BLUEBLEED Technical Analysis

Google/Apple contact tracing side-channel attack on Bluetooth Smart Privacy

Authors: Norman Luhrmann, V

daughter-of-v@protonmail.com / PGP key DF20D21B349C2A9A

Revision: 1.0 (2020-07-05) Initial draft
1.1 (2020-13-37) Release

CVE-2020-13702
BLUEBLEED
ATTACK VECTOR: BLUETOOTH LE SMART PRIVACY
AFFECTED: ALL ANDROID/IOS DEVICES
WITH BLUETOOTH LE
CONTACT TRACING APPS
AFFECTED EU USERS: CA. 100M
11 GDPR COMPLAINTS PENDING
BOTH VENDORS STAKED IN PROXIMITY MARKETING
25BN ATTACK VEHICLES
*IOT 2020

Contents

Definitions

Bluetooth beacon	Low energy Bluetooth device with years of battery life running standards like Apple iBeacon or Google Eddystone
Bluetooth LE	Bluetooth Low Energy standard for low impact wireless communications up to 20m
Bluetooth LE Generic Attribute Profile (GATT)	Generic Attribute Profile is a listing of Bluetooth LE application data sets
Bluetooth Smart Privacy	Smart Privacy is a mechanism implemented to protect user location data for Bluetooth communications.
Contact tracing app	Mobile application that utilises Bluetooth LE to detect close proximity encounters
Exposure Notification	Google/Apple joint contact tracing framework effort
Internet of Things (IoT)	All devices connected to the internet, including Bluetooth beacons
PEPP-PT/DP-3T	Generic Bluetooth LE based contact tracing architectures from which Exposure Notification derives

Introduction

BLUEBLEED is a vulnerability of the contact tracing technology Exposure Notification developed by Google and Apple, and in consequence implemented by many contact tracing app vendors.

The vulnerability at hand exposes potential hundreds of millions of app user locations by breaking Bluetooth LE “”Smart Privacy”. As shown in the course of the analysis this is easily exploited by a specific target audience.

The authors have communicated with Google, and to a lesser extent, with Apple to rectify the critical flaws in the Exposure Notification framework. Namely CVE-2020-13702 *“Catastrophic breach of user privacy in Apple/Google COVID-19 Exposure Notification API”* [1] has unsuccessfully tried to deescalate the loss of user location protection for users of said contact tracing stack.

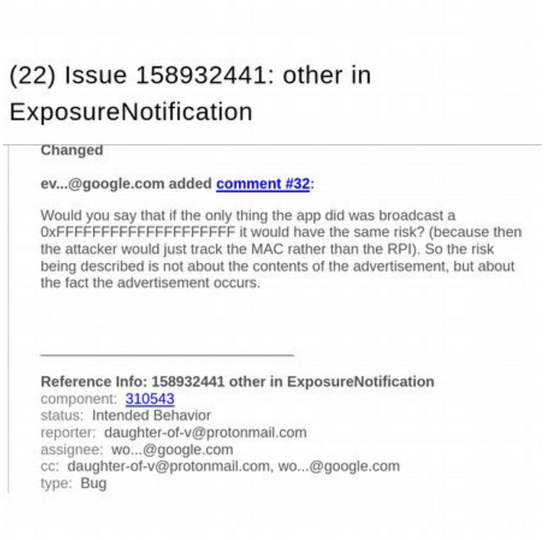
The Exposure Notification framework [2] is live in many countries of the European Union since national contact tracing apps have been updated to use the new Google/Apple device independent tracking mechanism. Millions of active users are currently already affected by the described vulnerability affecting all versions of Android and IOS.

Other PEPP-PT or DP-3T frameworks [3] are potentially suffering from the same vulnerability and can also be considered affected by loss of “Smart Privacy”, although an analysis of this extended effect of the vulnerability is outside of the scope of this paper.

Bluetooth LE “Smart Privacy” is a mechanism generally protecting users against such security exposures by protocol design. We will show that Google/Apple abuse the protocol mechanisms of

Bluetooth LE beyond their original scope which results in the complete loss of “Smart Privacy” protection.

Lengthy discussions with the Google Security team about the issue scope have resulted in a standing `Intended Behavior` status for the ticket. Google does not approve of the definition of Exposure Notification being responsible for frequency and structure of messages sent as part of it’s advertising scheme. This contradicts feedback from Google Security acknowledging the responsibility of “Smart Privacy” compatibility on the implementation side.



(22) Issue 158932441: other in ExposureNotification

Changed

ev...@google.com added comment #32:

Would you say that if the only thing the app did was broadcast a 0xFFFFFFFFFFFFFFFFFFFF it would have the same risk? (because then the attacker would just track the MAC rather than the RPI). So the risk being described is not about the contents of the advertisement, but about the fact the advertisement occurs.

Reference Info: 158932441 other in ExposureNotification
component: 310543
status: Intended Behavior
reporter: daughter-of-v@protonmail.com
assignee: wo...@google.com
cc: daughter-of-v@protonmail.com, wo...@google.com
type: Bug

Fig. 1: Google Security team on the scope of the vulnerability [4]

In the course of the discussions the vendor shifted to a specific flaw in the current implementation which relates to limitations of identifier rotations. The effect of this limitation to overall privacy leakage is minute though, since as shown below Exposure Notification is broken by design.

Apple product security does not acknowledge the implications of this vulnerability and the applicability to the IOS Exposure Notification implementation at all.

The analysis at hand is the direct consequence of the vendor inaction. Due to the lack of cooperation on the matter the authors composed this succinct analysis summarising previous finding for the purpose of escalation to the respective data protection authorities [5].

Context

Numerous national contact tracing app development initiatives have raised privacy concerns from the information security community. Data protection impact assessments [6] [7] have been executed against different mostly comparable situations with unclear results in either direction.

None of the existing privacy analysis though have concerned themselves with a specific intricacy of the Exposure Notification approach: the unconventional application of the high frequency advertising pattern in the Bluetooth LE proximity handshake mechanisms.

Existing Bluetooth LE applications do usually hold one of the following protocol usage patterns:

- Only process signals passively on the device
- Process signals actively on the device, but in a paired private communication channel

None of these applications hold the usage pattern of Exposure Notification:

- Process signals actively on the device with broadcast advertising to everyone in signal range

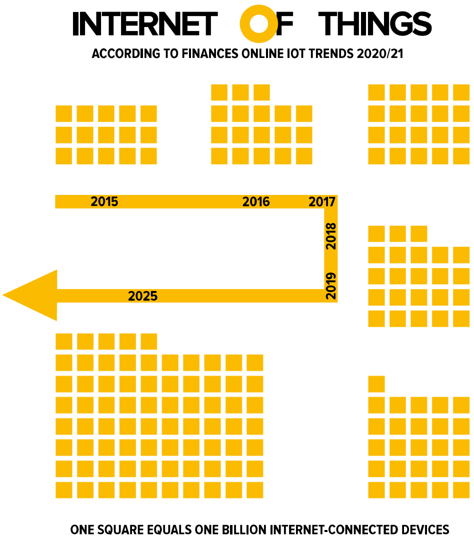
The basic premise of the pattern at hand is that there is a very frequent signalling mechanism (approx. 270ms recommended as per Google/Apple specifications). The second premise is that everyone within signal range can intercept and process the signal.

Previous privacy assessments and Google/Apple argued that user information is protected in Exposure Notification since it executes stringent data encryption mechanisms.

In this line of reasoning it is overseen that both the message structure and occurrence in a high frequency domain, as well as personally identifiable derivative identifiers included in the encrypted payload of Exposure Notification, provide ample attack space for severe privacy violations.

A proposed location recovery mechanism is shown to achieve close to 100% of tracking reliability over areas of devices covering Bluetooth LE, even in densely crowded clusters of devices. Proof of concept is provided in the form of an agent based simulation. A concrete example of this vulnerability is presented in the domain of Bluetooth LE beacons as they are operated in fleets in urban and commercial areas for a variety of purposes.

Fig. 2: growth of internet-connected devices in the IoT until 2025, IOT Trends



In consequence of the vulnerability operators of beacon networks are able to process location data without:

- User consent
- Lawful basis of processing
- Means to execute rights of the data holder

Looking at the growth rates of IoT devices it is easy to envision the real-world coverage of Beacon devices in state-of-the-art commercial context.

Even worse, as further shown advanced penetration threats are likely able to penetrate the weak security defenses of such IoT fleets or do already hold existing fleet capacity via botnets in the wild. Intelligence community access to such data sets seem granted.

The acceptance rate of apps based on vulnerable frameworks is expected to be very high due to general public awareness and semi-official sanctioning. Here is a (non-conclusive) list of current apps live and affected by the privacy leak:

Country	App Name	Estimated audience*
Austria	Stopp Corona	6.4M
Czech Republic	eRouška	7.8M
Denmark	smitte|stop	4.2M
Finland	Ketju	4.0M
France	StopCovid	47.4M
Germany	Corona-Warn-App	59.9M
Hungary	VírusRadar	7.1M
Italy	Immuni	43.3M
Norway	Smittestop	3.9M
Poland	ProteGO Safe	27.9M
Spain	Radar COVID	33.8M
TOTAL		**245.7M**

*Table 1: List of Exposure Notification framework consumer apps or apps based on Google/Apple Exposure Notification. Data set enriched with potential user base for their respective EU member state. (*as of Statista 2019 EU-28 individuals using a mobile phone to access internet)*

The excerpt of EU countries participating in Bluetooth LE based contact tracing technology in the list above totals to 245.7M potential contact tracing devices, which would all be prone to the location data leakage described in this document.

With studies showing acceptance rates of around 50% for contact tracing technology in EU countries [8] a 2020 baseline estimate of mobile devices vulnerable to the privacy attack described in this analysis would be 100M+ affected devices in these countries.

A mid-term scenario of hypothetical continued spread of COVID-19 disease pandemic and subsequent wave events forcing policy makers to encourage further contact tracing app usage might see global penetration of the affected technology numbering in the Billions. The vast scale of the affected data processing should highlight the special consideration required for this vulnerability.

Bluetooth LE Smart Privacy

Quoting the Bluetooth SIG Blog entry “Bluetooth Technology Protecting Your Privacy”, one might assume sensitive handling of location privacy in involved applications: *“One privacy issue concerns the possibility of being tracked »where you go« in the physical world without your awareness or consent. »Where you go« could mean the places you drive or the route you walk.”* [9]

Bluetooth LE "Smart Privacy" is a technology that is designed to protect Bluetooth LE applications from exposing users to device tracking. Bluetooth LE Generic Attribute Profile (GATT) enumerates design use cases for the protocol. Contrary to Exposure Notification traditional applications for Bluetooth LE on mobile devices are of less noisy and/or more private signalling patterns:

- Passive signal processing occurs on mobile devices, data sent via nearby beacons on public channel is received
- Active signal processing occurs on mobile device with peer device like smart watch, data sent between peered devices via encrypted private channel

Contact tracing reverts the beacon situation for mobile devices:

- Active signal processing occurs on mobile device via public channel, metadata and dual rotation identifier leaks too much personally identifiable information due to high advertising frequency

The situation is worsened by the fact that the Exposure Notification protocol introduces additional personally identifiable information via the encrypted advertising payload.

This leads to a broken "Smart Privacy" implementation in the design of Exposure Notification, as outlined below.

Attack Vector

The Exposure Notification protocol looses "Smart Privacy" due to a combination of high frequency signalling and introduction of secondary personally identifiable information in the encrypted payload.

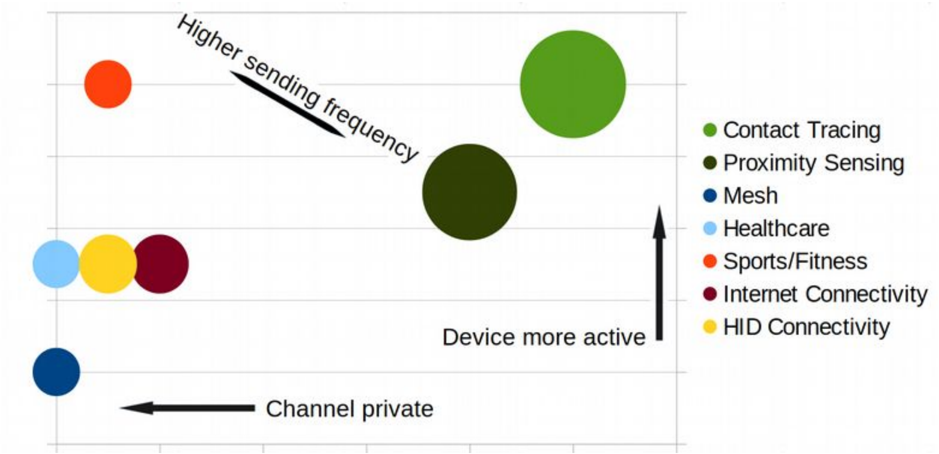


Fig. 3: Bluetooth LE Generic Attribute Profile (GATT) compared by channel privacy, user device activity and sending frequency

As can be seen on the GATT chart above, Bluetooth LE applications that are part of the stable protocol specifications use a very different signalling pattern to Exposure Notification and similar contact tracing frameworks.

Traditional applications are usually executing in paired mode or on public channels given that passive user devices keep a very low profile. Contrary to that mode of operations the Contact Tracing application pattern demands that a user device constantly advertises itself to all listeners in range. These signals occur up to multiple times per second.

This should intuitively highlight the compatibility issue of Exposure Notification with Bluetooth LE, and specifically “Smart Privacy” protection mechanisms in place.

Concrete examples of established applications applying Bluetooth LE fundamentally differently are:

Smart watch	Communicates every n minutes on avg.	With a paired peer via encrypted channel but mobile device is only passive in this secure communication path
Retail proximity marketing beacon	Communicates every n seconds on avg.	On public channel but mobile device is only passive in this communication path
Audio	Communicates constantly	With a paired peer via encrypted channel
Exposure Notification	**Communicates constantly**	**On public channel**

Table 5: Bluetooth LE application examples describing communication patterns

The following figure illustrates the signalling behaviour of consumer apps using Exposure Notification. According to the specification [2] each device sends out a signal via Bluetooth LE advertising approx. every 300ms. Neighbouring devices activate their Bluetooth scanning mechanism to receive advertises roughly every five minutes to detect proximity.

This pattern is abused by sniffers who can permanently scan to easily ingest the high frequency advertising signals.

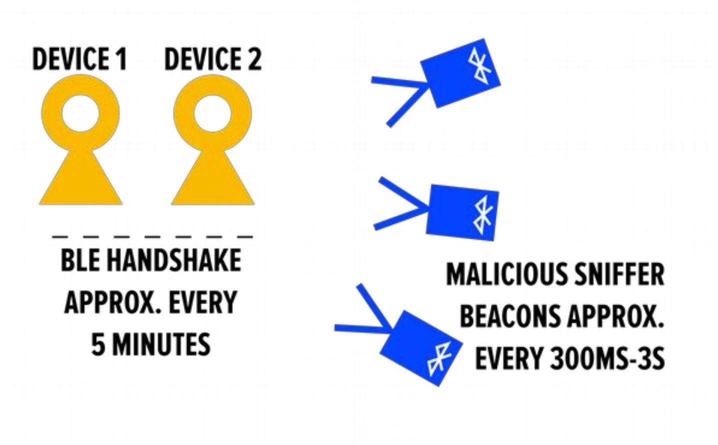

DEVICE 1
DEVICE 2
BLE HANDSHAKE APPROX. EVERY 5 MINUTES
MALICIOUS SNIFFER BEACONS APPROX. EVERY 300MS-3S

Fig. 4: regular handshake interval vs. malicious sniffer signalling activity

Bluetooth LE includes a MAC address device identifier in the network layer. “Smart Privacy” should see a rotation of the MAC address identifier around every 15 minutes to reset the device privacy and deny device tracking.

Exposure Notification introduces a secondary identifier called Rolling Proximity Identifier (RPI), which is encrypted and as such forms a pseudonymous identifier for the user device. The Exposure Notification protocol recommends the rotation of this identifier at the same interval as the MAC address rotation.

Due to limitations of the Bluetooth LE device drivers, current implementations on Android devices see this coupled rotation only working in 50% of the rotation scenarios, resulting in an offset of the rotation occurrences.

As the figure below shows the established advertising frequency and dual identifier situation introduces a location tracking vector not present without Exposure Notification. This vulnerability exposes device location data for every signal receiver in range.

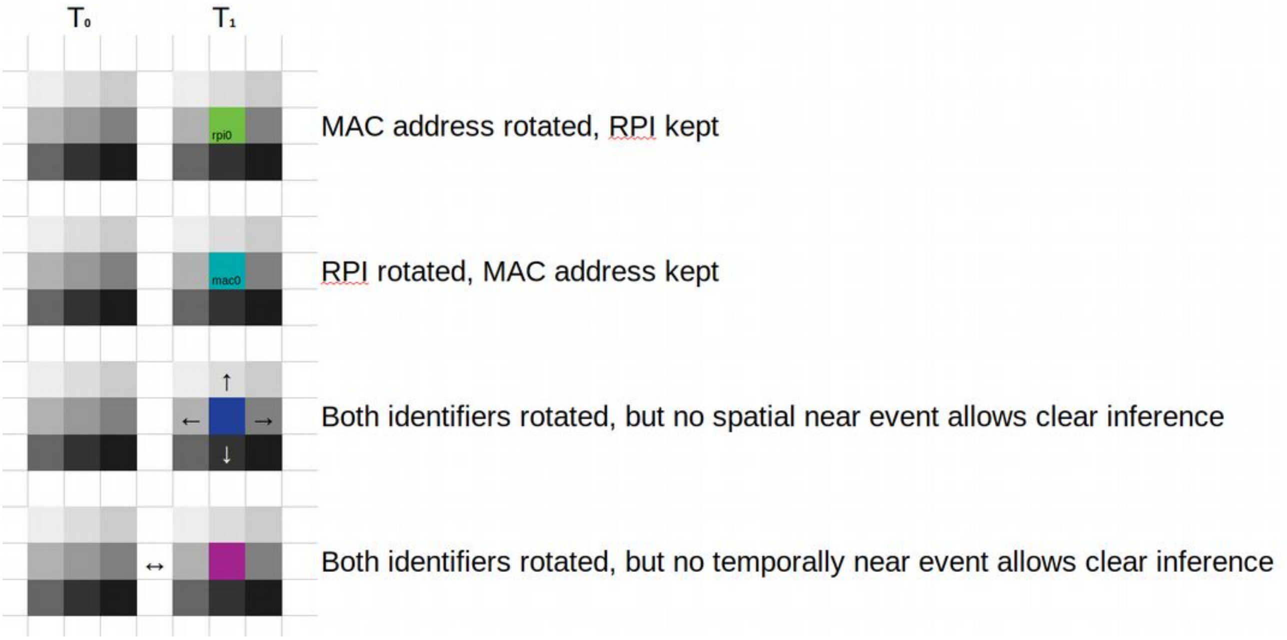

T₀
T₁
rpi0
MAC address rotated, RPI kept
mac0
RPI rotated, MAC address kept
↑
←
→
↓
Both identifiers rotated, but no spatial near event allows clear inference
↔
Both identifiers rotated, but no temporally near event allows clear inference

Fig. 5: four trackable rotation scenarios in a cluster of 9 devices showing vulnerable side channels for unique device identification

Agent-based black box simulations [11] for the exploit reported in CVE-2020-13702 show an extremely high tracking hit rate, even in highly clustered device groups. This device tracking is attainable with a trivial location resolver that handles spatial and temporal event data as well as the dual identifier rotation.

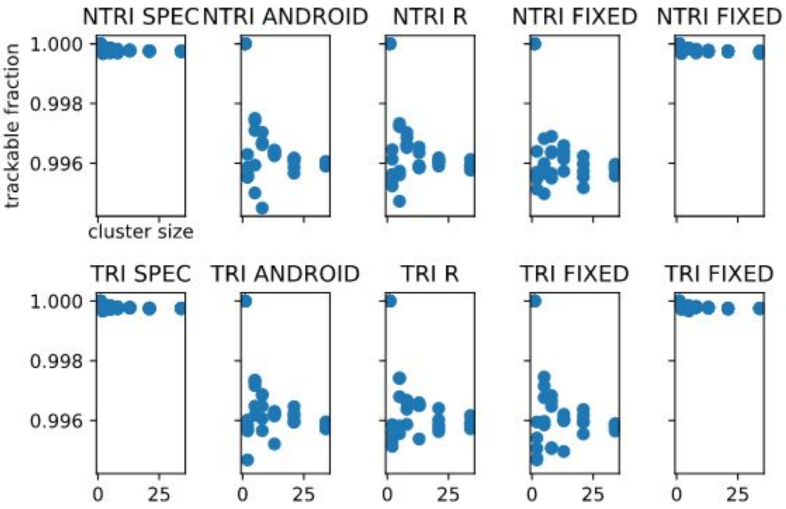


Fig. 6: regardless of timer setup and/or implementation quality the traceability is close to 100% due to the loss of Bluetooth Smart Privacy

The simulations have been executed against a different set of rotation timer scenarios. This includes official Exposure Notification specification timers and current live Android and Android R variants. The results show that regardless of the timer scenario the resolver is able to track the device location in all variants.

It can only be concluded that due to the combination of high frequency advertising and dual identifiers present, Bluetooth LE “Smart Privacy” is in effect lost on devices running Exposure Notification.

Exposure Notification is therefor susceptible to an easily exploited location data leak. For reference, exploit implementations similar to the aforementioned simulation resolver component are trivial to implement on top of a time-series log database ingesting beacon network logs.

Such databases are expected to be common in mid- to large-scale proximity marketing deployments to derive targeting segments.

Beacon Security

The gravity of the exploit shown above is multiplied by the large attack surfaces present in IoT deployments like Bluetooth beacons.

The BLEEDINGBIT attack of 2018 exposing Texas Instrument chipset based Bluetooth devices might serve as a random example of this situation [13]. The vulnerability exposed hardware from high profile vendors like Cisco to unauthorised access. MITRE CVE includes countless similar exploits and highlights the never-ending attack stream on IoT.

The OWASP Top 10 IoT security issues establish this situation from a different perspective [12]. Numerous items on that list are inherent for fire-and-forget IoT devices and create a permanently challenging security environment.

Mass surveillance provides a strong incentive for targeted measures, which makes it likely that advanced penetration actors like nation state backed groups will have or do already have the control of large international IoT device fleets.

Rank	Vulnerability
1	Weak, guessable or hard coded passwords
2	Insecure network services
3	Insecure ecosystem interfaces
4	Lack of secure update mechanism
5	Use of insecure or outdated components
6	Insufficient privacy protection
7	Insecure data transfer and storage
8	Lack of device management
9	Insecure default settings
10	Lack of physical hardening

Table 6: OWASP Top 10 Internet of Things 2018 as applicable to Bluetooth LE beacons

The existence of attack vehicles for the vulnerability at hand is underlined by the following Spamhaus study showing the number and distribution of distinct botnets detected by security teams in 2019. Note that this map shows the number of controlling entities, which should not be confused with the number of infected devices which is vastly larger.

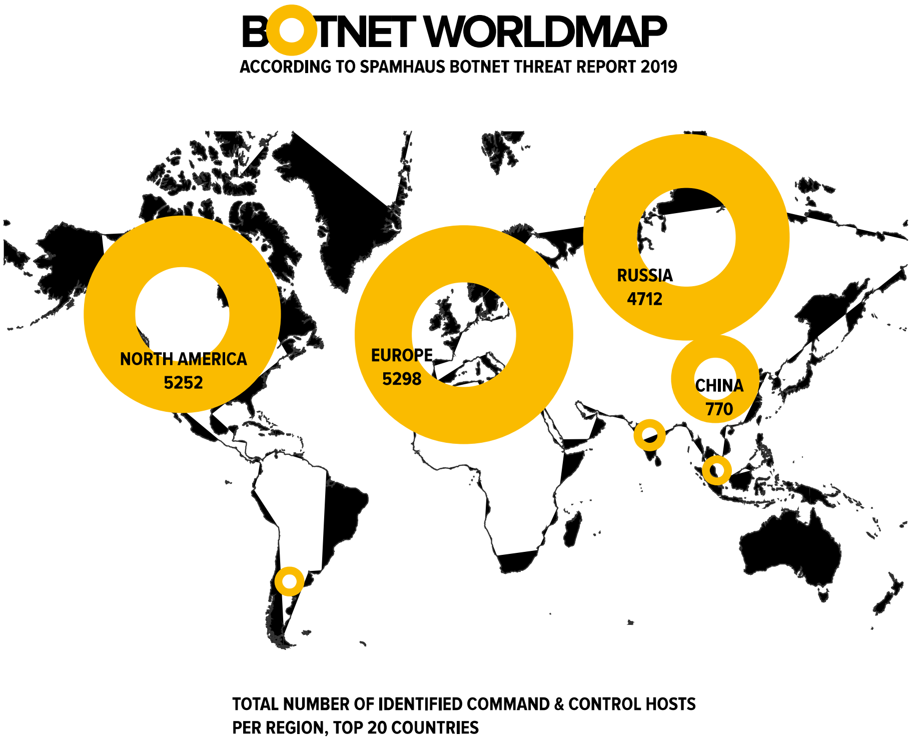

BOTNET WORLDMAP
ACCORDING TO SPAMHAUS BOTNET THREAT REPORT 2019
NORTH AMERICA
5252
EUROPE
5298
RUSSIA
4712
CHINA
770
TOTAL NUMBER OF IDENTIFIED COMMAND & CONTROL HOSTS
PER REGION, TOP 20 COUNTRIES

Fig. 7: botnet command&control distribution 2019, Spamhaus

Benefactors

Due to the complex interaction of Bluetooth LE Smart Privacy and Exposure Notification protocol design the demonstrated vulnerability has not been captured in preceding security or privacy assessments.

As a side channel attack it is an obscure vector that is difficult to spot and align with the attack goals. Non-the-less the situation demands the question if this is a well hidden surveillance package deployed in an opportune situation.

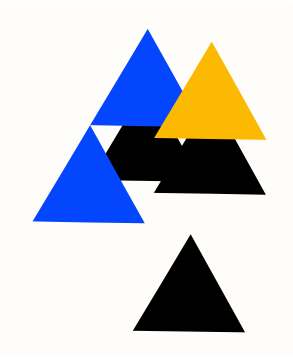
Without further elaboration of this context the following benefactors can be identified in regards to increased acceptance of Bluetooth LE technology and/or the loss of Bluetooth Smart Privacy (in no particular order):

Google: physical advertising space is on the agenda, as the successful transition from Google Nearby into Eddystone shows. Known for nasty partnerships with Location Services Providers functioning as beacon location data aggregators and resellers. Location data segmentation as vital component of business well known [15].

Apple: as the innovator and leader in proximity apps and business leverage behind such applications the increased acceptance of Bluetooth LE is desirable for the iBeacon company [16].

Advertising industry: existing physical advertising targeting profiles will be able to leverage improved data sets [17]. A whopping USD 52 Billion global market prediction from Market watch for the proximity marketing space speaks for itself.

Surveillance/intel community: the privacy leak enables the tracking of individuals throughout areas covered by accessible Bluetooth LE beacons. It is also useful in the augmentation of tracking technologies like face detection for difficult settings. Might be applied to offset the current impact on face detection based tracking due to face masks seeing highly increased usage.



Conclusion

The impact of the identified side channel attack on location data is large in multiple dimensions:

- Over **250M potential affected users**. 100M upwards seem realistic for the course of 2020
- Attack vector is Bluetooth LE broadcast scanning which is completely passive, so there is **no way for the user to opt out** of this communication
- Simulations of distinct or densely clustered mobile device groups have shown **close to 100% traceability success rate**
- There is **no legal grounds for the data processing capabilities** of Bluetooth beacon operators and the leaked location data
- Operators of Bluetooth beacon fleets are often involved in digital marketing demand-side platforms (DSPs) with active data exchange with a **large number of unspecified data sub processors**
- Non opt-out location data tracking is **politically and economically consequential**

There is no doubt that the legal grounds for processing this kind of high frequency beacon signal data are not provided for within Exposure Notification.

Both the contact tracing app publishers and Google/Apple as vendor for the Exposure Notification framework need to proceed to shut off the affected infrastructure until a revised protocol design is available.

References

[1] NIST NVD: CVE-2020-13702 Detail
https://nvd.nist.gov/vuln/detail/CVE-2020-13702

[2] Google/Apple: Exposure Notification – Bluetooth Specification v1.2
https://www.apple.com/covid19/contacttracing/

[3] PEPP-PT: Data Protection and Information Security Architecture
https://github.com/pepp-pt/pepp-pt-documentation/blob/master/10-data-protection/PEPP-PT-data-protection-information-security-architecture-Germany.pdf

[4] Google/Norman Luhrmann: CVE Conversation Log
https://github.com/normanluhrmann/infosec/raw/master/conversation-exposure-notification-google-2020-06-07.pdf

[5] Also see *"Appendix I – data protection authorities"*

[6] EDPB: Statement on the data protection impact of the interoperability of contact tracing apps
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_en_0.pdf

[7] Bock et al.: Data Protection Impact Assessment for the Corona App
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3588172

[8] Milson et al.: Survey of acceptability of app-based contact tracing in the UK, US, France, Germany and Italy
https://osf.io/7vgq9/

[9] Bluetooth SIG: Bluetooth Technology Protecting Your Privacy
https://www.bluetooth.com/blog/bluetooth-technology-protecting-your-privacy/

[10] IAB: The Programmatic Supply Chain; see "Shared Trading and Data Storage"
https://www.iab.com/wp-content/uploads/2016/03/Programmatic-Value-Layers-March-2016-FINALv2.pdf

[11] Norman Luhrmann: Agent-based simulation of Bluetooth LE Smart Privacy attack on scale
https://github.com/normanluhrmann/infosec/raw/master/agent-based-simulation-bluetooth-le-attack-20200629.pdf

[12] OWASP: Internet of Things (IoT) Top 10 2018:
https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

[13] Armis: How do the BLEEDINGBIT vulnerabilities work? CVE-2018-16986:
https://www.armis.com/bleedingbit/

[14] EU: General Data Protection Regulation (GDPR)
https://gdpr.eu/tag/gdpr/

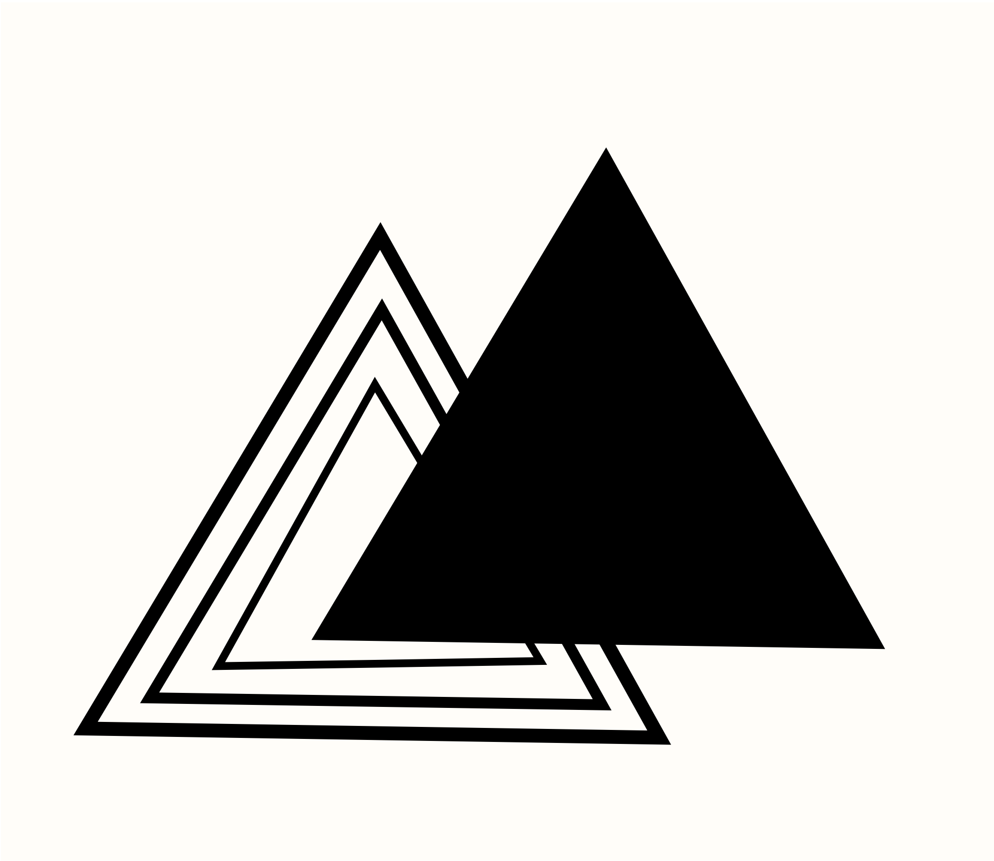
[15] Google: Google Ad Manager
https://admanager.google.com/home/

[16] Apple: iBeacon

https://developer.apple.com/ibeacon/

[17] Market Watch: Proximity Marketing Market 2020 - 2023: Business Trends, Size, COVID - 19 Outbreak, Sales, Supply, Demand and Regional Analysis

https://www.marketwatch.com/press-release/proximity-marketing-market-2020---2023-business-trends-size-covid---19-outbreak-sales-supply-demand-and-regional-analysis-2020-06-09?reflink=mw_share_email



Appendix I – data protection authorities

The tables below lists the data protection authorities supervising the respective contact tracing app vendor. As such both are responsible to take action to protect user privacy rights damaged by Exposure Notification.

Country	App Name	GDPR data protection authority
Austria	Stopp Corona	**Österreichische Datenschutzbehörde** Hohenstaufengasse 3 1010 Wien Tel. +43 1 531 15 202525 Fax +43 1 531 15 202690 e-mail: dsb@dsb.gv.at Website: http://www.dsb.gv.at/
Czech Republic	eRouška	**The Office for Personal Data Protection** Urad pro ochranu osobnich udaju Pplk. Sochora 27 170 00 Prague 7 Tel. +420 234 665 111 Fax +420 234 665 444 e-mail: posta@uoou.cz Website: http://www.uoou.cz/
Denmark	smitte|stop	**Datatilsynet** Borgergade 28, 5 1300 Copenhagen K Tel. +45 33 1932 00 Fax +45 33 19 32 18 e-mail: dt@datatilsynet.dk Website: http://www.datatilsynet.dk/
Finland	Ketju	**Office of the Data Protection Ombudsman** Ratapihantie 9 FIN-00520 Helsinki Switchboard: +358 (0)29 566 6700 Registry: +358 (0)29 566 6768 e-mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi/en/
France	StopCovid	**Commission Nationale de l'Informatique et des Libertés - CNIL** 8 rue Vivienne, CS 30223 F-75002 Paris, Cedex 02 Tel. +33 1 53 73 22 22 Fax +33 1 53 73 22 00 Website: http://www.cnil.fr/
Germany	Corona-Warn-App	**Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit** Husarenstraße 30

		53117 Bonn Tel. +49 228 997799 0; +49 228 81995 0 Fax +49 228 997799 550; +49 228 81995 550 e-mail: poststelle@bfdi.bund.de Website: http://www.bfdi.bund.de/
Hungary	VírusRadar	**Data Protection Commissioner of Hungary** Szilágyi Erzsébet fasor 22/C H-1125 Budapest Tel. +36 1 3911 400 e-mail: peterfalvi.attila@naih.hu Website: http://www.naih.hu/
Italy	Immuni	**Garante per la protezione dei dati personali** Piazza di Monte Citorio, 121 00186 Roma Tel. +39 06 69677 1 Fax +39 06 69677 785 e-mail: garante@garanteprivacy.it Website: http://www.garanteprivacy.it/
Norway	Smittestop	**Datatilsynet** P.O. Box 458 Sentrum NO-0105 Oslo Tel + 22 39 69 64
Poland	ProteGO Safe	**The Bureau of the Inspector General for the Protection of Personal Data - GIODO** ul. Stawki 2 00-193 Warsaw Tel. +48 22 53 10 440 Fax +48 22 53 10 441 e-mail: kancelaria@giodo.gov.pl; desiwm@giodo.gov.pl Website: http://www.giodo.gov.pl/
Spain	Radar COVID	**Agencia de Protección de Datos** C/Jorge Juan, 6 28001 Madrid Tel. +34 91399 6200 Fax +34 91455 5699 e-mail: internacional@agpd.es Website: https://www.agpd.es/
EU	-	**European Data Protection Supervisor** Rue Wiertz 60 1047 Bruxelles/Brussel Office: Rue Montoyer 63, 6th floor Tel. +32 2 283 19 00 Fax +32 2 283 19 50 e-mail: edps@edps.europa.eu Website: http://www.edps.europa.eu/EDPSWEB/

Table 7: list of GDPR data authorities responsible for published Exposure Notification apps

Country	App Name	App Vendor
Austria	Stopp Corona	**Österreichisches Rotes Kreuz** e-mail: thomas.marecek@roteskreuz.at Website: https://www.roteskreuz.at/
Czech Republic	eRouška	**Ministerstvo zdravotnictví České republiky** e-mail: verejnost@mzcr.cz Website: http://www.mzcr.cz/
Denmark	smitte|stop	**Sundheds- og Ældreministeriet** e-mail: sum@sum.dk Website: https://sum.dk/
Finland	Ketju	**Futurize** e-mail: michael.samarin@futurice.com Website: https://futurice.com/ **Reaktor** Tel. +358 (0)9 4152 0200 Website: https://www.reaktor.com/
France	StopCovid	**Commission Nationale de l'Informatique et des Libertés - CNIL** Tel. +33 1 53 73 22 22 Website: http://www.cnil.fr/
Germany	Corona-Warn-App	**Robert Koch Institut** Website/Contact: https://www.rki.de/EN/Service/Contact/Contact_node.html
Hungary	VírusRadar	**Kormányzati Informatikai Fejlesztési Ügynökség** e-mail: ugyfelszolgalat@kifu.hu Website: https://kifu.gov.hu/
Italy	Immuni	**Ministero della Salute** Tel. +39 06 59941 Website: http://www.salute.gov.it/
Norway	Smittestop	**Folkehelseinstituttet** e-mail: Folkehelseinstituttet@fhi.no Website: https://www.fhi.no/
Poland	ProteGO Safe	**Ministerstwo Cyfryzacji** e-mail: mc@mc.gov.pl Website: https://www.gov.pl/web/cyfryzacja
Spain	Radar COVID	**Ministerio de Asuntos Económicos y Transf. Digital** Tel. +34 91 258 28 52 Website: https://www.mineco.gob.es

Table 8: list of contact tracing app vendors responsible for published Exposure Notification apps