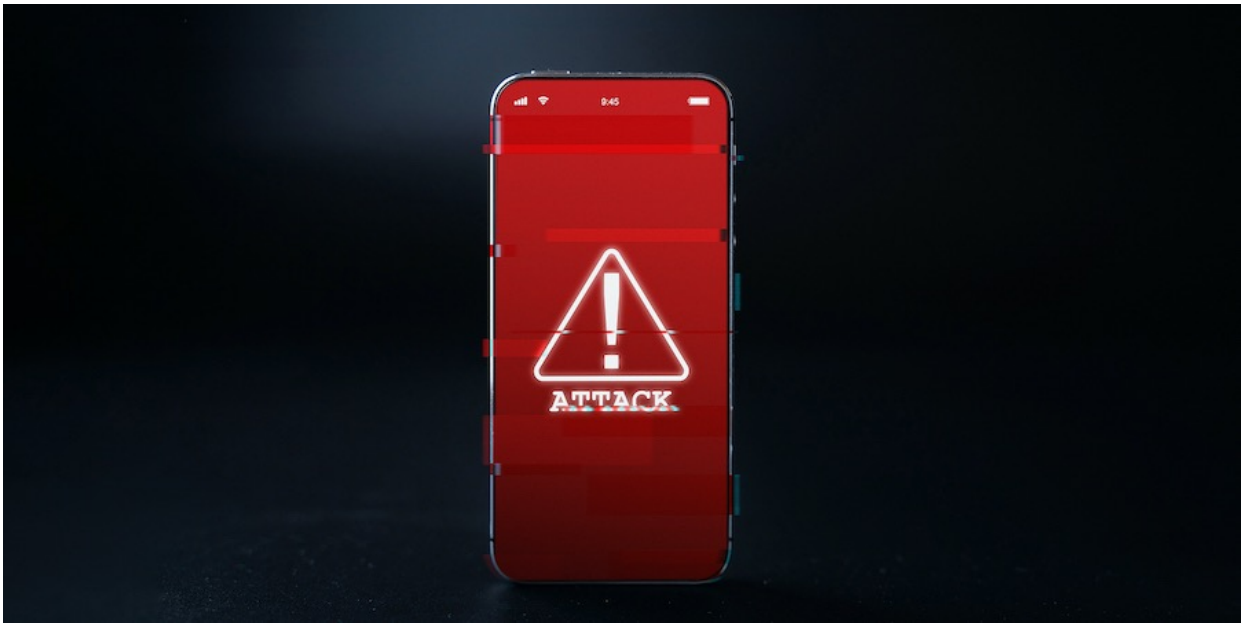
Timing Attacks on WhatsApp, Signal, and Threema can Reveal User Location

Alex Lekander ⋮ 6-8 minutes ⋮ 10/20/2022

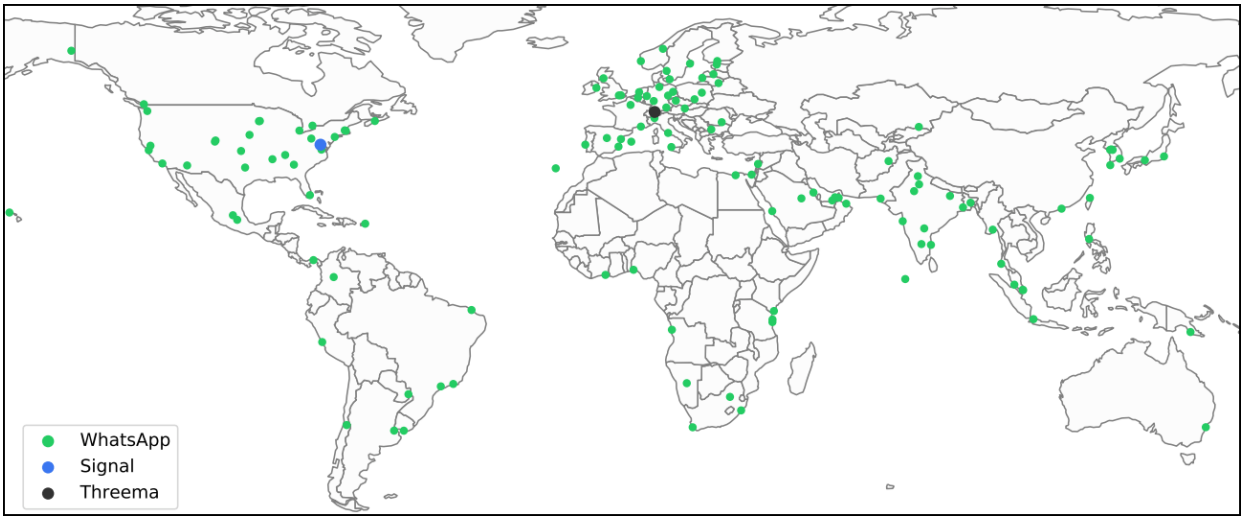


Researchers have identified a vulnerability that undermines location privacy for users of WhatsApp, Signal, and Threema. This report examines the researchers' findings and offers potential solutions for mitigating the attack vector.

A team of researchers has found that it's possible to infer the locations of users of popular instant messenger apps with an accuracy that surpasses 80% by launching a specially crafted timing attack.

The trick lies in measuring the time taken for the attacker to receive the message delivery status notification on a message sent to the target.

Because mobile internet networks and IM app server infrastructure have specific physical characteristics that result in standard signal pathways, these notifications have predictable delays based on the user's position.



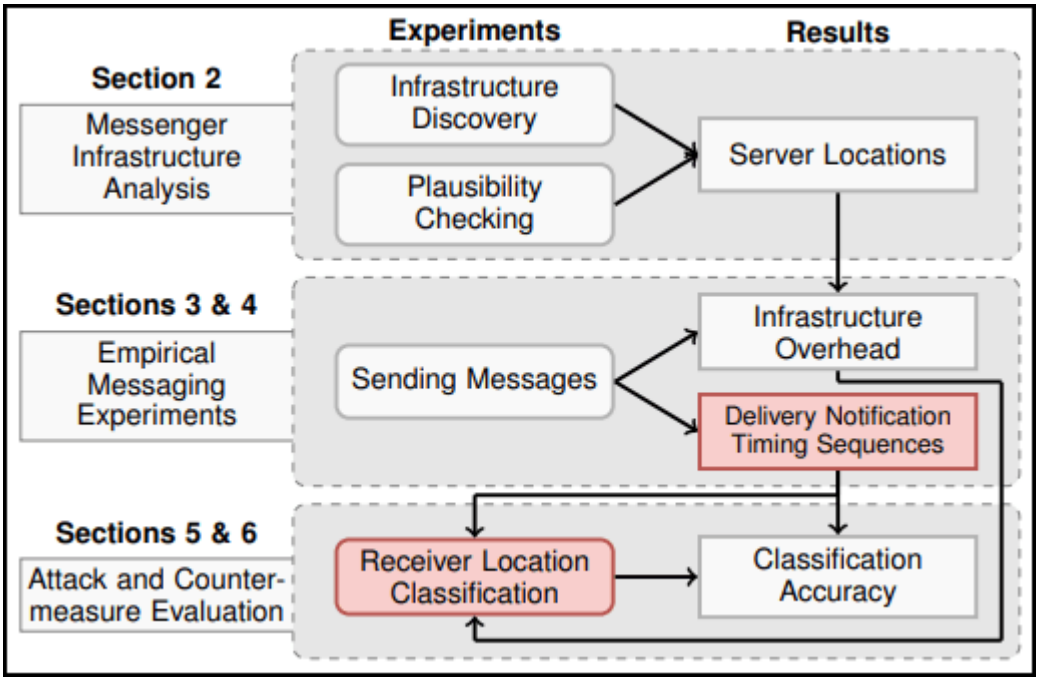
Mapping the infrastructure of popular IM apps
Source: Arxiv.org

By measuring these delays in a preparatory work stage, like sending messages when the target's location is

known, an attacker could figure out where the message recipient is located at any time in the future by simply sending them a new message and measuring the time taken for the delivery status notifications to arrive.

As the researchers analyzed in their technical paper, this timing attack could work well for locating the recipient's country, city, district, and even if they are connected to WiFi or mobile internet.

If the attackers perform enough tests to formulate an extensive dataset against a target, they could infer their position among a set of given possible locations in a city, like “home”, “office”, “gym”, etc., based on nothing else but the delivery notification delay.



Experiment steps to perform the attack
Source: Arxiv.org

These notifications are standard across many popular IM apps, and the researchers confirmed they are exploitable against even the most (generally) secure messenger services, like Signal and Threema, as well as WhatsApp.

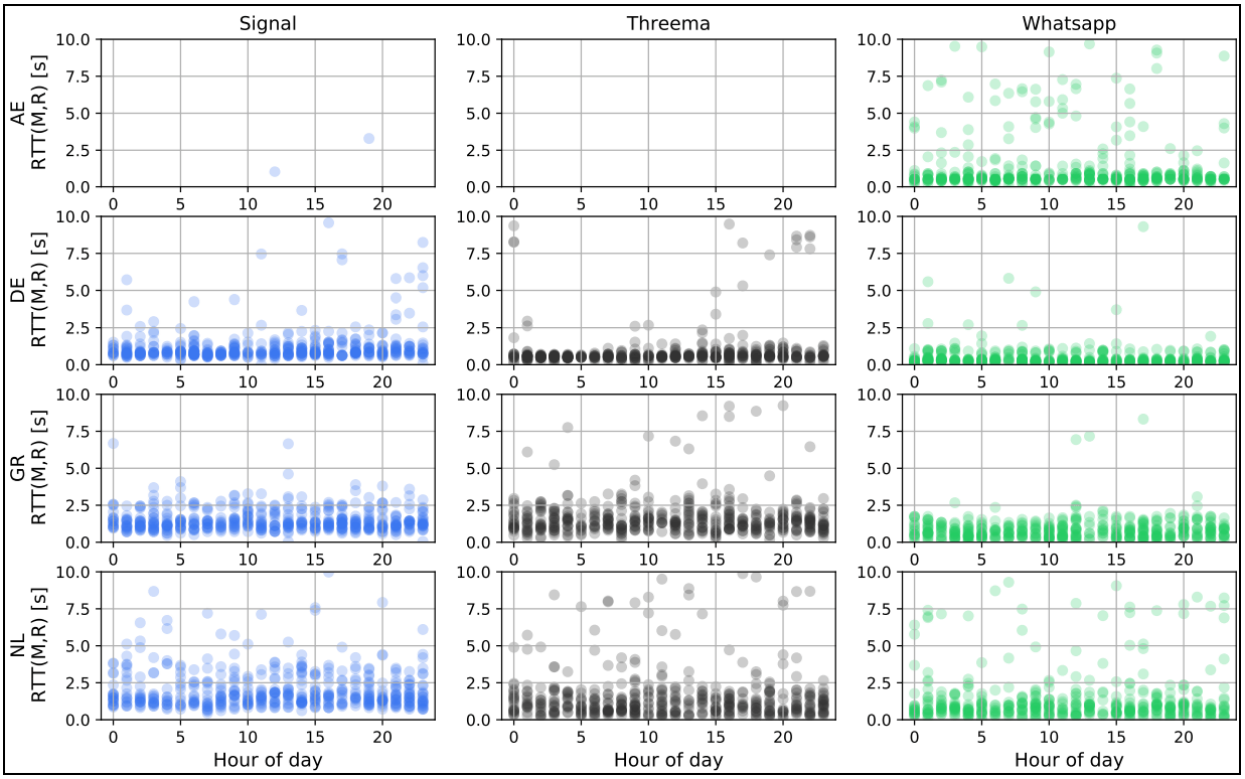
Attack Details

For the timing attack to work, the adversary needs to use a smartphone for sending the messages and a packet capture application like Wireshark to analyze their own TCP traffic and extract the timing information.

The attacker and the victim must know each other and must have engaged in previous conversation on the IM app, which is a requirement for both the attack and the preparatory work.

The network traffic analysis can help the attacker determine which packets are the delivered status notifications. In the apps tested by the researchers, these packets either have predetermined sizes or have identifiable structure patterns.

Next, the attacker needs to classify the different locations and match them to measured “round-trip” times, and then attempt to correlate these pairs with the target's location using the known data set.



Sample measurements of round-trip times
Source: Arxiv.org

The resulting **classification accuracy** based on the researchers\' experiments was:

- **82% for Signal targets**
- **80% for Threema**
- **72% for those using WhatsApp**

Implications of this vulnerability

The implications of this attack are alarming from a user privacy perspective. These platforms, particularly Signal and Threema, promote themselves as secure and private messengers that go above and beyond the security of other platforms.

WhatsApp, the largest of these three messengers, has around 2 billion users based on some estimates. Signal and Threema are much smaller, with around 40 million and 10 million users, respectively.

While billions of people around the world rely on these messengers for secure and encrypted communications, these findings show us that user location privacy remains vulnerable to attack. However, we do identify some potential solutions.

What to do about it

While performing the experiments, the researchers noticed that some devices were idling while receiving the messages, which can mess up the attack results and is practically an unreliable countermeasure.

A solid way for app developers to deal with this problem is to introduce a system that would **randomize the delivery confirmation times to the sender**.

Anything from 1 to 20 seconds would be enough to render this timing attack impossible to carry out while not hurting the practical usefulness of the delivery status notifications.

From the user's perspective, if the app allows **disabling the notification feature** that informs the sender when the message was received, using this setting would deal with the problem decisively by removing the abused element.

Finally, users can also **utilize a VPN (virtual private network)** on mobile devices to **increase latency** and help

obfuscate location data. For example, connecting to a VPN server that is not near one's physical location should interfere with the timing of status notifications. Intermittently switching VPN server locations would further add variability to message timing. However, this assumes these messenger apps are not bypassing the VPN, but recent reports also illustrate vulnerabilities with Android VPNs.

RestorePrivacy has contacted all three messenger apps mentioned in the report. We will update this article with any comments and new information.

UPDATE 1: Two of the named messengers have told RestorePrivacy via email (on October 20th) that they are investigating the situation and will provide a comment on the report shortly.

UPDATE 2: Threema provided RestorePrivacy with the following statement on October 21st:

> We have already considered different workarounds and conducted various tests, including ones where the client randomly delays delivery notifications slightly to render these kinds of timing analyses useless. (App updates containing this improvement should become available soon.)
>
> Please note, however, that the practical exploitability of these timing analyses is debatable: Users typically don't have their messenger app open all the time, and push notifications that wake up the app in the background already add a considerable delay of up to several seconds.
>
> – *Threema GmbH*