

When Signal Hits the Fan

On the Usability and Security of State-of-the-Art Secure Mobile Messaging

Svenja Schröder

Cooperative Systems Research Group

University of Vienna

<http://cosy.univie.ac.at>

Markus Huber, David Wind,

Christoph Rottermann

St. Pölten University of Applied Sciences

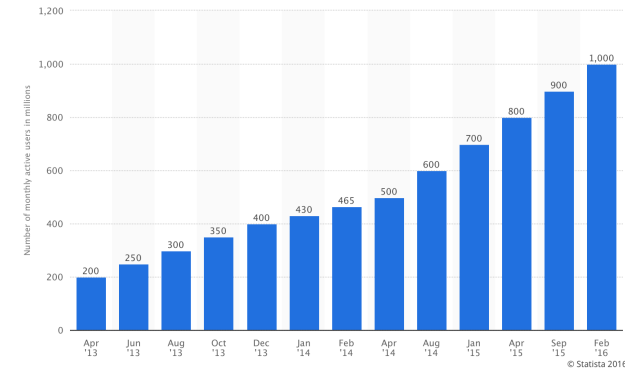
<http://fhstp.ac.at>

Darmstadt, July 18th 2016

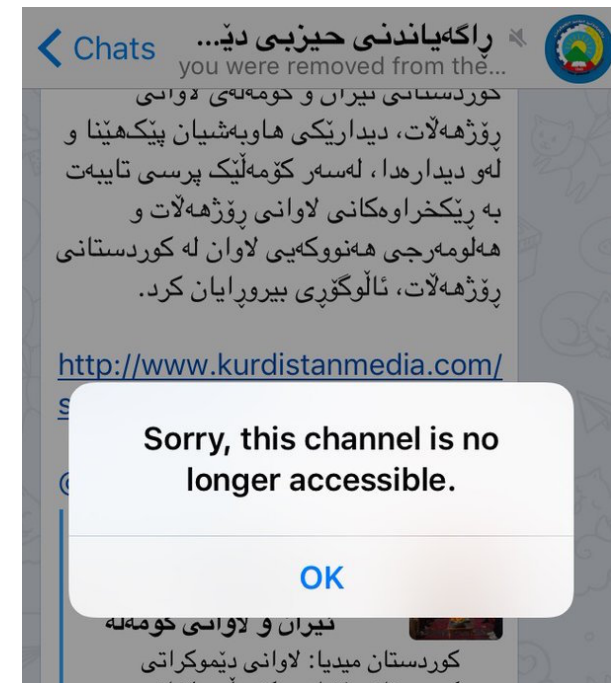


Motivation & Background

- Today: over 1 billion **WhatsApp** users worldwide
- Attacks on secure mobile messengers happen... (e.g. Telegram Iran: SMS Login¹)
- ... and good usability of security features is still hard to achieve²
- E2e encryption tools available for decades, but lack widespread adoption due to bad usability [1] [2] [3] [4]
- Today: two important aspects have changed:
 - » Ubiquitous communication via mobile devices continues to gain importance
 - » Increased general awareness of privacy and security
- → Rise of e2e encrypted mobile messengers



Source: <http://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users>



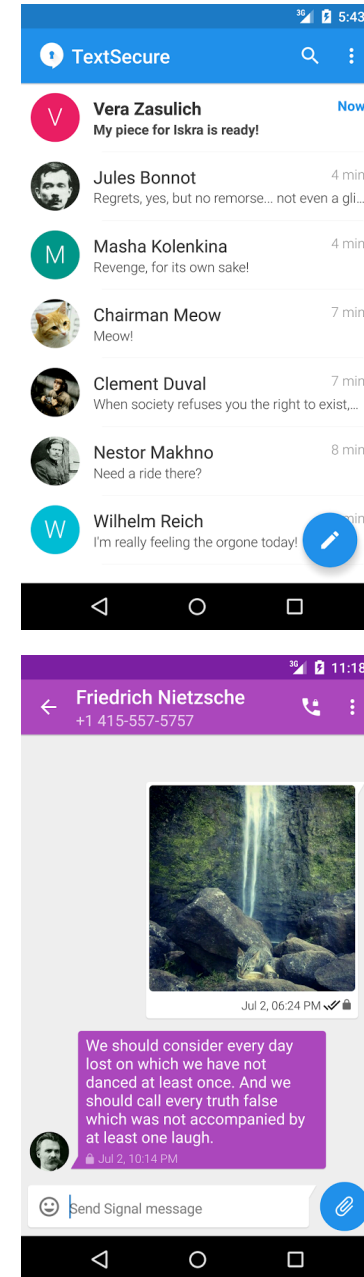
Source: <https://twitter.com/KevinMiston/status/686537567051890688/>

¹ <https://www.fredericjacobs.com/blog/2016/01/14/sms-login>

² <https://theintercept.com/2016/07/02/security-tips-every-signal-user-should-know/>

User Study of Signal

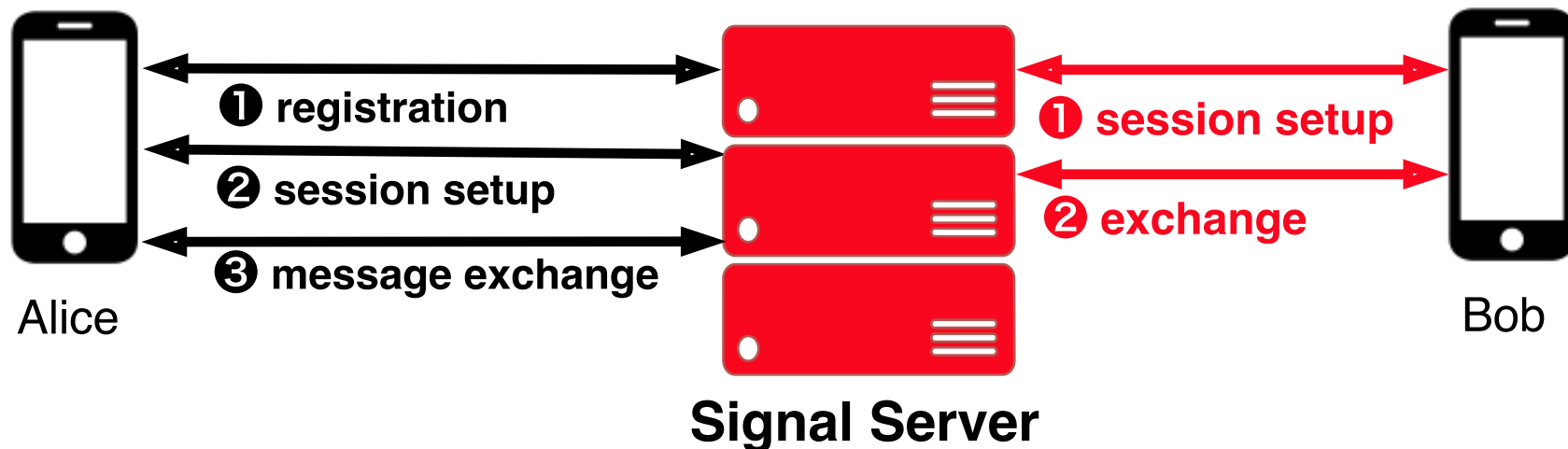
- **Signal**¹: State-of-the-art secure mobile messenger on Android and iOS
 - » Open Source and strong encryption protocol
 - » Protocol for e2e encrypted messaging adopted by **WhatsApp** (April 2016)
- User study to analyze **Signal**'s security and usability features
 - » Exploration of the users' abilities to notice, handle and mitigate man-in-the-middle attacks



¹ <https://whispersystems.org>

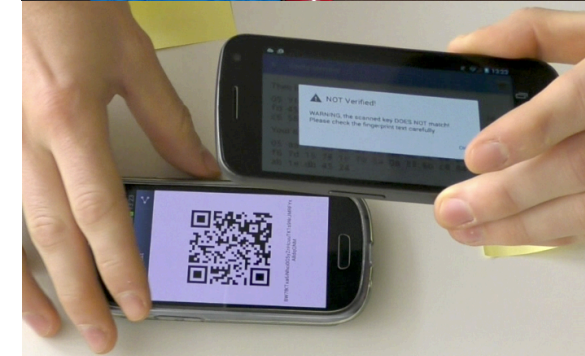
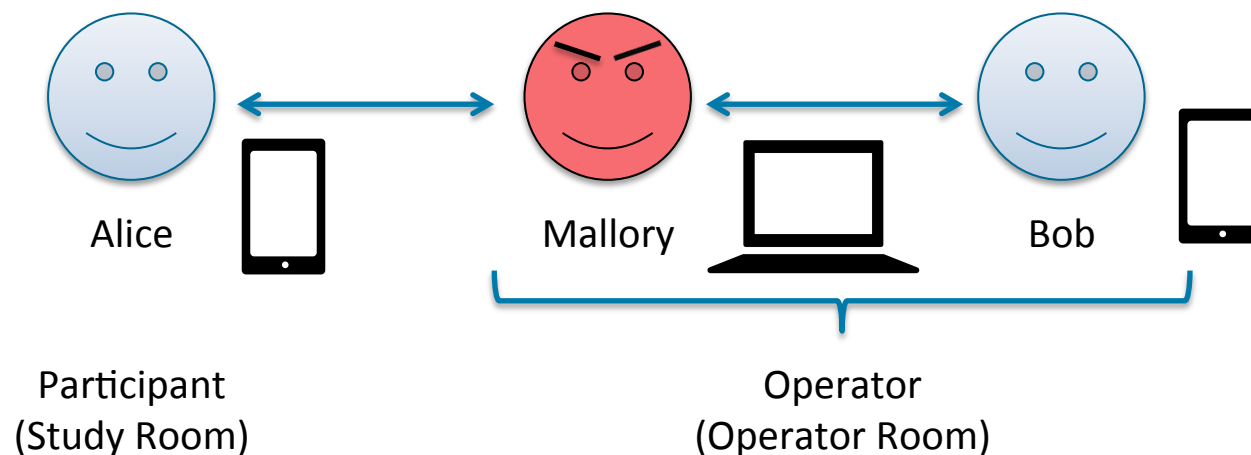
E2E Encryption in Signal

- Forward secrecy + asynchronous message exchange
 - » Combination of PGP-like asynchronous messaging with security properties of OTR [5]
- Central services to exchange cryptographic keys
 - » Man-in-the-Middle attack as compromise of essential infrastructure of today's service messaging apps
- Out-of-bound channel verification of public Identity Keys necessary



User Study: General Setting & Pilot Study

- User Study in a laboratory setting (COSY:lab) with 28 participants (7 f., 21 m.)
- Pilot study (6 p.) to refine experimental design
- Methodology: Questionnaire (quant., qual.), Think Aloud, observation



Study Design

- Two parts:

- 1) Usability study of messaging and security functionality

- » Questionnaire with demographics, general privacy/security behavior, instant messaging
- » Tasks: Chat functionality, setting password, export/import of data

In-between: Launch of simulated MITM attack with compromised server

- 2) Users' reactions to the MITM attack

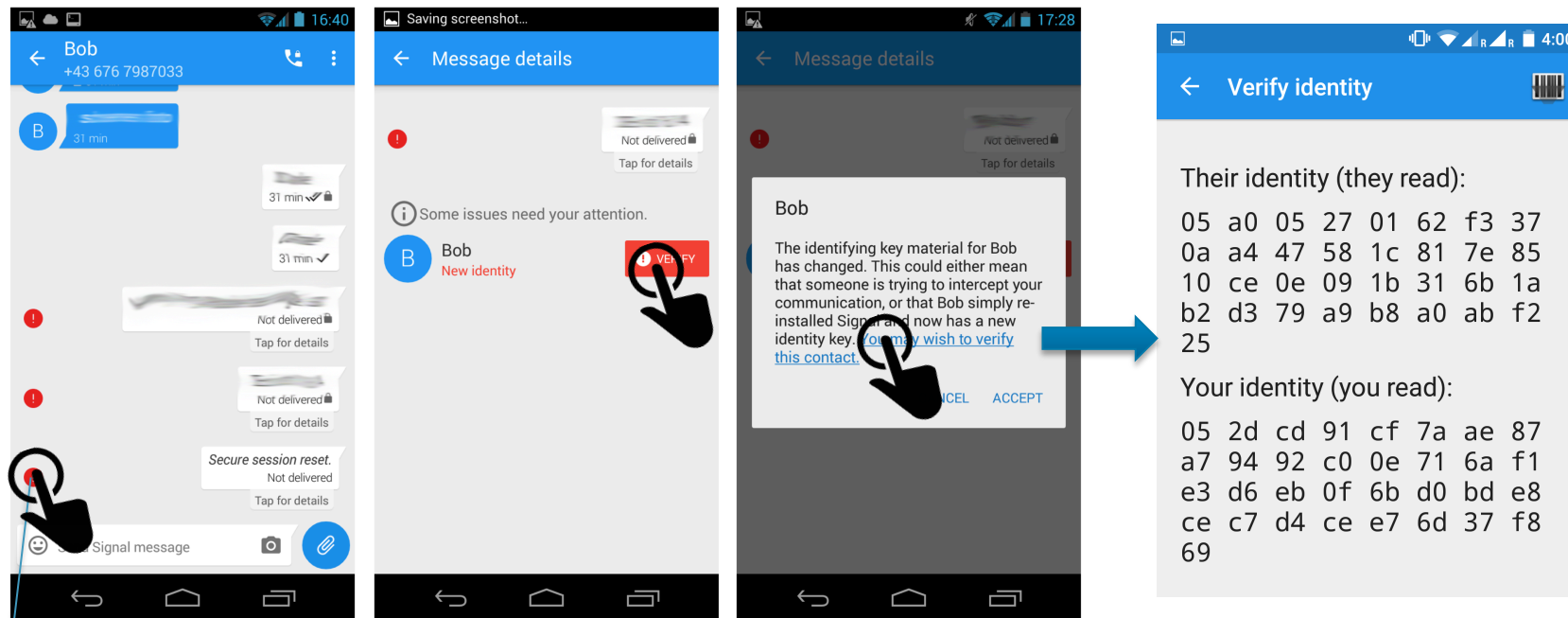
- » Task: further message exchange, verification of Bob's identity (users could ask Bob into the room at any time for verification purposes)
- » Debriefing questionnaire to assess mental models of the attack

Results: General Usability Results

- **Nearly all participants use messaging apps**
 - » (SMS/texting: 27, WhatsApp: 26, Telegram: 28, Viber: 8, Facebook Messenger: 4, ..., Signal: 1)
- **Privacy and security on smartphones are of importance to the participants**
 - » care about third parties reading their messages
- **Usability of chat functionality and security features generally positive**
 - » Chat functionality: sending of images confusing to six participants
 - » Setting the passphrase seemed easy
 - » Six participants didn't find the backup option

Results: Users' Reactions to the Attack

- Due to MITM attack sent messages weren't delivered:

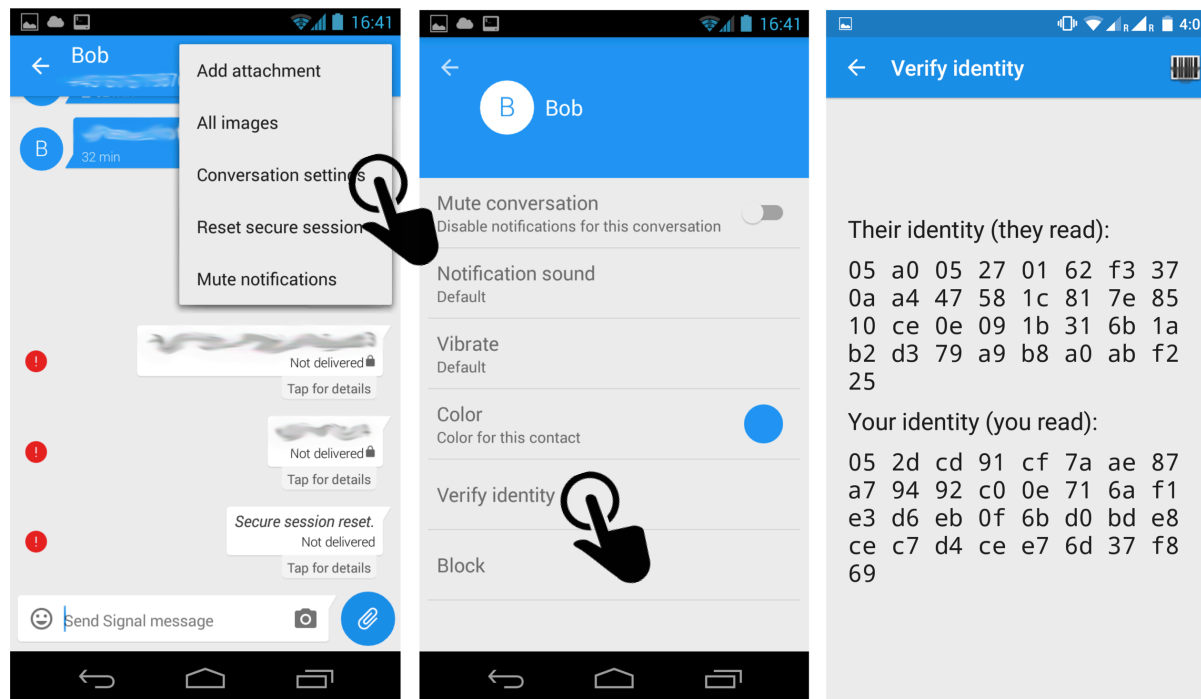


Error
notification

- Users seemed to follow “the flow”

Results: Users' Reactions to the Attack

- Verification at a later point:



- 8 users never accessed the key comparison page
- **21 of 28 participants failed to correctly compare encryption keys to verify identity of their chat partner**

Results: Mental Models of the Attack

- **13 users thought to have successfully verified Bob while they failed to correctly compare keys**
 - » Would likely have continued to communicate over insecure connection

False Verification Strategies

- Accepting Bob's new key in the error dialogue (6)
- "Verification" by personal meeting / identity check (4)
- Presence of keys on comparison page (1)
- Asking Bob whether the chat is secure (1)

Assumptions about the Attack

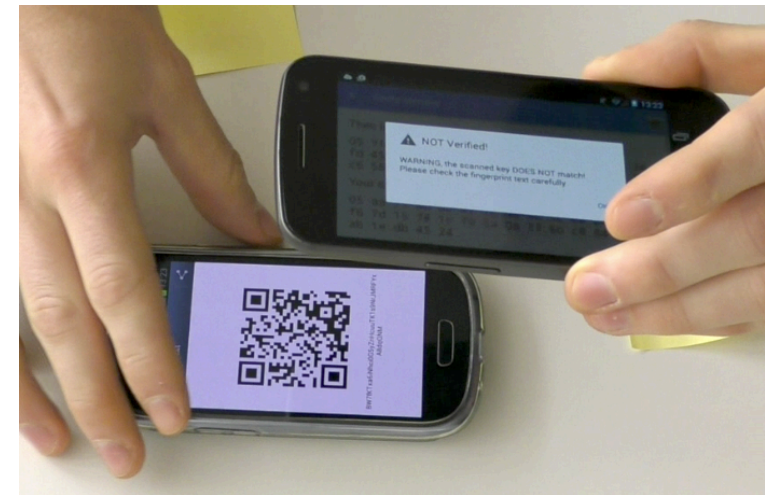
- MITM attack (7; only 1 compared keys correctly)
- Mallory impersonates Bob (4)
- Reinstallation / Malfunction (resp. 3)
- Non-specified attack (2)

Mitigation Strategies

- Uninstalling the app (11)
- Contacting Bob on another channel (8)
- Searching for information online (6)
- Asking friends (4)
- Inform developers (3)
- [...]

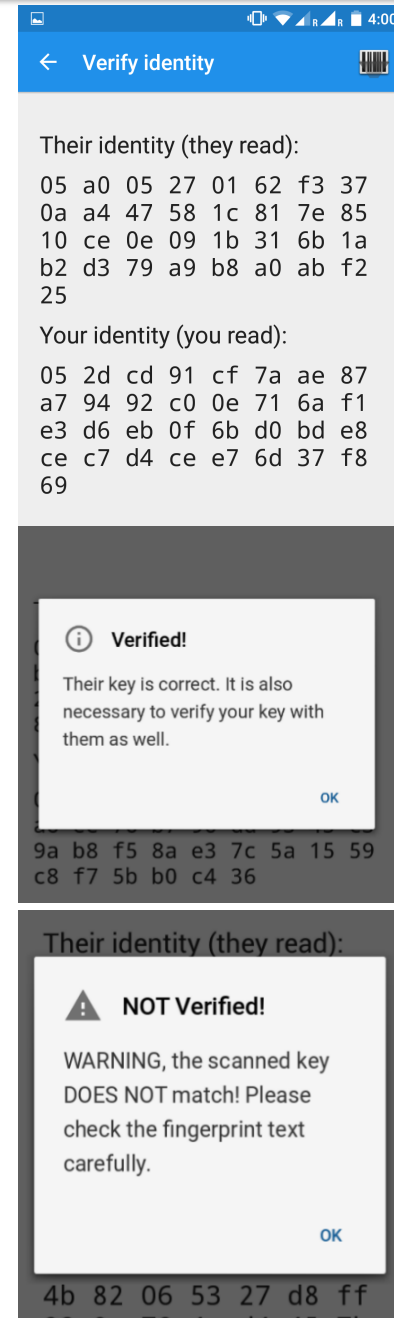
Discussion

- Surprising results: **21 of 28 users failed to correctly compare keys**
- **Serious gaps between self-assessment, mental models and outcome**
 - » Lack of required knowledge?
 - » App failed to support users?
 - » Different understanding of term “verification”?
 - » Effort for successful defense was too high?
- Assumption: **overall security of e2e encryption on mobile messengers faces serious usability obstacles**
 - » Users seemed to lack an understanding of e2e encryption in general, possible attack scenarios and risk potentials



Usability Recommendations for Signal

- **Awareness on security status of conversation**
 - » Verification status should be remembered
- **Comprehensible instructions for recommended actions**
- **Clear risk communication**
 - » Inform users about possible consequences
- **Easily accessible verification**
 - » Verification directly accessible from conversation
- Current implementation leads to more problems instead of mitigation, and ultimately to confusion, frustration and eventual uninstallation
- → not surprising that WhatsApp disabled all encryption related notifications by default



Limitations

- Participants recruited over HCI course
 - » Quite homogenous user group
- Balancing amount of information given on Signal's encryption/verification features
 - » Explicitly asked to verify each other to assess usability of core-security feature of Signal



Thank you for your attention!

svenja.schroeder@univie.ac.at
@svenjaschroeder

Literature

- [1] A. Whitten and J. D. Tygar, “Why johnny can’t encrypt: A usability evaluation of pgp 5.0.” in *Usenix Security*, vol. 1999, 1999.
- [2] S. L. Garfinkel, D. Margrave, J. I. Schiller, E. Nordlander, and R. C. Miller, “How to make secure email easier to use,” in *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM, 2005, pp. 701–710.
- [3] K. Renaud, M. Volkamer, and A. Renkema-Padmos, “Why doesn’t jane protect her privacy?” in *Privacy Enhancing Technologies*. Springer, 2014, pp. 244–262.
- [4] A. Fry, S. Chiasson, and A. Somayaji, “Not sealed but delivered: The (un) usability of s/mime today,” in *Annual Symposium on Information Assurance and Secure Knowledge Management (ASIA’12)*, Albany, NY, 2012.
- [5] T. Frosch, C. Mainka, C. Bader, F. Bergsma, and T. Holz, “How secure is textsecure?” 2014.

MITM Attack

- Technical setup:
 - » Modified version of Signal to accept new server on Alice's and Bob's phones
 - » WLAN hotspot on computer which intercepted traffic (mitmproxy with custom script)
 - » Rooted smartphones with circumvention of SSL certificate pinning
 - » Resetting and re-registering of device in-between participants
- Correct mitigation strategy:
 - » If verification due to key matching fails, Alice and Bob should stop communicating over Signal and uninstall the app