POSTER: Experimental Analysis of Popular Anonymous, Ephemeral, and End-to-End Encrypted Apps

Lucky Onwuzurike
Computer Science Department
University College London

Emiliano De Cristofaro
Computer Science Department
University College London

ABSTRACT

As social networking takes to the mobile world, smartphone apps provide users with ever-changing ways to interact with each other. Over the past couple of years, an increasing number of apps have entered the market offering end-to-end encryption, self-destructing messages, or some degree of anonymity. However, little work thus far has examined the properties they offer. We present a taxonomy of 18 of these apps: we first look at the features they promise in their appeal to broaden their reach and focus on 8 of the more popular ones. We present a technical evaluation, based on static and dynamic analysis, and identify a number of gaps between the claims and reality of their promises.

1. INTRODUCTION

Following Edward Snowden's revelations, privacy and anonymity technologies have been increasingly often in the news, with a growing number of users becoming aware – loosely speaking – of privacy and encryption notions [2]. Service providers have rolled out, or announced they will, more privacy-enhancing tools, e.g., support for end-to-end encryption or HTTPS by default. At the same time, a number of smartphone apps and mobile social networks have entered the market, promising to offer features like anonymity, ephemerality, and/or end-to-end encryption (E2EE). While it is not that uncommon to stumble upon claims like "military-grade encryption" or "NSA-proof" in the description of these apps, little work thus far has actually analyzed the guarantees they provide.

This motivates the need for a systematic study of a careful selection of such apps. To this end, we compile a list of 18 apps that either offer E2EE, anonymity, ephemerality, or a combination of any two, focusing on 8 popular ones (Confide, Frankly Chat, Secret, Snapchat, Telegram, Whisper, Wickr, and Yik Yak). We review their functionalities and perform an empirical evaluation, based on *static* and *dynamic* analysis, aimed to compare the claims of the selected apps against results of our analysis.

Highlights of our findings include that "anonymous" social network apps Whisper and Yik Yak actually identify users with persistent distinct user IDs. Users' (previous) activities are restored to their device after uninstalling and reinstalling the apps, and information collected by these apps could be used to de-anonymize them. We also find that the ephemeral-messaging app Snapchat does not always delete messages from its servers – in fact, "expired" chat messages are included in packets sent to the client. Then, we report that all actions performed by a user on Frankly Chat can be observed from the request URL, which is actually transmitted in the clear.

Note: An extended version of this poster abstract appears in [3].

2. BUILDING AN APP CORPUS

We build a list of smartphone apps that are categorized as "anonymous" on Product Hunt [1], and those popular among friends and colleagues. We then look at *similar apps* on Google Play, and focus on those described as offering end-to-end encryption, anonymity and/or ephemerality, as defined below:

Anonymity: is defined as the property that a subject is not identifiable within a set of subjects, known as the anonymity set [4]. In the context of this study, the term anonymity will be used to denote that users are anonymous w.r.t. other users of the service or w.r.t. the app service provider.

End-to-End Encryption (E2EE): Data exchanged between two communicating parties is encrypted in a way that only the sender and the intended recipient can decrypt it, so, e.g., eavesdroppers and service providers cannot read or modify messages.

Ephemerality: In cryptography, it denotes the property that encryption keys change with every message or after a certain period. Instead, here ephemerality is used to indicate that messages are not available to recipients from the user interface after a period of time [1]. For instance, in apps like Snapchat, messages "disappear" from the app (but may still be stored at the server) a few seconds after they are read.

First List. We initially select 18 apps, listed in Table 1, where we also report their first release date, number of downloads as reported by Google Play, the kind(s) of content that can be shared, and whether the apps create persistent social links.

Apps Selection. We focus on apps with the most downloads that offer ephemerality, anonymity, E2EE, or, preferably, a combination of them. We reduce our selection to the top 8 apps (bold entries in Table 1) with most downloads, selecting an app with more than one of our desired property when there is more than one app with same number of download. We exclude Silent Circle and TigerText as they require paid subscription and registered company email respectively.

[1] http://www.producthunt.com/e/anonymous-apps

WiSec'16 July 18-22, 2016, Darmstadt, Germany
© 2016 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-4270-4/16/07.
DOI: http://dx.doi.org/10.1145/2939918.2942424

App	Launch	#Downloads	Type	Content	Anonymity	Ephemerality	E2EE	Social Links
20 Day Stranger	2014	Unknown	Temporary OSN	Photos and location	Yes	No	No	No
Armortext	2012	50–100K	Chat (Enterprise)	Text and files	No	User-defined	Yes	Yes
BurnerApp	2012	100–500K	Temporary numbers	Call and SMS	N/A	N/A	No	Yes
Confide	2014	100–500K	Chat	Text, documents, photos	No	**After message is read**	**Yes**	Yes
CoverMe	2013	100–500K	Chat	Text, voice, photos, videos	No	User-defined	Yes	Yes
Disposable Number	Unknown	100–500K	Temporary numbers	Call and SMS	N/A	N/A	No	Yes
Frankly Chat	2013	500K–1M	Chat	Text, pictures, videos, voice	Optional for group chat	**10s**	No	Yes
Secret	2014	5–10M	Anonymous OSN, Chat	Text, photos,	**Yes**	No	No	Yes/No
Seecrypt SC3	2014	10–50K	Chat	Text, voice, files	No	No	Yes	Yes
Silent Circle	2012	100–200K	Encrypted Phone	Call, SMS, files	No	User-defined	Yes	Yes
Snapchat	2011	100–500M	Transient OSN	Photos, videos	No	**1 – 10s**	No	Yes
Telegram	2013	50–100M	Chat	Text, photos, audio, videos, files, location	No	**Optional**	**Optional**	Yes
TextSecure	2010	500K–1M	Chat	Text, files	No	No	Yes	Yes
TigerText	2010	500K–1M	Chat	Text, files	No	User-defined	Yes	Yes
Vidme	2013	50–100K	Video Sharing	Videos	Yes	No	No	No
Whisper	2012	1–5M	Anonymous OSN, Chat	Text, photos	**Yes**	No	No	No
Wickr	2012	100–500K	Chat	Text, files, photos, audio, videos	No	**User-defined**	**Yes**	Yes
Yik Yak	2013	1–5M	Local Bulletin	Text	**Yes**	No	No	No

Table 1: Our first selection of 18 smartphone apps providing at least one among ephemerality, anonymity, or end-to-end encryption. N/A denotes ‘Not Applicable’. Apps in bold constitute the focus of our analysis.

3. ANALYSIS

Static Analysis. We perform static analysis of the 8 apps using dex2jar and JD-GUI to decompile them, aiming to analyze SSL/TLS implementations and look for potential information leakage. We inspect the `TrustManager` and `HostnameVerifier` interfaces used to accept or reject a server’s credentials.

We find Frankly Chat, Whisper, and Wickr all contain `TrustManager` and `HostnameVerifier` that accept all certificates or hostnames. Alas, this makes it possible for an adversary to perform *Man-in-The-Middle (MiTM)* attacks and retrieve information sent on the sockets that use the vulnerable `TrustManager` and/or `HostnameVerifier`.

Dynamic Analysis. We conduct our experiments on a LG Nexus 4 running Android 5.1, that connects to a Wi-Fi access point under our control. We perform actions that include: sign-up, login, profile edit, send/read messages, while at the same time, monitoring traffic transmitted and received by the apps. We collect traffic using Wireshark and analyze unencrypted traffic to check for sensitive information transmitted in the clear. We also rely on HTTP proxies such as Fiddler and SSLSplit to mount Man-in-The-Middle (MiTM) attacks and decrypt HTTPS traffic. We used two different proxies because some Android apps are programmed to ignore proxy settings, hence, we used Fiddler as a regular proxy and SSLSplit as a transparent proxy.

When no proxy is used, traffic captured by Wireshark show that Frankly Chat leaks the Android advertising ID (a unique identifier) and Secret leaks Google Maps location requests (and responses). A summary of the results when a proxy is used is shown in Table 2. We found that anonymous social networks Whisper and Yik Yak actually identify their users with distinct IDs that are persistent as previous activities like chats, *whispers* and *yaks* are restored to the device even if the user uninstalls and reinstalls the app. This behavior shows that, although they do not require users to provide their email or phone number, they can still persistently link – and possibly de-anonymize – users. Also, while Snapchat promises that messages will “disappear” after 10 seconds, they are not immediately deleted from its servers, as old messages are actually included in responses sent to the clients even though not always.

App	Fiddler	SSLSplit
Confide	No connection	No connection
Frankly Chat	TLS traffic is decrypted but packets containing chat messages not routed through proxy	TLS traffic is decrypted but there is no connection to the server when chat is attempted
Secret	All packets decrypted	Not Available (discontinued before we started using the transparent proxy)
Snapchat	All packets decrypted	All packets decrypted
Telegram	Connects but traffic does not pass through proxy	TLS traffic is decrypted but E2EE is enabled
Whisper	No connection	No connection
Wickr	Connects but traffic does not pass through proxy	TLS traffic is decrypted but E2EE is enabled
Yik Yak	All packets decrypted	All packets decrypted

Table 2: Summary of Dynamic Analysis Results.

Acknowledgments. We wish to thank Balachander Krishnamurthy for motivating our research. This research is partly supported by PRESSID, a Xerox’s University Affairs Committee award, and EU grants H2020-MSCA-ITN-2015 “Privacy&Us” and H2020-MSCA-RISE “ENCASE.”

4. REFERENCES

[1] N. Bilton. Why I Use Snapchat: It’s Fast, Ugly and Ephemeral, New York Times. http://nyti.ms/1jBMZrQ, 2014.

[2] P. H. O’Neill. The state of encryption tools, 2 years after Snowden leaks. http://www.dailydot.com/politics/encryption-since-snowden-trending-up/, 2015.

[3] L. Onwuzurike and E. De Cristofaro. Experimental Analysis of Popular Smartphone Apps Offering Anonymity, Ephemerality, and End-to-End Encryption. In *NDSS Workshop on Understanding & Enhancing Online Privacy*, 2016.

[4] A. Pfitzmann and M. Hansen. A Terminology for Talking about Privacy by Data Minimization. https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf, 2010.