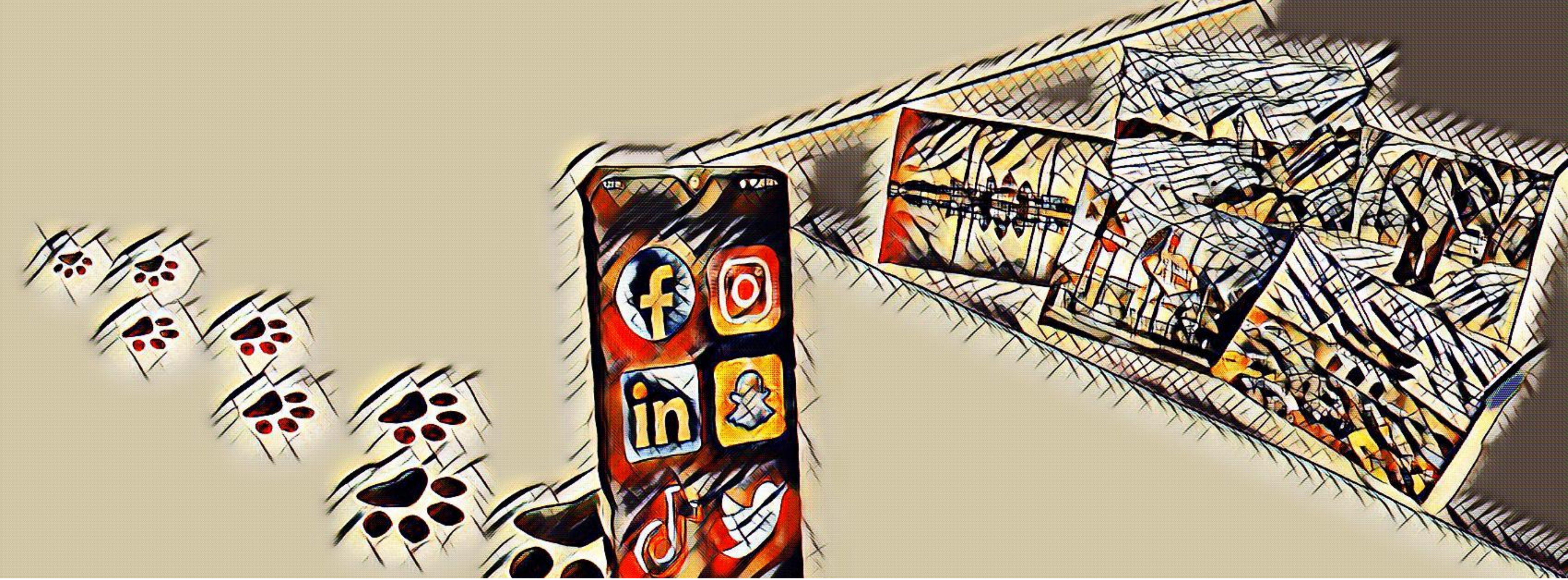


ANALYZING PRIVACY AND END USER INFORMATION EXPOSURE IN DIGITAL COMMUNICATION ENVIRONMENTS

PhD Defense
Bochum, June 24, 2022

Theodor Schnitzler
Ruhr-Universität Bochum
theodor.schnitzler@rub.de

END USER INFORMATION EXPOSURE

Data Sharing

Instagram	1 539 120 photos
Twitter	13 259 400 tweets

during this talk (22 minutes)
[https://www.internetlivestats.com/one-second/]

Permanent? For Everyone?

⇨ *Data Revocation*

Self-Published Online Data
Deliberately Shared

LONGITUDINAL MANAGEMENT OF ONLINE DATA

Data Sharing

1 539 120 photos

13 259 400 tweets

during this talk (22 minutes)
[https://www.internetlivestats.com/one-second/]

Permanent? For Everyone?

⇨ *Data Revocation*

HCI Research
(*Human-Computer Interaction)

- Reasons for Data Sharing
- Perception of Exposure
- Reasons for Unsharing

Technical Research

- Encrypted Publishing
- Expiration by Time
- No Threats During Data Lifetime

The State of Data Revocation Research

Systematization of Knowledge:

Develop taxonomies and bring both perspectives together

RESEARCH CONTRIBUTIONS

Part I: Managing Self-Published Online Data

TODAY — **The State of Data Revocation Research** — **PETS ’21**

User Perception of Message Deletion — **EuroUSEC ’18**, **J-CySec ’20**

Contractual Agreements for Data Revocation — **IFIP SEC ’19**

OVERVIEW OF DATA REVOCATION RESEARCH

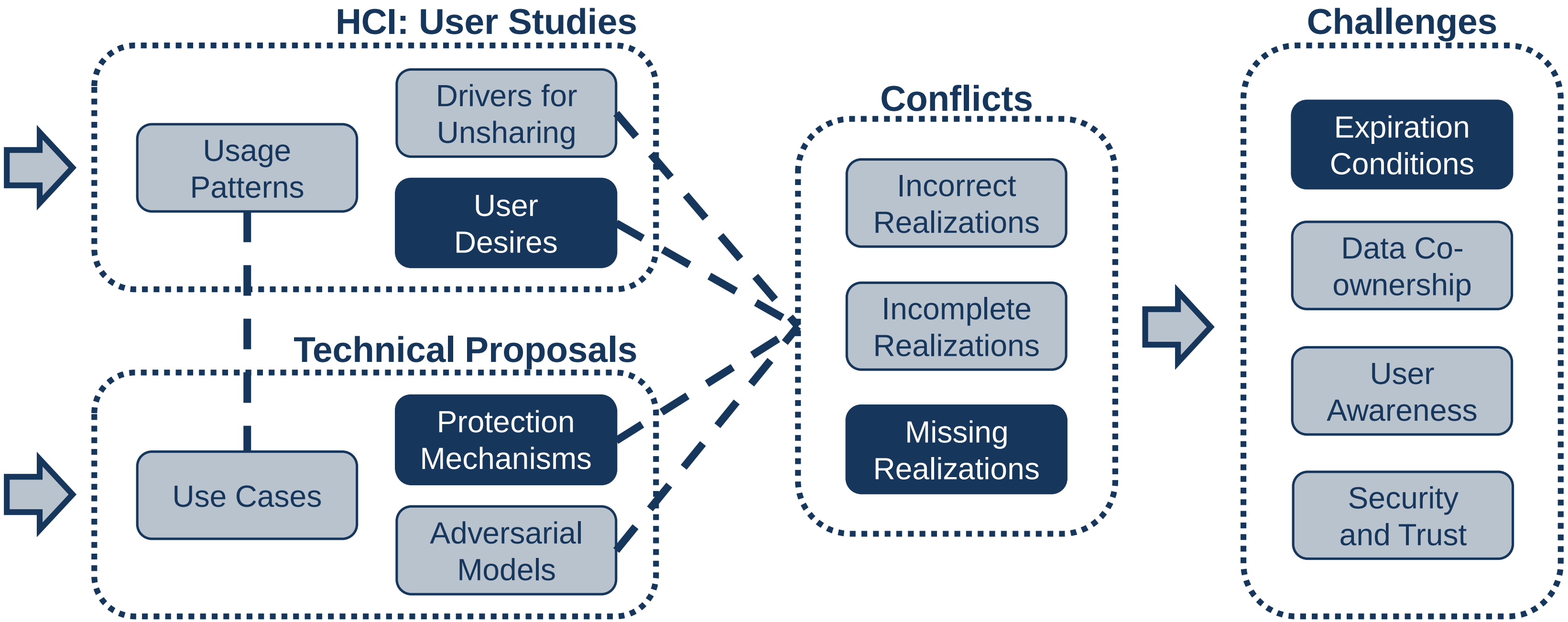
HCI Research (33 papers)

[H01] Mondal et al. CCS‘19
[H02] Mohamed et al. SOUPS‘18
[H03] Murillo et al. SOUPS‘18
[H04] Khan et al. CHI‘18
[H05] Mondal et al. J-IEEE-IC‘17
[H06] Ayalon et al. J-HCI‘17
[H07] Mondal et al. SOUPS‘16
[H08] Barth et al. WPES‘13
[H09] Ayalon et al. SOUPS‘13
[H10] Alqhatani et al., SOUPS‘19
[H11] Habib et al., CHI‘19
[H12] Rashidi et al. SOUPS‘18
[H13] Schlesinger et al. CHI‘17
[H14] Zhou et al. WWW‘16
[H15] Bhattacharya et al. WLSM‘16
[H16] Dhir et al. J-CHB‘15
[H17] Liu et al. WLSM‘14
[H18] Sleeper et al. CHI‘13
[H19] Netter et al. HICCS‘13
[H20] Almuhimedi et al. CSCW’13
[H21] Madejski et al. PERCOM‘12
[H22] Johnson et al. SOUPS‘12
[H23] Wang et al. SOUPS‘11
[H24] Egelman et al. CHI‘11
[H25] Reynolds et al. IFIP-HCI‘11
[H26] Besmer et al. CHI‘10
[H27] Richter-Lipford et al. UPSEC‘8
[H28] Coopamootoo et al. PETS‘17
[H29] Fiesler et al. CSCW‘17
[H30] Sleeper et al. CHI‘16
[H31] Mondal et al. SOUPS‘14
[H32] Stutzman et al. J-SPM‘13
[H33] Liu et al. IMC‘11

Technical Research (35 papers)

[T01] Minaei et al. PETS‘19
[T02] Xue et al. ForensicSec‘19
[T03] Schnitzler et al. IFIP-SEC‘19
[T04] Ginart et al. NeurIPS‘19
[T05] Olteanu et al. NDSS‘18
[T06] Amjad et al. CODASPY‘18
[T07] Ilia et al. CODASPY‘17
[T08] Oh et al. ICCV‘17
[T09] Moosavi-Dezfooli et al. CVPR‘17
[T10] Rajtmajer et al. GameSec‘17
[T11] Wegberg et al. TechRep‘17
[T12] Bacis et al. CCS‘16
[T13] Zarras et al. CODASPY‘16
[T14] Such et al. TKDE‘16
[T15] Cao et al. S&P‘15
[T16] Niderée et al. SIGMOD‘15
[T17] Abouzied et al. ACM-SCC‘15
[T18] Snyder et al. CCSW‘13
[T19] Bishop et al. NSPW‘13
[T20] Stokes et al. PST‘13
[T21] De Cristofaro et al. S&P‘12
[T22] Reimann et al. WPES‘12
[T23] Beato et al. PETS‘11
[T24] Castelluccia et al. ICNP‘11
[T25] Geambasu et al. TechRep‘11
[T26] Carminati et al. CollabCom‘11
[T27] Thomas et al. PETS‘10
[T28] Besmer et al. CHI‘10
[T29] Wishart et al. POLICY‘10
[T30] Pöpper et al. ACSAC‘10
[T31] Geambasu et al. USENIX‘09
[T32] Squicciarini et al. WWW‘09
[T33] Luo et al. CSE‘09
[T34] Bowen et al. SecureCom‘09
[T35] Perlman et al. SMLI‘05

THE STATE OF DATA REVOCATION RESEARCH



HCI: User Studies

Usage Patterns

Drivers for Unsharing

User Desires

Technical Proposals

Use Cases

Protection Mechanisms

Adversarial Models

Conflicts

Incorrect Realizations

Incomplete Realizations

Missing Realizations

Challenges

Expiration Conditions

Data Co-ownership

User Awareness

Security and Trust

EXPIRATION CONDITIONS

Technical Realizations

- Elapsed time (e.g. Stories 24h)
  [T22, T31, T35]
  [Gmail, Instagram, Signal, Snapchat, Telegram, WhatsApp]
- Interactions with content
  [T13]
- One-time view
  [Snapchat, WhatsApp]

User Perspective

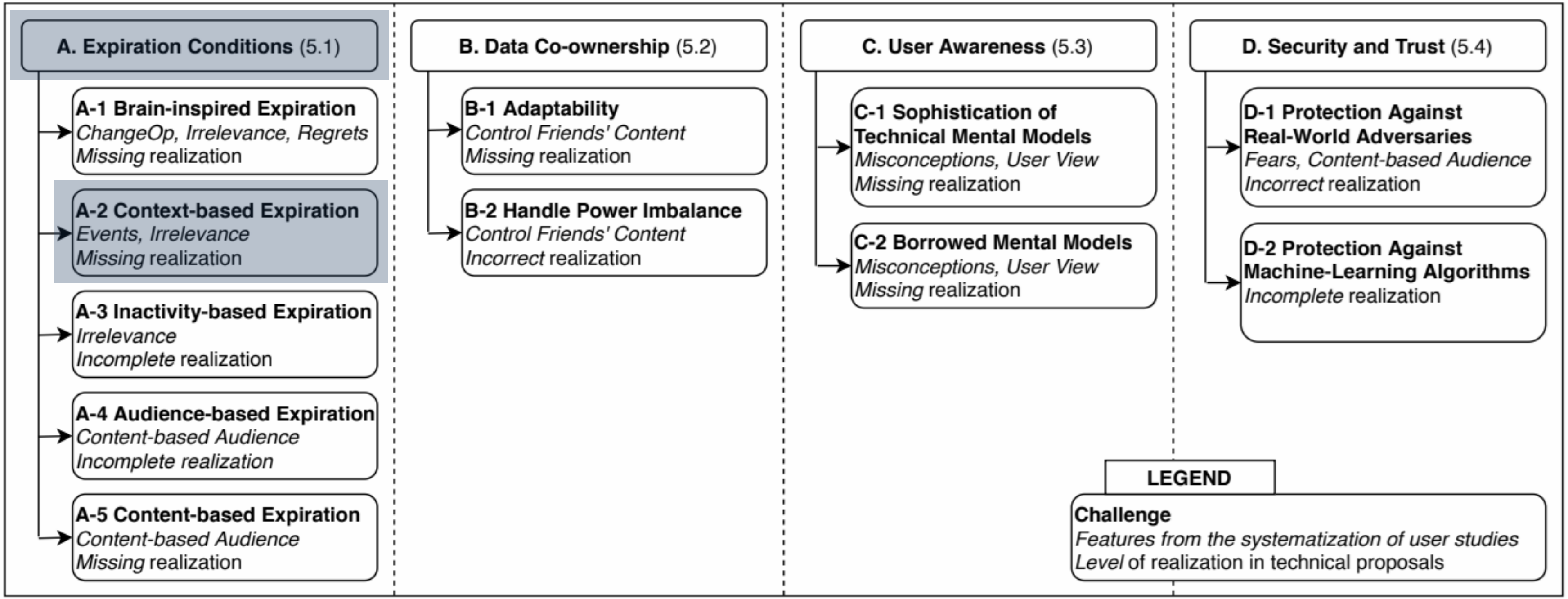
- Not all content should expire by time
  [H04, H06, H08]
- Context
  [H05, H13, H23]
- Major life changes
  [H09]

Conflict

Missing realization of deletion
as a **context-dependent**, implicit feature

→ *Context-based expiration*

CHALLENGES IN DATA REVOCATION RESEARCH



A. Expiration Conditions (5.1)

A-1 Brain-inspired Expiration
ChangeOp, Irrelevance, Regrets
Missing realization

A-2 Context-based Expiration
Events, Irrelevance
Missing realization

A-3 Inactivity-based Expiration
Irrelevance
Incomplete realization

A-4 Audience-based Expiration
Content-based Audience
Incomplete realization

A-5 Content-based Expiration
Content-based Audience
Missing realization

B. Data Co-ownership (5.2)

B-1 Adaptability
Control Friends' Content
Missing realization

B-2 Handle Power Imbalance
Control Friends' Content
Incorrect realization

C. User Awareness (5.3)

C-1 Sophistication of Technical Mental Models
Misconceptions, User View
Missing realization

C-2 Borrowed Mental Models
Misconceptions, User View
Missing realization

D. Security and Trust (5.4)

D-1 Protection Against Real-World Adversaries
Fears, Content-based Audience
Incorrect realization

D-2 Protection Against Machine-Learning Algorithms
Incomplete realization

LEGEND

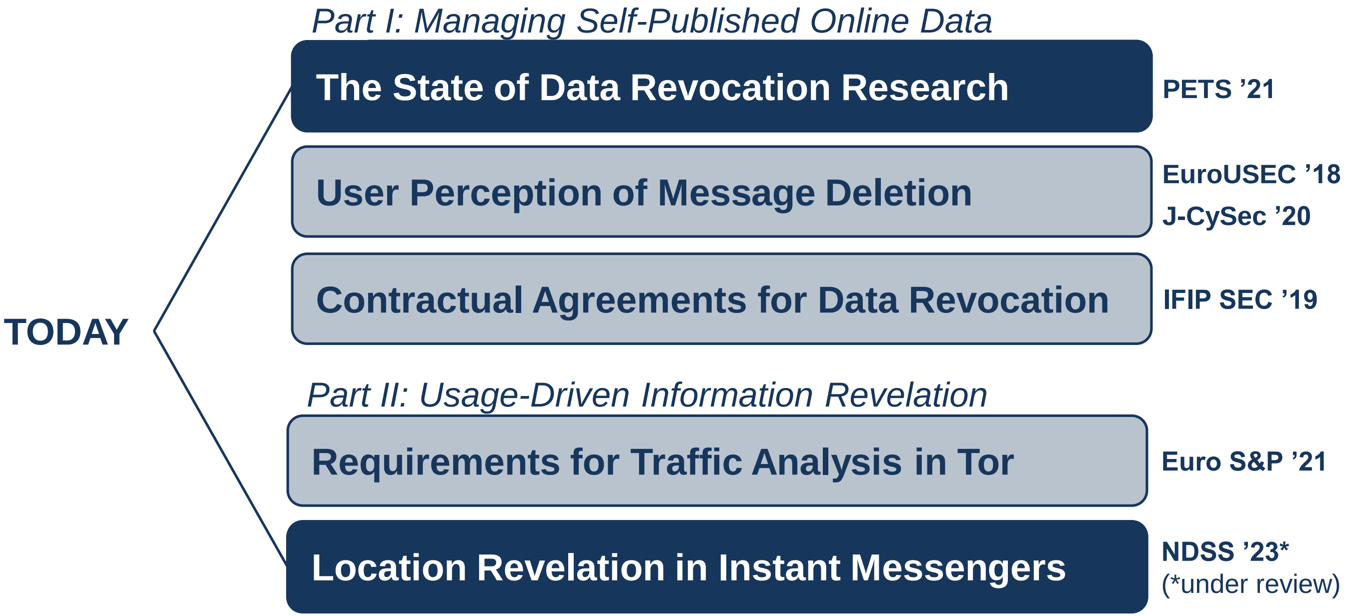
Challenge
Features from the systematization of user studies
Level of realization in technical proposals

END USER INFORMATION EXPOSURE

Self-Published Online Data
Deliberately Shared

Usage-Driven Information
Undeliberately Revealed

RESEARCH CONTRIBUTIONS



TODAY

Part I: Managing Self-Published Online Data

The State of Data Revocation Research – **PETS ’21**

User Perception of Message Deletion – **EuroUSEC ’18**, **J-CySec ’20**

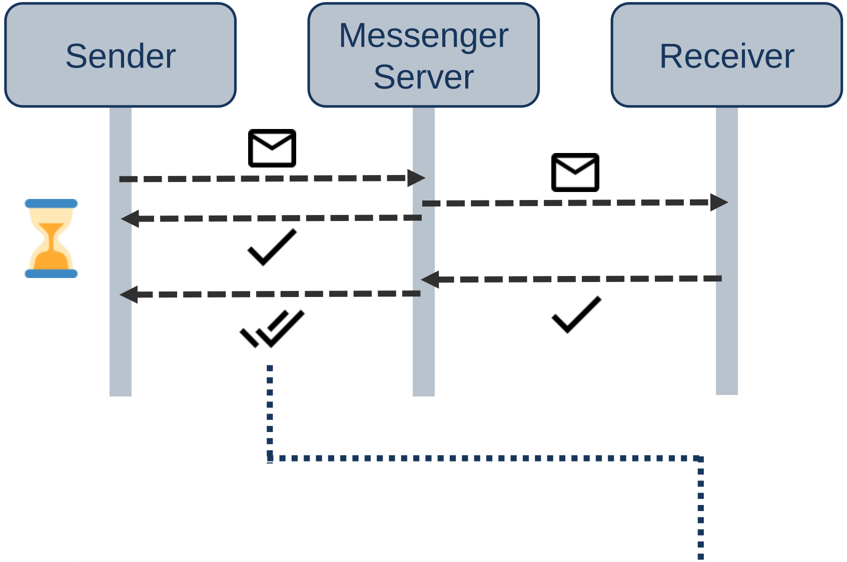
Contractual Agreements for Data Revocation – **IFIP SEC ’19**

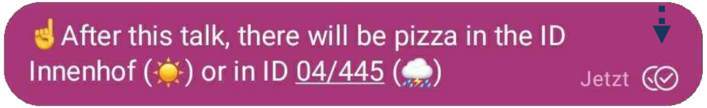
Part II: Usage-Driven Information Revelation

Requirements for Traffic Analysis in Tor – **Euro S&P ’21**

Location Revelation in Instant Messengers – **NDSS ’23***
(*under review)

PROBLEM STATEMENT




☝ After this talk, there will be pizza in the ID Innenhof (☀) or in ID 04/445 (⛈)

Scenario

Sender: *Bochum*
Server: *Düsseldorf*

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

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

Receiver	$2 * dist_{e2e}$	RTT
Bochum	$\geq 167\,\mathrm{km}$	$\geq 0.84\,\mathrm{ms}$
Abu Dhabi	$\geq 10\,090\,\mathrm{km}$	$\geq 50.48\,\mathrm{ms}$

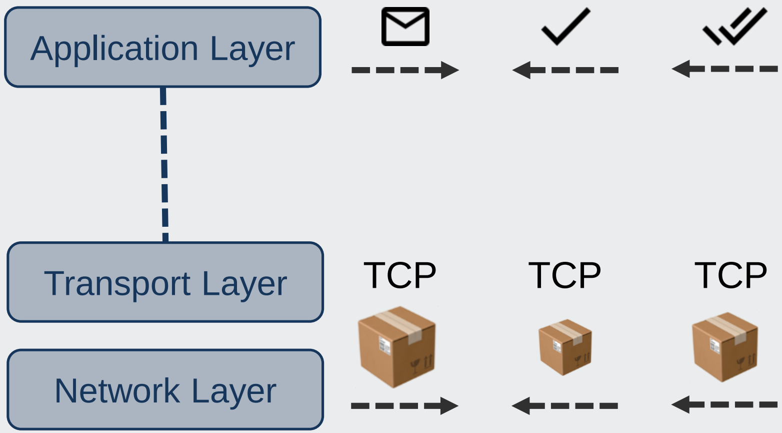
Side Channel

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

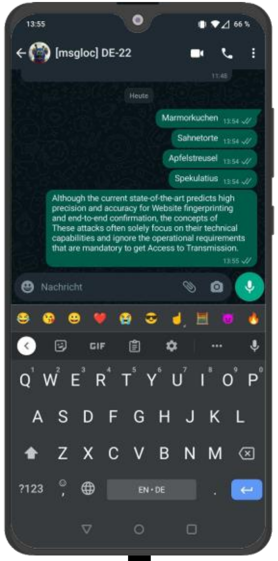
(2) … is able to capture their own network traffic

(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



13:55 66 %

[msgloc] DE-22

11:48

Heute

Marmorkuchen 13:54

Sahnetorte 13:54

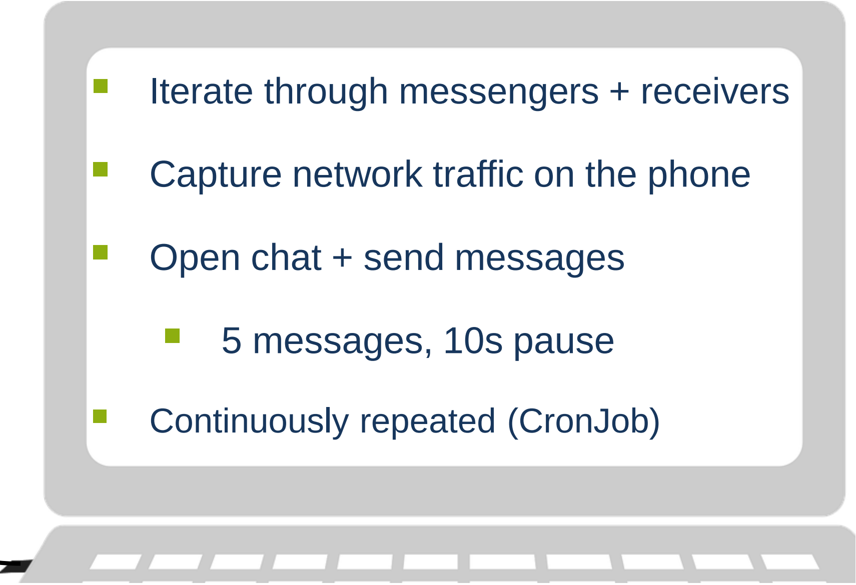
Apfelstreusel 13:54

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)

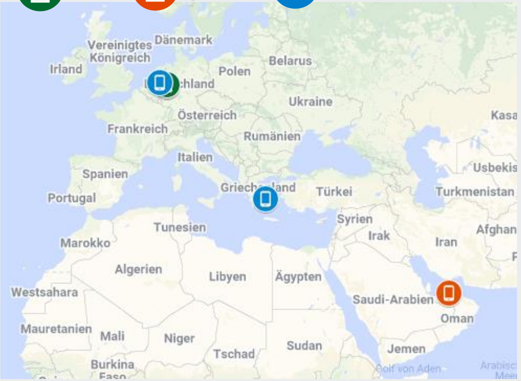
Receiving Messages

MEASUREMENT LOCATIONS

Round 1

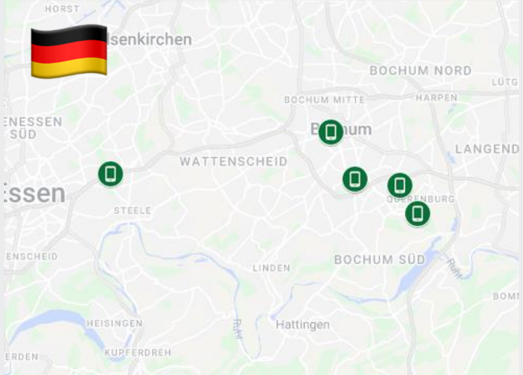
- Fixed Locations
- WiFi-only
- (Mostly) country-level

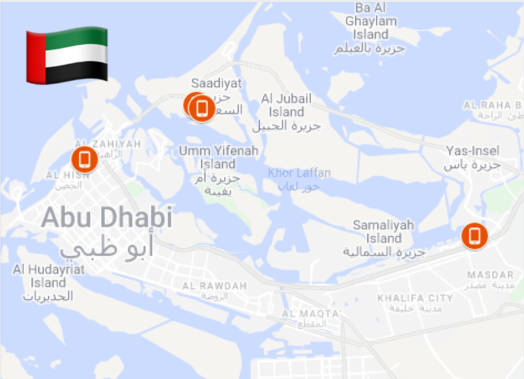
● DE ● UAE ● OTHER



Round 2 (Germany + UAE)

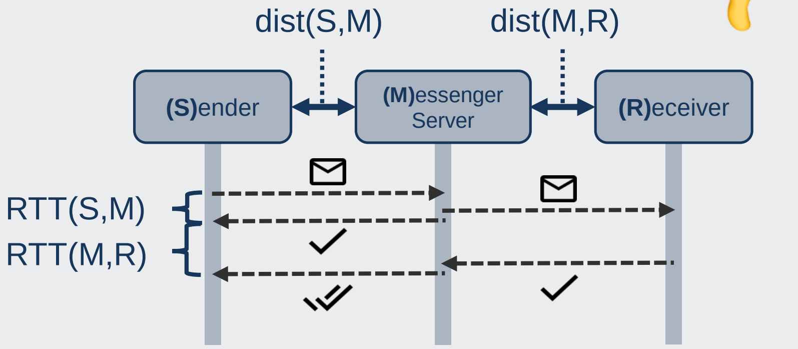
- Local setups at city-area-level
- Rotating devices through locations
- WiFi + mobile data

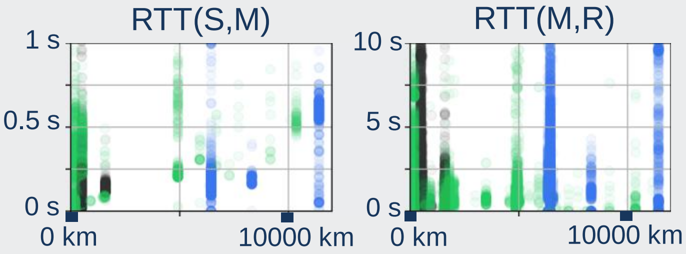




DETERMINING THE RECEIVER LOCATION

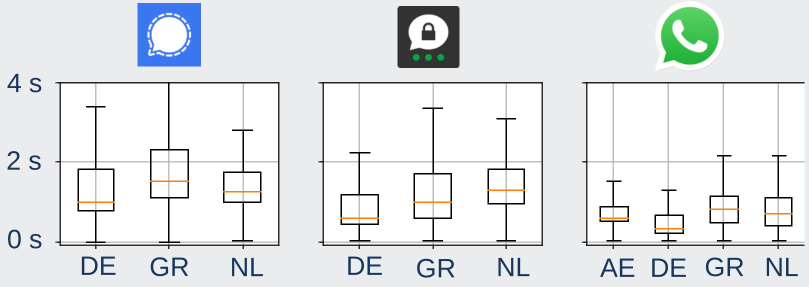
Time vs. Distance





Time vs. Receiver Location

Message Sender: 📱 DE-11 📍RUB

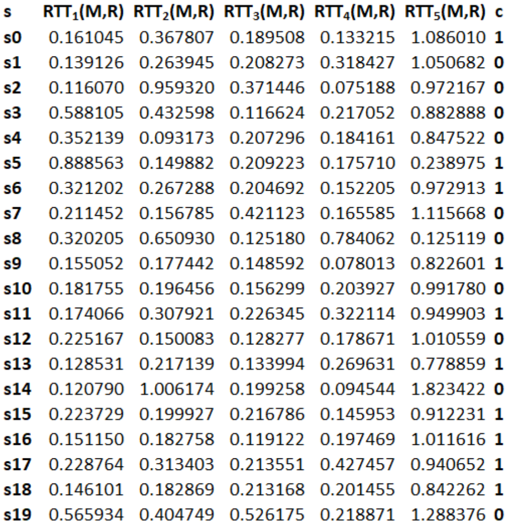


Classification

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

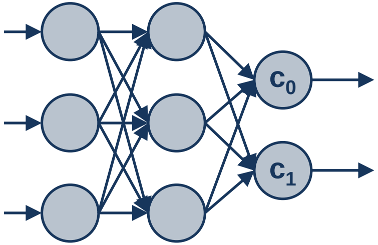
Classification Tasks (Examples)

Receiver country

Within a country (yes/no)

Locations of a single receiver

Network connection (WiFi/Mobile)



$P(s_i \in c_0)$

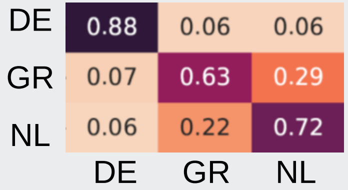
$P(s_i \in c_1)$

For each sample s_i select class c_j with highest probability

Repeat 5x for cross validation

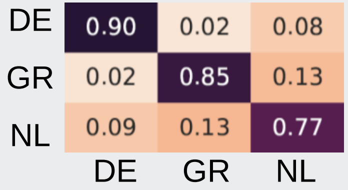
RESULTS OVERVIEW

Receiver Country (Round 1)



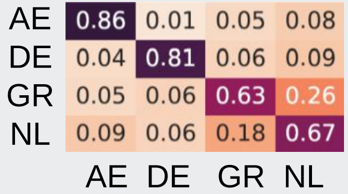
	DE	GR	NL
DE	0.88	0.06	0.06
GR	0.07	0.63	0.29
NL	0.06	0.22	0.72

💬 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

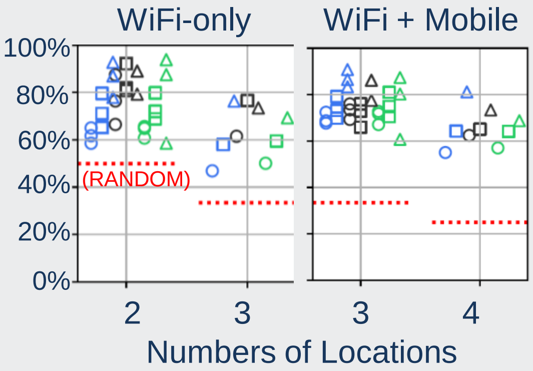
🔒 84%



	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)



○ DE-22 □ DE-23 △ DE-24

Receiving Phones

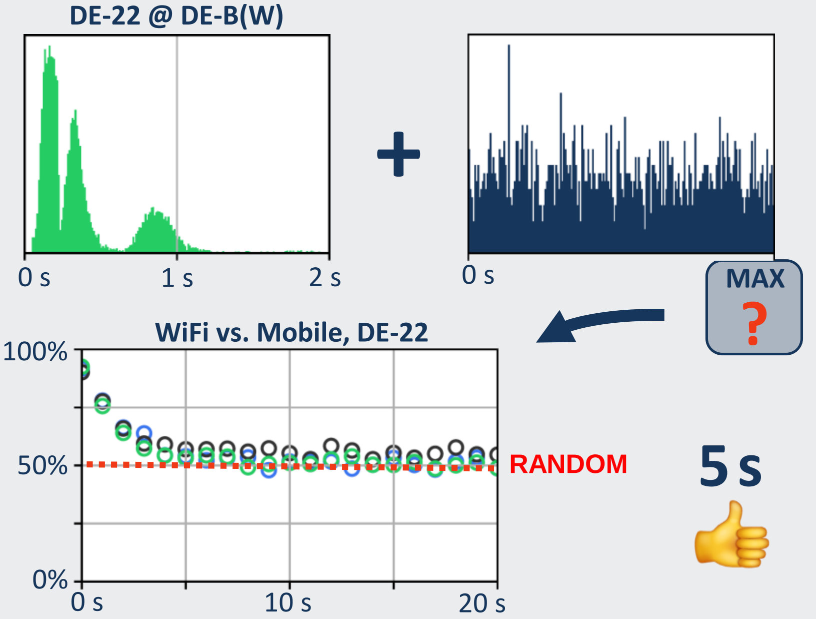
Network Connection (R2)

🇩🇪	💬	🔒	📞
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

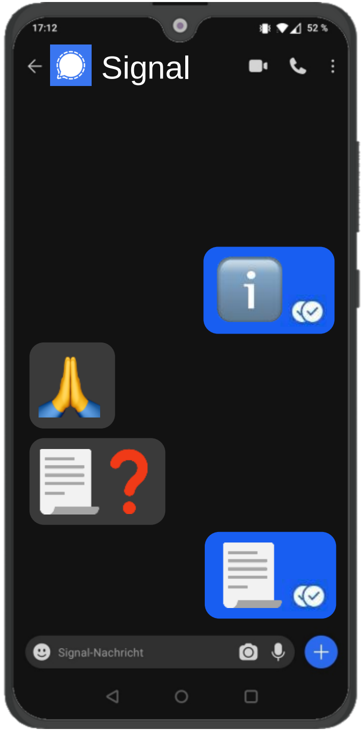


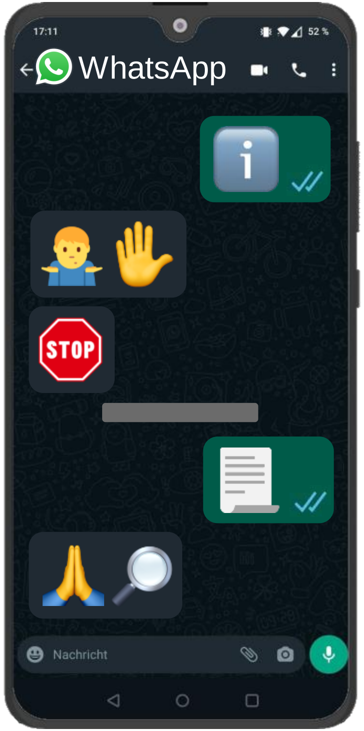
Add Disable Option

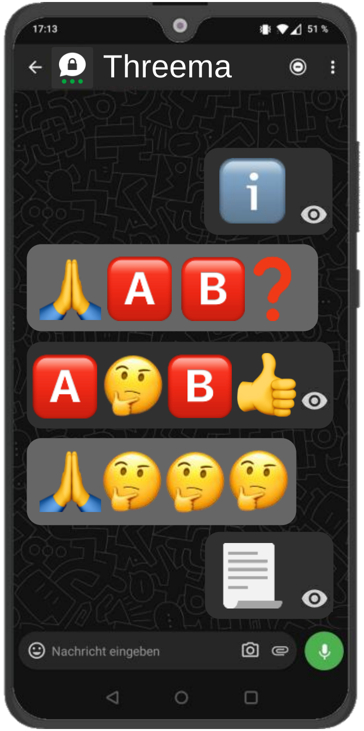
Last Online	-	-	✓
Typing Indicators	✓	✓	✗
Read Confirmation	✓	✓	✓
Delivery Confirmation	✗	✗	✗

Disabling the confirmation would render the timing side channel entirely unusable

DISCLOSURE PROCESS

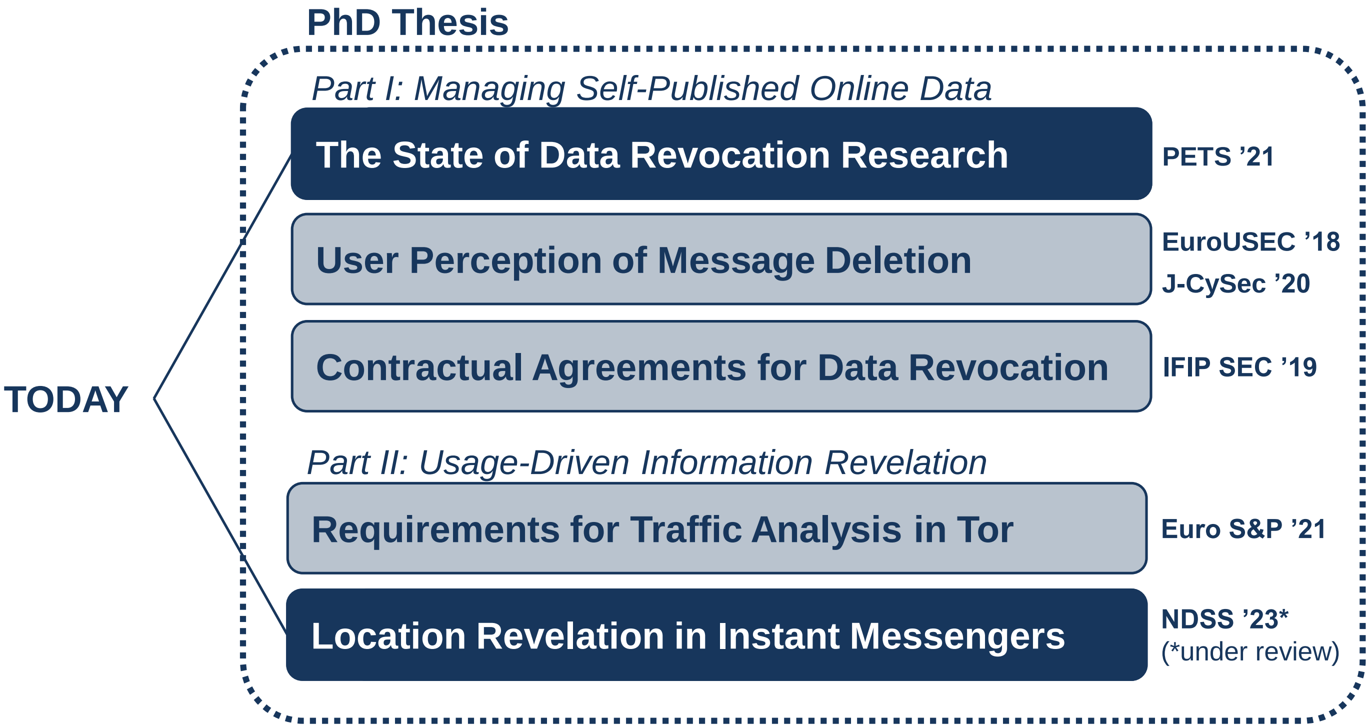






> *“We will discuss this internally and consider adding one or the other option in an upcoming update.“*
> (Threema)

RESEARCH CONTRIBUTIONS - PUBLICATIONS



PhD Thesis

Part I: Managing Self-Published Online Data

The State of Data Revocation Research — **PETS ’21**

User Perception of Message Deletion — **EuroUSEC ’18**, **J-CySec ’20**

Contractual Agreements for Data Revocation — **IFIP SEC ’19**

Part II: Usage-Driven Information Revelation

Requirements for Traffic Analysis in Tor — **Euro S&P ’21**

Location Revelation in Instant Messengers — **NDSS ’23*** (*under review)

TODAY

Traffic Analysis in Anonymous Communication

Rimmer et al. @**PETS ’22**
Heijligenberg et al. (in submission)

Sensitive Personal Data in Digital Health Applications

Utz et al. @**CHI ’21**
Kowalewski et al. @**PETS ’22**
Herbert et al. @**SOUPS ’22**
Kowalewski et al. (in submission)

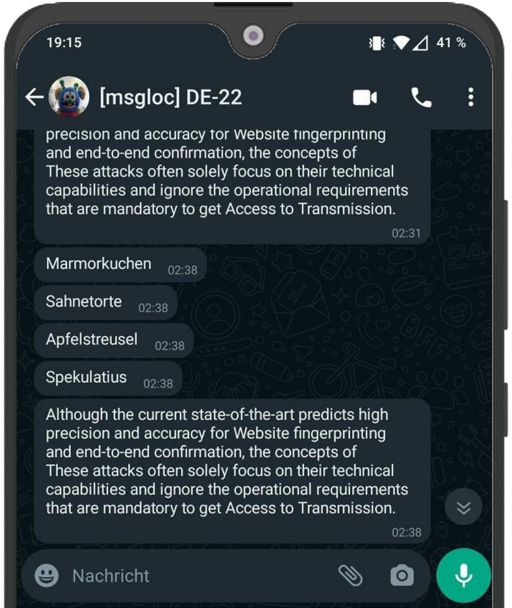
Authentication: Password Alternatives

Golla et al. @**WAY ’18**
Farke et al. @**SOUPS ’20**
Markert et al. @**SOUPS ’22**

RUHR
UNIVERSITÄT
BOCHUM
RUB

ANALYZING PRIVACY AND END USER INFORMATION EXPOSURE IN DIGITAL COMMUNICATION ENVIRONMENTS

PhD Defense
Bochum, June 24, 2022



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. 02:31

Marmorkuchen 02:38

Sahnetorte 02:38

Apfelstreusel 02:38

Spekulatius 02:38

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. 02:38

Theodor Schnitzler
Ruhr-Universität Bochum
theodor.schnitzler@rub.de

Key Takeaways

- Paths to solve open challenges in digital information exposure
- Alignment: Protection mechanisms do not fulfill user desires w.r.t. data they deliberately share
- Unintended and unexpected information revelation through the use of secure applications