RUHR UNIVERSITÄT BOCHUM RUB

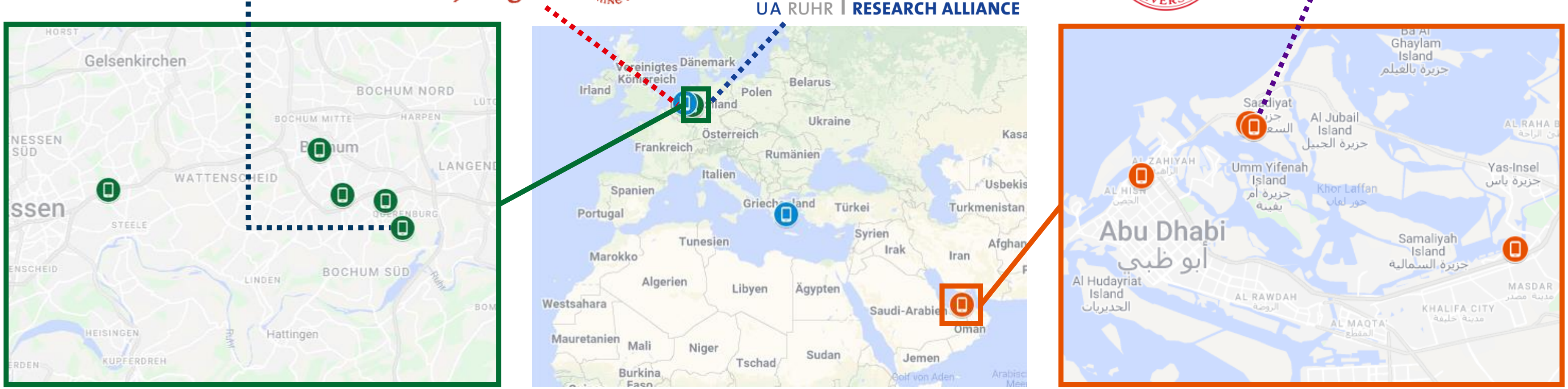
Radboud Universiteit Nijmegen

technische universität dortmund

CENTER FOR TRUSTWORTHY DATA SCIENCE AND SECURITY

UA RUHR | RESEARCH ALLIANCE

جامعة نيويورك أبوظبي NYU | ABU DHABI



HOPE OF DELIVERY: EXTRACTING USER LOCATIONS FROM MOBILE INSTANT MESSENGERS

NDSS 2023 | The Network and Distributed System Security Symposium
San Diego, CA, USA | March 02, 2023

Theodor Schnitzler
Research Center Trustworthy Data Science and Security
theodor.schnitzler@tu-dortmund.de

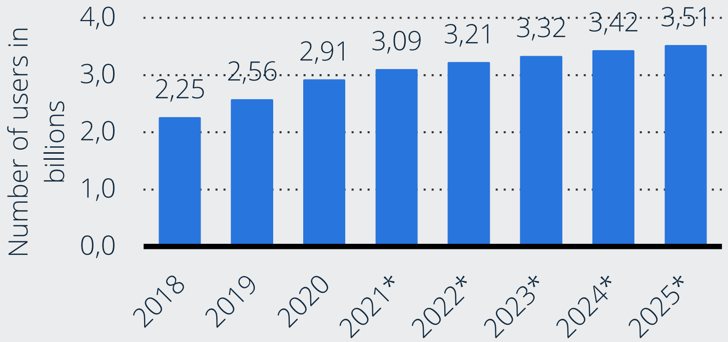
Katharina Kohls
Radboud University

Evangelos Bitsikas
Northeastern University

Christina Pöpper
New York University Abu Dhabi

MESSENGERS ARE EVERYWHERE

Messenger App Users Worldwide



Data from early 2021 | *future projection

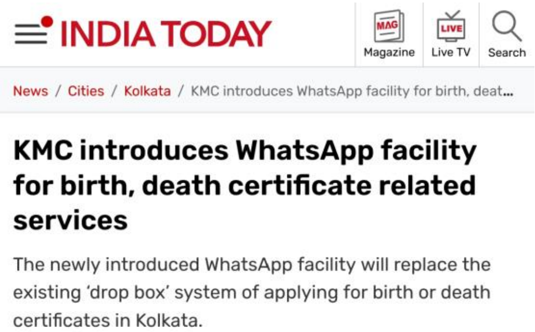
[statista.com/statistics/483255/number-of-mobile-messaging-users-worldwide]

711 111 360 messages *during this talk (16 minutes)*

[zettasphere.com/mind-boggling-stats-for-1-second-of-internet-activity/]

[order.kfc.co.za/WhatsApp]

[@rta_dubai / Twitter]


INDIA TODAY Magazine Live TV Search

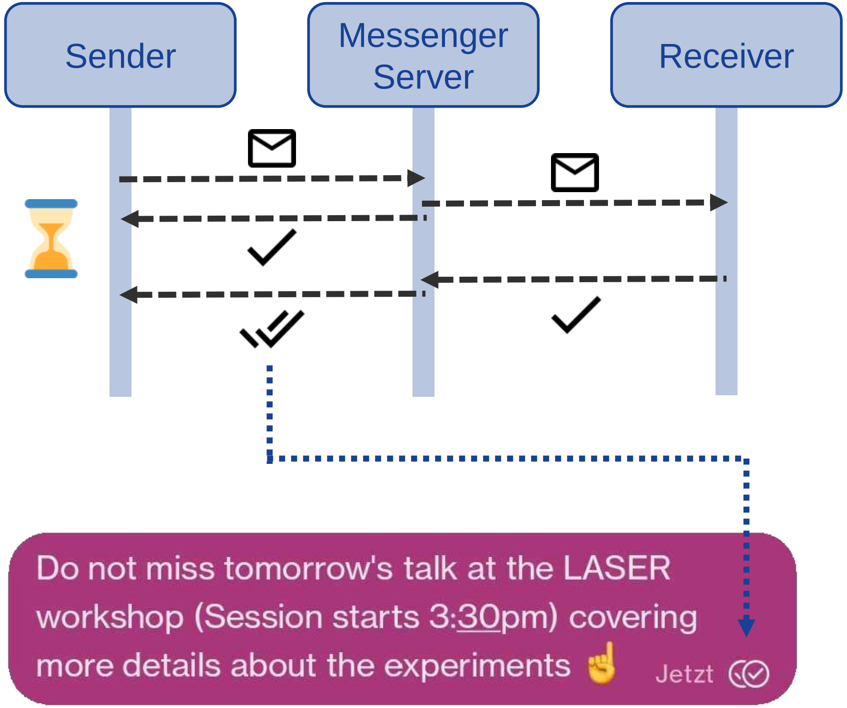
News / Cities / Kolkata / KMC introduces WhatsApp facility for birth, deat...

KMC introduces WhatsApp facility for birth, death certificate related services

The newly introduced WhatsApp facility will replace the existing 'drop box' system of applying for birth or death certificates in Kolkata.

[indiatoday.in]

PROBLEM STATEMENT



Do not miss tomorrow's talk at the LASER workshop (Session starts 3:30pm) covering more details about the experiments ☝

Scenario

Sender: *San Diego*
Server: *Los Angeles*

$c = 299\,792\,458 \text{ m/s}$

$v_{Internet} \leq \frac{2}{3}\, c$

Receiver:	$2 * dist_{e2e}$	RTT
San Diego	$\geq 660 \text{ km}$	$\geq 3.30 \text{ ms}$
Bochum	$\geq 9\,200 \text{ km}$	$\geq 46.03 \text{ ms}$

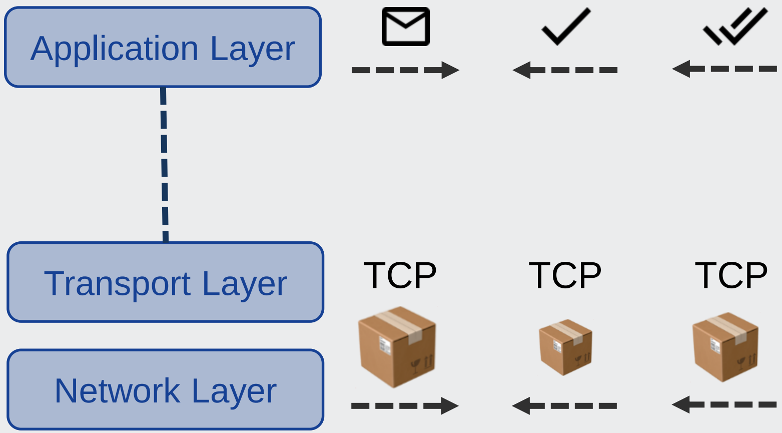
Side Channel

Time for delivery confirmation reveals information about the receiver‘s location

Does this work in practice?

ATTACK CONCEPT

Under the Hood



Threat Model

The attacker…

(1) … operates a regular Android phone capable of running messengers

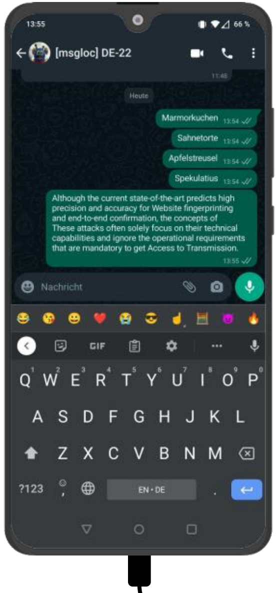
(2) … is able to capture their own network traffic

(3) … **and the victim** are in each others‘ contact lists in one of the messengers

(4) … knows plausible locations **of the victim**

(3) *and* ***(4)*** *limit the threat scope to people who likely know each other!*

MEASUREMENT SETUP



[msgloc] DE-22

11:48

Heute

Marmorkuchen 13:54

Sahnetorte 13:54

Apfelstreusel 13:54

Spekulatius 13:54

Although the current state-of-the-art predicts high precision and accuracy for Website fingerprinting and end-to-end confirmation, the concepts of These attacks often solely focus on their technical capabilities and ignore the operational requirements that are mandatory to get Access to Transmission. 13:55

ADB-USB
Android Debug Bridge

Sending Messages

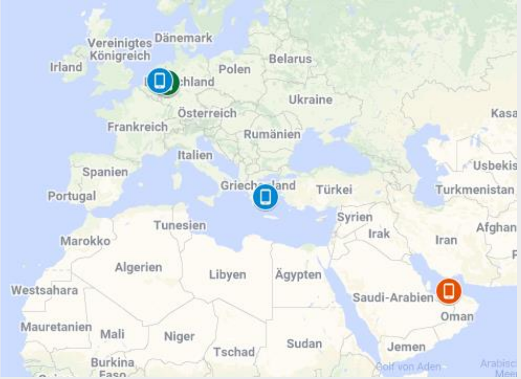
- Iterate through messengers + receivers
- Capture network traffic on the phone
- Open chat + send messages
  - 5 messages, 10s pause
- Continuously repeated (CronJob)

Receiving Messages

DATA COLLECTION

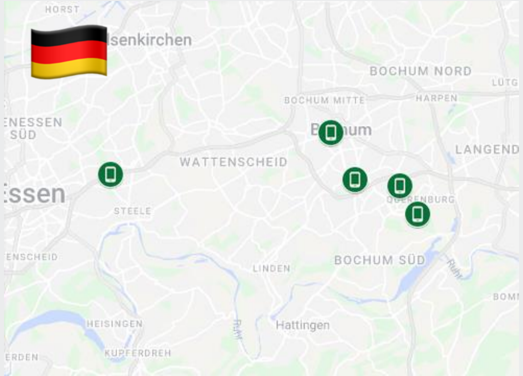
Round 1

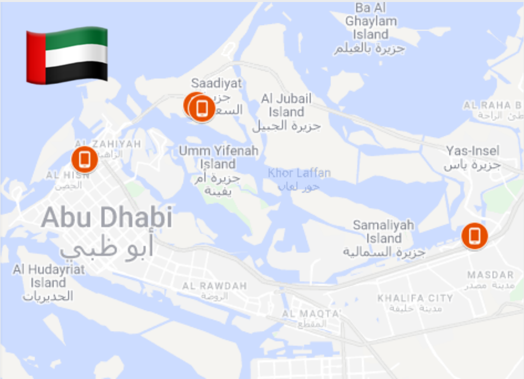
- Fixed Locations
- WiFi-only
- (Mostly) country-level



Round 2 (Germany + UAE)

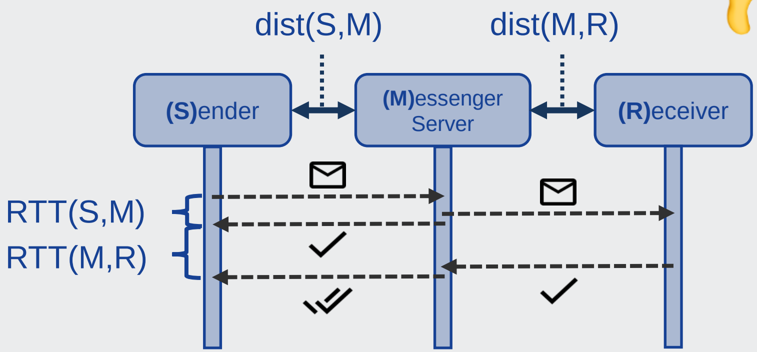
- Local setups at city-area-level
- Rotating devices through locations
- WiFi + mobile data

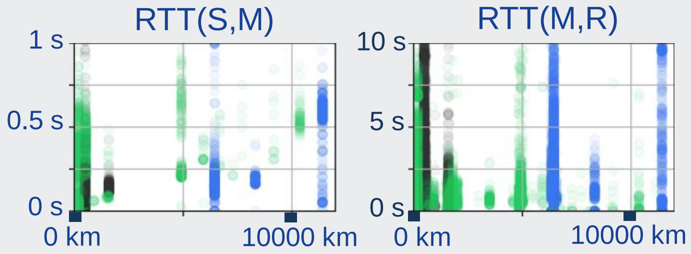




DETERMINING THE RECEIVER LOCATION

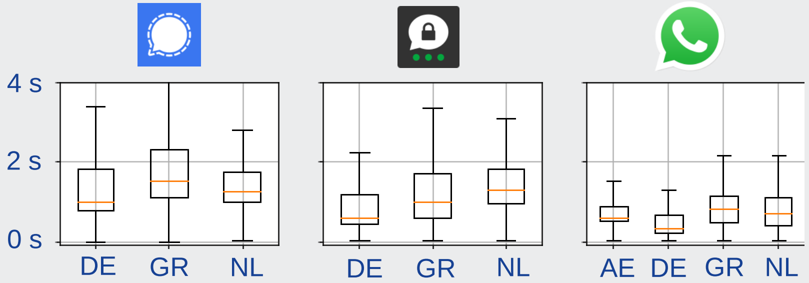
Time vs. Distance





Time vs. Receiver Location

Message Sender: 📱DE-11 📍RUB

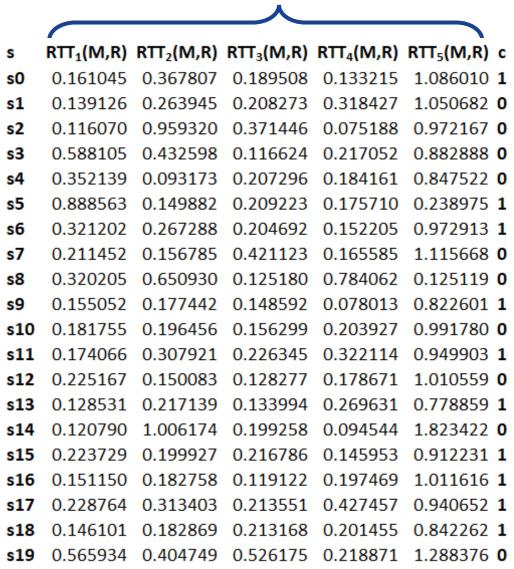


Classification

Assign newly measured RTTs a location based on previously observed data

RECEIVER CLASSIFICATION

RTT(M,R) of 5 subsequently sent messages



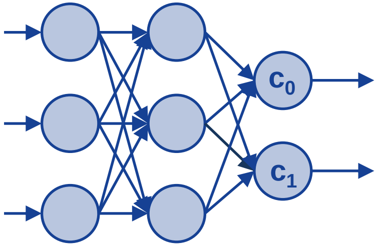
s	$RTT_1(M,R)$	$RTT_2(M,R)$	$RTT_3(M,R)$	$RTT_4(M,R)$	$RTT_5(M,R)$	c
s0	0.161045	0.367807	0.189508	0.133215	1.086010	**1**
s1	0.139126	0.263945	0.208273	0.318427	1.050682	**0**
s2	0.116070	0.959320	0.371446	0.075188	0.972167	**0**
s3	0.588105	0.432598	0.116624	0.217052	0.882888	**0**
s4	0.352139	0.093173	0.207296	0.184161	0.847522	**0**
s5	0.888563	0.149882	0.209223	0.175710	0.238975	**1**
s6	0.321202	0.267288	0.204692	0.152205	0.972913	**1**
s7	0.211452	0.156785	0.421123	0.165585	1.115668	**0**
s8	0.320205	0.650930	0.125180	0.784062	0.125119	**0**
s9	0.155052	0.177442	0.148592	0.078013	0.822601	**1**
s10	0.181755	0.196456	0.156299	0.203927	0.991780	**0**
s11	0.174066	0.307921	0.226345	0.322114	0.949903	**1**
s12	0.225167	0.150083	0.128277	0.178671	1.010559	**0**
s13	0.128531	0.217139	0.133994	0.269631	0.778859	**1**
s14	0.120790	1.006174	0.199258	0.094544	1.823422	**0**
s15	0.223729	0.199927	0.216786	0.145953	0.912231	**1**
s16	0.151150	0.182758	0.119122	0.197469	1.011616	**1**
s17	0.228764	0.313403	0.213551	0.427457	0.940652	**1**
s18	0.146101	0.182869	0.213168	0.201455	0.842262	**1**
s19	0.565934	0.404749	0.526175	0.218871	1.288376	**0**

80% data for training

1

2

20% data for testing



$P(s_i \in c_0)$

$P(s_i \in c_1)$

For each sample s_i select class c_j with highest probability

Classification Tasks (Examples)

Receiver country

Within a country (yes/no)

Locations of a single receiver

Network connection (WiFi/Mobile)

Repeat 5x for cross validation

RESULTS OVERVIEW

Receiver Country (Round 1)

	DE	GR	NL
DE	0.88	0.06	0.06
GR	0.07	0.63	0.29
NL	0.06	0.22	0.72

💬 **74%**

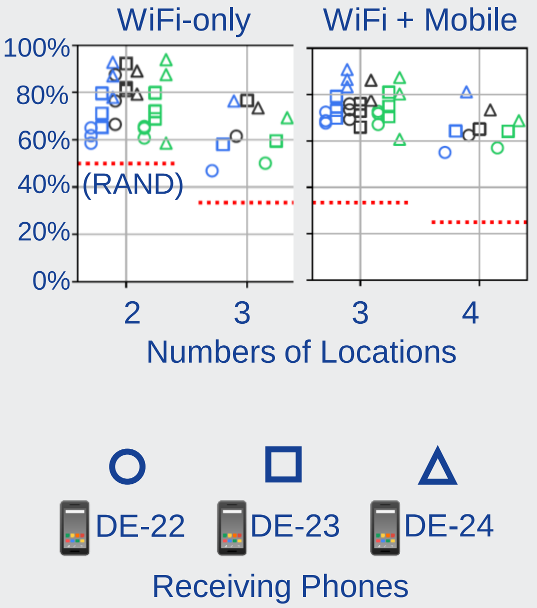
	DE	GR	NL
DE	0.90	0.02	0.08
GR	0.02	0.85	0.13
NL	0.09	0.13	0.77

🔒 **84%**

	AE	DE	GR	NL
AE	0.86	0.01	0.05	0.08
DE	0.04	0.81	0.06	0.09
GR	0.05	0.06	0.63	0.26
NL	0.09	0.06	0.18	0.67

📞 **74%**

Device-at-Location (R2)



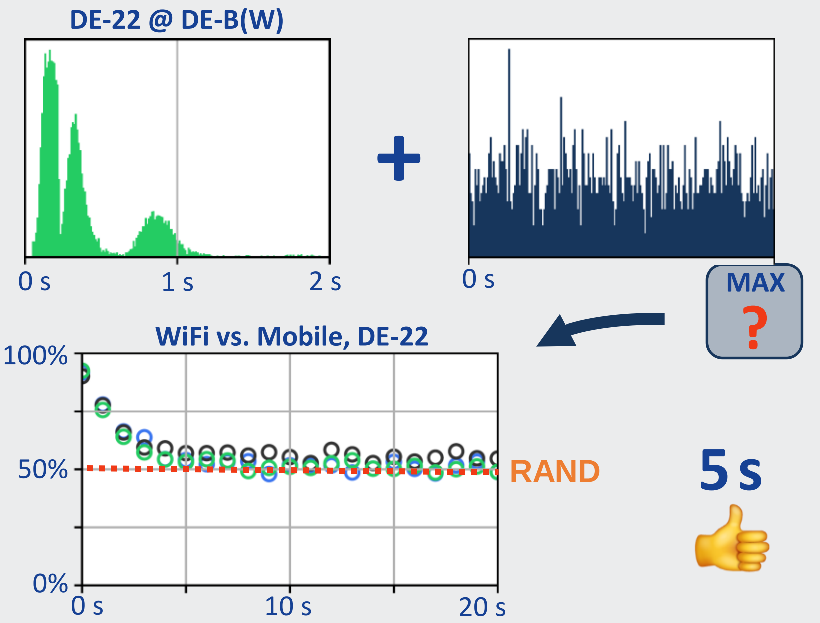
Network Connection (R2)

🇩🇪	💬	🔒	📞
DE-22	92%	90%	92%
DE-23	90%	73%	89%
DE-24	94%	94%	92%

🇦🇪	💬	📞
AE-22	56%	91%
AE-23	63%	82%
AE-24	76%	89%

COUNTERMEASURES

Delay Delivery Confirmations

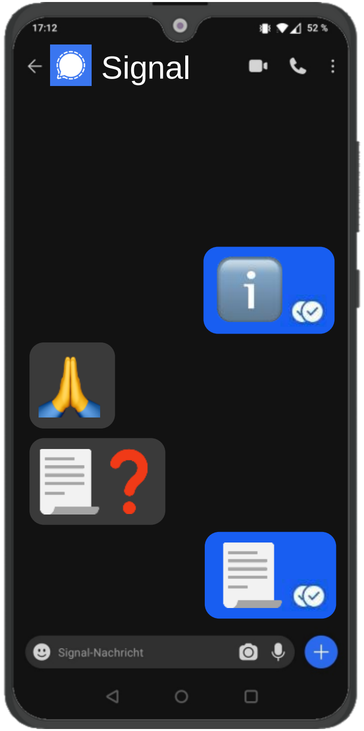


Add Disable Option

Last Online	-	-	✓
Typing Indicators	✓	✓	✗
Read Confirmation	✓	✓	✓
Delivery Confirmation	✗	✗	✗

Disabling the confirmation would render the timing side channel entirely unusable

DISCLOSURE PROCESS

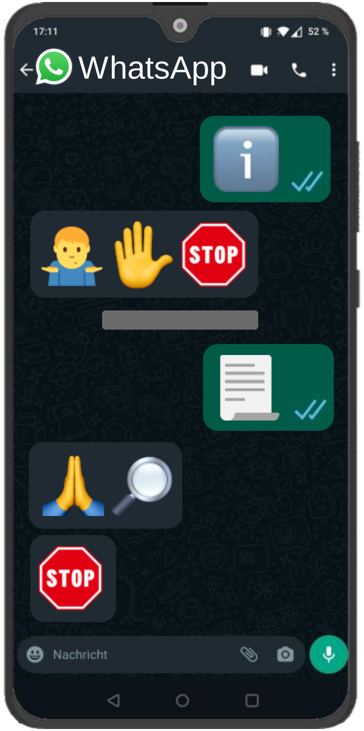


ℹ️

🙏

📄❓

📄



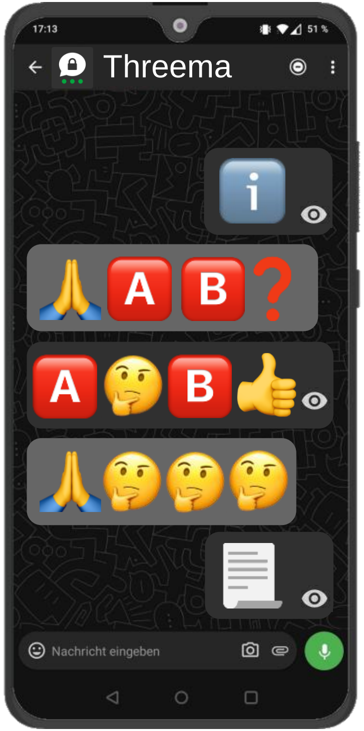
ℹ️

🤷‍♂️✋🛑

📄

🙏🔍

🛑



ℹ️

🙏🅰️🅱️❓

🅰️🤔🅱️👍

🙏🤔🤔🤔

📄

“We will discuss this internally and consider adding one or the other option in an upcoming update.“

(Threema)

CENTER FOR TRUSTWORTHY
DATA SCIENCE AND SECURITY

UA RUHR | RESEARCH ALLIANCE

HOPE OF DELIVERY: EXTRACTING USER LOCATIONS FROM MOBILE INSTANT MESSENGERS

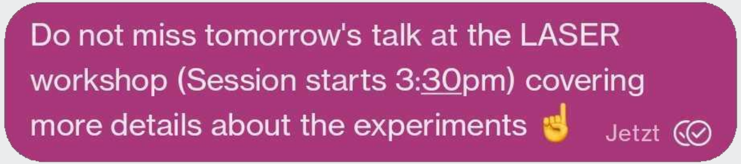
The Network and Distributed System Security Symposium
San Diego, CA, USA | March 02, 2023

Theodor Schnitzler
theodor.schnitzler@tu-dortmund.de
@the0retisch

Research Center Trustworthy Data Science and Security, Germany
@rctrustworthy

Key Takeaways

- Unintended and unexpected information revelation through the use of secure messengers
- Low technical requirements
- Different locations of message receivers can be distinguished by measuring delivery timings



Do not miss tomorrow's talk at the LASER workshop (Session starts 3:30pm) covering more details about the experiments ☝️ Jetzt ✓✓