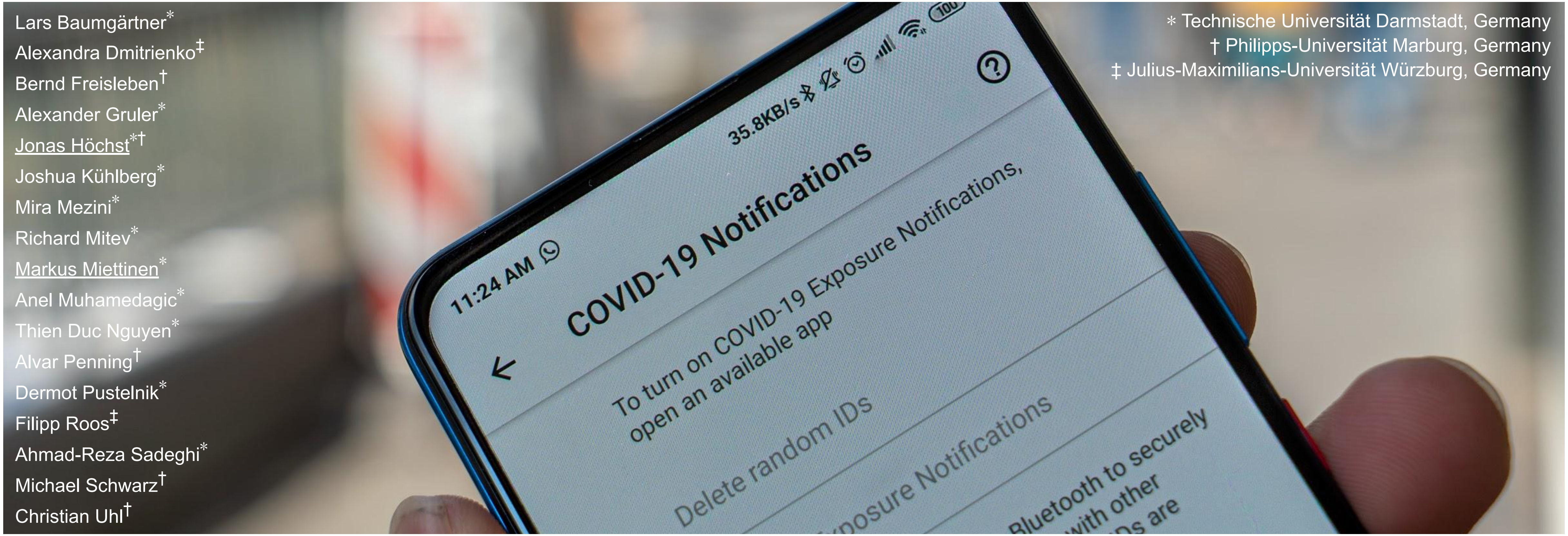
Mind the GAP:
Security & Privacy Risks of Contact Tracing Apps

IEEE TrustCom 2020



Lars Baumgärtner[*]
Alexandra Dmitrienko[‡]
Bernd Freisleben[†]
Alexander Gruler[*]
Jonas Höchst[*†]
Joshua Kühlberg[*]
Mira Mezini[*]
Richard Mitev[*]
Markus Miettinen[*]
Anel Muhamedagic[*]
Thien Duc Nguyen[*]
Alvar Penning[†]
Dermot Pustelnik[*]
Filipp Roos[‡]
Ahmad-Reza Sadeghi[*]
Michael Schwarz[†]
Christian Uhl[†]

∗ Technische Universität Darmstadt, Germany
† Philipps-Universität Marburg, Germany
‡ Julius-Maximilians-Universität Würzburg, Germany

Photo by Mika Baumeister on Unsplash

Introduction
Digital contact tracing apps in various countries

Manual vs. Digital

Global Position vs. Local Beaconing

Tracking vs. Tracing

Centralized vs. Decentralized

Base Technologies

OS Integration

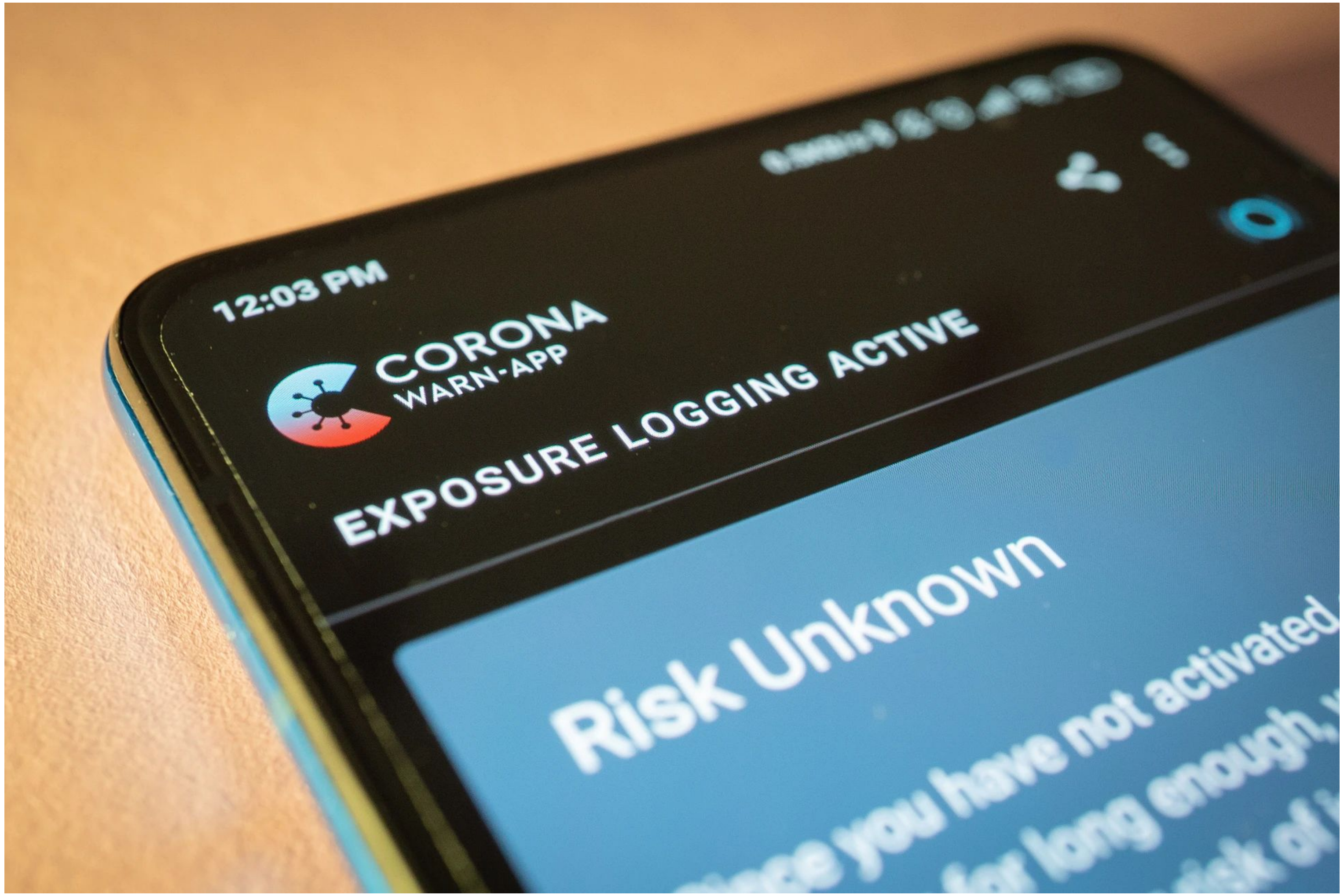


Photo by Mika Baumeister on Unsplash

GAP: Google's and Apple's Proposal for Contact Tracing

Joint effort for decentralized digital contract tracing

Contact tracing API to be used by state-specific applications

- Contact information remains in the API, hence is protected by OS security mechanisms
- Access to contact information only through specific functions

Decentralized approach

- Contact information stays on the device
- Personal infection state can be shared voluntarily after positive diagnosis
- Matching is based on a state-maintained public list

Academic discussion on GAP contact tracing

- Profiling attacks [14, 15]
- Relay attacks [14], [16]–[19]
- Theoretical attacks discussed in the literature, practical evaluation in this work

GAP: Overview

Basic concept of privacy-preserving contact tracing [29]

Temporary Exposure Keys (TEK)

- Independently generated (daily)

Rolling Proximity Identifier (RPI)

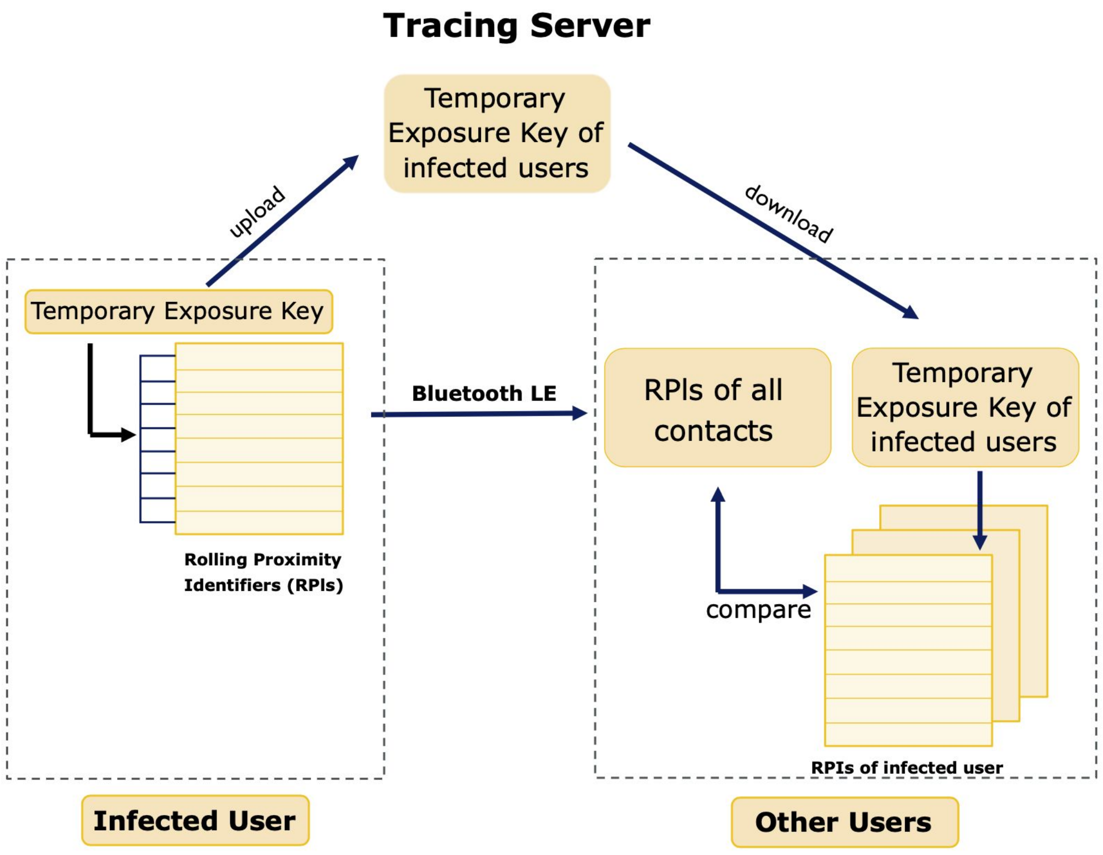
- Derived from TEK (every 10 minutes)
- Broadcasted continuously via Bluetooth LE
- Analogously other users receive and store surrounding RPIs

Infected user

- Shares TEKs of previous 14 days through the tracing server

Other users

- Download publicly available TEKs
- Derive corresponding RPIs
- Match against received RPIs



Overview of the GAP contact tracing approach

[29] Apple Inc, "Exposure Notification Bluetooth Specification v1.2"

Mind the Privacy GAP: Profiling Attacks

Conceptual vulnerability of GAP

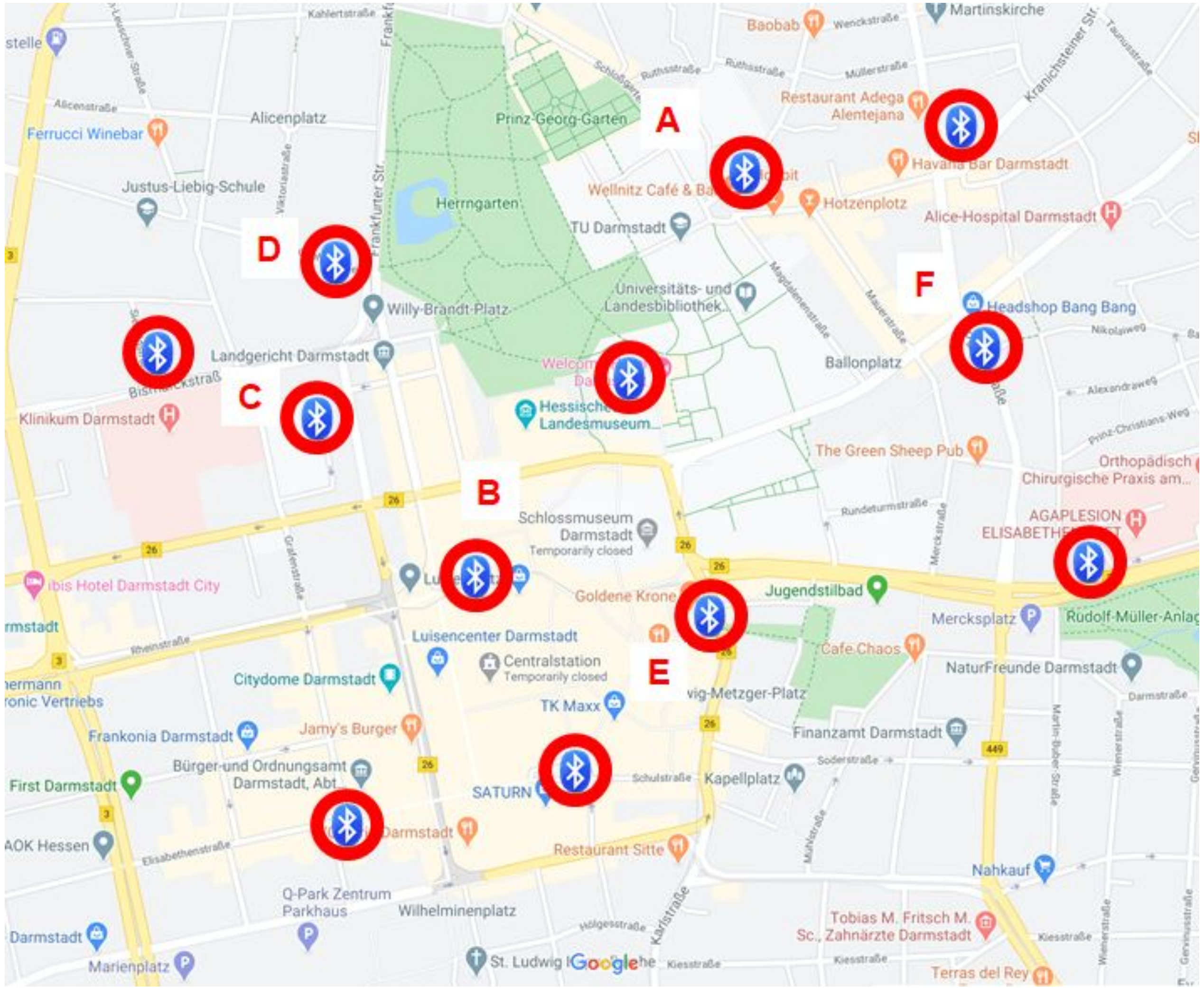
- TEKs are valid for 24 hours during which 144 RPIs are derived from a TEK (one every 10 minutes)
- All RPIs originating from same TEK are **trivially linkable** by all participants in the system **if TEK is known**
- Infected users are expected to **publish their TEKs** of the past 14 days in order to warn others

Attack scenario

- Adversary collects observations of RPIs emitted by tracing apps from a number of **strategically-chosen sensing points** in targeted area
- Using **published TEK information**, RPIs of infected users can be after-the-fact trivially **linked** with each other
- Adversary can thus construct **movement profiles** of infected users

Attack Setup

Strategically selected observation points in Darmstadt, Germany



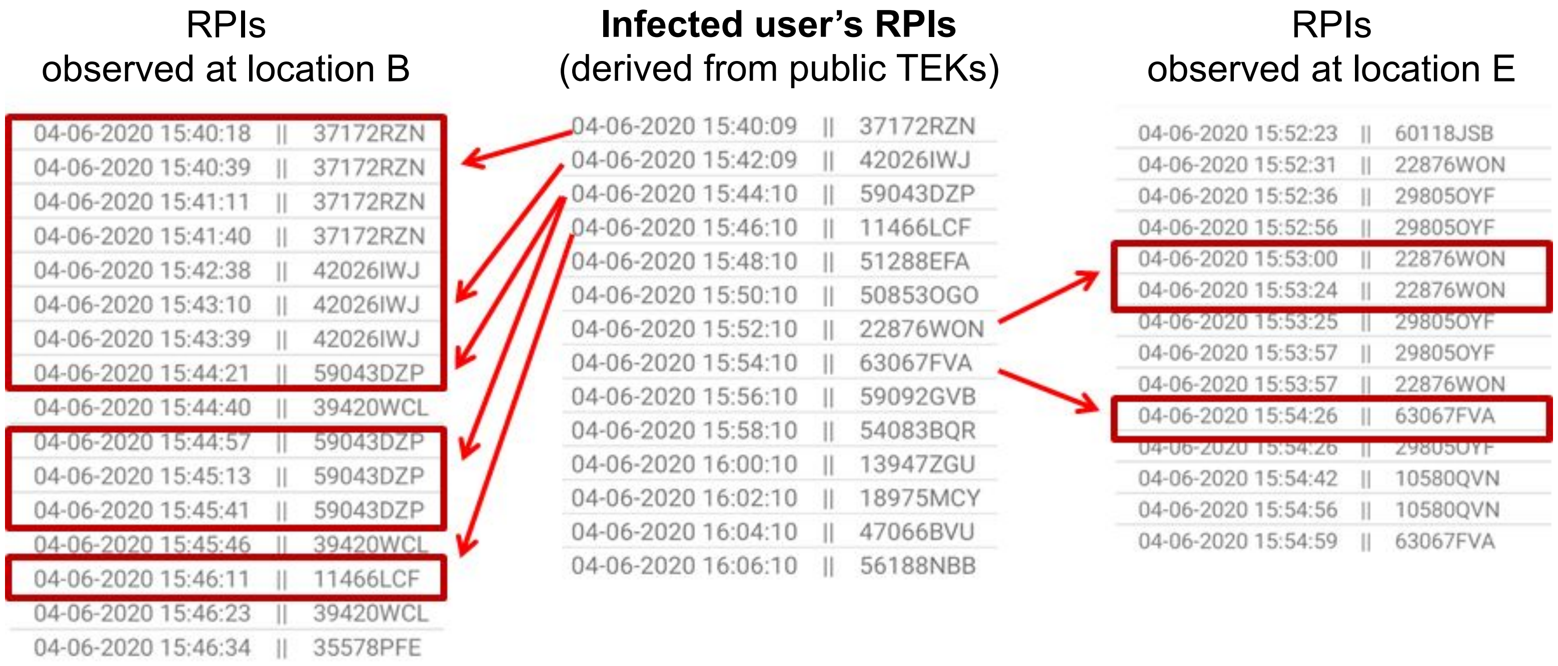
A	Residential area
B	City hall
C	Police station
D	Clinic and pharmacy
E	Outside a pub
F	Outside a head shop and a sports gambling bookmaker

Attack Execution

Observation points record tracing app RPIs emitted in their proximity

RPIs derived from published TEKs are cross-checked against RPI observations

- **Any visits** of infected users to observation points **can be identified** based on emitted RPIs



Identifying Movement Profiles

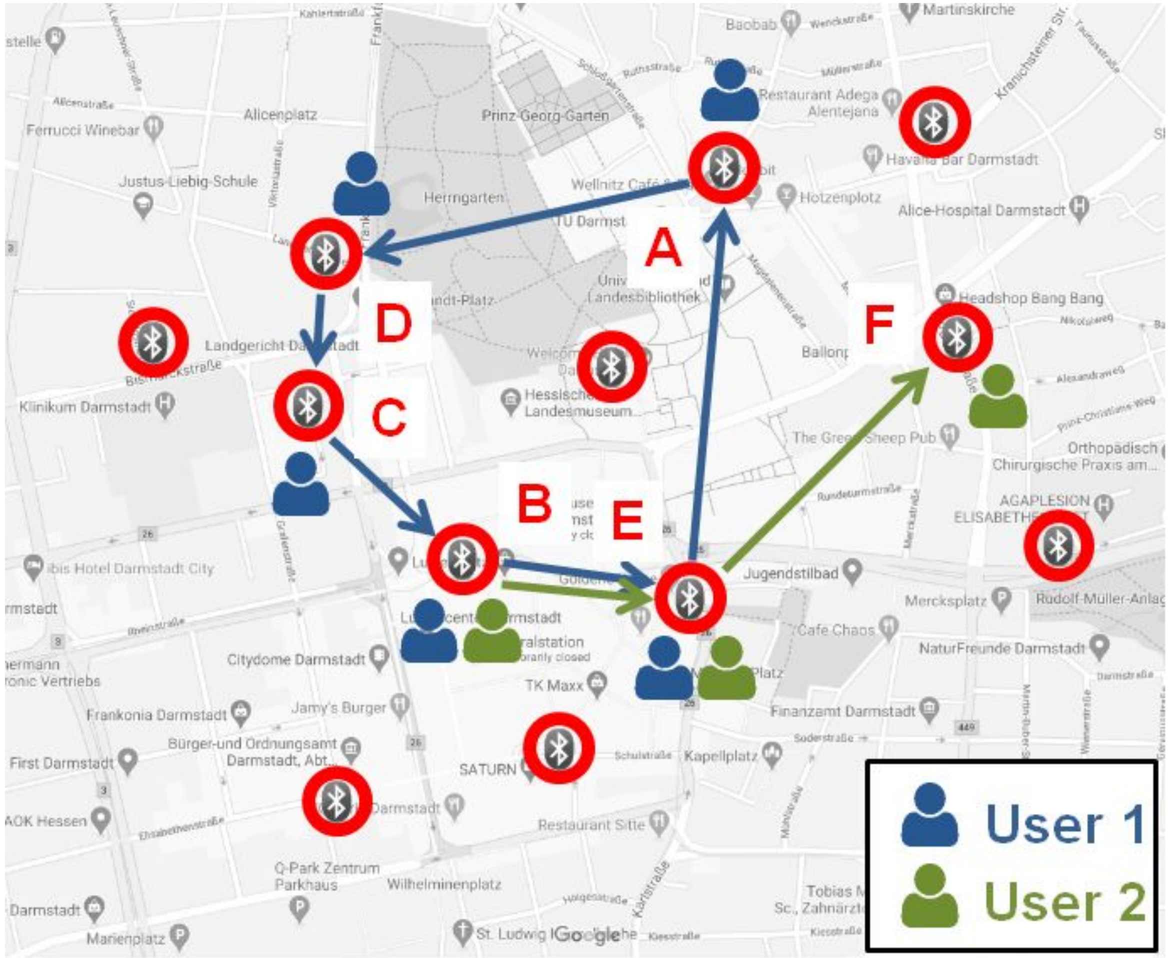
By linking RPI observations, **detailed movement profiles** of infected users can be constructed.

Movement profiles can reveal identifying information about users.

For example:

- Main point of presence during night times identifies person’s likely **home address**
- Main point of presence during working hours identifies likely **workplace**

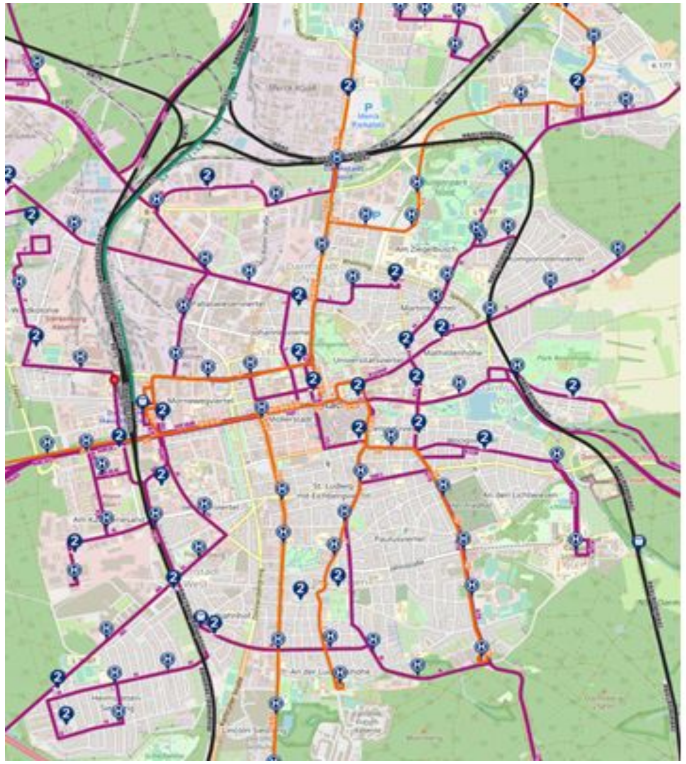
Given sufficient movement profile information potentially allows us to **completely de-anonymize** infected users.



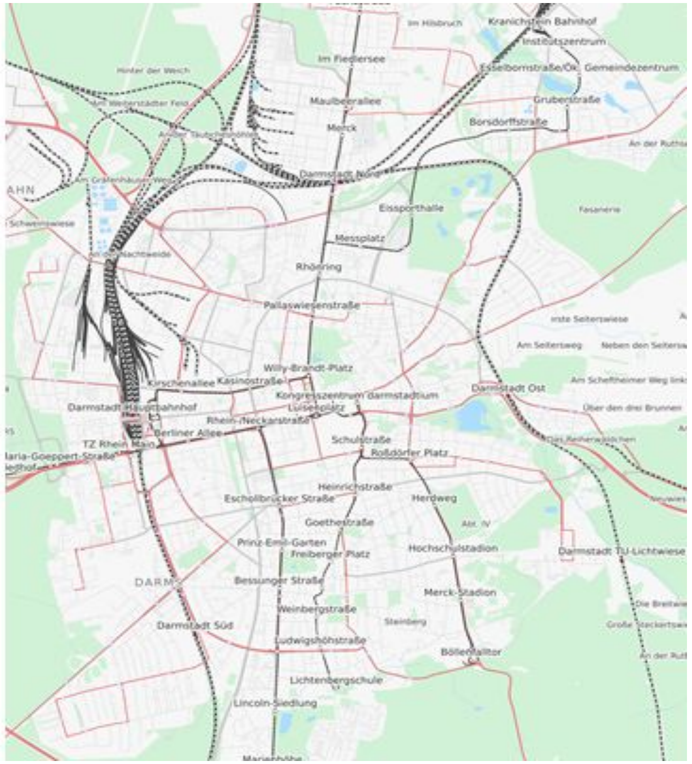
Surveillance Case Study: Darmstadt, Germany

How many sensing points would be necessary to cover a majority of movement profiles in a city of ca. 160 000 inhabitants and an area of ca. 122 km²?

Main transport routes in Darmstadt



Train, tram and bus line network

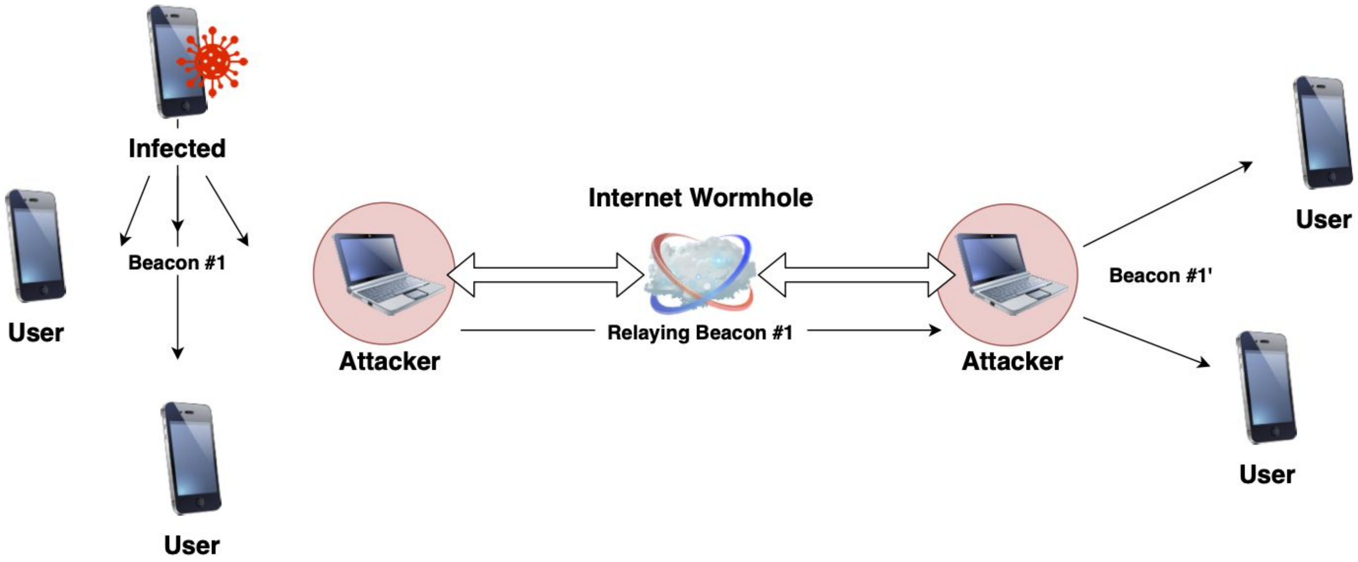


Main roads (cars & railways)

Transport system	**Sensing stations needed**
Trams	25
Buses	60-80
Railways	60
Car traffic	200-250
Pedestrians	50
Total	**395 - 465**

Mind the Security GAP: Wormhole attacks on Bluetooth beaconing

- **Replay attack:** Record BLE signal at location A, replay at other location
  - Countermeasure: limit validity period of BLE signal / introduce handshake
- **Relay attack:** Satisfy domain-specific real-time requirements
  - 10-minute RPI validity period in GAP
- **Wormhole attack:** Link physical locations and forward BLE signals in between these locations
  - Combination of replay and relay



Wormhole attack setup to relay BLE beacons

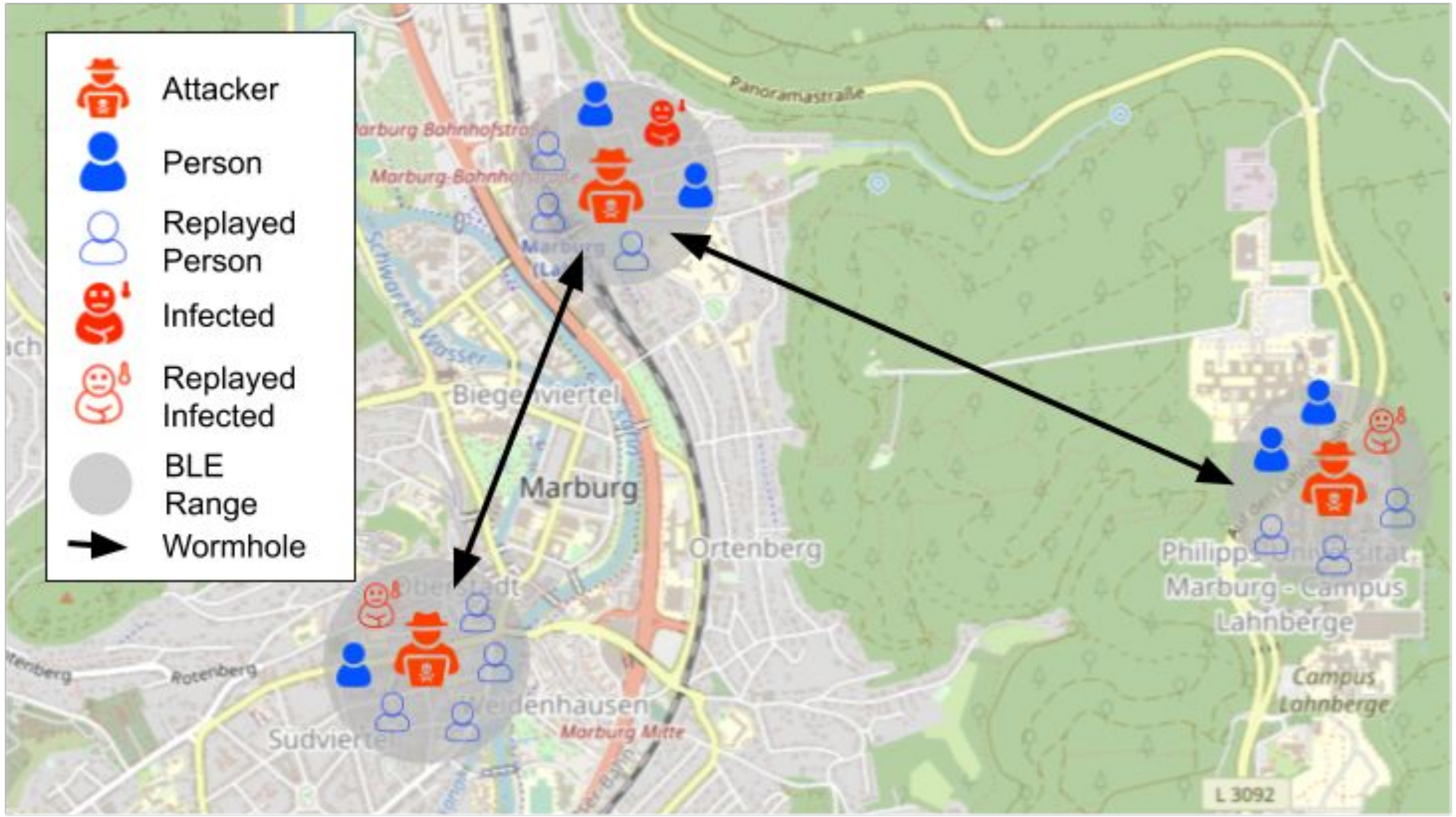
Wormhole Attack: Experiment 1

Devices and setup

Raspberry Pi-based wormhole receivers distributed at multiple locations:

1. Receive Bluetooth beacons
2. Send beacons to central server
3. Query server for new beacons and redistribute at own location

Tests conducted with DP-3T sample app.



Wormhole attack in the city of Marburg

Wormhole Attack: Experiment 1

Devices and setup: server logs

Raspberry Pi-based wormhole receivers distributed at multiple locations:

1. Receive Bluetooth beacons
2. Send beacons to central server
3. Query server for new beacons and redistribute at own location

Tests conducted with DP-3T sample app.

```
1 Jun 09 20:45:13 wormpi-mr wormhole[472]: [provider    ] [
      INFO] [in ] [7E:09:47:A6:EE:7F] [Dp3t_ScanRequest]
      fd68
2 Jun 09 20:45:13 wormpi-mr wormhole[472]: [wormhole-out] [
      INFO] [7E:09:47:A6:EE:7F]       [Dp3t_ScanRequest]
      fd68
3 Jun 09 20:45:13 wormpi-mr wormhole[472]: [wormhole-in ] [
      INFO] [5A:A2:81:40:7A:B3]       [Dp3t_ScanResponse]
      fd68 6d:72:34:32:30:80:1d:62:d7:c9:ff:d0:71:a3:37:b0
4 Jun 09 20:45:13 wormpi-mr wormhole[472]: [provider    ] [
      INFO] [out] [5A:A2:81:40:7A:B3] [Dp3t_ScanResponse]
      fd68 6d:72:34:32:30:80:1d:62:d7:c9:ff:d0:71:a3:37:b0
```

Raspberry Pi with our wormhole implementation

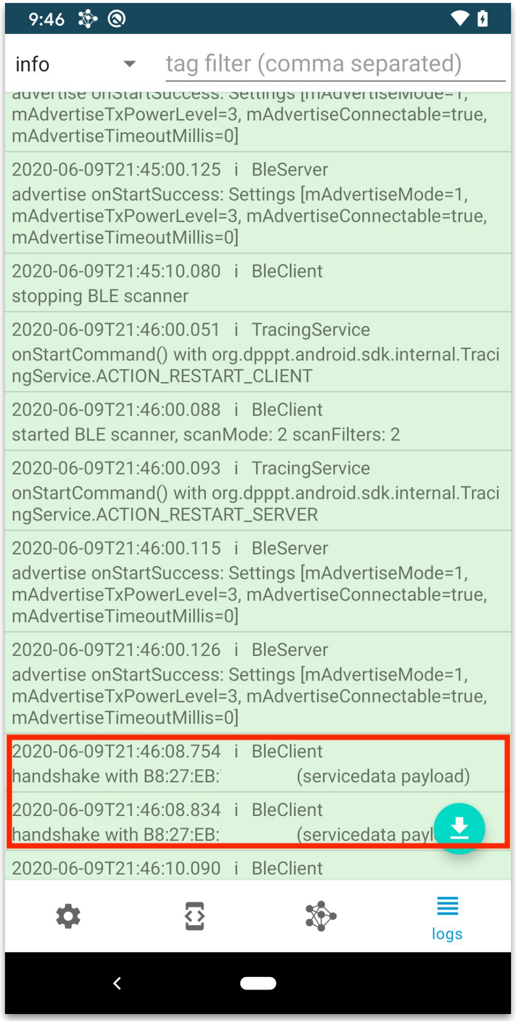
Wormhole Attack: Experiment 1

Devices and setup: successful RPI wormholing

DP-3T prestandard SampleApp instances with confirmed beacons transmitted through the wormhole "wormpi"

a) **Android:** handshake conducted with MAC address of wormhole device (Raspberry Pi)

b) **iOS:** confirms receipt of a beacon with the manually set ephemeral ID of "mr42"



Wormhole Attack: Experiment 2

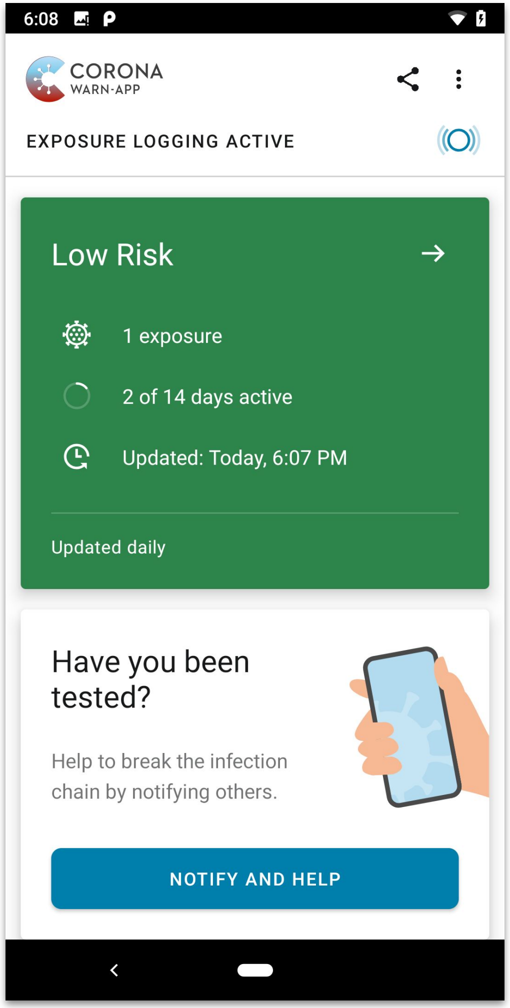
Validation with GAP and the German “Corona-Warn-App”

Access to the GAP API is restricted:

- Impossible to access the API without being *whitelisted* by Google / Apple
- Whitelisting only for one Government approved institution per country

Using real-world TEKs

- Download list of “positive” TEKs from official server
- Derive RPIs from a TEK
- Block access to the official server for our test device
- Set the system time to the time in which an RPI was valid
- Install and activate the official Corona-Warn-App
- Send the RPIs (together with valid metadata) using our wormhole
- After ~ 10 - 15 min:
  - Reset the date/time
  - Unblock access to the server and force the app to download the list
- => The app will then trigger a warning



Exposure Notification Wormholing

Technical limitations: basic considerations

Beacons according to the Bluetooth LE standard

- Transmission speed up to 1 Mbps
- GAP payload size of 26 bytes [29]
  - Advertisement size of 39 bytes [28]
  - Packet data unit size of 47 bytes
  - Airtime of 376 µs + inter-frame space of 150 µs
- 10^6µs / (376µs + 150µs) = **1,901 packets/s**

Real-world factors

- Receivers hop between three Bluetooth announcement channels
- Connection intervals forced by device vendors
- Receiver / sender distance and transmission power
- Interferences and collisions


Bluetooth®

Bluetooth Core Specification

Bluetooth® Specification

- Revision: v5.2
- Revision Date: 2019-12-31
- Group Prepared By: Core Specification Working Group
- Feedback Email: core-main@bluetooth.org

Abstract:
This specification defines the technologies required to create interoperable Bluetooth devices.

Bluetooth SIG Proprietary

[28] Bluetooth Special Interest Group (SIG), “Bluetooth Core Specification 5.2”
[29] Apple Inc, “Exposure Notification Bluetooth Specification v1.2”

Exposure Notification Wormholing

Technical limitations: practical evaluation

Experimental Evaluation

- HackRF One (sender & receiver)
- Raspberry Pi (receiver)
- Surrounding WiFi and BLE device for disruptions
- **4.3% of theoretical maximum achieved: 82 packets/s**

Findings

- Bluetooth / host communication batched, scheduled in 2 second windows
- Stable tests in 10 meter range, up to 50 meter enhanced range when using hardware amplification

Exposure Notification Wormholing

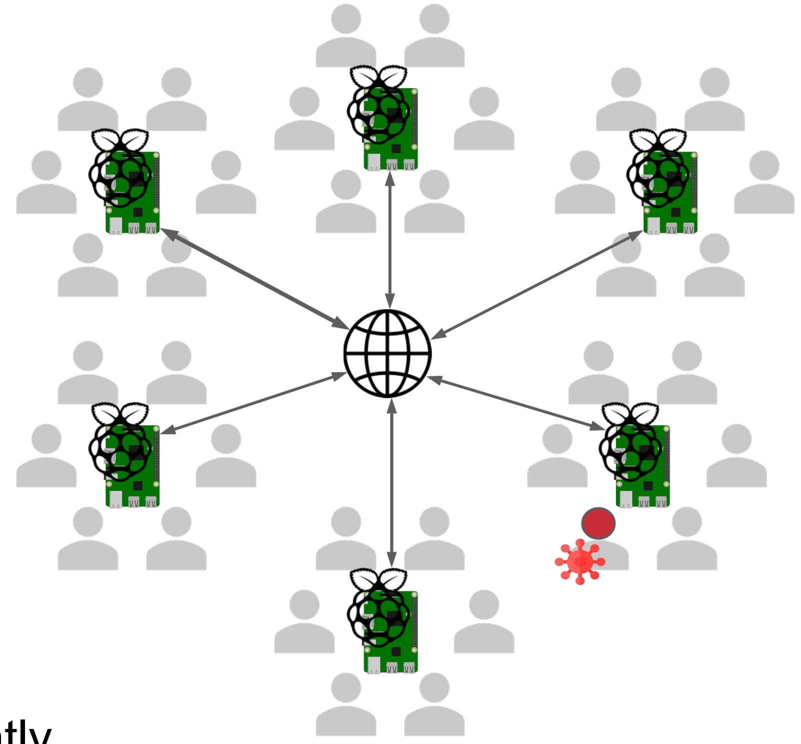
Attack scenario: opportunistic linking (1)

Idea:

- Bridging multiple high traffic locations with wormholes
- Increasing the impact of later positively reported beacons
- Getting at least one positive advertisement each 10 minutes

Parameters:

- **5.1** infections per 100.000 (Germany, week 32 of 2020)
- **30.43** unique BLE advertisements per minute
  - Obtained by field study at Central Train Station in Frankfurt, Germany



Results:

- On avg., **1 per 9,804 RPIs** will be positive
- => **65 wormhole devices** to have on avg. one positive RPI constantly
- High-risk warning requires contacts for over 10 minutes

Exposure Notification Wormholing

Attack scenario: opportunistic linking (1)

Idea:

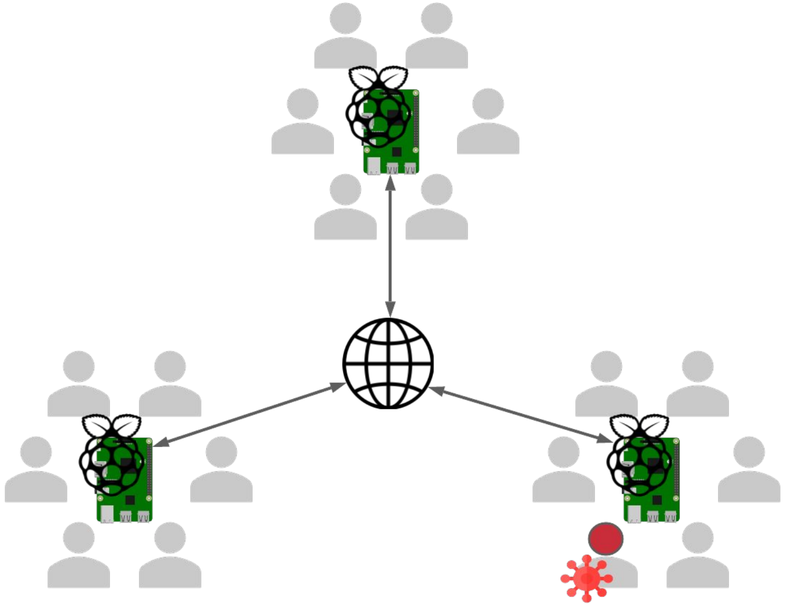
- Bridging multiple high traffic locations with wormholes
- Increasing the impact of later positively reported beacons
- Getting at least one positive advertisement each 10 minutes

Parameters:

- **45.4** infections per 100.000 (Germany, week 42 of 2020)
- **30.43** unique BLE advertisements per minute
  - Obtained by field study at Central Train Station in Frankfurt, Germany

Results:

- On avg., **1 per 1,101 RPIs** will be positive
- => **8 wormhole devices** to have on avg. one positive RPI constantly
- Still relatively high load for the system to handle



Exposure Notification Wormholing

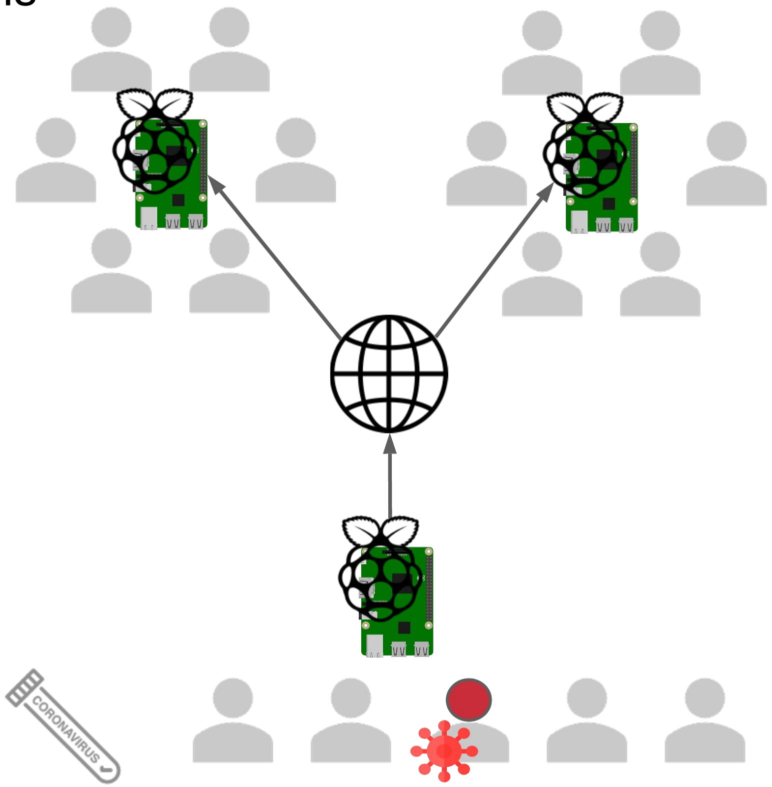
Attack scenario: opportunistic linking with high infection probability

Idea:

- Bridging a location with a high infection probability with other locations
- Getting at least one positive advertisement each 10 minutes

Parameters:

- **300** unique beacons per hour
  - Obtained from a local testing facility near Frankfurt, Germany
- **9.84%** of infected persons share their infection status using the app
  - Based on submitted TEKs in correlation to overall infections in week 41 and 42, 2020 in Germany
- **3.62%** positive test rate (Germany, week 42 of 2020)



Results:

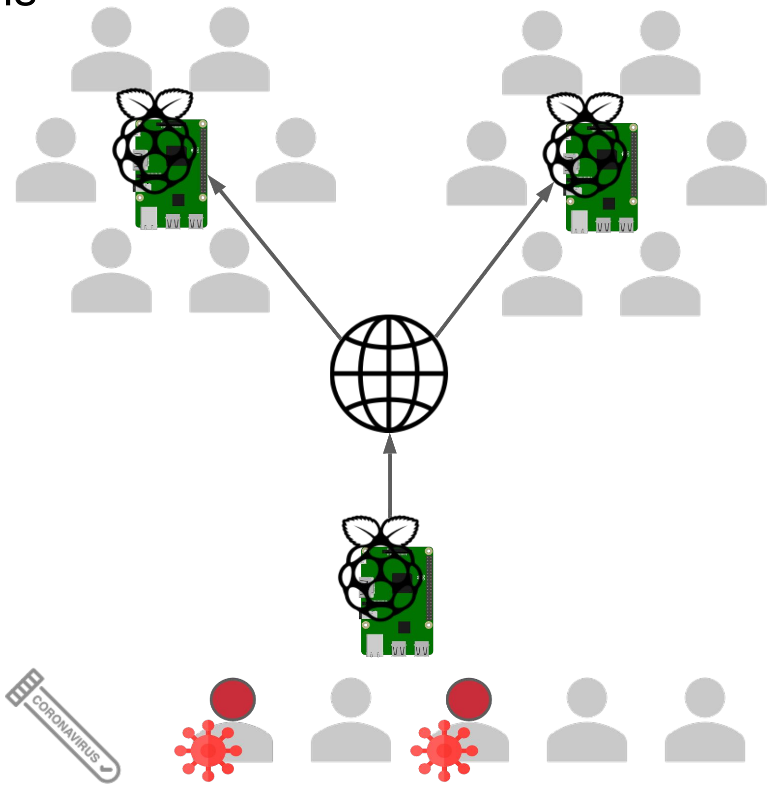
- **1.07** positive RPIs per hour
- **Limited effect** with one test center, **better scalability** due to relatively low number of total RPIs.

Exposure Notification Wormholing
Attack scenario: opportunistic linking with high infection probability

Idea:
- Bridging a location with a high infection probability with other locations
- Getting at least one positive advertisement each 10 minutes

Parameters:


- **300** unique beacons per hour
  - Obtained from a local testing facility near Frankfurt, Germany
- **9.84%** of infected persons share their infection status using the app
  - Based on submitted TEKs in correlation to overall infections in week 41 and 42, 2020 in Germany
- **41%** positive test rate (Mexico, October of 2020)



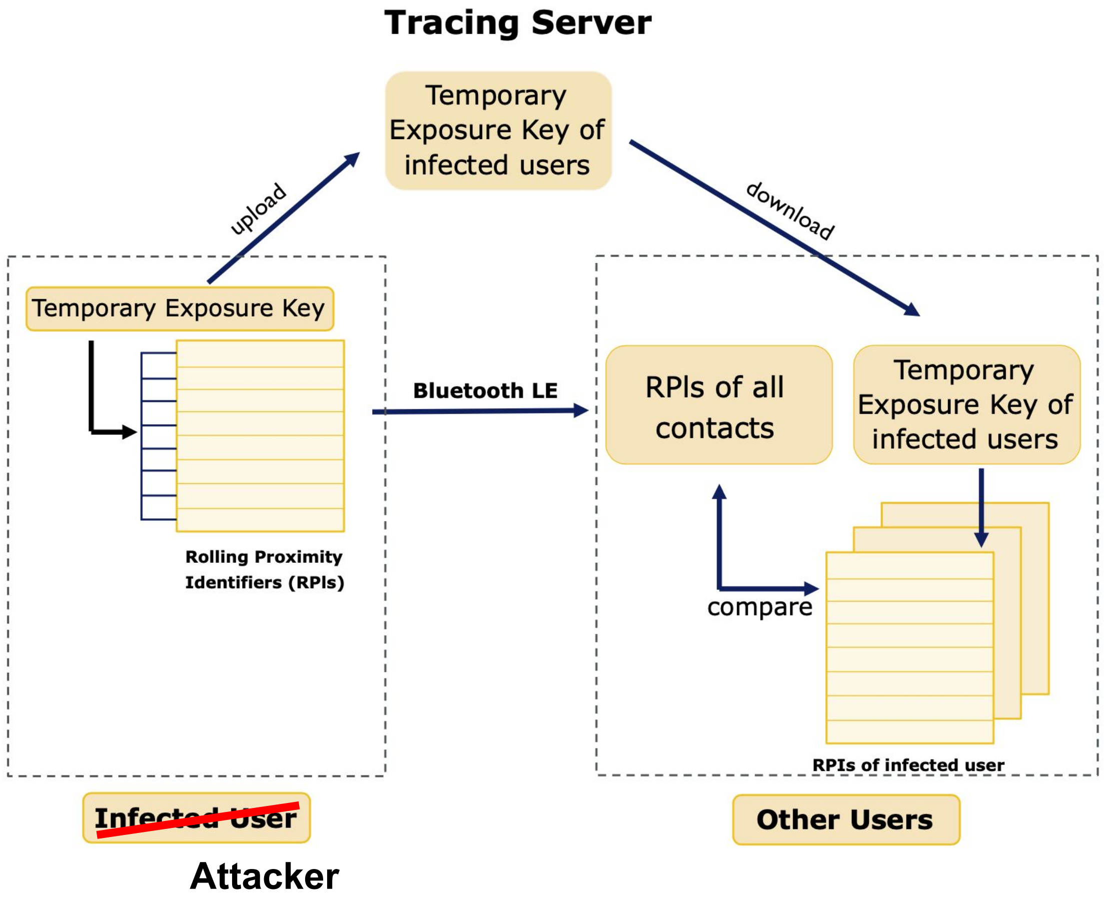
Results:
- **12.10** positive RPIs per hour
- **Reduced attacker effort**, good scalability properties, effectively allowing the attacker to invalidate the app for reached users.

Exposure Notification Wormholing
Attack scenario: targeted attack

Idea:
- Flood own beacons to as many people as possible
- Upload own key by using a valid TAN of a (fake) infection to the official servers

Parameters:
- **825** contacts per hour per wormhole (based on field study)
- Submitting for **14 days**, 12 hours per day
- High traffic location (e.g., train station)

Results:
- **306.600** registered, positive RPIs
- **High-risk warnings** for users if targeted > 10 minutes



Conclusion

Demonstration of theoretical vulnerabilities:

- Profiling and possibly de-anonymizing infected persons
- Relay-based wormhole attacks to generate fake contacts that may affect the accuracy of GAP-based contact tracing apps
- Evaluated with DP-3T development app and German Corona-Warn-App, applicable to all GAP-based apps

Countermeasures:

- Increase TEK rollovers to limit de-anonymization
- Reduce 2 hour RPI validity period to reduce impact of wormhole attack [29]
- Validate time and location of received RPIs by additional metadata
- Revise protocol to include a handshake mechanism [25]

Questions?

- Questions now @TrustCom
- Offline via mail: hoechst@informatik.uni-marburg.de

[25] ConTra Corona: Contact Tracing against the Coronavirus by Bridging the Centralized–Decentralized Divide for Stronger Privacy
[29] Exposure Notification Bluetooth Specification v1.2

References

[1] I. Braithwaite, T. Callender, M. Bullock, and R. W. Aldridge, “Automated and Partly Automated Contact Tracing: A Systematic Review to Inform the Control of COVID-19,” The Lancet Digital Health, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/ pii/S2589750020301849

[2] M. Miettinen, T. D. Nguyen, and A.-R. Sadeghi, “Comparison of Tracing Approaches,” https://tracecorona.net/comparison-of-tracing-approaches/.

[3] R. Raskar, I. Schunemann, R. Barbar, K. Vilcans, J. Gray, P. Vepakomma, S. Kapa, A. Nuzzo, R. Gupta, A. Berke, D. Greenwood, C. Keegan, S. Kanaparti, R. Beaudry, D. Stansbury, B. B. Arcila, R. Kanaparti, V. Pamplona, F. B. and| Alina Clough, R. Das, K. J. K. Louisy, G. Nadeau, S. Penrod, Y. Rajaee, A. Singh, G. Storm, and J. Werner, “Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic,” https://arxiv.org/pdf/2003.08567.pdf.

[4] Government of India, “Aarogya Setu Mobile App,” https://www.mygov.in/aarogyasetuapp/.

[5] K. Merry and P. Bettinger, “Smartphone GPS Accuracy Study in an Urban Environment,” PLOS ONE, vol. 14, no. 7, pp. 1–19, 07 2019. [Online]. Available: https://doi.org/10.1371/journal.pone.0219890

[6] D. J. Leith and S. Farrell, “Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection,” CoRR, vol. abs/2006.06822, 2020. [Online]. Available: https://arxiv.org/abs/2006.06822

[7] ——, “Measurement-Based Evaluation Of Google/Apple Exposure Notification API For Proximity Detection in a Commuter Bus,” CoRR, vol. abs/2006.08543, 2020. [Online]. Available: https://arxiv.org/abs/ 2006.08543

[8] ——, “Measurement-based Evaluation of Google/Apple Exposure Notification API for Proximity Detection in a Lightrail Tram,” PLOS ONE, vol. 15, no. 9, pp. 1–16, 09 2020. [Online]. Available: https://doi.org/10.1371/journal.pone.0239943

[9] Government of Singapore, Ministry of Health, “TraceTogether Contact Tracing App,” https://www.tracetogether.gov.sg/.

[10] Australian Government, Department of Health, “CovidSafe Contact Tracing App,” https://www.health.gov.au/resources/apps-and-tools/ covidsafeapp.

[11] Pan-European Privacy-Preserving Proximity Tracing Consortium, “Documentation for Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT),” https://github.com/pepp-pt/pepp-pt-documentation.

[12] Government of France, “StopCovid France,” https://www.economie.gouv.fr/stopcovid.

[13] Apple and Google, “Exposure Notification: Cryptography Specification, v1.2,” April 2020, https://www.apple.com/covid19/contacttracing.

[14] J. Chan, S. Gollakota, E. Horvitz, J. Jaeger, S. Kakade, T. Kohno, J. Langford, J. Larson, S. Singanamalla, J. Sunshine et al., “PACT: Privacy-Sensitive Protocols And Mechanisms for Mobile Contact Tracing,” arXiv preprint arXiv:2004.03544, April 2020.

[15] Y. Gvili, “Security Analysis of the COVID-19 Contact Tracing Specifications by Apple Inc. and Google Inc.” Cryptology ePrint Archive, Report 2020/428, April 2020, https://eprint.iacr.org/2020/428.

[16] e-Health Network, “Mobile Applications to Support Contact Tracing in the EU’s Fight Against COVID-19,” 2020. [Online]. Available: https:// ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

[17] S. Vaudenay, “Analysis of DP-3T,” Cryptology ePrint Archive, Report 2020/399, April 2020, https://eprint.iacr.org/2020/399.

[18] ——, “Centralized or Decentralized? The Contact Tracing Dilemma,” Cryptology ePrint Archive, Report 2020/531, May 2020, https://eprint. iacr.org/2020/531.

[19] K. Pietrzak, “Delayed Authentication: Preventing Replay and Relay Attacks in Private Contact Tracing,” Cryptology ePrint Archive, Report 2020/418, April 2020, https://eprint.iacr.org/2020/418.

[20] S. Ji, W. Li, P. Mittal, X. Hu, and R. Beyah, “SecGraph: A Uniform and Open-source Evaluation System for Graph Data Anonymization and De-anonymization,” in 24th USENIX Security Symposium, Washington, D.C., 2015, pp. 303–318.

[21] L. Radaelli, P. Sapiezynski, F. Houssiau, E. Shmueli, and Y. de Montjoye, “Quantifying Surveillance in the Networked Age: Node-based Intrusions and Group Privacy,” CoRR abs/1803.09007, August 2018, http://arxiv.org/abs/1803.09007.

[22] Apple Inc, “Exposure Notification Addendum,” https://developer.apple.com/contact/request/download/Exposure_Notification_Addendum.pdf.

[23] Decentralized Privacy-Preserving Proximity Tracing (DP-3T), “Security and Privacy Analysis of the Document "PEPP-PT: Data Protection and Information Security Architecture",” 2020, https://github.com/DP- 3T/documents.

[24] Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), “Data Protection and Security Architecture: Illustrated on the German Implementation,” 2020, https://github.com/pepp-pt/pepp-pt-documentation.

[25] W. Beskorovajnov, F. Dörre, G. Hartung, A. Koch, J. Müller-Quade, and T. Strufe, “ConTra Corona: Contact Tracing against the Coronavirus by Bridging the Centralized–Decentralized Divide for Stronger Privacy,” Cryptology ePrint Archive, Report 2020/505, April 2020, https://eprint.iacr.org/2020/505.

[26] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Wormhole Attacks in Wireless Networks,” IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370–380, 2006.

[27] J. Höchst, A. Penning, P. Lampe, and B. Freisleben,“PIMOD: A Tool for Configuring Single-Board Computer Operating System Images,” in 2020 IEEE Global Humanitarian Technology Conference (GHTC) (GHTC 2020), Seattle, USA, Oct. 2020.

[28] Bluetooth Special Interest Group (SIG), “Bluetooth Core Specification 5.2,” https://www.bluetooth.com/specifications/bluetooth-corespecification/.

[29] Apple Inc, “Exposure Notification Bluetooth Specification v1.2,” https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotificatio n-BluetoothSpecificationv1.2.pdf.