German Corona-Warn-App: Lessons learned and why we need to replace it!

Ahmad-Reza Sadeghi Cybersecurity & Privacy Research Centre, TU Darmstadt, Germany

World View of Contact Tracing



World View of Contact Tracing



World View of Contact Tracing





• **Goal:** efficiently and quickly detect and interrupt infection chains



- **Goal:** efficiently and quickly detect and interrupt infection chains
- **Technology:** based on Google & Apple exposure notification (GAEN)



- **Goal:** efficiently and quickly detect and interrupt infection chains
- Technology: based on Google & Apple exposure notification (GAEN)
- Number of downloads > 20 millions



- **Goal:** efficiently and quickly detect and interrupt infection chains
- Technology: based on Google & Apple exposure notification (GAEN)
- Number of downloads > 20 millions
- **Costs:** 68 million Euros by the end of 2021, 20 million Euro for app development



Google & Apple Exposure Notification (Dystopia?)

Security and Privacy Attacks on GAEN

Security and Privacy Attacks on GAEN

| 12 | |
|---|-----|
| Decentralized? | |
| teplized or Decent | |
| Centraine + Tracing Dilemm | |
| The Contact II | |
| Inc | |
| Serge Vaudenay | |
| 2020, May 600 | |
| Switzerland | |
| EPFL, Lausan | |
| Abstract. The COVID-19 pandomic created a and/crable challenge to the cryptogrammen assignment with the de-dogment of contact turcing applications. The median property PT and the projection, the property of the strength of the strength of the projection of the strength of the streng | la |
| The freedom of peop | oit |
| duction de Great Lockdown. The | 170 |
| Introduced In the Gran As a result, analog and to impression of the second to impression of the second to impression of the second terms and the second terms and the second terms and the second terms are second to impression of the second terms and the second terms are second to impression of terms are second to | 1 |
| the hostages of a virus more pro- | |
| The 2020 part have been one on the spice would let people | |
| and the cost automated toor After all, such a toor Many aca | |
| aupport human factoring economies and tool in the | |
| and the lock-down, restored to develop such o | |
| end domains onered | |
| running on smartputact tracing is to | |
| The goal of contain | |

Security and Privacy of Decentralized **Cryptographic Contact Tracing**

Noel Danz, Oliver Derwisch, Anja Lehmann^{*}, Wenzel Puenter, Marvin Stolle, and Joshua Ziemann

Hasso-Plattner-Institute, University of Potsdam

Abstract. Automated contact tracing leverages the ubiquity of smartphones to warn users about an increased exposure risk to COVID-19. In the course of only a few weeks, several cryptographic protocols have been proposed that aim to achieve such contract tracing in a decentralized and privacy-preserving way. Roughly, they let users' phones exchange random looking pseudonyms that are derived from locally stored keys If a user is diagnosed, her phone uploads the keys which allows othe users to check for any contact matches. Ultimately this line of work l to Google and Apple including a variant of these protocols into th phones which is currently used by millions of users. Due to the ob ous urgency, these schemes were pushed to deployment without a form analysis of the achieved security and privacy features. In this work address this gap and provide the first formal treatment of such de tralized cryptographic contact tracing. We formally define three properties in a game-based manner: pseudonym and trace u to guarantee the privacy of users during healthy at and *integrity* ensuring that triggering false. A particular focus of our work is or as both keys and pseudony

On the Effectiveness of Time Travel to Inject COVID-19 Alerts*

Vincenzo Iovino¹, Serge Vaudenay², and Martin Vuagnoux³

¹ University of Salerno, Italy ² EPFL, Lausanne, Switzerland base23, Geneva, Switzerland

Abstract. Digital contact tracing apps allow to akert people who have been in contact with Abstract. Dubial contact tracing apps above to akert people who have been in contact with people who may be contagious. The Apple/Coogle Exposure Notification (EN) system is based people was may be contagons. In: Apply/Loogie Exposure Northeston (EN) system is based on Bisecooth provinsity estimation. It has been adopted by many countries around the world. on lineatouth proximity estimation. It has been anopted to many countries around the versus Rowever, many possible attacks are known. The goal of some of them is to inject a faile after However, many possible attacks are known. The goal of some of them is to inject a take alert on someone class's plone. This way, an adversary can eliminate a competitor in a sport event or on sourcease search prome, this way, an adversary can summane a competition a business in general. Political parties can also prevent people from volting. a manness in general. Political partnes can also prevent people from votage. In this report, we review several methods to inject false alerts. One of them requires to corrupt In tan report, we review several methods to meet take acers. One of them requires to corrupt the clock of the anartphone of the victim. For that, we build a time-traveling machine to be a several se the clock of the mariphone of the vierus. For that, we built a time-traveling machine to be able to removed, set up the clock on a smartphone and experiment our statick. We show how and to remotely set up the clock on a marphone and experiment our attack. We show how easy this can be done. We successfully tested several smartphones with either the Swiss or the

1 Introduction

Apple and Google deployed together the Exposure Notification (EN or GAEN) system as a Appe and Google deployed together the Exposure Notification (EN or GAEN) system as a tool to fight the pandemic [1]. The goal of an EN-based app is to alert people who have been in almost productive for the United States and the St toot to ngnt the pandemic [2]. The goal of an EX-based app is to alert people who have been in close proximity for long enough with someone who was positively tested with COVID-10 and who volunteered to report. How a user responds to such alert is up to the would expect that such user would contact authorities and bedays. In Switzerland, the alerted user is eligible to have of the test would not change his quarantine star EN is provided by default in all rec

Security and Privacy Attacks on GAEN

Centralized or Decentralized? The Contact Tracing Dilemma Serge Vaudenay 2020, May 6th EPFL, Lausanne, Switzerland Abstract. The COVID-19 pandemic created a noticeable challenge to the cryptographic whither, the COVID-19 participate creases a not recover ensures of the development of contact tracing applications. The used a report sing a centralized or a decentralized solution Exposure Notification System May Allow for Large-Scale Voter Suppression Rosario Gennaro, Adam Krellenstein! James Krellenstein[†] Exposure Notification is a system designed by Goode and Apple ("GAEN", in the followine) for marine individuals when their bare bare encount in a Superior Notification is a system designed by Google and Apple ("GAEN", "the following, for molifying, individuals when they have been expended to BASC/N-2 be remained to resource only accurate above to restrict resource conin the following) for multipling individuals when they have been exposed to SARS-CoV-2 by coming in contact with concern who has total positive for the sime? It is also device its the "heteroid decoursiloud constituter reason" 1 Introduction SARSCOV2 by coming in consist with someone who has tested positive for the struct by a deady related to the "deard dearnational processing resonance (10).576 the virus.¹ It is choosy related to the "loyled decentrational proximity tracing, (pp. 57) Protocol from the Decentralized Prime-Preserving Primity Tracing, (pp. 57) Prime-Primeprotocol from the Decentralized Privacy-Preserving Prozentials Tracing (DPA) project2 GAEN is intended to be a minimulation and privacy-preserving system for extended companying companying and an end of the privacy preserving system. project-2 GAEN is intended to be a minimulatic and privacy-preserving evad-for automated automatical coposate coefficients, to complement automatical for automatical automatical evaluation and highly evaluation. In this document we a for automated anonymized exposure nutifications, to complement narrand conta-tucing effects in an efficient and highly exalting the bahim. In this document, we ad distantiate specificity between CANS and TRUST become of their specific tracing efforts in an efficient and highly available fashion. In this document, we will difficult antefally between GAES and DP-37 because of their similar of the Foreigner Neutronics and the documentation for the trace areas and The Foreigner Neutronics and the documentation for the trace areas vi distinguish extedity between GAEX and DP-3T iscense of their similar The Expressive Notification system is characterized by its strong empiric transmission the automation of automatic of moments and and the strong manifestion intermediate the section of automatic of moments and and the strong manifestion. The Esspance Notification system is characterized by its strong empiri-on preserving the privacy and anotenity of seers, and and the strict equation before on the responsible for above economication memory-acted data evaluation on preserving the privacy and anonymity of users, and and the article language of the second se places on the potential for abuse comprising unamburized data collection uses surrellinare. Within GAEN, no user-dentifying data is ever upon to the second nons surveillance. Within GAEN, no user-identifying data is ever us, to the central server: users establish their proximiting exclusively serve-and surveillance with the sub-concentration of branches shadow transients. to the central server; users establish their products esclusively and aurogeously, with the sale purpose of howing whether they produce only on industant other mean track is a track of the track. and anonymously, with the size purpose of knowing spical contact with an individual who may later be deemed to be untact with an mouringai who may later be deed. The design choices of the protocols in questi-The design choices of the protocols i against data collection attacks, unfortunat agamise onto concernor association tible to data injection by malici

Security and Privacy of Decentralized **Cryptographic Contact Tracing**

Noel Danz, Oliver Derwisch, Anja Lehmann^{*}, Wenzel Puenter, Marvin Stolle, and Joshua Ziemann

Hasso-Plattner-Institute, University of Potsdam

Abstract. Automated contact tracing leverages the ubiquity of smartphones to warn users about an increased exposure risk to COVID-19. In of only a few weeks, several cryptographic p

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

Lars Baumgärtner*, Alexandra Dmitrienko[‡], Bernd Freisleben[†], Alexander Gruler, Jonas Höchst*[†], Joshua Kühlberg*, Mira Mezini*, Richard Mitev*, Markus Miettinen*, Anel Muhamedagic*, Thien Duc Nguy Alvar Penning[†], Dermot Pustelnik^{*}, Filipp Roos[†], Ahmad-Reza Sadeghi^{*}, Michael Schwarz[†], Christian Uh * Technische Universität Darmstadt, Germany E-mail: [baumgaertner, mezini, markus.miettinen, ducthien.nguyen, ahmad.sadeghi]@cs.tu-darmstadt.de [†] Philipps-Universität Marburg, Germany E-mail: (hoechst, freisleb, penning, schwarzx, uhlc)@informatik.uni-marburg.de [‡] JMU Würzburg, Germany E-mail: [alexandra.dmitrienko, filipp.roos]@uni-wuerzburg.de

Abstract-Google and Apple have jointly provided an API for exposure notification in order to implement decentralized contract tracing apps using Bluetooth Low Energy, the so-called "Google/Apple Proposal", which we abbreviate by "GAP". We demonstrate that in real-world scenarios the current GAP design is vulnerable to (i) profiling and possibly de-anonymizing infected persons, and (ii) relay-based wormhole attacks that basically can generate fake contacts with the potential of significantly affecting the accuracy of an app-based contact tracing system. For both types of attack, we have built tools that can be easily used on mobile phones or Raspberry Pis (e.g., Bluetooth sniffers). We hope that our findings provide valuable input for designing and implementing secure and privacy-preserving digital contact tracing systems.

Index Terms-contact tracing apps, exposure notification API

for these two privacy and security risks. We selected the GAP approach for the following reas First, GAP will be broadly adopted, since several Europ contact tracing apps, such as the Swiss SwissCOVID. Italian Immuni, and the German Corona-Warn-App, based on the GAP API. Second, the GAP API is alr opt-in for iOS and Android devices, hence, it will potent stay with us for a long time.

towards possibly providing empirical real-world evide

We demonstrate that in real-world scenarios the rent GAP design is vulnerable to (i) profiling and bly de-anonymizing infected persons, and (ii) relaywormhole attacks that can generate fake potential of significantly

based contact

Vincenzo Iovino¹, Serge Vaudenay², and Martin Vuagnoux³ ¹ University of Salerno, Italy ² EPFL, Lausanne, Switzerland base23, Geneva, Switzerland

On the Effectiveness of Time Travel

to Inject COVID-19 Alerts*

Abstract. Digital contact tracing apps allow to alert people who have been in contact with Abstract. Dupta contact tracing apps aloos to alert prophs who have been in contact with people who may be contagious. The Apple/Congle Exposure Notification (EN) system is based in the second people who may no contagoons. The Approvidence exposure commonsterior steay system a sense on Binetooth provinity estimation. It has been adopted by many countries around the work on muctoota proximity estimation, it has been adopted by However, many possible attacks are known. The goal of some

TEnK-U: Terrorist Attacks for Fake Exposure Notifications in Contact Tracing Systems

Gennaro Avitabile¹, Daniele Friolo¹, and Ivan Visconti¹

¹DIEM, University of Salerno, Italy

Abstract

In this work we show that an adversary can leverage blockchain technology to attack the in turns out, we snow that an anternaty can be crash to be composed to account integrity of contact tracing systems based on Google Apple Exposure Notifications (GAEN). We design a suite of smart contracts named TEnK-U allowing an on-line market where inwe using a since or smark contracts names: remove anowing an on-one market where in-fected individuals interested in monetizing their status will then upload to the servers of the revery matyanous metricore in moneyaning their status with their approximation in extractor true GAEN-based systems some keys (i.e., TEKs) chosen by an adversary. As a consequence, structures is some as some actions of at-risk contacts arbitrarily decided by the adver-there will be fake exposure notifications of at-risk contacts arbitrarily decided by the adversary and allowed by infected individuals looking for money.

(3) and answer of micecen marganase meaning on meney. Such vulnerability can be exploited to anonymously and digitally trade valuable contact sten vuncautury can be exposed to monymously and ugitanty trans vanable contact tracing data without a mediator and without risks of being cheated. This makes infected

vacang unta warman a neuror and warman reas or owng vacance. Any masses more that individuals prone to get bribed by adversaries willing to compromise the integrity of the nurryanus pone to get briest by strensmes singly to composite the magnetic strength of the str

catastrophic consequences (e.g., jeopardizing the health system, compromising the result of catastropine consequences (e.g., poputating the meanin system, compromising one results or elections) are easy to mount and attacks to specific targets are completely straight-forward de sources, surpres, notces, notces, notces, notces, not contract with two collateral deposits that works, in We show as main contribution a smart contract with two collateral deposits that works, in

general, on GAEN-based systems and concretely with Immuni and SwissCovid. In addition, we show smart contracts with one collateral deposit that work with SwissCovid. Finally, we also suggest the design of a more sophisticated smart contract that could potentially to attack GAEN-based system even in case those systems are repaired to attacks ineffective. This last smart contract crucially uses DF

Our work shows that risks envisioned by And in particular TEnK-U shows how to reitralized syste

Contact Tracing by Giant Data Collectors: Opening Pandora's Box of Threats to Privacy, Sovereignty and National Security

Antoine Boutet, Claude Castelluccia, Mathieu Cunche, Alexandra Dmitrienko, Vincenzo Iovino, Markus Miettinen, Thien Duc Nguyen, Vincent Roca, Ahmad-Reza Sadeghi, Serge Vaudenay, Ivan Visconti, and Martin Vuagnoux



Real-world Attacks on GAEN

Baumgärtner et al. Mind the GAP: Security & Privacy Risks of Contact Tracing Apps (2020), TrustCom 2020 (to appear)

https://arxiv.org/abs/2006.05914



Wormhole Attack



Tracing Attack





Tracing Attack





Tracing Attack





Tracing Attack





Tracing Attack









Contact Tracing Across Borders vs. Cross-country Relay Attacks



Contact Tracing Across Borders vs. Cross-country Relay Attacks



Contact Tracing Across Borders vs. Cross-country Relay Attacks





Source: Robert-Koch-Institut (RKI) and CWA via https://micb25.github.io/dka/

 Estimated 93.062 persons have shared their diagnosis keys through CWA (by Nov 28)



- Estimated 93.062 persons have shared their diagnosis keys through CWA (by Nov 28)
- Corresponds to 10% of persons tested positive for SARS-CoV-2 since start of the app



Source: Robert-Koch-Institut (RKI) and CWA via https://micb25.github.io/dka/

- Estimated 93.062 persons have shared their diagnosis keys through CWA (by Nov 28)
- Corresponds to 10% of persons tested positive for SARS-CoV-2 since start of the app
- No information on how many tests were triggered by CWA



Source: Robert-Koch-Institut (RKI) and CWA via https://micb25.github.io/dka/

- Estimated 93.062 persons have shared their diagnosis keys through CWA (by Nov 28)
- Corresponds to 10% of persons tested positive for SARS-CoV-2 since start of the app
- No information on how many tests were triggered by CWA
- No information on how many of these were actually positive



Other problems of Corona-Warn-App

- The app does not notify (exposure status) in the background for many users
- The majority of users on Google Play Store have negative comments on the usability of the app
- Some infected users cannot share TEKs (Temporary Exposure Keys)
- Location setting needs to be enabled



Some other Decentralized Contact Tracing Solutions

- TraceCORONA (TU Darmstadt & UC San Diego) <u>www.tracecorona.net</u>
- PACT

https://pact.mit.edu/

• DP-3T-2 (EPFL and ETH)

https://github.com/DP-3T

 Pronto-C2 (University of Salerno) https://eprint.iacr.org/2020/493.pdf



Disaster Capitalism: Properties of Tracing Apps based on GAEN



Disaster Capitalism: Properties of Tracing Apps based on GAEN



What is Needed?

- A European solution
- An privacy-preserving infrastructure allowing feedback
- Framework for most effective solutions and not based on lobbying



0 I WON'T BE IMPRESSED WITH TECHNOLOGY **UNTIL I CAN** DOWNLOAD FOOD.