PACT: Private Automated Contact Tracing[1]

Mission and Approach - May 19, 2020
https://pact.mit.edu/

Ronald L. Rivest, PhD
Daniel J. Weitzner, JD
MIT CSAIL
MIT Internet Policy Research Initiative
Cambridge, MA USA

Louise C. Ivers, MD MPH
MGH Center for Global Health
Harvard Medical School
Boston, MA USA

Israel Soibelman, PhD
Marc A. Zissman, PhD
MIT Lincoln Laboratory
Lexington, MA USA

PACT is a collaboration led by the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL), MIT Internet Policy Research Initiative, Massachusetts General Hospital Center for Global Health and MIT Lincoln Laboratory. It includes close collaborators from Boston University, Brown University, Carnegie Mellon University, the MIT Media Lab, the Weizmann Institute and a number of public and private research and development centers. The PACT team is a partnership among cryptographers, physicians, privacy experts, scientists and engineers.

PACT's mission is to enhance contact tracing in pandemic response by designing exposure detection functions in personal digital communication devices that have maximal public health utility while preserving privacy.

The PACT effort began in mid-March 2020 with the development of the PACT protocol specification, which is a simple, decentralized approach for using personal digital communication devices for automating exposure detection using Bluetooth Low Energy signaling. Version 0.1 of the PACT protocol was released on 8 April 2020. The Apple and Google plan for exposure notification services are largely consistent with the PACT protocol and were released shortly afterwards. Initial proof of concept technology demonstrations were completed by MIT around the same time.

As of mid-May 2020, PACT has four major lines of effort:

1. Proximity Detection Efficacy: Collect the experimental data required to demonstrate and evaluate objectively and quantitatively the extent to which Bluetooth Low Energy (BLE) can be used to detect when two people have been closer than some medically relevant distance from each other for too long a period of time, i.e. "too close for too long" (TC4TL). Collect BLE data (and related metadata) to find the best way to compute TC4TL and measure TC4TL performance (using receiver operating characteristic curves, decision cost functions, etc.) Determine how performance depends on various equipment, user and environmental factors and measure the impact that different approaches for computing TC4TL have on smartphone battery life and compute resources. Assess the exposure notification software developed and distributed by Apple and Google ("A|G"). Recommend improvements to the A|G approach where appropriate. Share all results openly and explain the implications to public health authorities (PHAs), A|G and

others to inform decision-making. Simultaneously begin investigation of other signaling protocols (e.g. ultrasound, UWB) in case BLE communication is shown to have insufficient efficacy.

2. Privacy: Advocate for digital exposure detection approaches to contact tracing that preserve individual privacy and civil liberties. Develop, publish and seek feedback on private automated contact tracing protocols. Continue to monitor Apple|Google progress on development and deployment of their exposure notification protocol, whose decentralized architecture is based in part on PACT, to ensure continued A|G adherence to the highest standards of privacy and security. Develop improvements to protocols based on theoretical and experimental results. Assess privacy impact of the integration of digital exposure detection within public health systems and study the larger legal and public policy dimensions of the collection and use of contact tracing information. Share all results openly and explain the implications to the PHAs, A|G and others to inform decision-making.

3. Integration: Advise Public Health Authorities (e.g. mainly US states, counties and municipalities, but also PHAs in other nations and other types of enterprises) regarding development of the best system architectures and deployment strategies so that they can be smart designers, buyers and users of new digital exposure detection functions within operational, integrated contact tracing systems that combine core PHA functions with new private automated contact tracing capabilities. For US states, advise one or more state PHAs on selection of an end-user smartphone app that leverages the A|G exposure notification service and can be deployed in a manner that meets usability requirements of diverse communities and protects privacy and the public trust.

4. Public health efficacy: Study whether and how automated exposure detection can provide measurable improvements in manual contact tracing efforts to slow infection rates. Investigating this question requires a controlled pilot conducted with public health or other medical officials under study by an epidemiology team. PACT will expand our partnerships with public health authorities, researchers and NGOs.

The first three lines of effort map to the three layers of the PACT stack (see Figure 1): Layer 1 (Proximity Detection Efficacy), Layer 2 (Privacy) and Layer 3 (Integration).

In support of these, PACT executes several cross-layer activities that demonstrate public health efficacy:

- Prototypes. PACT is building prototypes that implement end-to-end integrated (manual and automated) contact tracing systems. The purpose of the prototypes is to enable PHAs to become familiar with how all the parts work together toward public health goals, what the interfaces are, and how initial assumptions may need to be adjusted. The prototypes will also be helpful for PHAs to develop well-informed requirements and deployment strategies for the systems they will need to acquire.

- System Analysis. PACT will be performing system analysis along with modeling and simulation to learn whether integrated privacy-preserving contact tracing can actually be expected to slow the spread of COVID-19. At the moment, this claim is yet unproven. This analysis is a

multi-disciplinary collaboration among systems analysts, epidemiologists and public health experts. We will share all results openly and explain the implications to the PHAs, A|G and others to inform decision-making.

- Data Collection and Experiments. PACT will conduct a series of hypothesis-driven experiments of increasing fidelity in the following order: constructive, virtual, and live. These experiments will help validate the predictive power of the models developed in system analysis.

- Pilots. As warranted from the experimental results, PACT may deploy a prototype system for a limited period of time to some select organizations in operational settings, help them use it, collect and assess all relevant data, and try to evaluate the system's public health and privacy efficacy. We will use the resulting experience to improve the functionality and relevance of the prototype, to validate our analysis and to broaden and deepen our understanding of the problem.
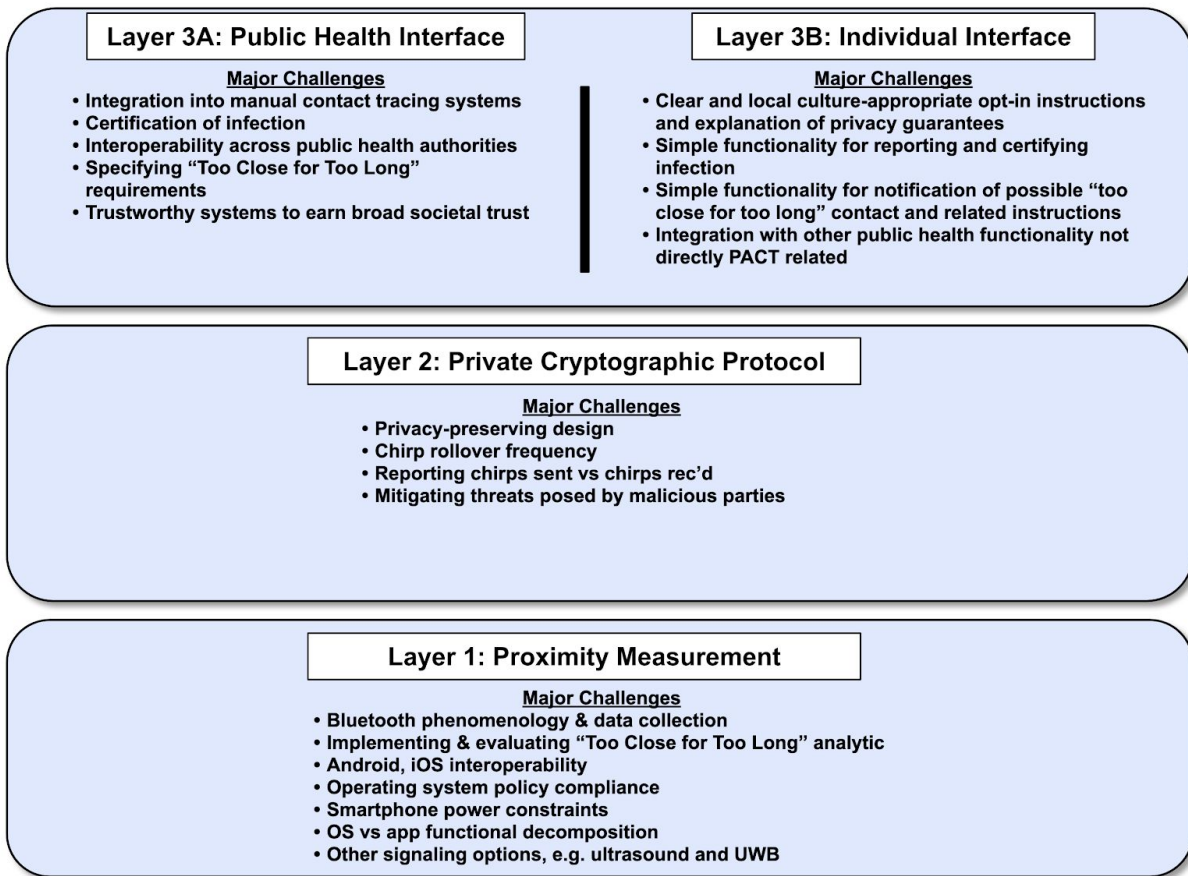

Layer 3A: Public Health Interface

Major Challenges
- Integration into manual contact tracing systems
- Certification of infection
- Interoperability across public health authorities
- Specifying "Too Close for Too Long" requirements
- Trustworthy systems to earn broad societal trust

Layer 3B: Individual Interface

Major Challenges
- Clear and local culture-appropriate opt-in instructions and explanation of privacy guarantees
- Simple functionality for reporting and certifying infection
- Simple functionality for notification of possible "too close for too long" contact and related instructions
- Integration with other public health functionality not directly PACT related

Layer 2: Private Cryptographic Protocol

Major Challenges
- Privacy-preserving design
- Chirp rollover frequency
- Reporting chirps sent vs chirps rec'd
- Mitigating threats posed by malicious parties

Layer 1: Proximity Measurement

Major Challenges
- Bluetooth phenomenology & data collection
- Implementing & evaluating "Too Close for Too Long" analytic
- Android, iOS interoperability
- Operating system policy compliance
- Smartphone power constraints
- OS vs app functional decomposition
- Other signaling options, e.g. ultrasound and UWB

Figure 1 - PACT Stack

For more information visit https://pact.mit.edu/