NIST Approach to Exposure Notification

Purpose

Electronic devices have the potential to help suppress the spread of infectious diseases like COVID-19 through exposure notification. During exposure notification, the devices automatically record other devices with which they come into close proximity. NIST is building and demonstrating a secure, privacy-preserving, and robust implementation of exposure notification.

Evaluating Accuracy of Distance Measured

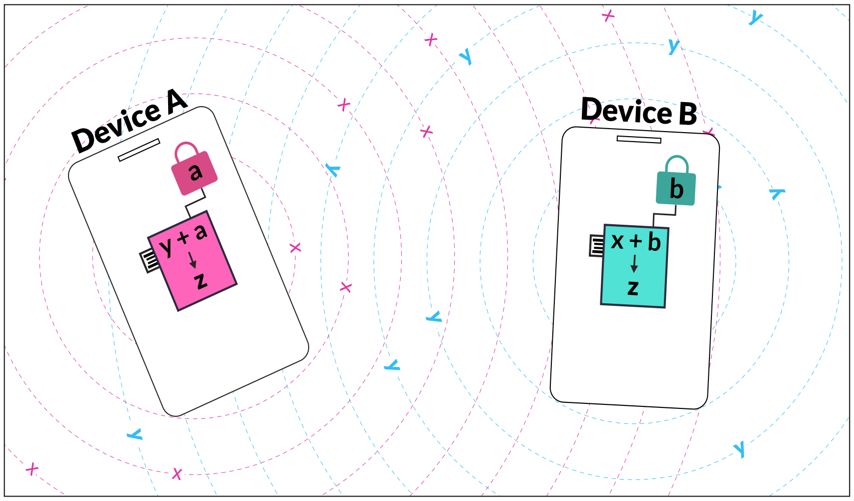
BLE (Bluetooth Low Energy) exposure notification uses received radio power to estimate the distance between the devices. The farther away the devices are from each other, the smaller the received radio signal. However, the real-world environment may contain factors that alter the received radio signal, leading to errors in spatial localization. NIST is currently testing in a real-world context.

NIST's Privacy-preserving Approach

The NIST BLE devices use a cryptographic approach that allows for exposure notification while preventing the compromise of people's identities from third party surveillance. These devices do not have GPS and cannot track absolute location. This is a huge improvement in privacy capabilities compared to other current approaches to exposure notification.

In the NIST approach, each NIST BLE device periodically generates a new private and public key from random numbers. When two devices come into contact with each other, they exchange their public keys in order to produce an encounter ID that is cryptographically secure. Each device only records the encounter ID and does not record any identification of the other device. All devices upload their recorded encounter IDs along with encounter time and signal level to the server on a regular basis.

When an infection occurs, an infected user's device can post its encounter IDs for the last 14 days on a central server. Then, when another device communicates with the server, the device will be alerted if any encounter ID in its memory is also on the server. The central server cannot link encounter IDs to device IDs. No trusted third party is necessary.

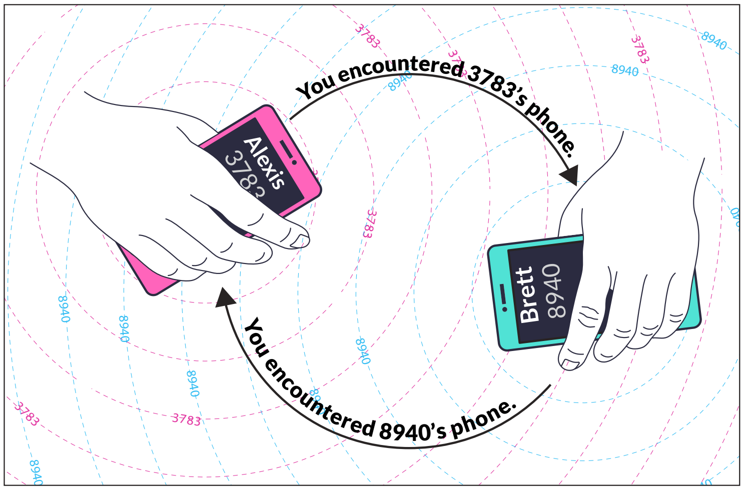


NIST's approach to exposure notification, where z is the cryptographically secure encounter ID recorded by each device.

NIST's cryptographic protocol distinguishes it from other exposure notification systems. For example, in one publicly available approach, each device (e.g. phone) constantly broadcasts its dynamic, random ID. As the device passes another device, it records the random ID of the device it passes. A server maintains a list of the random IDs of people who have tested positive for COVID-19.

Depending on how the approach is carried out, either 1. every device periodically checks to see if any of the random IDs they have come into contact with are listed as testing positive, or 2. when a person tests positive, they upload all of the random IDs of devices that they have come into contact with previously.

There are major privacy concerns with this approach. Each Random ID is linked to the identity of the device-owner in an unencrypted broadcast allowing third parties to compromise identities. Also, the server must be maintained by an entity that can be trusted to respect privacy.

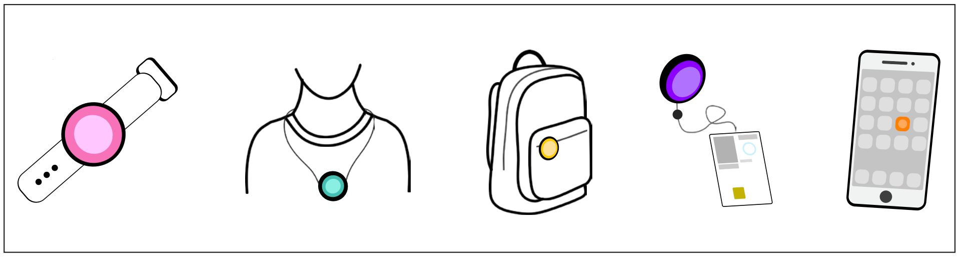


A different approach to exposure notification, not developed by NIST. The protocol permits third party correlation attacks that could derive the identities.

Unlike this approach, the NIST approach does not record any information linked to individuals at any point throughout the entire process. It is impossible to rederive the identity of the devices, or of the device-owners, from the encounter IDs.

For More Information

This project is on-going and collaborative. For more information or to participate, please contact Rene Peralta (rene.peralta@nist.gov) or SaeWoo Nam (saewoo.nam@nist.gov)



Possible designs for NIST's BLE-based exposure notification system.