**Analyze on Germany’s Paper**

**Paper Link: “**[**Mind the GAP: Security & Privacy Risks of Contact Tracing Apps**](https://arxiv.org/pdf/2006.05914.pdf)**”**

**Two Problems raised:**

**Problem1: Profiling and possibly de-anonymizing infected persons**

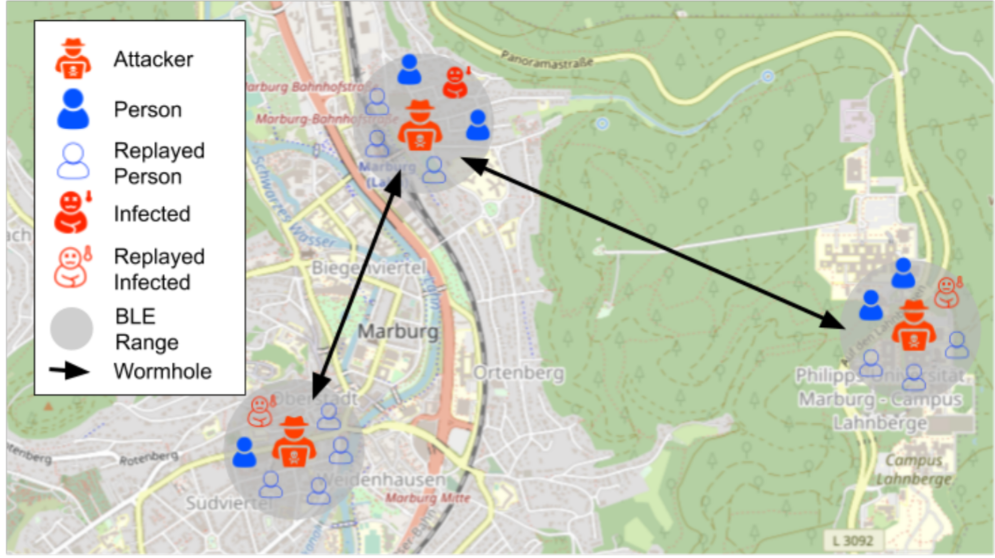
**Argument**: Once get the TEK of an infected person, we can generate RPI. By frequently comparing this RPI with the RPIs collected on sniffing devices, we can trace the infected person:

**Analyze**: This argument is true when we know the exact process of how Google/Apple API generate TEK and RPI. This issue is going to be solved once Google/Apple integrate this API into Operating system.

**Problem2: Relay-based wormhole attacks that principally can generate fake contacts**

**Argument**: They can build internet connection between attacking devices. Attackers can collect RPI from high infection rate areas and broadcast them everywhere.

**Analyze**: This is a serious issue we need to think about. Integrating this API into the operating system or doing encryption will not solve this problem. This problem has the potential to make contact tracing applications useless.

**Possible Solution**: Greatly increase the renew frequency of RPI might help to solve this problem. In the paper, they said transmission between attacking devices will take seconds. If the renew frequency of RPI is increased to seconds, RPI received by other attacking devices will be invalid. However, the renew frequency of RPI cannot be too high. The interval should at least include generating time, broadcast time, scanning time, and decode time.