Not as Private as We Had Hoped: Unintended Privacy Problems in Some Centralized and Decentralized COVID-19 Exposure Notification Systems

Vanessa Teague
vanessa@thinkingcybersecurity.com or vanessa.teague@anu.edu.au

Real World Crypto
Jan 13, 2021

Centralised vs decentralised contact tracing: we were mostly right

From the cryptographers' open letter:

> Some of the Bluetooth-based proposals respect the individual's right to privacy, whilst others would enable (via mission creep) a form of government or private sector surveillance that would catastrophically hamper trust in and acceptance of such an application by society at large. It is crucial that citizens trust the applications in order to produce sufficient uptake to make a difference in tackling the crisis. It is vital that, in coming out of the current crisis, we do not create a tool that enables large scale data collection on the population, either now or at a later time. Thus, solutions which allow reconstructing invasive information about the population should be rejected without further discussion. Such information can include the "social graph" of who someone has physically met over a period of time.

... but we were also partly wrong (part 1)

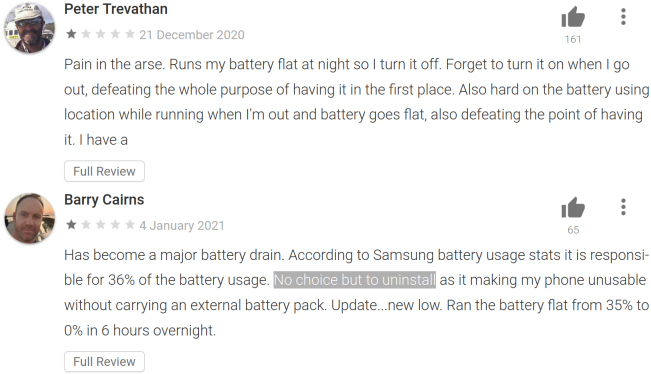
- Australia's (centralised) COVIDSafe App has some privacy advantages

... but we were also partly wrong (part 1)

- Australia's (centralised) COVIDSafe App has some privacy advantages
- Non-running apps gather no data

... but we were also partly wrong (part 1)

- Australia's (centralised) COVIDSafe App has some privacy advantages
- Non-running apps gather no data



Peter Trevathan

★ ☆ ☆ ☆ ☆ 21 December 2020

161

Pain in the arse. Runs my battery flat at night so I turn it off. Forget to turn it on when I go out, defeating the whole purpose of having it in the first place. Also hard on the battery using location while running when I'm out and battery goes flat, also defeating the point of having it. I have a

Full Review

Barry Cairns

★ ☆ ☆ ☆ ☆ 4 January 2021

65

Has become a major battery drain. According to Samsung battery usage stats it is responsible for 36% of the battery usage. No choice but to uninstall as it making my phone unusable without carrying an external battery pack. Update...new low. Ran the battery flat from 35% to 0% in 6 hours overnight.

Full Review

Non-functional apps are great for privacy

…nor do apps that send payloads that can't be decrypted

14. iPhone app can't exchange messages as expected with other iPhones

Status: Fixed in v1.8.
Type: Functionality
Affects: iOS
More info: Earlier blog post, GitHub issue on errors in the attempted fix

When the V2 payload was introduced (see #3 above), the iPhone implementation incorrectly truncated the new messages, resulting in the encounters being silently ignored and not logged to the database. Fortunately due to redundancy in the design, there is a second mechanism where the payload is exchanged, but this bug overall decreases the reliability of the contact tracing functionality.

A fix was attempted, however it contains a new bug, which means that while the encounters are now logged, they are actually corrupted, which means they will not be able to be decrypted by the server.

Non-functional apps are great for privacy

…nor apps that max out the phone's BLE connections and open no more.

13. iPhone app prevents new connections after 100 exchanges

Status: Fixed in v1.9
Type: Functionality
Affects: iOS
More info: GitHub issue

Once a remote device is found during a scan, the app will then attempt to connect and record an encounter with it every 15 seconds. This allows the duration of the encounter to be inferred, even though the background-mode scanning will not find the same device multiple times.

These connection attempts do not time out, and so for every device that goes out of range the phone will remain in an "attempting to connect" state to that device. In addition, phones change their address every few minutes, which means that any nearby phone will appear to go out of range every few minutes.

After about 100 pending connections, the phone becomes unable to connect to new devices. This prevents further encounters from being recorded, but also prevents other apps from initiating connections to other BLE devices (e.g. smart watches, diabetes continuous glucose monitoring, etc).

But does Australia's COVIDSafe app work?

- It's an unusual example of an app for which a *functionality failure* is undetectable by ordinary users.

[1] Parliament of Victoria, Inquiry into the Victorian Government's COVID–19 contact tracing system and testing regime. Dec 2020. https://www.parliament.vic.gov.au/file_uploads/LCLSIC_59-05_Vic_Gov_COVID-19_contact_tracing_testing_wtnKCs70.pdf

But does Australia's COVIDSafe app work?

- It's an unusual example of an app for which a *functionality failure* is undetectable by ordinary users.
- In Aus, we just don't know

[1] Parliament of Victoria, Inquiry into the Victorian Government's COVID–19 contact tracing system and testing regime. Dec 2020. https://www.parliament.vic.gov.au/file_uploads/LCLSIC_59-05_Vic_Gov_COVID-19_contact_tracing_testing_wtnKCs70.pdf

But does Australia's COVIDSafe app work?

- It's an unusual example of an app for which a *functionality failure* is undetectable by ordinary users.
- In Aus, we just don't know
  - how many people are running it

[1] Parliament of Victoria, Inquiry into the Victorian Government's COVID–19 contact tracing system and testing regime. Dec 2020. https://www.parliament.vic.gov.au/file_uploads/LCLSIC_59-05_Vic_Gov_COVID-19_contact_tracing_testing_wtnKCs70.pdf

But does Australia's COVIDSafe app work?

- It's an unusual example of an app for which a *functionality failure* is undetectable by ordinary users.
- In Aus, we just don't know
  - how many people are running it
  - what fraction of proximity events it detects

[1] Parliament of Victoria, Inquiry into the Victorian Government's COVID–19 contact tracing system and testing regime. Dec 2020. https://www.parliament.vic.gov.au/file_uploads/LCLSIC_59-05_Vic_Gov_COVID-19_contact_tracing_testing_wtnKCs70.pdf

But does Australia's COVIDSafe app work?

- It's an unusual example of an app for which a *functionality failure* is undetectable by ordinary users.
- In Aus, we just don't know
  - how many people are running it
  - what fraction of proximity events it detects
- "...the effectiveness of the COVIDSafe app for Victoria's contact tracing efforts was insignificant."[1]
- "The app has helped find an additional 17 contacts not found through manual contact tracing."

[1] Parliament of Victoria, Inquiry into the Victorian Government's COVID–19 contact tracing system and testing regime. Dec 2020. https://www.parliament.vic.gov.au/file_uploads/LCLSIC_59-05_Vic_Gov_COVID-19_contact_tracing_testing_wtnKCs70.pdf

Long list of issues

Privacy, security, functionality, usability...

`https://github.com/vteague/contactTracing/blob/master/blog/2020-07-07IssueSummary.md`

Discovered by: Chris Culnane, Eleanor McMurtry, Ben Frengley, Geoffrey Huntley, Hubert Seiwert, Jim Mussared, John Evershed, Manabu Nakazawa, Richard Nelson, Robert Merkel, Vanessa Teague, Alwen Tiu, Yaakov Smith

Plenty of privacy issues too, e.g. (now fixed)

[2] Jim Mussared and Alwen Tiu, `https://github.com/alwentiu/COVIDSafe-CVE-2020-12856`

Plenty of privacy issues too, e.g. (now fixed)

Issue 5 CVE-2020-12856 "This vulnerability allows an attacker to bond silently with an Android phone running a vulnerable version of the app. The bonding process involves exchanges of permanent identifiers of the victim phone: the identity address of the bluetooth device in the phone and a cryptographic key called Identity Resolving Key (IRK). Either one of these identifiers can be used for long term tracking of the phone."[2]

[2] Jim Mussared and Alwen Tiu, `https://github.com/alwentiu/COVIDSafe-CVE-2020-12856`

Plenty of privacy issues too, e.g. (now fixed)

Issue 5 CVE-2020-12856 "This vulnerability allows an attacker to bond silently with an Android phone running a vulnerable version of the app. The bonding process involves exchanges of permanent identifiers of the victim phone: the identity address of the bluetooth device in the phone and a cryptographic key called Identity Resolving Key (IRK). Either one of these identifiers can be used for long term tracking of the phone."[2]

[2] Jim Mussared and Alwen Tiu, `https://github.com/alwentiu/COVIDSafe-CVE-2020-12856`

Plenty of privacy issues too, e.g. (now fixed)

Issue 19 Payload encryption algorithm included a plaintext counter, so you broadcasted how many other exchanges you had made in the last few minutes

Conclusion (Part 1)

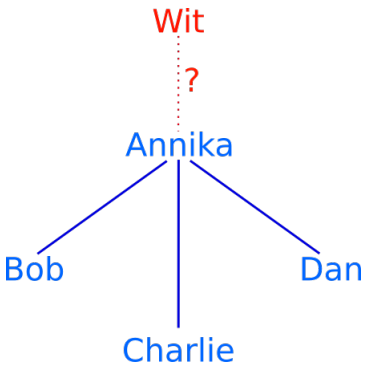
For centralised apps like COVIDSafe, inferring social graph edges is the least of our worries.

Part 2: Early versions of GAEN could expose social graph edges in some circumstances

- Only if users opted in to uploading (detailed) ExposureInfo
  - I don't know of any apps that did this,
  - nor of any prohibition against this
- This was fixed in June, before I notified A & G
- It all depends on whether the ExposureInfo is shuffled before upload

Setting: Annika omits to tell contact tracers about her meeting with Wit

- Annika tests positive
  - tells contact tracers about Bob, Charlie and Dan
  - including proximities & durations
- later, Bob, Charlie, Dan & Wit all test positive and upload their Diagnosis Keys.
- the authorities want to know whether Annika met with Wit



How can the authorities tell whether Annika was near Wit?

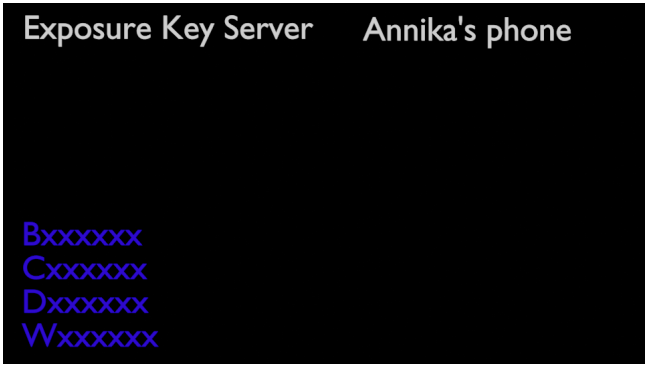


Figure: If Annika opts in to uploading detailed ExposureInfo, and if the metadata is enough to re-identify Bob, Charlie and Dan's records, the authorities can tell whether a record for Wit appears after them.

Conclusion

- *All other things being equal* decentralised apps protect the privacy of users—especially the social graph—better than centralised ones

Conclusion

- *All other things being equal* decentralised apps protect the privacy of users—especially the social graph—better than centralised ones
- but centralised apps are probably used much less because of their various other problems

Conclusion

- *All other things being equal* decentralised apps protect the privacy of users—especially the social graph—better than centralised ones
- but centralised apps are probably used much less because of their various other problems
- It was possible to infer social edges in early versions of GAEN
  - with explicit user opt-in for uploading extra info
  - this was fixed (with client-side shuffling) before I noticed

Conclusion

- *All other things being equal* decentralised apps protect the privacy of users—especially the social graph—better than centralised ones
- but centralised apps are probably used much less because of their various other problems
- It was possible to infer social edges in early versions of GAEN
  - with explicit user opt-in for uploading extra info
  - this was fixed (with client-side shuffling) before I noticed
- Overall, GAEN apps are *much* better than centralised apps
  - but there may be other privacy impacts we don't know