Itamar Chinn

Design Project Prep Assignment

The current "exposure tracing" systems in place on a national level are unfit for the demands of a university. The 6.033 DP specification proposes a "Better Exposure Tracing System" (BET). This document summarizes and examines the specification by focusing on improving existing systems, with attention to its requirements, important use cases, and key questions for further inquiry.

The main objective of the BET system is to find the ideal balance between functionality (accuracy and reliability), ease of use, low impact on the phone's computation abilities and individual privacy (p.9-10) that best suits a university and supports the healthcare system behind it. The BET system aims to take advantage of the unique nature and resources of a university, such as routers across campus and the widespread use of smartphones.

Context for Evaluation

During the COVID-19 pandemic, many countries tried to implement "exposure tracing" systems to curtail infections – with limited success or at the expense of their citizens' privacy. The downfalls of existing systems can be examined by comparing exposure tracing in a large, medium and small country (p.6-7). In the large country system, the central authority relied heavily on citizens' phone records and locations and cross-examined these with citizens' personal health information on a central server. This centralization and phone access deprioritizes privacy in exchange for more accurate outcomes and scalability. The medium country system places a larger emphasis on privacy by adding protocols to disconnect a phone ID with a specific person, but still handles large amounts of personal data on a central server and provides human intervention if needed. The small country puts the largest emphasis on privacy, by using a complex ID encryption process and by handling exposure matches on the phone rather than on a server, however, this significantly impacts the system's scalability at times of high infection. Both the medium and small country apps do not track geolocation and therefore are not able to verify isolation compliance. Clearly all three of these examples prioritize functionality, ease of use, low impact on the phone's computation abilities and an individual's privacy differently – none of which perfectly suit the needs of a university campus.

Modules and Use Cases

As detailed in the specification (Section B.1, p.11), there are three key modules in the system: smartphones using Bluetooth Low-Energy (BLE) technology, Wi-Fi routers (hotspots) whose range covers the university campus, and a central server. The key design elements will focus on the role of each module, in particular the location of data storage and data computation, the communication protocols between the modules and the protection of user privacy. All three of these, if badly designed, could introduce bottlenecks to the system. The central server and the routers have high-end specs (server - 64GB of memory, 12TB of storage, two 10Gb ethernet ports; router 8GB of storage) allowing for flexibility, but the phones' specs (1GB of storage) are low, which must be considered (p.11-12) when implementing the required behaviors of the system.

The system must be able to track meetings of 20 minutes or more at a distance of less than 3m between individuals; to notify the central authority of exposure; to record a positive infection test and notify the infected individual; and to notify any individuals who came into close contact with an infected individual during the infectious period. There is also a list of events in which the system should notify users that they are required to isolate regardless of confirmed exposure (see p.12-13). The specification allows the designer to decide how to protect individual privacy, although it clearly evaluates this as a high priority (p.1, 5, 8, 9, 10, 14). Furthermore, the specification encourages designers to share collected data with government and public health researchers, though this is considered low priority. The designer may decide how to provide data in a privacy-focused way. Current systems fail on two fronts – either considered "untrustworthy or lacking in utility" (p.8) – and so focusing on privacy and accurate and timely notifications is essential.

Itamar Chinn

The specification considers three key use cases which indicate possible pressures on the system. The system should be able to handle “very low numbers”, “very high numbers” or “compressed very high numbers” (large amounts of data pushed to the system in a short time). Additionally, the specification recommends modularity as further features may be requested, for example, isolation compliance verification or updating system behavior in response to scientific developments (long distance exposure may be discovered as significant or vaccinated individuals might require different consideration).

Key Questions for Inquiry

- The specification mentions routers as a potential resource only available at a university – what added benefits does the system get by including routers as a module? Do routers simply store data on who is connected to them or can we use them for geolocation triangulation instead of GPS?
- The healthcare provider is not considered a module in the specification but is considered a player. Can we use the healthcare provider as a trusted party or even as a module to help protect privacy? For example, the healthcare provider could store mappings of IDs to name rather than the central server (as they are already exposed to personal data)
- Many students and staff live off-campus. How should the system track exposure differently when off-campus? Are there other modules we can use to get information off-campus, such as local databases of locations where infected individuals visited?