Anonymous Remote Attestation in Mobile Devices

Luis A. Saavedra, Alastair R. Beresford
Computer Laboratory, University of Cambridge
luis.saavedra@cl.cam.ac.uk, alastair.beresford@cl.cam.ac.uk

Most mobile apps and online services require users to log in with their personal information to access advanced features and prevent abuse of service infrastructure. For example, authentication is used to limit the effect of Sybil attacks where malicious adversaries pose as multiple users to attack a system. This is particularly important in apps which crowd-source data from users, think everything from star ratings of products on shopping sites to congestion data from travellers gathered by car navigation apps.

A neat example of such a Sybil attack is Weckert's use of 99 old smartphones to trick Google Maps into showing traffic jams on otherwise empty streets.[1] A more scalable attack than Weckert's would analyse how Google Maps' online service functions and submit fake requests programmatically, something which is hard to do because Google makes it difficult to create and authenticate a large number of Google Accounts via a script.

Unfortunately, the requirement to authenticate means that users associate contributed data, such as their current location or product ratings, with their identity. In this talk, we explore an alternative mechanism to reduce the effect of Sybil attacks on crowd-sourced data without requiring users to authenticate. In particular, we propose combining features available in modern smartphones (such as Secure Enclaves and blind signatures) to provide anonymous *remote attestation*, allowing apps to generate anonymous, cryptographically-signed single-use tokens which can be shared with online services.

Services can validate these tokens to see if they come from a real device and therefore whether the information provided with the token is likely to be legitimate. By limiting the number of tokens any given smartphone can send in a particular time period, we can limit the number of verified reports that any given device can send to a service. This can be done without requiring the user to reveal their identity to the online service.

Our approach means that an adversary who wishes to carry out a Sybil against an online service would need to purchase many smartphones in order to generate sufficient tokens to submit crowd-sourced data in bulk. In doing so, we increase the economic cost of an attack significantly.

While this mechanism is useful in general, it is particularly helpful in apps with strong security and privacy requirements. For example, in earlier work we collaborated with The Guardian to embed an anonymous whistleblowing feature inside their news app.[2]

Since such an online service does not (and cannot) require authentication, the current platform is susceptible to spam and can be overwhelmed by an adversary sending large volumes of messages, effectively flooding a journalist's inbox with so many messages that they are unable to find the few real messages amongst the junk. Our proposed approach can be used to limit the number of messages any device can send in a given period, significantly increasing the cost to the adversary of generating large numbers of fake messages.

[1] https://www.wired.com/story/99-phones-fake-google-maps-traffic-jam/
[2] https://www.coverdrop.org