Technische Universität München, Department of Informatics

Chair for Network Architectures and Services
Prof. Dr.-Ing. Georg Carle

Thesis B.Sc.

Thesis M.Sc.

Investigating Mobile Messaging Security – Who can read your WhatsApp/Threema/$other messages?

Motivation

© OpenWhisper

SmartPhone messaging apps have seen an astonishing growth in usage in recent years – according to WhatsApp's own claims, they achieved 500 Million active users and 30 billion messages per day in January 2015. Numerous reports of security flaws in these apps as well as the purchase of WhatsApp by Facebook for USD ∼19 billion raise the question of data security and privacy of these apps: Depending on the level of encryption and the transport path, not only the backend operator but various entities will be able to copy and potentially decrypt messages. Threema e.g. is advertised to only process messages in Switzerland under Swiss jurisdiction and hence "save" from access of foreign agencies. However, messages still could be intercepted on their path to Switzerland. The aim of this work is to determine both the country that messages are processed in as well as the path messages typically take to get there. This yields insight into potential eavesdroppers on these messages. A potential extension is to evaluate what kind of encryption is applied in the messages (only transport to server or end-to-end, message only or metadata as well) and derive what capabilities an attacker would need to gain what level of insight.

Your Task

- Build a set of popular and/or allegedly secure smartphone messaging apps (e.g. WhatsApp, Threema, SIMSme, iMessage, weChat)
- Build a small testbed to conduct security measurements (Linux WiFi router)
- Conduct measurements on this testbed (Target IP extraction, possibly classification of crypotgraphy)
- Traceroute target servers from various vantage points (TUM, PlanetLab, ...)
- Assess target and transit organizations/geographies of messages (traceroute)

Contact

Quirin Scheitle scheitle@net.in.tum.de
Matthias Wachs wachs@net.in.tum.de

http://go.tum.de/644204