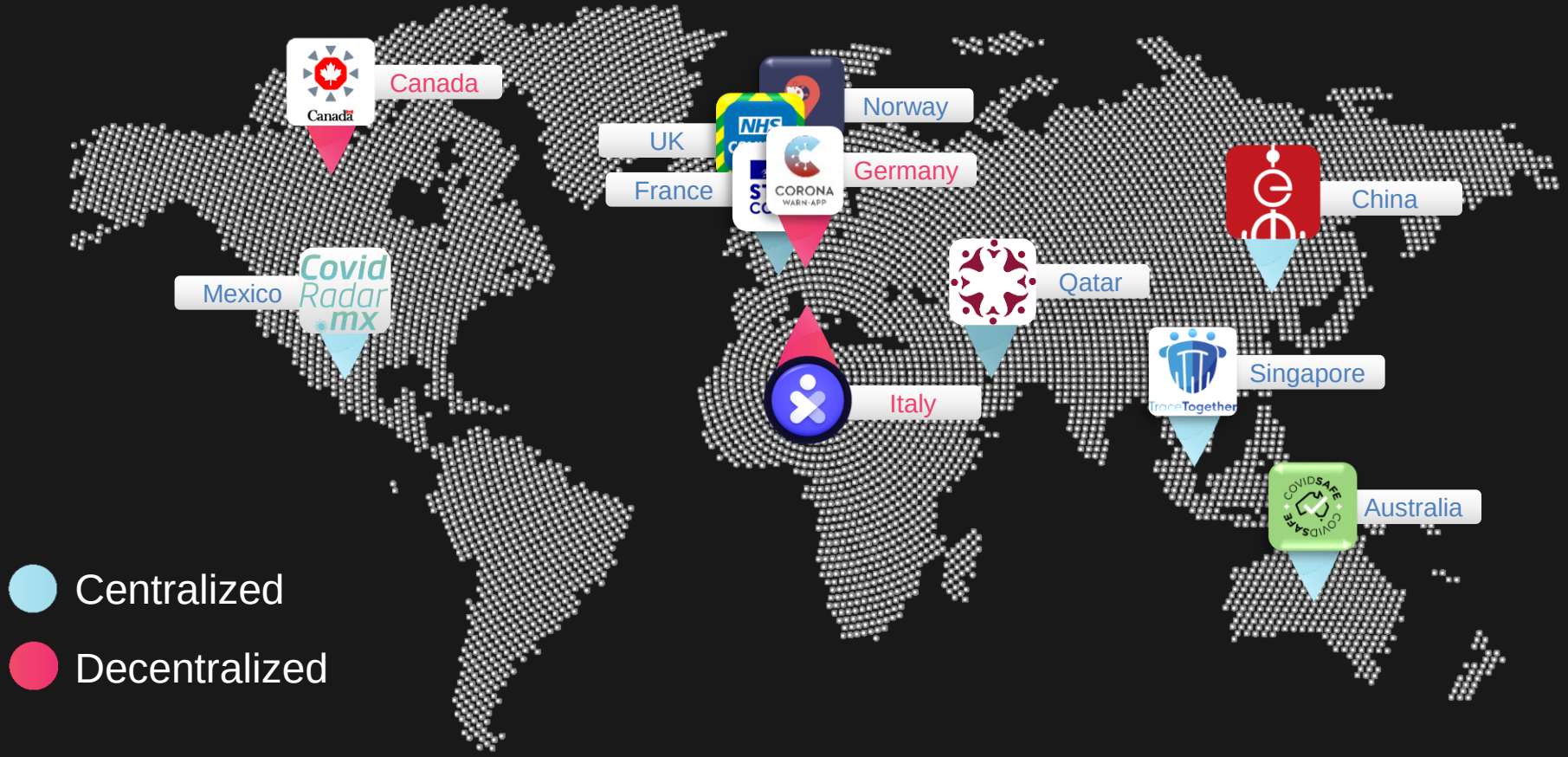
German Corona-Warn-App: Lessons learned and why we need to replace it!

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

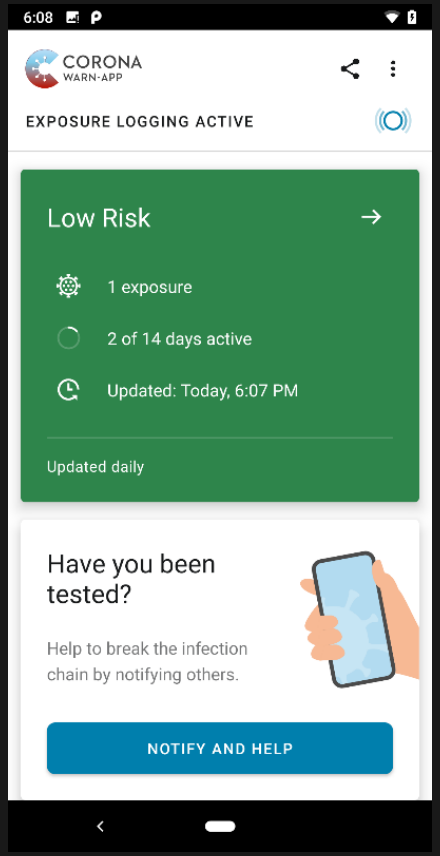
World View of Contact Tracing

World View of Contact Tracing

World View of Contact Tracing

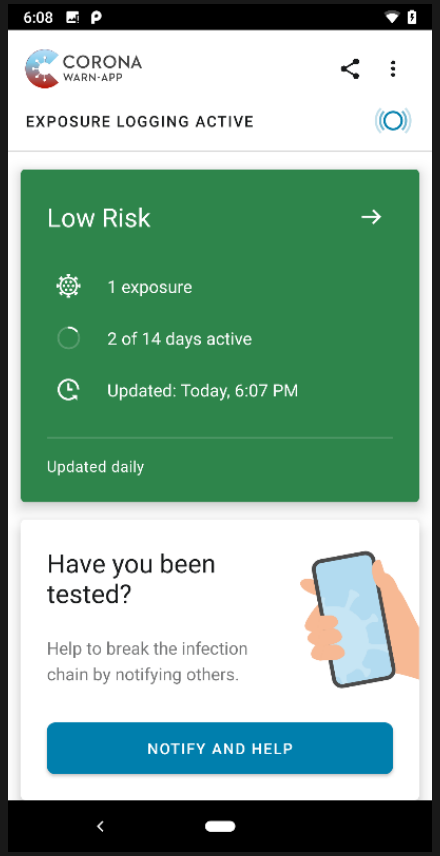


German Corona-Warn-App



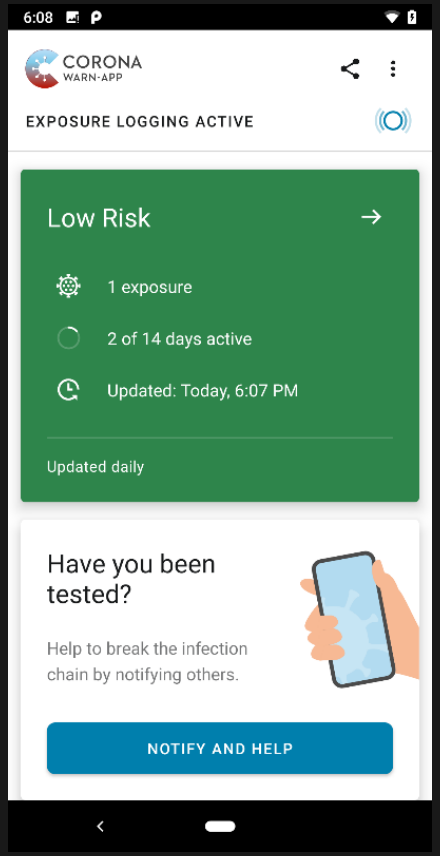
German Corona-Warn-App

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



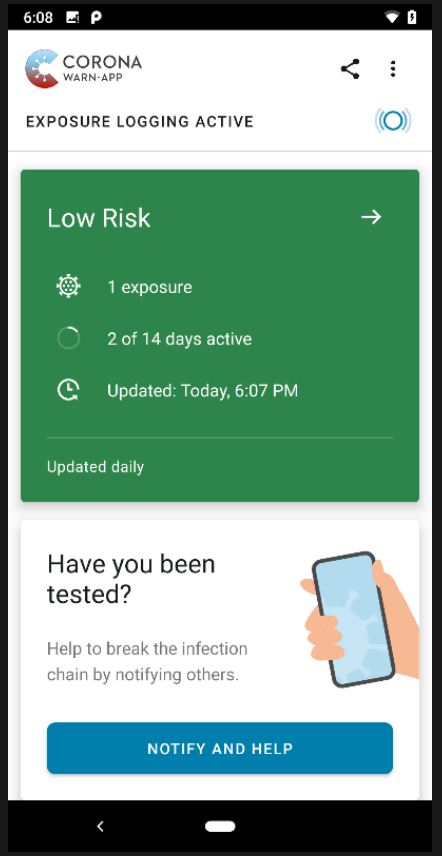
German Corona-Warn-App

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



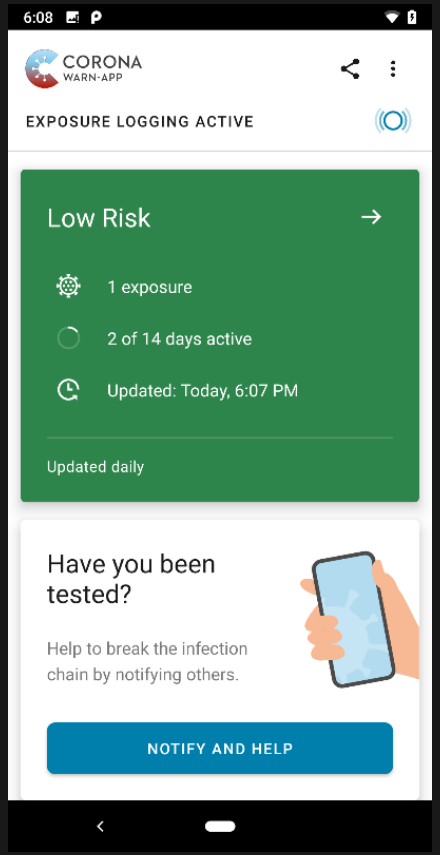
German Corona-Warn-App

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



German Corona-Warn-App

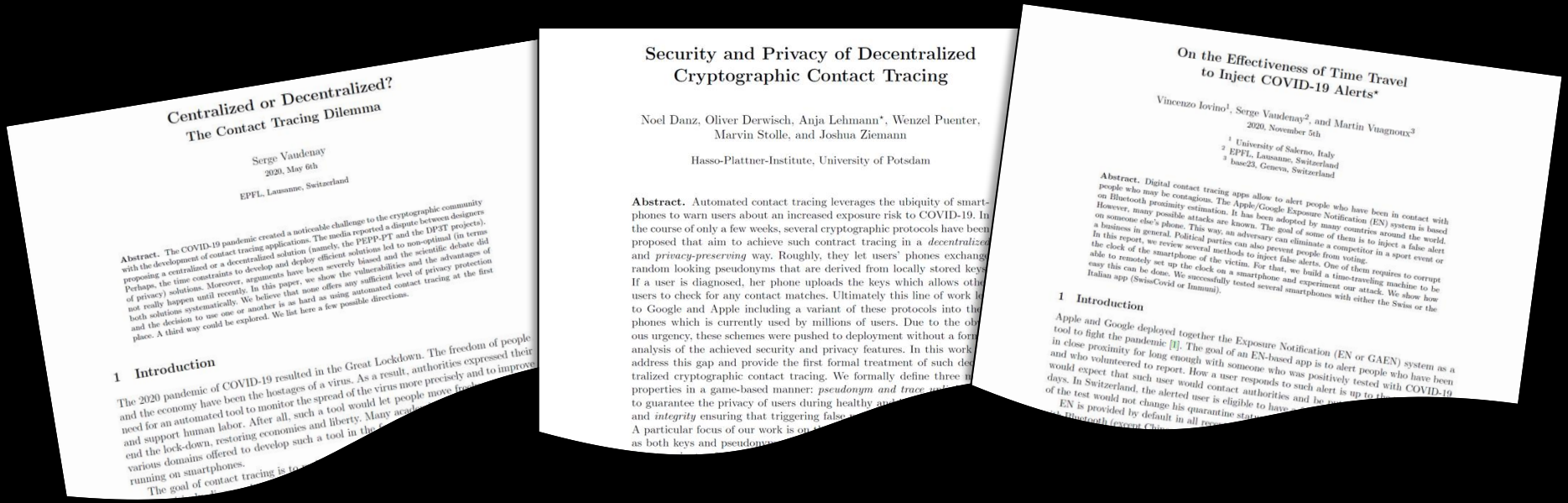
- **Goal:** efficiently and quickly detect and interrupt infection chains
- **Technology:** based on Google & Apple exposure notification (GAEN)
- **Number of downloads** > 20 millions
- **Costs:** 68 million Euros by the end of 2021, 20 million Euro for app development



Google & Apple Exposure Notification (Dystopia?)

Security and Privacy Attacks on GAEN

Security and Privacy Attacks on GAEN



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 community with the development of contact tracing applications. The media reported a dispute between designers proposing a centralized or a decentralized solution (namely, the PEPP-PT and the DP3T projects). Perhaps, the time constraints to develop and deploy efficient solutions led to non-optimal (in terms of privacy) solutions. Moreover, arguments have been severely biased and the scientific debate did not really happen until recently. In this paper, we show the vulnerabilities and the advantages of both solutions systematically. We believe that none offers any sufficient level of privacy protection and the decision to use one or another is as hard as using automated contact tracing at the first place. A third way could be explored. We list here a few possible directions.

1 Introduction

The 2020 pandemic of COVID-19 resulted in the Great Lockdown. The freedom of people and the economy have been the hostages of a virus. As a result, authorities expressed their need for an automated tool to monitor the spread of the virus more precisely and to improve and support human labor. After all, such a tool would let people move fr
end the lock-down, restoring economies and liberty. Many acad
various domains offered to develop such a tool in the
running on smartphones.

The goal of contact tracing is to

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 smart-
phones 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 exchang
random looking pseudonyms that are derived from locally stored keys
If a user is diagnosed, her phone uploads the keys which allows oth
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 for
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*
to guarantee the privacy of users during healthy
and *integrity* ensuring that triggering false
A particular focus of our work is on
as both keys and pseudony

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

Vincenzo Iovino[1], Serge Vaudenay[2], and Martin Vuagnoux[3]
2020, November 5th

[1] University of Salerno, Italy
[2] EPFL, Lausanne, Switzerland
[3] bsse23, Geneva, Switzerland

Abstract. Digital contact tracing apps allow to alert people who have been in contact with people who may be contagious. The Apple/Google Exposure Notification (EN) system is based on Bluetooth proximity estimation. It has been adopted by many countries around the world. However, many possible attacks are known. The goal of some of them is to inject a false alert on someone else's phone. This way, an adversary can eliminate a competitor in a sport event or a business in general. Political parties can also prevent people from voting.
In this report, we review several methods to inject false alerts. One of them requires to corrupt the clock of the smartphone of the victim. For that, we build a time-traveling machine to be able to remotely set up the clock on a smartphone and experiment our attack. We show how easy this can be done. We successfully tested several smartphones with either the Swiss or the Italian app (SwissCovid or Immuni).

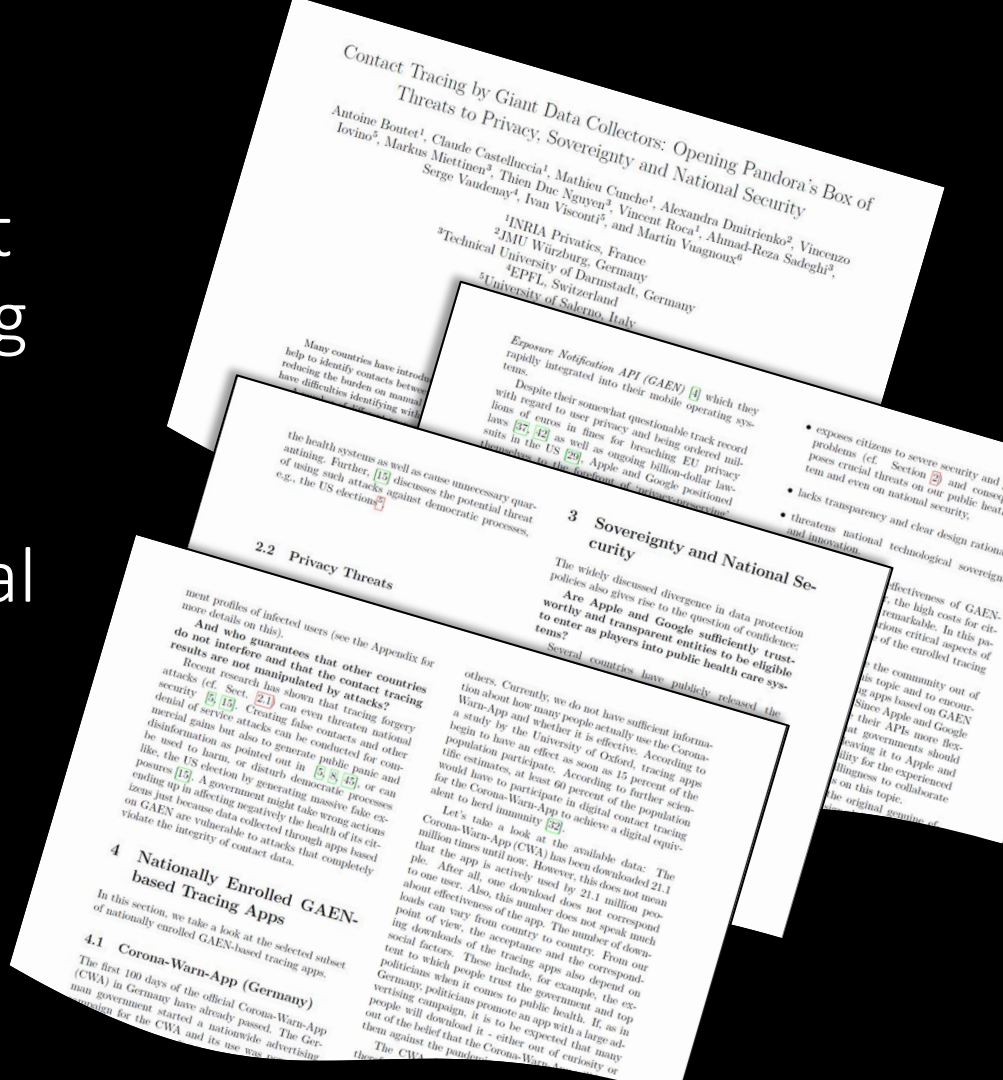
1 Introduction

Apple 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 close proximity for long enough with someone who was positively tested with COVID-19 and who volunteered to report. How a user responds to such alert is up to t
would expect that such user would contact authorities and be
days. In Switzerland, the alerted user is eligible to have
of the test would not change his quarantine sta
EN is provided by default in all re
Bluetooth (except Chi

Security and Privacy Attacks on GAEN

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

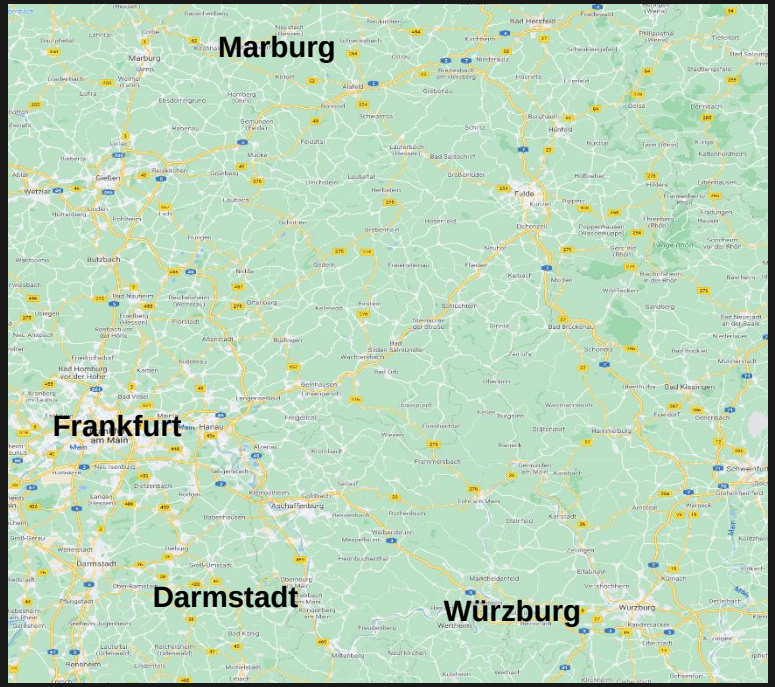
GAEN’s shaky Security and Privacy

Wormhole Attack

Tracing Attack

Baumgärtner et al. **Mind the GAP: Security & Privacy Risks of Contact Tracing Apps (2020). TrustCom 2020 (to appear)**
https://arxiv.org/abs/2006.05914

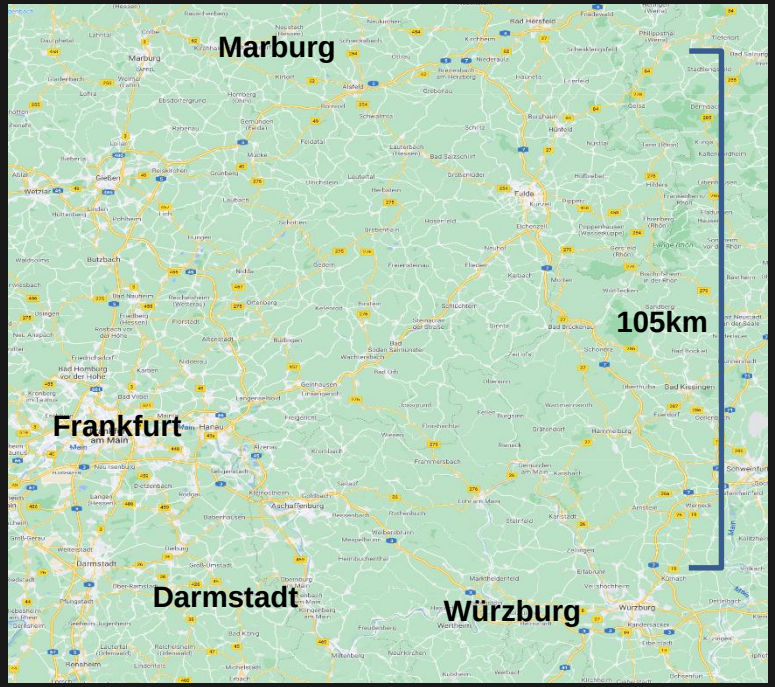
GAEN’s shaky Security and Privacy



Tracing Attack

Baumgärtner et al. **Mind the GAP: Security & Privacy Risks of Contact Tracing Apps (2020). TrustCom 2020 (to appear)**
https://arxiv.org/abs/2006.05914

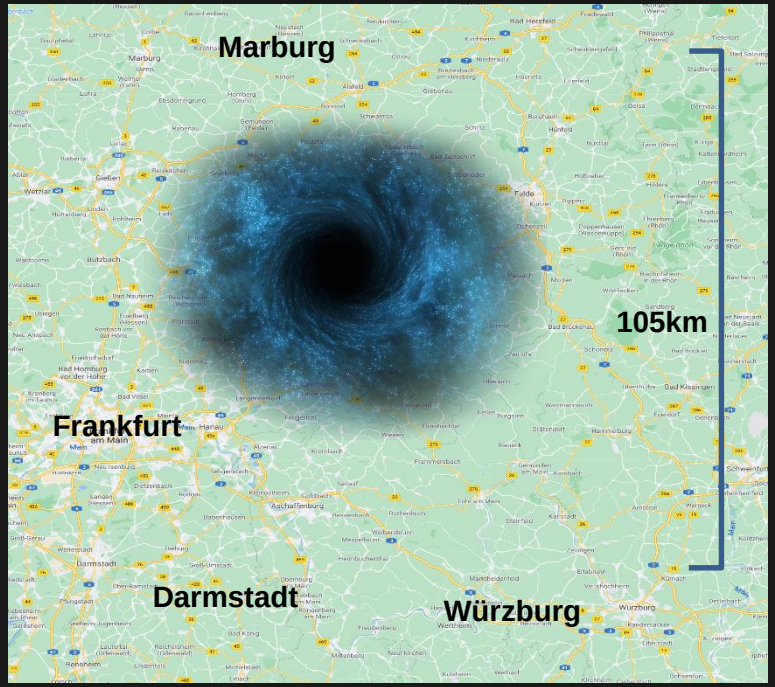
GAEN’s shaky Security and Privacy



Tracing Attack

Baumgärtner et al. **Mind the GAP: Security & Privacy Risks of Contact Tracing Apps (2020). TrustCom 2020 (to appear)**
https://arxiv.org/abs/2006.05914

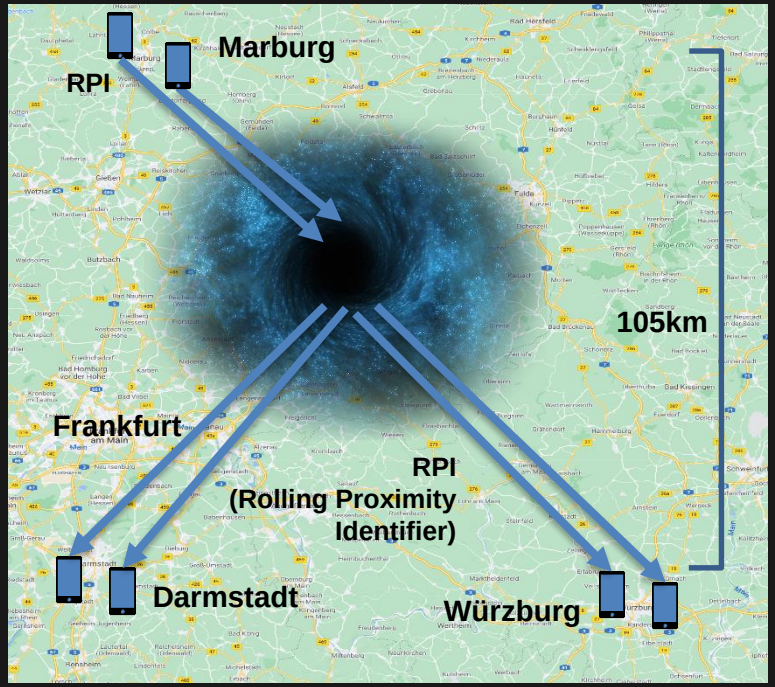
GAEN’s shaky Security and Privacy



Tracing Attack

Baumgärtner et al. **Mind the GAP: Security & Privacy Risks of Contact Tracing Apps (2020). TrustCom 2020 (to appear)**
https://arxiv.org/abs/2006.05914

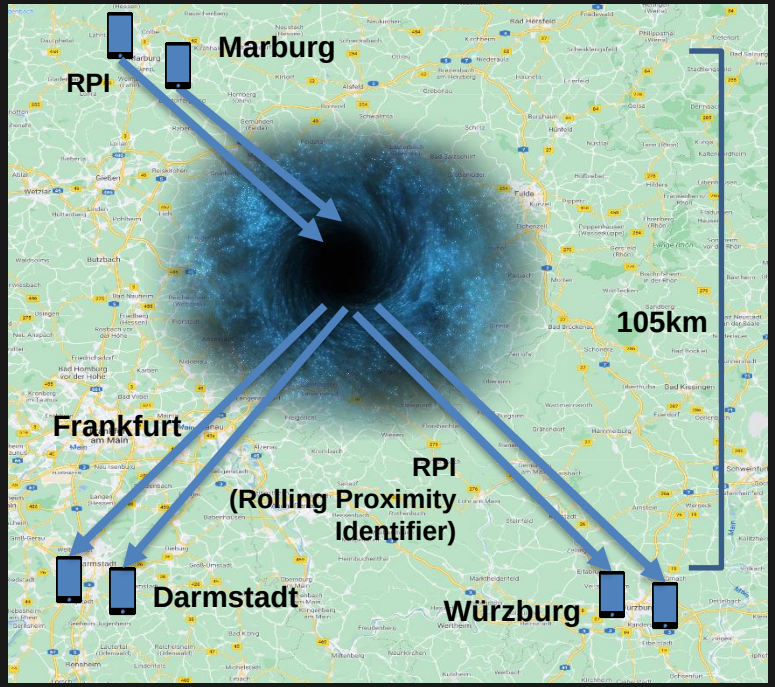
GAEN’s shaky Security and Privacy

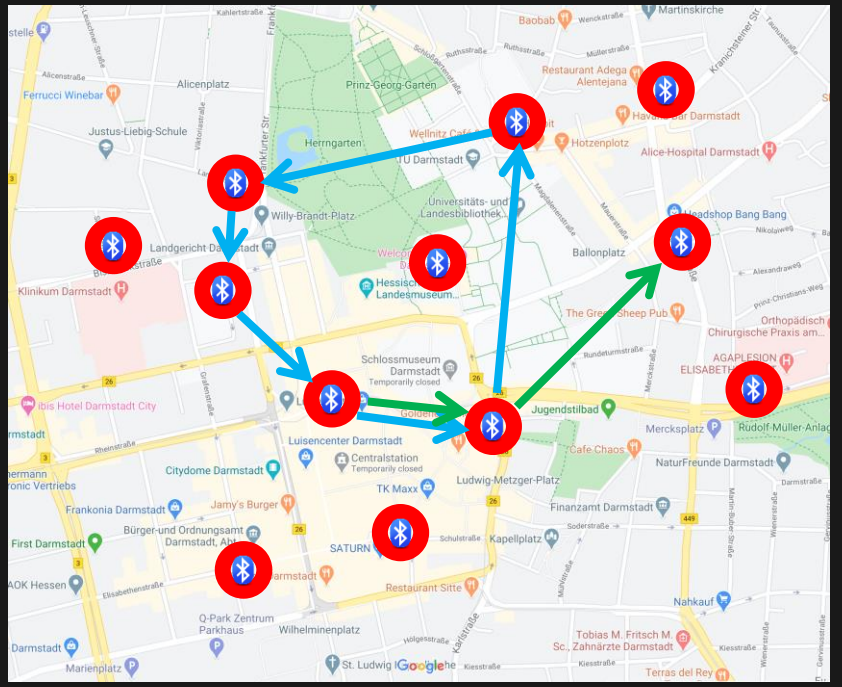


Tracing Attack

Baumgärtner et al. **Mind the GAP: Security & Privacy Risks of Contact Tracing Apps (2020). TrustCom 2020 (to appear)**
https://arxiv.org/abs/2006.05914

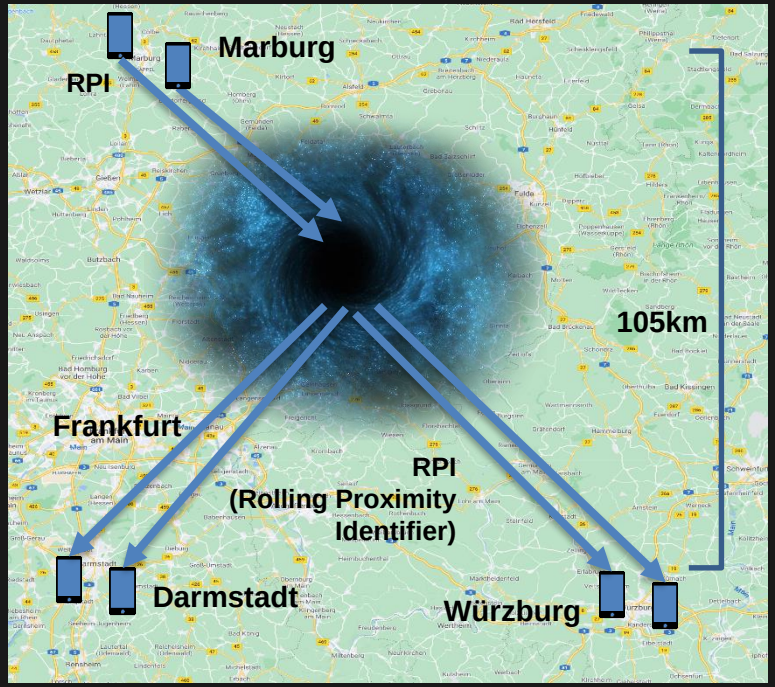
GAEN's shaky Security and Privacy

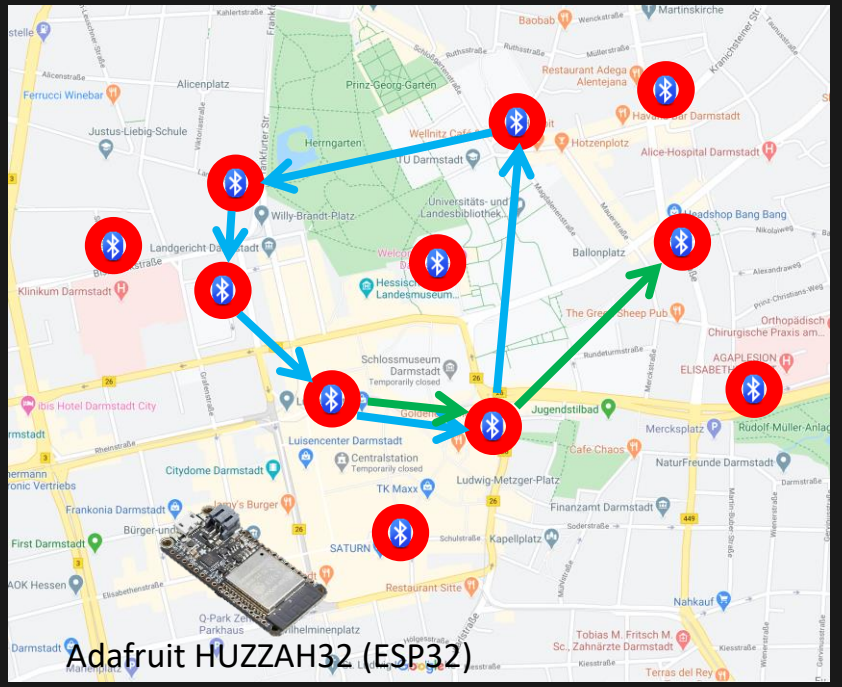




Baumgärtner et al. **Mind the GAP: Security & Privacy Risks of Contact Tracing Apps (2020). TrustCom 2020 (to appear)**
https://arxiv.org/abs/2006.05914

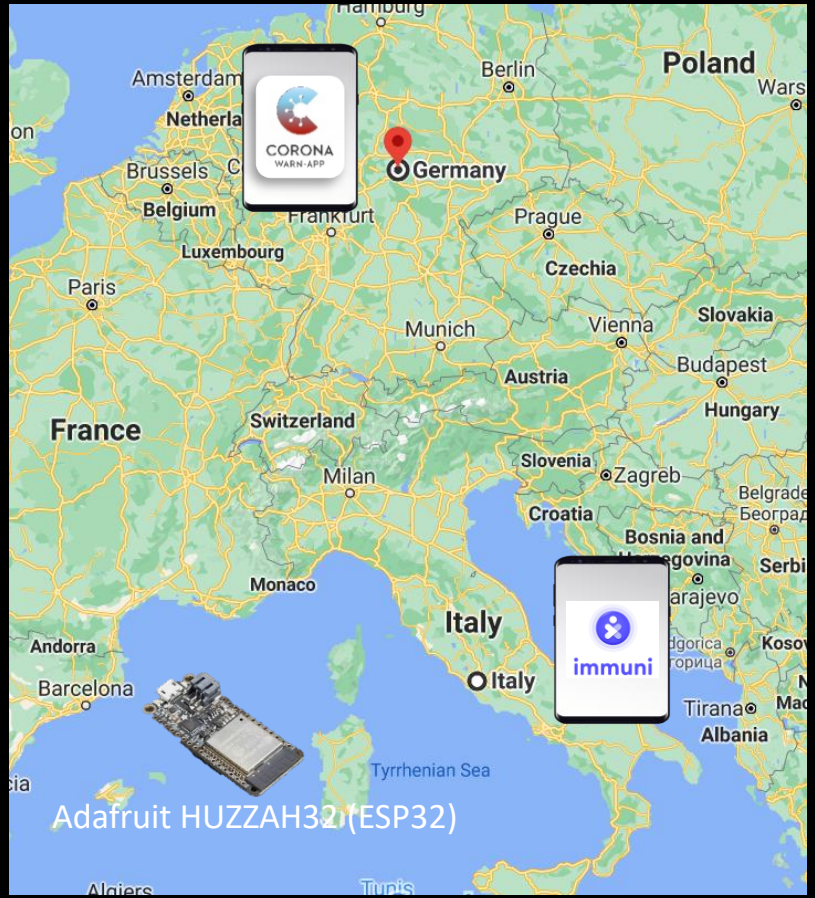
GAEN's shaky Security and Privacy



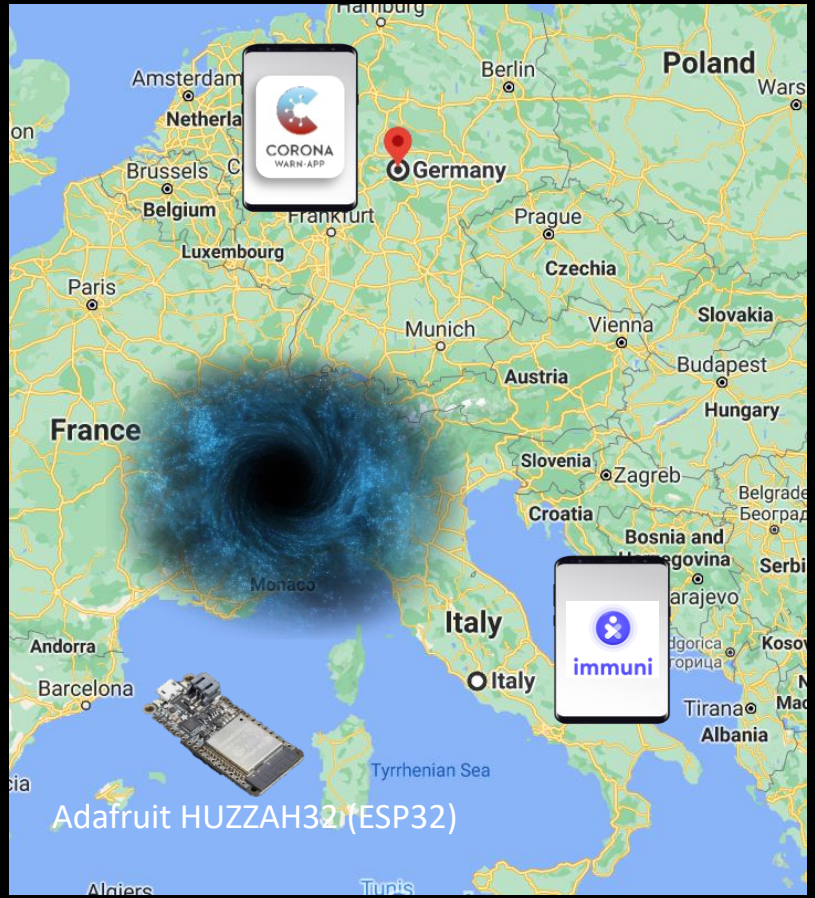


Baumgärtner et al. **Mind the GAP: Security & Privacy Risks of Contact Tracing Apps (2020). TrustCom 2020 (to appear)**
https://arxiv.org/abs/2006.05914

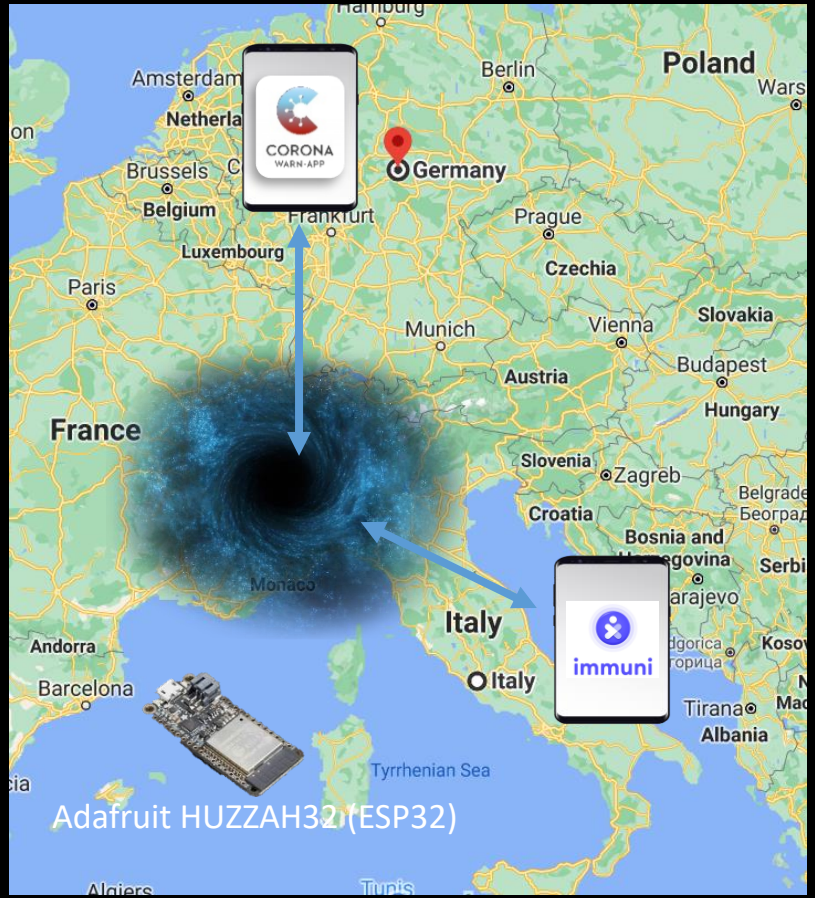
Contact Tracing Across Borders vs. Cross-country Relay Attacks



Contact Tracing Across Borders vs. Cross-country Relay Attacks



Contact Tracing Across Borders vs. Cross-country Relay Attacks



How effective is CWA?

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

How effective is CWA?

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

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

How effective is CWA?

- 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/

How effective is CWA?

- 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/

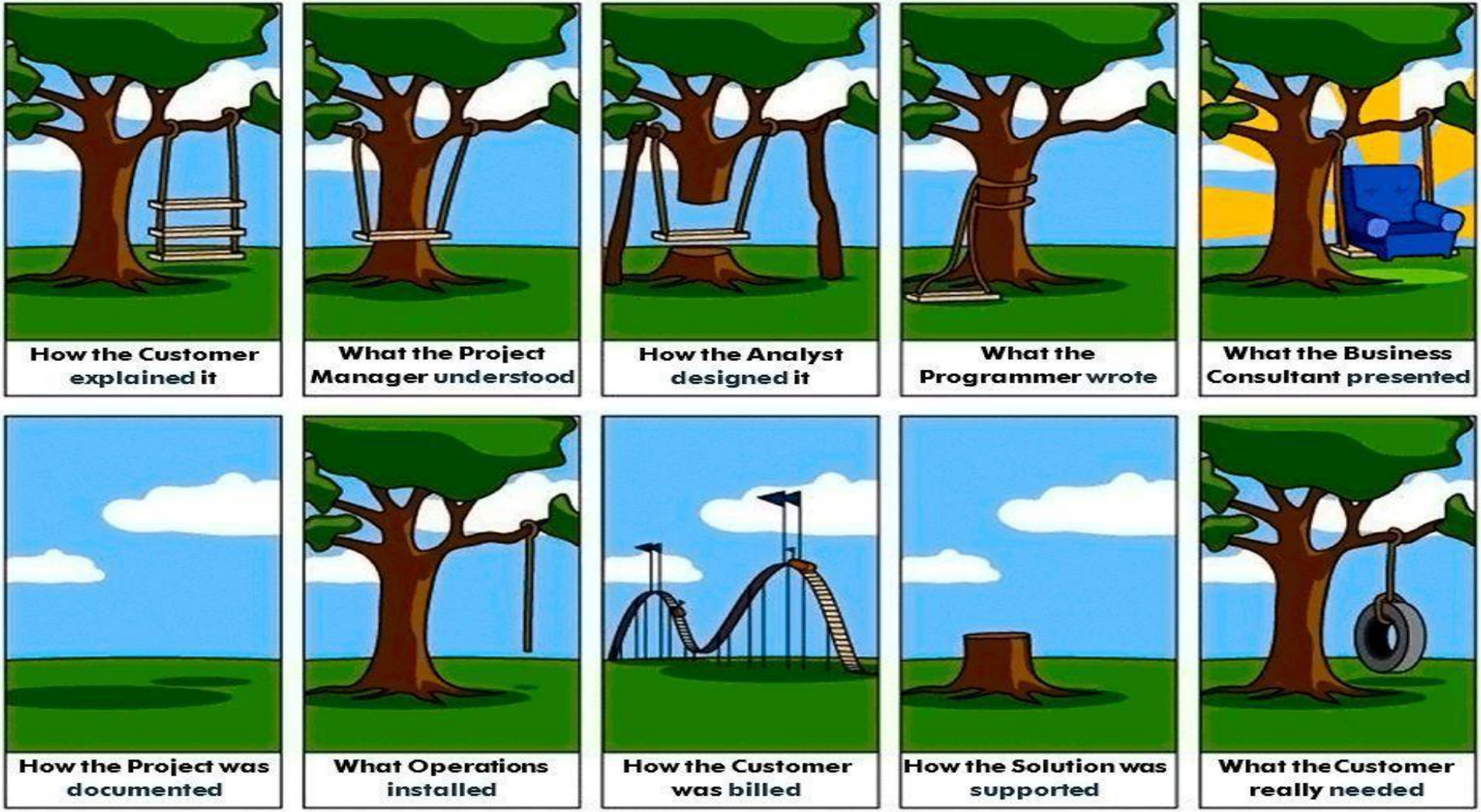
How effective is CWA?

- 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

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

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


How the Customer explained it
What the Project Manager understood
How the Analyst designed it
What the Programmer wrote
What the Business Consultant presented
How the Project was documented
What Operations installed
How the Customer was billed
How the Solution was supported
What the Customer really needed

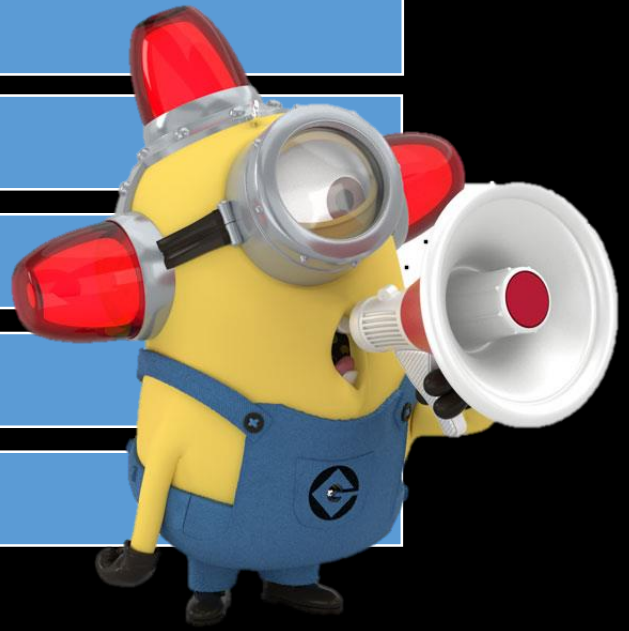
Some other Decentralized Contact Tracing Solutions

- TraceCORONA (TU Darmstadt & UC San Diego)
  www.tracecorona.net
- 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

- Government-industrial complex
- Disproportionate costs
- Suppressing innovation
- Threatening sovereignty
- Security & Privacy
- Lack of effectiveness evaluation



What is Needed?

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


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