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 2 – How strong is WhatsApp/Threema/$others' transport security?

Motivation

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. This thesis will focus on the transport layer security of mobile messaging apps and to determine whether it can be broken to allow for message interception or even modification. For this, it will 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. We then try to build these capabilities in our testbed, using e.g. Man-in-the-middle proxies.

© OpenWhisper

Your Task

- Understand layers of data and encryption in use (based on existing traffic captures)
- Analyze global distribution of TLS/HTTPS certificates in those traffic captures
- Conduct your own measurements in our existing testbed and try to break the transport layer encryption

Contact

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

http://go.tum.de/644204