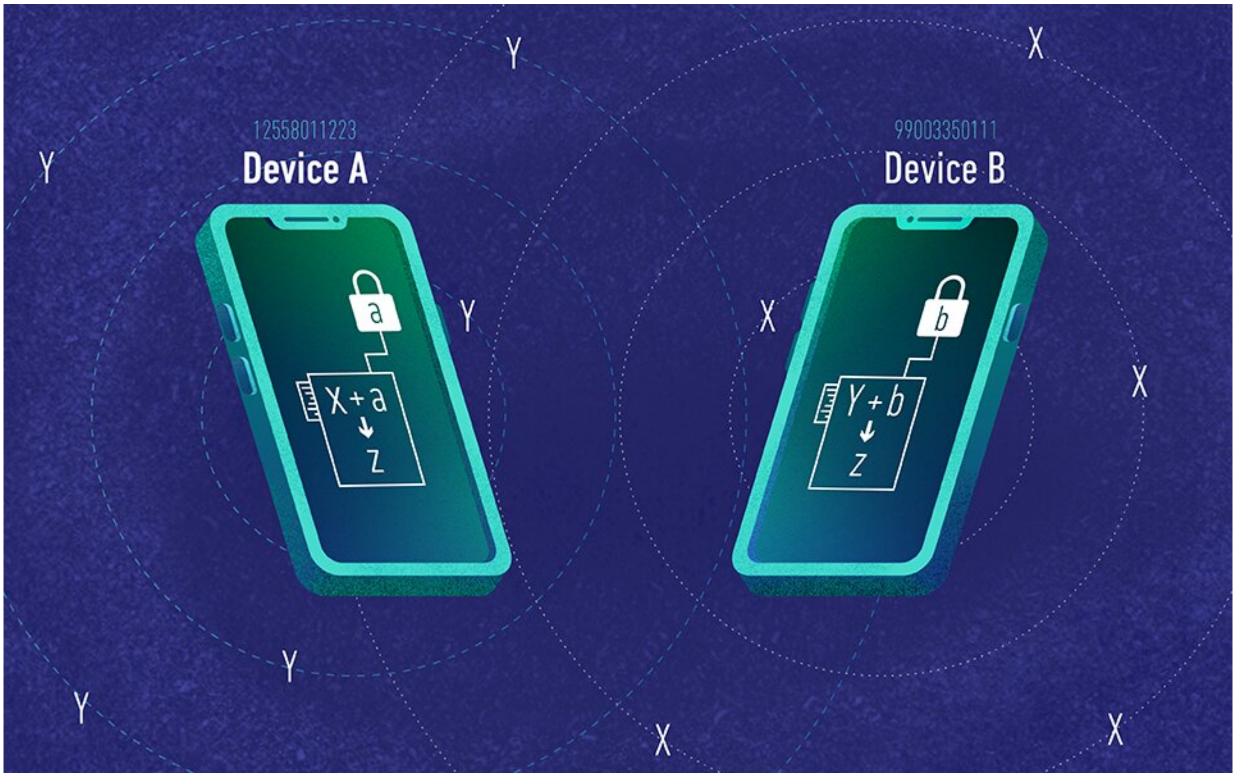
TechXplore

Privacy-preserving 'encounter metrics' that could slow down future pandemics

March 29 2021



NIST researchers developed a cryptographic system using encounter metrics. Encounter ID is a way of labeling an encounter between two people through a random number not linked to the device each person carries. To generate the randomized number Z, each device calculates using their private info (a and b) and what the other device is broadcasting (X and Y). Cryptography ensures that device A's Z is the same as Device B's Z. Credit: B. Hayes/NIST

When you bump into someone in the workplace or at your local coffee shop, you might call that an 'encounter.' That's the scientific term for it, too. As part of urgent efforts to fight COVID-19, a science is rapidly developing for measuring the number of encounters and the different levels of interaction in a group.

At the National Institute of Standards and Technology (NIST), researchers are applying that science to a concept they have created called "encounter metrics." They have developed an encrypted method that can be applied to a device such as your phone to help with the ultimate goal of slowing down or preventing future pandemics. The method is also applicable to the COVID-19 pandemic.

Their research is explained in a pilot study published in the *Journal of Research of NIST*.

Encounter metrics measure the levels of interactions between members of a population. A level of interaction could be the number of people in a bathroom who are talking to each other or a group of people walking down a hallway. There are numerous levels of interactions because there are so many different ways people can interact with one another in different environments.

In order to mitigate the spread of an infectious disease there is the assumption that less communication and interaction with people in a community is essential. Fewer interactions among people means there is less of a chance of the disease spreading from one person to another. "We need to measure that. It's important to develop technology to measure that and then see how we can use that technology to shape our working environment to slow future pandemics," said NIST researcher René Peralta, an author of the NIST study.

Picture two people walking from opposite ends of a hallway who meet in the middle. To record this encounter, each person could carry their own phone or a Bluetooth device that broadcasts a signal as soon as the encounter occurs. One way of labeling this encounter is through the exchange of device IDs or pseudonyms. Each device sends its own pseudonym that belongs to the device itself. The pseudonyms could be changed every 10 minutes as a way to promote the privacy of the person's identity.

However, another way of labeling the encounter between two people is through a random number that is not linked to the device each person carries. This is what the researchers call an "encounter ID." Peralta developed an encrypted system that uses encounter IDs to not only measure the encounter between two people but to strengthen the privacy of the identities of the two people from third parties.

Current approaches for mitigating the spread of infectious disease in a population include exposure notification systems, also known as contact tracing, that rely on the pseudonyms. These systems are currently used on smartphones as a way to digitally track if a person comes into contact with someone who has contracted COVID-19. This can help health officials mitigate the spread of the disease by isolating individuals at risk of infecting others.

But the benefit of the NIST method that uses encounter IDs is its promotion of privacy. By labeling each encounter with a random number and not linking the encounter to the device the person is carrying, this makes it much harder for a cyber attacker to obtain that user's identity.

The target audience for this approach would be for a smaller population in a controlled setting like NIST's campus or nursing homes, said NIST researcher Angela Robinson, also an author of the new paper. "We are advancing a different approach to contact tracing using encounter metrics."

Gathering these measurements of how individuals interact with one another can help with better understanding ways of modifying working environments, such as altering building layouts and establishing mobility rules, so as to slow the spread of disease. These architectural changes though are part of a longer-term goal. "Encounter metrics will give health experts and officials more tools to understand interactions of people and infection events," said Peralta.

Through a broader initiative at NIST in which various groups met and discussion occurred to help address the COVID-19 pandemic, Peralta and Robinson collaborated with NIST researcher Sae Woo Nam, who developed a NIST prototype Bluetooth device that uses the cryptographic system developed by Peralta.

The device is slightly smaller than the size of a playing card and can be easily worn around a person's neck or stored in their pocket. It has a sensor to detect a Bluetooth signal and the duration and strength of the signal. The strength of the signal is used to approximate the distance between two individuals. So, if the signal is weaker, one can conclude that the person is following proper social distancing guidelines and is more than 2 meters (6.56 feet) away.

The NIST prototypes rely on ultrasonic ranging where the device transmits a sound wave and researchers can measure the time it takes for the sound wave to reflect off an object and back to the origin. This means that the reflection time is proportional to the distance that the target object is from the source, in this case the device. Ultrasonic ranging allows for a more accurate determination of distance between two people compared to relying solely on the Bluetooth signal.

Researchers also propose an alternative protocol to current approaches for contact tracing using their method of encounter IDs. The alternative proposal follows three parts: reporting, server storage and risk exposure notification. A person who is diagnosed with COVID can voluntarily and anonymously send their encounter IDs to a central server. The server then maintains a running window of all the reported encounter IDs. Lastly, every day each person participating in contact tracing performs a two-party encrypted computation with the server to get the number of encounter IDs that are both in their list and the server's. That number is the person's measure of risk.

It's important to note that this approach relies on each participant being honest or a good actor when sending their encounter IDs. More detailed information on the approach can be found in the paper.

As for next steps, NIST researchers hope to expand beyond the NIST community to work with the larger research community to invest in privacy-preserving encounter metrics. They also aim to further develop the techniques that are already in place to see how they will hold out in scenarios where there are actual malicious threats. To learn more about other research projects addressing the COVID-19 pandemic that are currently underway at NIST, check out the NIST and COVID-19 web portal.

More information: René Peralta et al, Encounter Metrics and Exposure Notification, *Journal of Research of the National Institute of Standards and Technology* (2021). DOI: 10.6028/jres.126.003

Provided by National Institute of Standards and Technology

Citation: Privacy-preserving 'encounter metrics' that could slow down future pandemics (2021, March 29) retrieved 7 May 2024 from https://techxplore.com/news/2021-03-privacy-preserving-encounter-metrics-future-pandemics.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.