Push Away Your Privacy: Precise User Tracking Based on TLS Client Certificate Authentication

Matthias Wachs
Technical University of Munich (TUM)
wachs@net.in.tum.de

Quirin Scheitle
Technical University of Munich (TUM)
scheitle@net.in.tum.de

Georg Carle
Technical University of Munich (TUM)
carle@net.in.tum.de

ABSTRACT

While the Transport Layer Security (TLS) protocol is typically used to authenticate servers, it also offers the possibility to use Client Certificates for to authenticate clients (CCA). We investigate the use of CCA based on two specific concerns:

First, CCA is prone to being used in a context that encodes personal data into client certificates, such as identifying persons, e.g. in voting systems or VPN applications.

Second, in versions prior to TLS1.3, the client certificate (as well as the server certificate) is being sent in clear text, permitting systematic and large-scale eavesdropping.

Based on these two concerns, we investigate the use of CCA at an ISP uplink. Besides confirming our two concerns by finding, e.g., person names in VPN certificates, we also identify the Apple Push Notification Service (APNs) to leverage TLS CCA to identify client devices. We consider this use highly critical as APNs is an integral part of all Apple operating systems, and APNs establishes a connection immediately upon connecting the device to a network. We show that these properties can be used by various attacker types to track devices (and hence, likely users) with great precision across the global Internet.

This work was published in 2017, with the TLS1.3 standardization still ongoing, and we aimed to emphasize the necessity of encrypting client certificates in the TLS handshake, which was adopted in the TLS1.3 standard. Based on work published at TMA'17 [1].

[1] Matthias Wachs, Quirin Scheitle, Georg Carle. 2017. Push Away Your Privacy: Precise User Tracking Based on TLS Client Certificate Authentication. In Proceedings of the 2017 Network Traffic Measurement and Analysis Conference (TMA '17)

ANRW '18, July 16, 2018, Montreal, QC, Canada
© 2018 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-5585-8/18/07.
https://doi.org/10.1145/3232755.3232763

CCS CONCEPTS

• **Security and privacy** → **Network security**;

KEYWORDS

TLS; Privacy.

ACM Reference Format:
Matthias Wachs, Quirin Scheitle, and Georg Carle. 2018. Push Away Your Privacy: Precise User Tracking Based on TLS Client Certificate Authentication. In *ANRW '18: Applied Networking Research Workshop, July 16, 2018, Montreal, QC, Canada.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3232755.3232763