even for groups and venues. The devices share secrets that allow anonymous notifications using the health authorities' trusted database. This work illustrates the concept, provides initial security analysis, first results, and gives an outlook on possible extensions.

## 1 Introduction

Contact tracing allows for tracking and breaking chains of infectious deseases [11]. For example, the Decentralized Privacy-Preserving Proximity Tracing (DP3T) protocol provides automatic and anonymous tracing by exchanging random identifiers in the background using Bluetooth beacons [3]. While DP3T and other passive solutions are effortless (see [2] for details), they can not guarantee precise tracing. Obstacles may reduce accuracy, resulting in false positive and false negative contacts [7, 2]. Pen and paper solutions represent an active tracing method, but while being precise, they force the users to disclose private information, being a significant caveat for user acceptance [10].

Based on QR codes, Singapore's SafeEntry [4] and the NHS COVID-19 app [8] integrate digital check-ins for venues. CrowdNotifier extends privacy in digital presence tracing for public venues [1]. Upon infection, the authorities anonymously inform (in cooperation with the specific venue) other participants at risk using a public database. This mechanism restricts reliable contact tracing to venues and still requires an infected user to disclose private information leaving room for errors and a higher demand for privacy.

The Zwaai App utilizes two-way communication to exchange random identifiers for each encounter to prevent linkage attacks [6, 9]. Zwaai supports personal meetings as well as venues. However, because two-way communication needs two active parties, connecting every pair of devices is laborious for bigger groups. Moreover, additional servers are incorporated to support static QR codes.

We argue that active, privacy-preserving tracing as a valuable supplement to passive broadcasts should not be restricted to venues and not limited in privacy. Therefore, we propose Tracey for anonymous tracing for personal contacts, groups, and venues that builds on shared secrets to allow easy, anonymous notifications.

**Challenges.** The system must allow reliable tracing with the highest privacy possible. It should allow for easy deployment and usage.

**Approach.** This work proposes a simple, decentralized tracing system called Tracey. Users share random secrets for each encounter using e.g. QR codes or NFC. The parties use their secret to send anonymous notifications to another over a trusted, public channel. We sketch our prototype implementation and discuss possible attacks as well as the feasibility of its system design.

## 2 Anonymous Contact Tracing with Tracey

In Tracey, each device stores individual secrets for each encounter and provides each party with a reliable but private tracing option. No registration is required as the devices randomly generate the secrets.

Tracey establishes random secret keys within the parties of an encounter: Whenever a device receives such a key, it saves it locally and assigns the current day. If a party gets infected, it prepares notifications to all its relevant encounters of a specific time window. The responsible health authorities would then collect and publish those notifications in

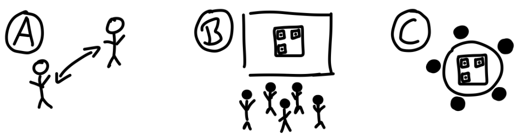

**Figure 1. With Tracey, groups of arbitrary size share a secret, covering (A) one-to-one tracing, (B) groups like school classes, and (C) contact points in venues or meeting rooms.**

International Conference on Embedded Wireless Systems and Networks (EWSN) 2021
17–19 February, Delft, The Netherlands © 2021 Copyright is held by the authors.
Permission is granted for indexing in the ACM Digital Library
ISBN: 978-0-9949886-5-2

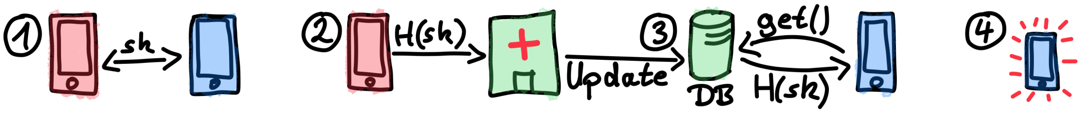

**Figure 2. The parties use their shared secret (sk) to anonymously notify each other using the health authorities' public database. When in contact, devices exchange a secret key (1). Upon infection, the infected party collects the relevant anonymous notifications, which the health authorities publish in their database (2). All users download the data and check for matches on their devices (3). The devices report matches back to the user (4).**

their public database. While published, the notifications stay anonymous because the parties use their random secret *sk* to publish $Hash(sk)$. Other users regularly download all published entries and compare them to locally known secrets. Figure 2 depicts the tracing process for two smartphones.

This communication channel allows groups of arbitrary size (see Figure 1). Two persons can meet and anonymously log their encounter with the same ease as colleagues in the office or students of the same class. Also, pre-generated secrets allow easy administration. For example, a restaurant could prepare and distribute distinct keys for each table and renew them after each visitor.

## 3 Easy Key Sharing with NFC and QR Codes

Tracey lets users create and share secrets using NFC or a QR code[1]. NFC's close range of less than 10 cm and support for various smart devices, including phones, watches, and even passive smart cards, are perfectly suited for fast and private one-to-one tracing or small groups. QR codes allow the simple distribution of secrets, especially for larger groups.

## 4 Discussion

The system relies on active contact exchanges, and the devices store anonymous information. Moreover, it does not broadcast wireless beacons, preventing device tracking, location confirmation, or linkage attacks [2].

The health authorities provide a trusted source for public notifications of infected people, and every user can download all notifications to hide access patterns. Because the secrets are stored on the devices and only shared within the parties of interest, the saved information does not reveal the other parties. Consequently, an infected user could rely on anonymous notifications and does not need to disclose all contacts and locations to the authorities required in CrowdNotifier's digital presence tracking [1].

The system is vulnerable to relay and replay attacks: Malicious users could redistribute secrets, adding members to the same group. In the current version, multiple messages using the same secret can be linked. Eavesdropping on the exchange is easy with QR codes, but NFC supports secure channels that our implementation can use [5].

While the notifications could save laborious work for the health authorities, they also lose control: the authorities can not verify the data or its reception. Also, the system depends on voluntary participation and does not provide any way to enforce a quarantine.

Each group would receive individual notifications. If we truncate the hash value to 16 Bytes per notification and assume that a user shares and receives ten secrets on average per day, an infected person would upload 2240 Bytes for the notifications of the last 14 days. An infection rate of 1,000 out of 100,000 per 7 days results in 2.24MB of raw data per 100,000 users and seven days. This amount could be problematic for large populations. Probabilistic data structures could offer more efficient storage with limited false-positive rate [3].

## 5 Conclusion and Outloook

This work proposes a simple notification scheme based on group-specific secrets and a trusted, public database. Infected users do not need to disclose private information about their contacts and can notify them reliably. While the protocol offers easy deployment and usage, we need to further analyze it regarding privacy, utility, scalability, and epidemiological insights. Extensions could support additional information for more meaningful notifications using e.g. the secret for symmetric encryption. Further on, the key exchange should incorporate additional information to ensure that users join the correct groups, prevent replay attacks, and exchange default values such as the expected duration.

## 6 Acknowledgements

This work is supported by the Federal Ministry of Health based on a resolution of the German Bundestag.

## 7 References

[1] Crowdnotifier. https://github.com/CrowdNotifier, 2020 (accessed Nov. 18, 2020).

[2] 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.

[3] DP-3T. Dp3t - decentralized privacy-preserving proximity tracing, 2020 (accessed Nov. 28, 2020).

[4] Government of Singapore. Safeentry, 2020 (accessed Nov. 30, 2020).

[5] E. Haselsteiner and K. Breitfuß. Security in near field communication (nfc). In *Workshop on RFID security*, pages 12–14. sn, 2006.

[6] A. S. Hoffman, B. Jacobs, B. van Gastel, H. Schraffenberger, T. Sharon, and B. Pas. Towards a seamful ethics of covid-19 contact tracing apps? *Ethics and Information Technology*, pages 1–11, 2020.

[7] G. Li, E. Geng, Z. Ye, Y. Xu, J. Lin, and Y. Pang. Indoor positioning algorithm based on the improved rssi distance model. *Sensors*, 18(9):2820, 2018.

[8] NHS England. Nhs test and trace, 2020 (accessed Nov. 30, 2020).

[9] Radboud University. Zwaai.app, 2020 (accessed Nov. 30, 2020).

[10] S. Trang, M. Trenz, W. H. Weiger, M. Tarafdar, and C. M. Cheung. One app to trace them all? examining app specifications for mass acceptance of contact-tracing apps. *European Journal of Information Systems*, 29(4):415–428, 2020.

[11] World Health Organization. Contact tracing in the context of covid-19. https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19, 2020 (accessed Nov. 28, 2020).

[1] https://github.com/prathje/tracey