UCL

UEOP 2016

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

Lucky Onwuzurike and Emiliano De Cristofaro

University College London

https://emilianodc.com

Politics

The state of encryption tools, 2 years after Snowden leaks

Yahoo, like Google, plans encrypted email

NSA-proof encryption exists. Why doesn't anyone use it?

NSA Docs Reveal Spy-Proof Encryption Tools

***BY** DAMON POETER* 30 DEC 2014, 12:52 A.M.

Cryptography: How is military grade encryption defined?

If possible from Restricted to above Top Secret.

7 Answers

Andy Manoske, I do my own cryptanalytic stunts

9.4k Views • Upvoted by Jim Gordon, Third generation to serve in the US military, grew up on air bases, served (USAF 1966-70 VN); US De…

TL;DR: The term military grade encryption is generally marketing BS.

Wed Jan 27, 2016 11:44am EST

Related: ENTERTAI

Sean Penn Used BlackBerry Messenger & Encrypted 'BlackPhone' to Keep in Touch With Drug Lord 'El Chapo'

By JOMAR ENDRIGA (NEWS@GOSPELHERALD.COM) Jan 10, 2016 11:36 PM EST

"Sometimes I just wish we would crash so I

Keep sensitive data in texts private and screenshot-proof with Confide

If you're concerned about the privacy of sensitive data transmitted via SMS, you may want to employ the Confide app for all business-related SMS messages.

By Jack Wallen | November 18, 2015, 9:41 PM PST

Our Work

More and more apps marketed as offering some privacy/anonymity properties…

- But very little work has actually analyzed their property

We present a preliminary, experimental study of 8 popular apps, offering:

- Anonymity
- End-to-End Encryption (E2EE) and/or
- Ephemeral Messaging

Main Goal:

- Static and dynamic analysis “everyone” can do

Building an App Corpus

Build a list of "privacy" apps from:

- Producthunt ("anonymous")
- Popular apps among friends and colleagues
- Google Play's similar apps

First list yields 18 apps, then we select based on:

- Popular apps (100K+ downloads on Google Play)
- Offering anonymity, E2EE, ephemerality
- Exclude paid/business apps (e.g., TigerText, Silent Circle)

Apps (1/2)

1. Confide

E2EE & ephemeral chat, notification of screenshot attempts

Need to wand over messages, displaying one line at a time

2. Frankly Chat

Ephemeral chat, anonymous group chats

Messages deleted from server after 24 hours

3. Secret (discontinued)

Posting anonymously to nearby users, can chat privately

4. Snapchat

Chat with text and media disappearing after 1-10s

Apps (2/2)

5. Telegram

Supports E2EE “secret chats” with proprietary algorithm

6. Whisper

Anonymously share texts atop images, can respond with private chats

7. Wickr

E2EE and ephemeral chats

8. Yik Yak

Bulletin-board social network, post yik anonymously

Static Analysis

Decompiled the apps using dex2jar, looked for vulnerable interfaces:

TrustManager, HostnameVerifier, SSLSocketFactory, HttpsURLConnection

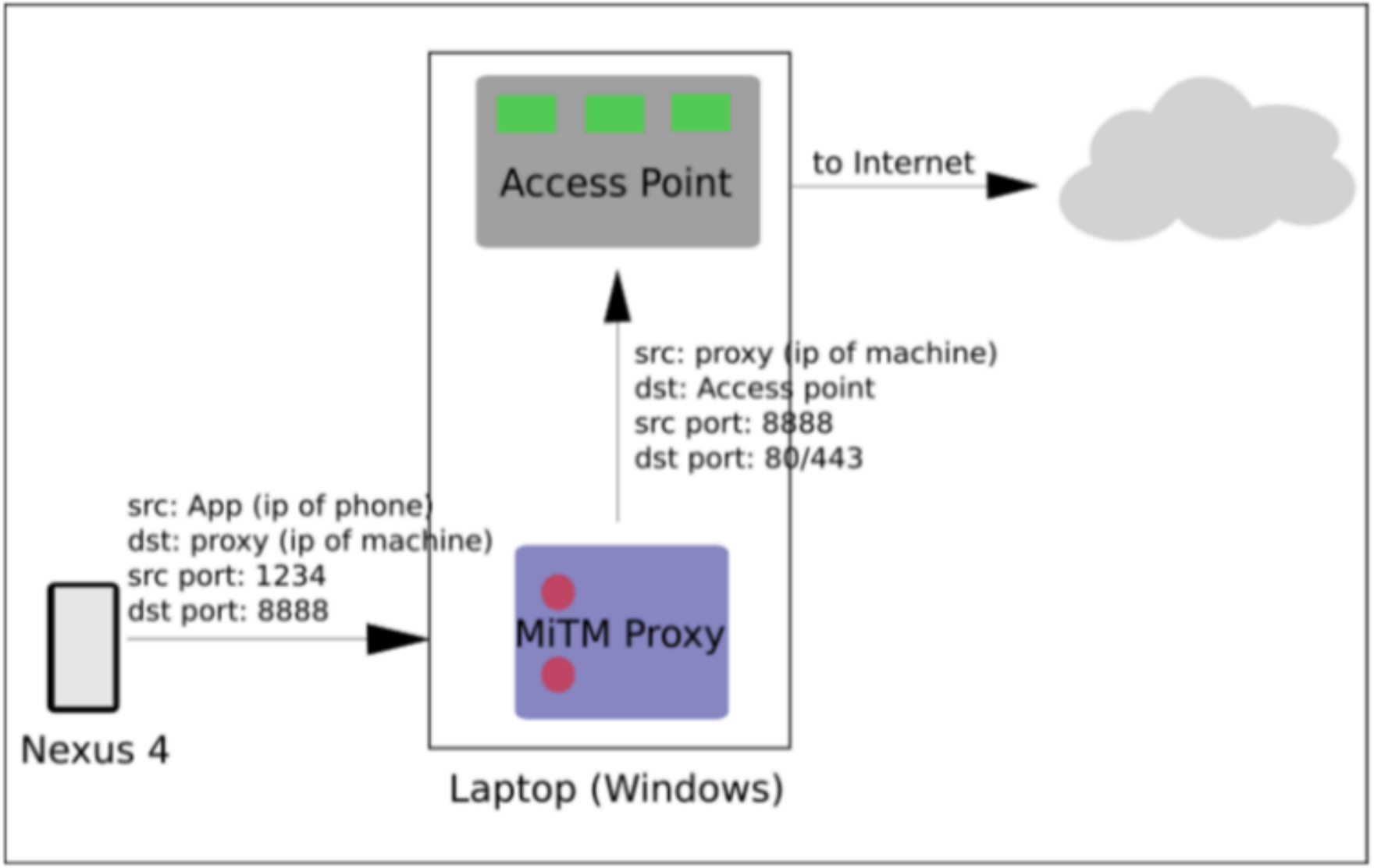
Frankly Chat (partly), Whisper, Wickr maybe vulnerable to Man in The Middle attacks

TrustManager and HostnameVerifier accept all certificates and hostnames

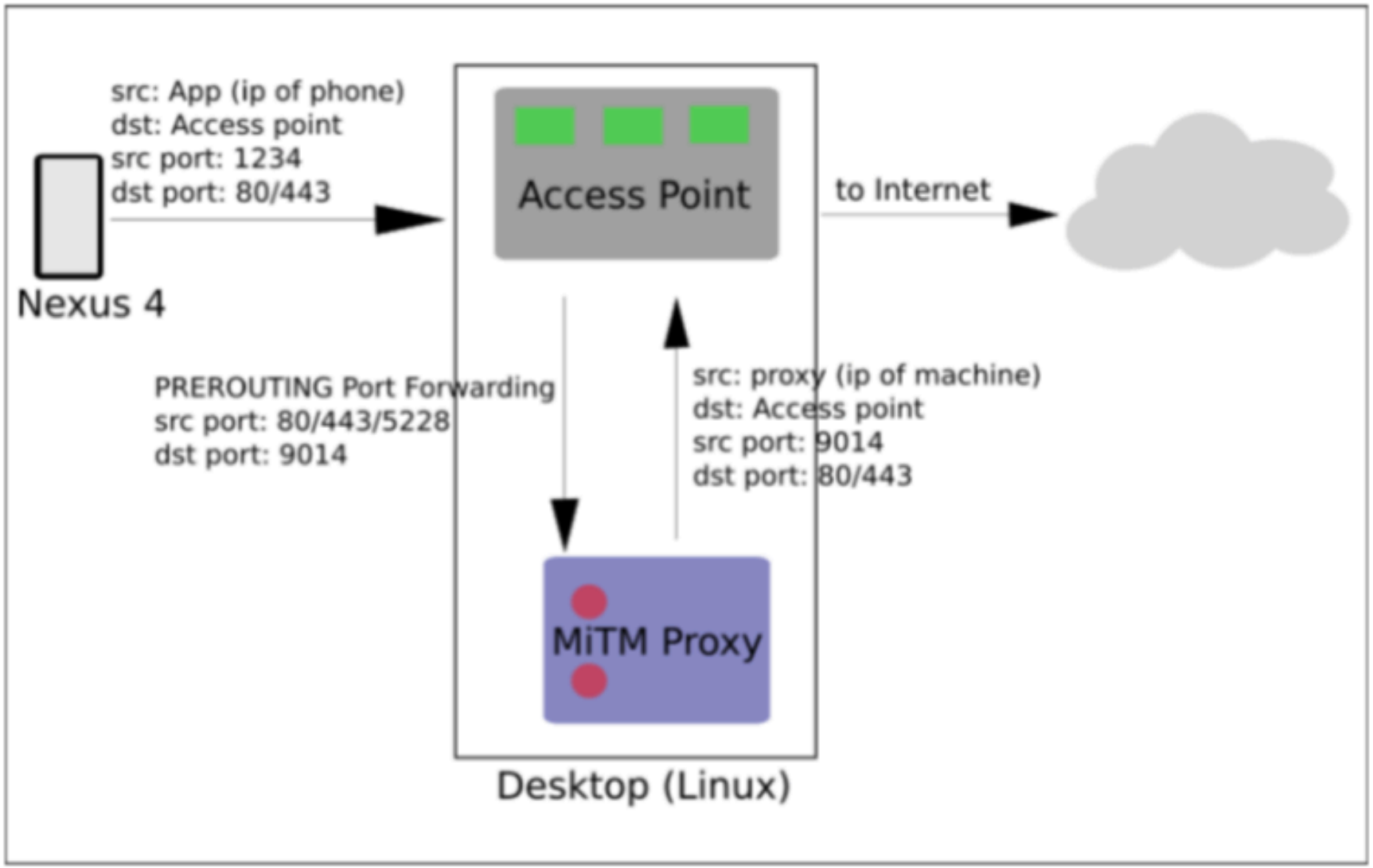
Certificate Pinning in

Confide, Frankly Chat (chat sockets), Whisper (from April 2015)

Dynamic Analysis: Fiddler



Dynamic Analysis: SSLsplit



Dynamic Analysis Feasibility 1/2

Confide

No connection with either Fiddler or SSLsplit due to pinning

Frankly Chat

Fiddler: Decrypted but chats not going through proxy

SSLsplit: No connection to the server when chat attempted

Secret

Fiddler: All TLS packets decrypted
SSLsplit: Discontinued before we could experiment

Snapchat

Fiddler & SSLsplit: All TLS packets decrypted

Dynamic Analysis Feasibility 2/2

Telegram (Secret Chats)

Fiddler: Connects but chats not going through proxy

SSLsplit: Decrypts TLS but chats E2EE'ed

Whisper

Fiddler: No connection, SSLsplit: No connection

Wickr

Fiddler: Traffic does not go through the proxy

SSLsplit: TLS decrypted but E2EE is enabled

Yik Yak

Fiddler & SSLsplit: All TLS packets decrypted

Anonymity

W.r.t. other users:

All good but…in Whisper, one can link whispers to a display name while querying the distance to a target (also in IMC'14)

W.r.t. service provider:

All apps associate identifiers to its users, allowing to link each user across multiple sessions

Identifiers are persistent in Secret, Whisper, and Yik Yak ***even after uninstall***

Apps also collect information like device ID, IP address, geo-location, which can be used to track users

Ephemerality

Messages do disappear from the apps interface

But, in **Snapchat**, previous chat messages part of the response received from the server (?!?)

Screenshot protection/notification works but obviously one can take a picture/video

- Confide claims to offer *"plausible deniability"*
  (need to wand over messages, so can't take snapshot)

E2EE

E2EE seems to work in Telegram & Wickr

- Telegram uses homebrew encryption
- Bounty program, no attack so far (other issues though…)
- See http://motherboard.vice.com/read/encryption-app-telegram-probably-isnt-as-secure-for-terrorists-as-isis-thinks

Other Comments

Impersonation via SMS interception

Metadata often more relevant

Monetization?

Related Work 1/2

Measurement-based studies

- Whisper vulnerability (recover Whispers)
- Anonymity sensitivity & choices in Quora

Flaws

- Reconstructing Snapchat's user base
- Linkability in Wickr
- Security of E2EE cryptography

Related Work 2/2

Privacy Perceptions

- Discrepancy between actual and desired privacy settings
- Why use ephemeral messages?
- Perceptions of privacy issues with apps and social networks

Ideas for Future Work

Larger, automated analysis of apps

- Using PlayDrone's metadata as corpus

Cryptanalysis of E2EE tools

Privacy analysis of metadata

Whatsapp and Signal

The End

Questions?

Acknowledgments: Balachander Krishnamurthy, Ruba Abu-Salma, PRESSID, Xerox's University Affairs Committee, Marie Curie Program