universität wien

SBA Research

Careless Whisper

Exploiting Silent Delivery Receipts to Monitor Users on Mobile Instant Messengers

Gabriel K. Gegenhuber

Whoami

Gabriel Gegenhuber

PhD Candidate at University of Vienna

Researcher at SBA Research

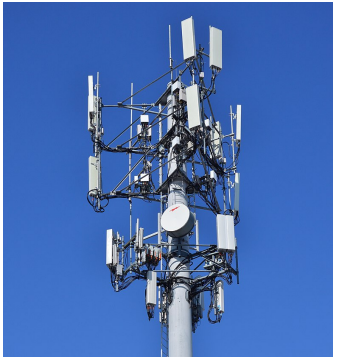
Bachelor’s and Master’s from TU Wien (Computer Science)

Research Focus: Mobile networks, offensive security

Research Group Security and Privacy (UniVie)

Networks and Critical Infrastructures Security Group (SBA)

Communication over Mobile Networks



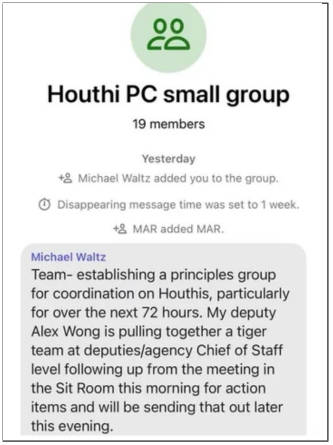
© Raysonho @ Open Grid Scheduler [CC0]

- Access Technology
  - Cellular Networks via SIM Card
  - Fixed-Line Networks via Wi-Fi AP

- Communication Protocol
  - VoLTE (or CSFB) via Cellular Network
  - WiFi Calling via Wi-Fi AP
  - **Messaging Apps**
    - e.g. WhatsApp, Signal

Motivation: Instant Messengers Everywhere

- Instant messengers (WhatsApp, Signal) are super popular
  - Politicians love them as well ☺
    - US 2025: Houthi PC small group *"Signalgate"*
    - AT 2021: ÖVP/ÖBAG chat affair *"Beidlgate"*



Information Leakage via Side Channels

- Besides
- Every action has (sometimes unwanted) side effects
  - Can be observed by third parties
  - **Accidental information leak**
- Real Life Examples
  - Less power consumption when not at home (e.g., holiday)
- Side channels in instant messengers
  - **Delivery receipts** ✓✓ and read receipts ✓✓

Message Sending Process: Delivery- and Read Receipts

- Sending a message on WhatsApp
  - Confirmed by server ✓
  - Confirmed by recipient ✓✓
  - Read by recipient ✓✓
- Read receipts can be turned off
  - In WhatsApp's privacy settings
  - No such settings for delivery receipts
    - **Delivery receipts cannot be turned off!**

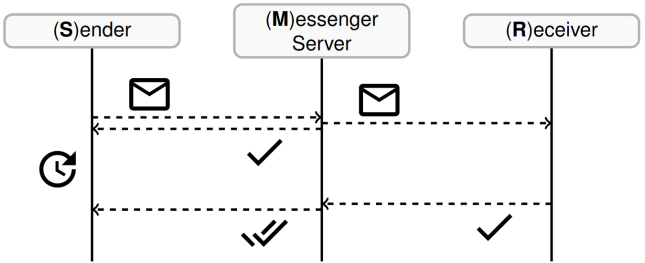
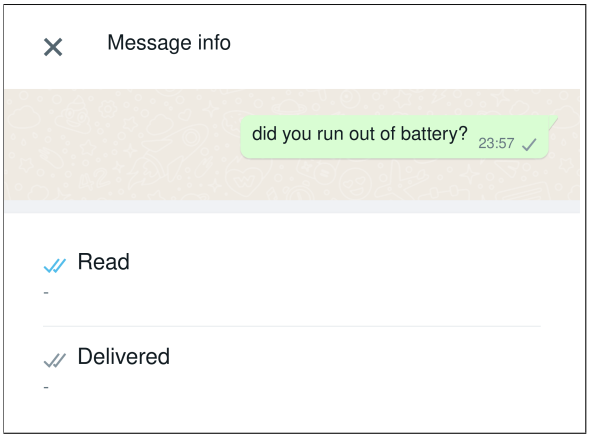


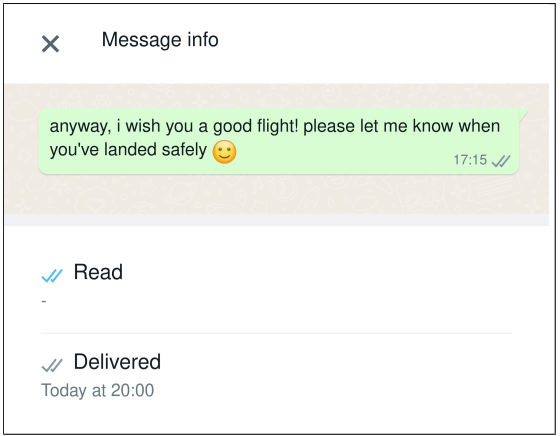
Image source: *Hope of Delivery: Extracting User Locations From Mobile Instant Messengers, Schnitzler et al., NDSS 2022*

Example: Delivery Receipts as Side Channel



Example: Delivery Receipts as Side Channel

Example: Delivery Receipts as Side Channel

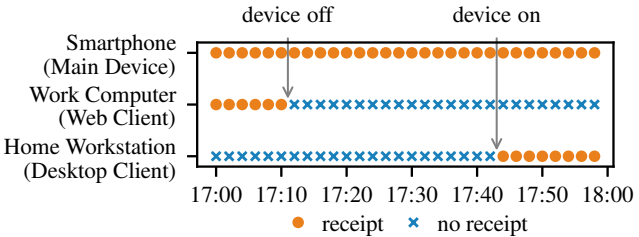


Silent Pinging via Delivery Receipts

- We wanted to evaluate how delivery receipts could be abused by an malicious actor
- Besides normal message, other actions also trigger delivery receipts (although not displayed in UI)
  - Editing messages, reacting to messages
  - Leading to **silent probing capabilities** (no visible notifications at the victim)
- Attacker does not need to be within contact list
  - Silent pings can be sent to anybody having these apps installed on their phone
  - **Only requirement: knowing a person's phone number**

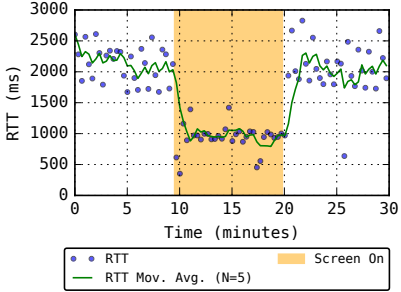
Silent Pinging via Delivery Receipts

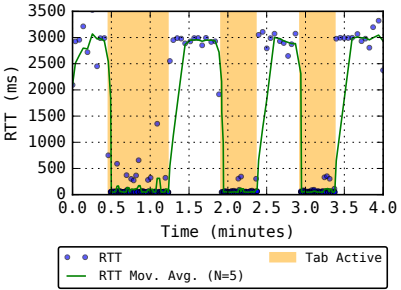
- Multi-device environments
  - **Companion devices** (WhatsApp Web/Desktop) **send independent delivery receipts**
  - When device comes online, receipts for all missed messages are triggered
  - Victim can be **tracked across devices**, potentially revealing their location



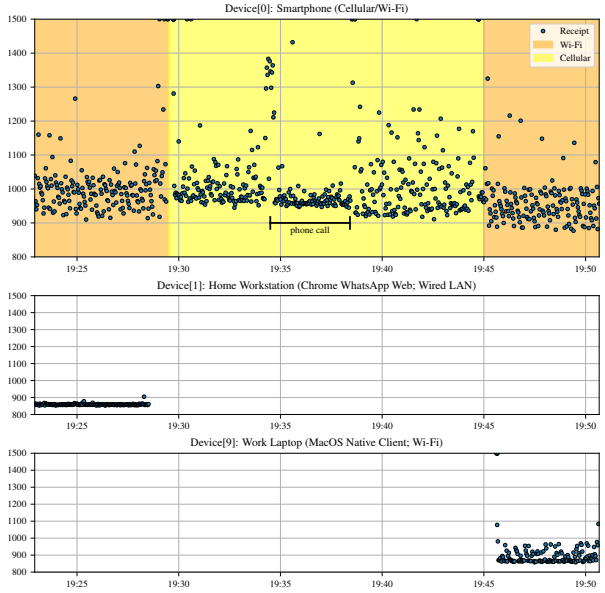
Investigating Delivery Receipt Timing Deviations

- Current phone state influences how fast delivery receipts are issued
  - **Active** state (screen on), receipts are issued **immediately**
  - **Standby** state (screen off), receipts are issued **delayed**





Continuous Monitoring



Device Operating System Fingerprinting

- Independent source code for different architectures (Android, iOS, Windows)
  - Creates distinct artifacts in receipt handling
  - Can be used to **determine** the victim's **operating system**
  - Can be abused for **reconnaissance**, in complex attack scenario

	OS	Delivery Receipts	Read Receipts
WhatsApp	Android	Separate	Stacked
	iOS	Separate	Stacked (Reversed)
	Web	Stacked	Stacked
	Windows	Stacked	Stacked
	macOS	Stacked (Reversed)	Stacked (Reversed)
Signal	Android	Separate	Stacked
	iOS	Separate	Stacked (Random)
	Desktop	Stacked	Stacked (Reversed)

Resource Exhaustion: Battery- and Data Drainage

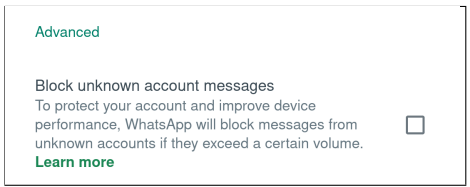
- **Spamming silent reactions** to the victim
  - Phone still receives and parses the packets
- Uses resources at the victim's phone
- WhatsApp did not rate-limit our requests
  - **Battery drainage : 18 % per hour**
  - **Data traffic consumption: 13.3 GB per hour**
- Signal had better rate-limiting, thus harder to exploit

Conclusion

- Silent pinging capabilities on instant messengers (WhatsApp, Signal)
  - Allows constant monitoring and tracking across devices
  - OS fingerprinting, resource exhaustion
- Anybody having these apps installed is a potential victim
  - Only requirement is knowing the phone number
- High value targets
  - Politicians and industrial espionage
  - Relevant for intelligence agencies and prosecution
- Personal targets
  - Stalking and partner abuse

Responsible Disclosure with Meta

- In some sense *Von der Forschung in den Markt* :)
  - Fixing bugs in prevalent messengers will profit everybody
- Reported findings to Meta on September 5th, 2024
- (Internally) forwarded to relevant development team on September 24th, 2024
- New privacy settings introduced in October 2024



- Since September 2024, no official/additional information or feedback from Meta ☹