Karlsruhe Institute of Technology

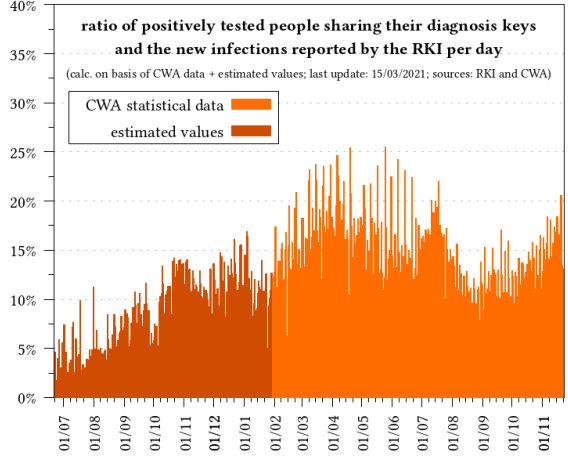
KASTEL

ConTra Corona: Contact Tracing against the Coronavirus

ASIACRYPT 2021

W. Beskorovajnov, F. Dörre, G. Hartung, A. Koch, J. Müller-Quade, T. Strufe | 10. December 2021

State of Exposure Notification

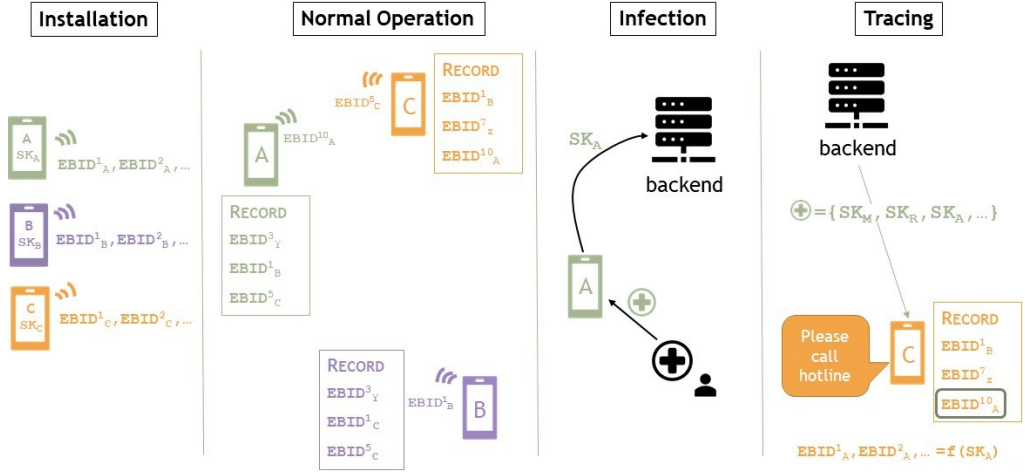


CWA UI Design under Apache 2.0, Chart under CC-BY-NC-SA-3.0 by Michael Böhme

Outline

1. Google–Apple Exposure Notification (GAEN) and Privacy Problems
2. Our Goals and Approach for Improving Privacy
3. Modeling Security and Remaining Data Leakage

GAEN and Theoretical Privacy Problems



DP3T Overview Figure CC-BY-SA-4.0 of Ludovic Barman

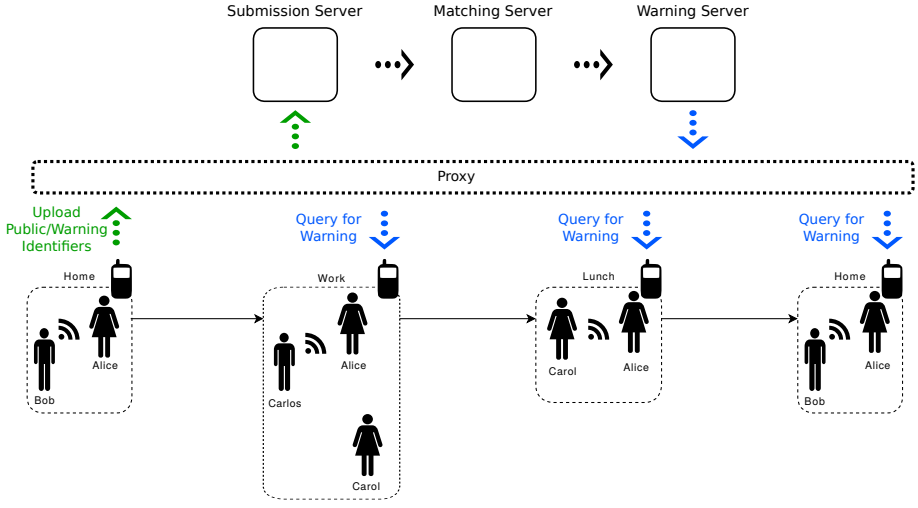
Privacy Problems for Infected Participants

- linking encounters with an infected person on the same day
- learning which and how many encounters on a day led to a warning

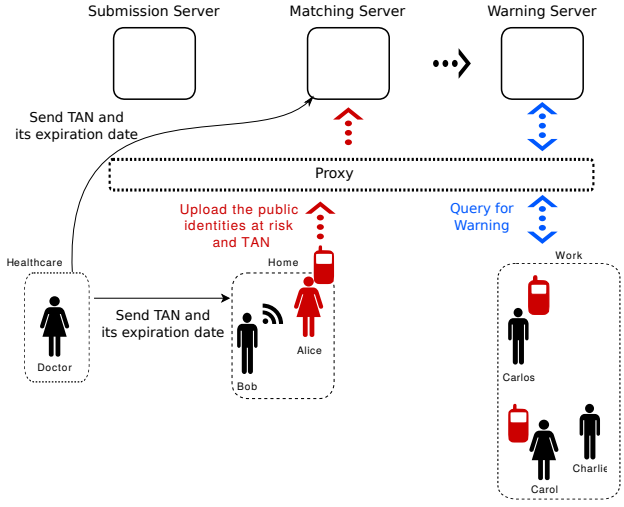
Our Goals

- Protect the privacy of infected participants
  - Less risk of blame: “You infected me, and therefore X died. This is your fault!”
  - Hence infected participants are more likely to share the keys.
- While not compromising the privacy of other participants
  - No central authority can trace participants
  - Model the information leaked to each subset of participants explicitly.

Our “Hybrid” Approach with Server Pipeline

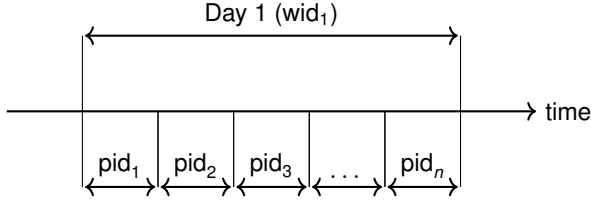


Reporting Infections via Upload-What-You-Saw



Our Security Model

- Comparison with an ideal functionality.
- Environment is allowed to choose physical scenario (contact graph, infections) arbitrarily.
- Participants can only learn the day of a risky encounter:



Leakage About the Contact Graph

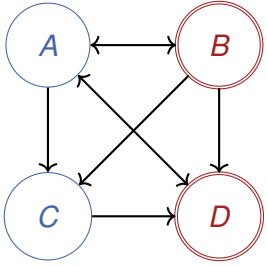


Figure: Contact Graph

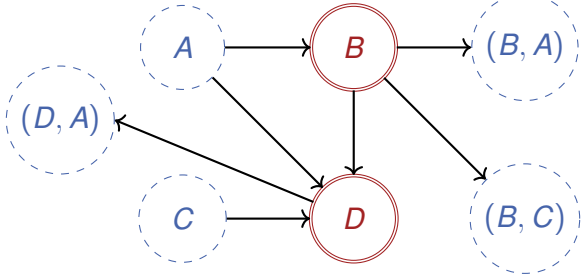
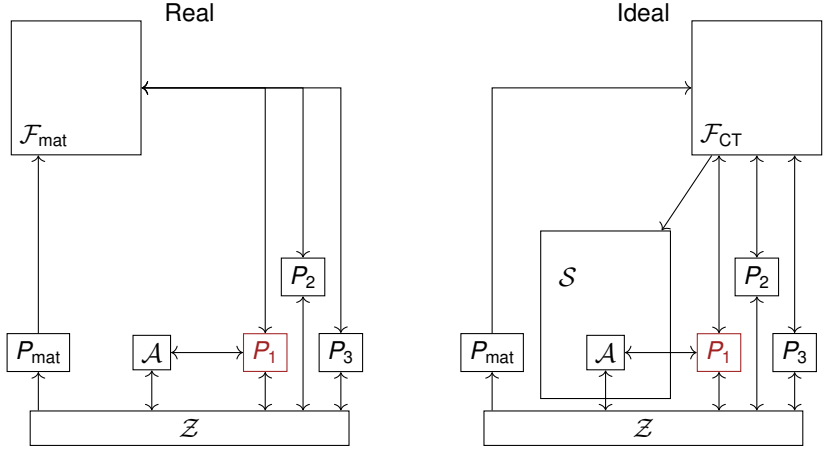


Figure: Leakage Graph (Given to Simulator)

Blue: Honest, Red/Double-Line: Corrupted, Dashed Circle: Pseudonomized

Excerpt of Real–Ideal Modelling



Conclusion

- D3PT/Google-Apple Exposure Notification are already a great first step but still have potential privacy leakage
- We present an approach that protects privacy better
- We provide a security model to demonstrate the remaining privacy leakage

For more details, see our full version at `https://ia.cr/2020/505`.