Studying TLS Usage in Android Apps

Abbas Razaghpanah
Stony Brook University
arazaghpanah@cs.stonybrook.edu

Arian Akhavan Niaki
UMass-Amherst
arian@cs.umass.edu

Narseo Vallina-Rodriguez
IMDEA Networks Institute/ICSI
narseo.vallina@imdea.org

Srikanth Sundaresan
Facebook
srknth.s@gmail.com

Johanna Amann
ICSI/Corelight
johanna@icir.org

Philippa Gill
UMass-Amherst
phillipa@cs.umass.edu

ABSTRACT

First standardized by the IETF in the 1990's, SSL/TLS is the most widely-used encryption protocol on the Internet. This makes it imperative to study its usage across different platforms and applications to ensure proper usage and robustness against attacks and vulnerabilities. While previous efforts have focused on the usage of TLS in the desktop ecosystem, there have been no studies of TLS usage by mobile apps at scale. In our study, we use anonymized data collected by the Lumen mobile measurement app to analyze TLS usage by Android apps in the wild. We analyze and fingerprint handshake messages to characterize the TLS APIs and libraries that apps use, and evaluate their weaknesses. We find that 84% of apps use the default TLS libraries provided by the operating system, and the remaining apps use other TLS libraries for various reasons such as using TLS extensions and features that are not supported by the Android TLS libraries, some of which are also not standardized by the IETF. Our analysis reveals the strengths and weaknesses of each approach, demonstrating that the path to improving TLS security in the mobile platform is not straightforward.

Based on work published at: Abbas Razaghpanah, Arian Akhavan Niaki, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Johanna Amann, and Phillipa Gill. 2017. Studying TLS Usage in Android Apps. In Proceedings of CoNEXT '17. ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3143361.3143400

KEYWORDS

Security Protocols; Android; Mobile; Network Measurements; Transport Layer Security; Secure Sockets Layer; SSL; TLS; Transport Layer Protocols; Mobile Security.

ACM Reference Format:
Abbas Razaghpanah, Arian Akhavan Niaki, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Johanna Amann, and Philippa Gill. 2018. Studying TLS Usage in Android Apps. In *ANRW '18: Applied Networking Research Workshop, July 16, 2018, Montreal, QC, Canada.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3232755.3232779

CCS CONCEPTS

• **Security and privacy** → **Security protocols**;

ANRW '18, July 16, 2018, Montreal, QC, Canada

ACM ISBN 978-1-4503-5585-8/18/07.
https://doi.org/10.1145/3232755.3232779