Response to 'Analysis of DP3T: Between Scylla and Charybdis'

DP-3T Project

23 April 2020

A recent paper[1] lists a selection of attacks claimed to work against DP-3T. We have received requests for clarification of our views on this paper. Upon analysis, these attacks can be grouped into three categories:

- Risks or attacks **common to all proposed European Bluetooth contact tracing systems, whether centralized or decentralized** (A, B, D, F, G, H, I, K)

- **Attacks that do not work on DP-3T** (C, E, J)

- **One attack that works, albeit can be mitigated, and is also possible against proposed centralized designs** (L)

We previously described all of the functioning attacks and risks elsewhere, and so will refer to our other documentation for details:

- White Paper (WP)

- Overview of Data Protection and Security (DPS)

- Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems (PSRE)

A: Page 2: '*having Bluetooth turned on already creates privacy issues*'

- **All Bluetooth contact tracing systems share this risk** (see Generic Risk 5, PSRE)

B: *Page 3: security of communication between participants*

- **All contact tracing systems require secure communication** between the apps and both the backend server and the health authorities. Our designs use standard end-to-end encryption and authenticates the backend and health authorities.

- Secure upload of infection results to the backend. We believe **that all contact tracing systems** should process the tracing data of infected patients only if authorized by the health authority. The specific mechanism will depend on the national rules and practice, but we have laid out a clear proposal (DPS, p. 9).

[1] Serge Vaudenay, 'Analysis of DP3T: Between Scylla and Charybdis'.

- Protecting communication between apps. This is very difficult in practical tracing systems based on Bluetooth. We note, however, that the specific attacks enabled by this lack of protection (F and G, addressed below) apply to **all Bluetooth based tracing systems** (including DP-3T, ROBERT, and NTK).

C: *s 4.1: Backend Impersonation*

- Phones authenticate data from the backend. **This attack is not an issue** (PSRE, p. 11).

D: *s 4.2: False reports*

- Reporting keys should only be possible after authorization from the health authority. Details of the authorization protocol need to be decided in conjunction with the national health authorities. However, false reports (or false alarms) are a **problem common to all Bluetooth based contact tracing systems** (DPS, Generic Risks 1 & 2).

E: *s 4.3: Replay of released cases*

- **This attack is not possible in either of the DP-3T designs** as phones will not check released data against new observations (WP, p. 11).

F: *s 4.4 Replay attacks*

- Replay within a coarse time window is acknowledged as a weakness of the low-cost design. However, **the DP-3T unlinkable design only admits replays within the same epoch.** Moreover, **replay attacks within a short time after broadcast is a generic risk shared by centralised systems including NTK and ROBERT** (PSRE, Generic Risk 2/s 3.3).

G: *s 4.4 Relay attacks*

- Active relay attacks are a **generic problem in all Bluetooth based systems**. (PSRE, Generic Risk 2).

H: *s 5.1 Using the Bluetooth beacon*

- These weaknesses are **both minor and a generic problem in all designs based on Bluetooth proximity detection** (PSRE, Generic Risk 5).

I: *s 5.2 Deanonymizing Known Reported User*

- This is a known attack vector **inherent to all contact tracing systems, whether centralised or decentralised** (PSRE, Inherent Risk 1).

J: *s 5.3 Disclosing Private Encounters*

- **This attack does not work** as it assumes that at-risk people will also report their keys, which they do not in DP-3T.

K: *s 5.4 Coercion threats: Information*

- Determined attackers having access to local storage on a phone can try and deduce information. We acknowledge this attack (PSRE, System-specific Risks 1, 2). **However, this type of attack applies to all systems storing Bluetooth observations on the phone (centralized and decentralized) including DP-3T, NTK and ROBERT**.

L: *s 5.4 Coercion threats: Tracing*

- Gaining access to a user's phone might also enable *tracing* in decentralized systems storing identifiers on the phone (PSRE, System-specific Risk 3). Mitigation options are discussed there. **In a centralized system, tracing is possible with information on the server for both infected and non-infected individuals, without access to individual's phones, and without the necessity of compromising a phone's software security.**

Centralised systems also raise an array of attacks and risks that are not mentioned in either this paper or the one being analysed. For further discussion, please read:

- Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems
- Privacy and Security Analysis of PEPP-PT-ROBERT
- Privacy and Security Analysis of PEPP-PT-NTK