universität wien

SBA Research

Prekey Pogo

Investigating Security and Privacy Issues in WhatsApp's Handshake Mechanism

Gabriel K. Gegenhuber, **Philipp É. Frenzel**, **Maximilian Günther**, **Aljosha Judmayer**

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

universität wien SBA Research

WhatsApp

- More than 3 billion users worldwide
  - Especially popular within Europe and South America
- Messages are **End-To-End-Encrypted (E2EE) via Signal protocol** since 2016
  - Perfect Forward Secrecy (PFS): protecting past messages
  - Post-Compromise Security (PCS): protecting future messages (*self-healing*)
- Formal protocol verification vs. **auditing implementation in practice**

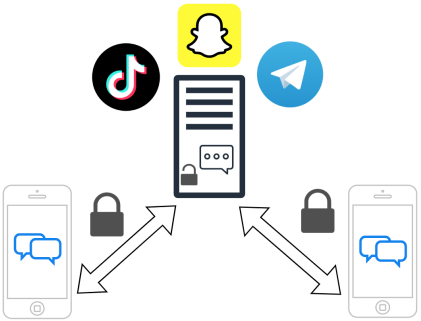
universität wien SBA Research

Testing Methodology

- Scrutinizing real world implementation and deployment
  - Target: official clients and server
- Attacker model:
  - Knowing victim's phone number
  - Using unofficial clients for API-level access
- Ethical considerations:
  - Only targeting own testing accounts

Background

Transport Encryption vs. End-to-End-Encryption (E2EE)



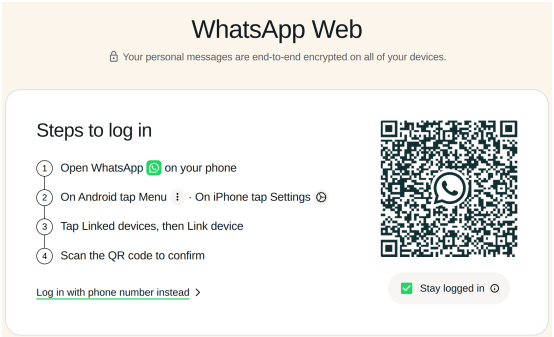
Transport Encryption

E2EE

Multi-Device + E2EE

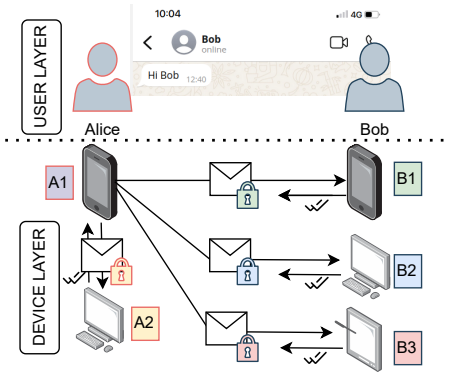
- WhatsApp allows adding secondary (also called *companion*) devices

- Two approaches
  - Leader-based approach
  - Client-fanout approach



Leader-based Approach vs. Client Fanout

- Leader-based approach
  - Secondary devices synchronize internally
  - Main device is single point of failure
- Client fanout
  - Used by WhatsApp and Signal
  - Pairwise E2EE sessions between all devices



universität wien SBA Research

Key Directory and Prekey-Bundle

- Leaking a user's devices

```
pogo@prekey:~$ ./query-devices -t 123456789
Querying registered devices for target number.

Found 3 existing devices: [0, 1, 3]
```

```
{
  "jid": "123456789:1@s.whatsapp.net",
  "t": "1740182155"          // epoch timestamp
  "registration": "000005DB",
  "type": "05",              // key type (djb)
  "identity": "76..77",      // 32 bytes pubkey
  "skey": {
    "id": "000001",          // signed prekey
    "value": "44...6a",      // 32 bytes pubkey
    "signature": "0d..02" // 64 bytes
  },
  "key": {
    "id": "0001a",           // one-time prekey
    "value": "0e..0b"        // 32 bytes pubkey
  }
}
```

universität wien SBA Research

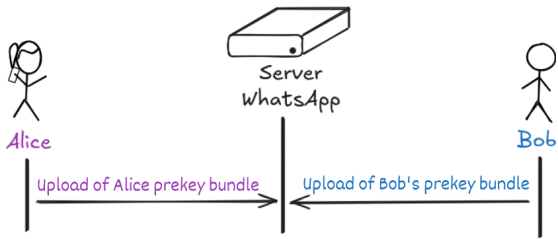
Defense in Depth: Three Key Layers

- **Long-term identity key:** created at install time
- **Medium-term signed prekey:** rotates once a month
- **Short-term one-time prekey:** ephemeral key, single use

- All three **keys are combined to initiate a new conversation**
  - Medium- and short-term keys ensure PFS at conversation start

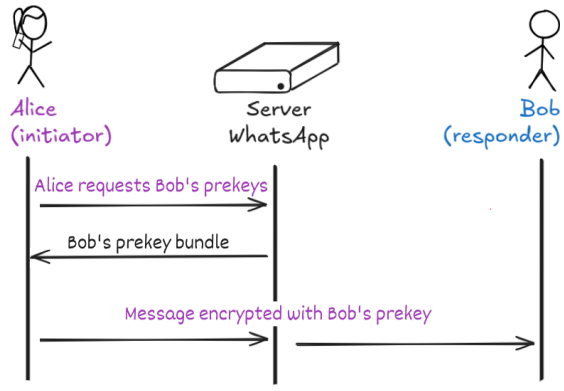
Prekey Refilling Mechanism

- Each client device regularly uploads a **stash of one-time prekeys** to WhatsApp
- **Refilling mechanism** is triggered when less than 10 one-time prekeys are left on the server



Conversation Start

- To start a new conversation:
  - Alice fetches prekey bundle from server for Bob
  - Alice encrypts the message with Bob’s prekeys
  - Bob receives the message which establishes the E2EE session



universität wien SBA Research

Vulnerabilities

universität wien SBA Research

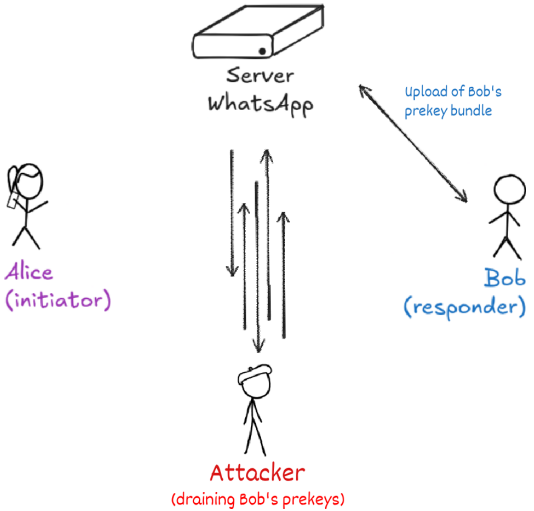
OS Disclosure

Client Implementation	Initialization Values for *key IDs*			Prekey Batch Size		Refill Trigger
	Registration	Signed PK	One-Time PK	Initial	Refill	
Android	*R*	0	*R*	812	812	10
iPhone	*R*	*R*	1	812	812	10
WhatsApp Web[a]	*R* & 0x3FFF	1	1	200	812	10
Desktop App macOS	*R*	*R*	1	200	812	10
Desktop App Windows	*R*	1	1	50	812	10

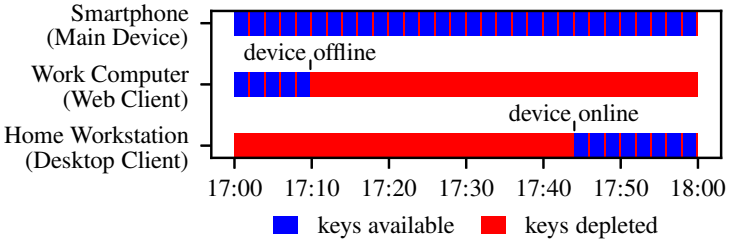
R Random number. [a] Verified on Firefox, Chrome, Safari.

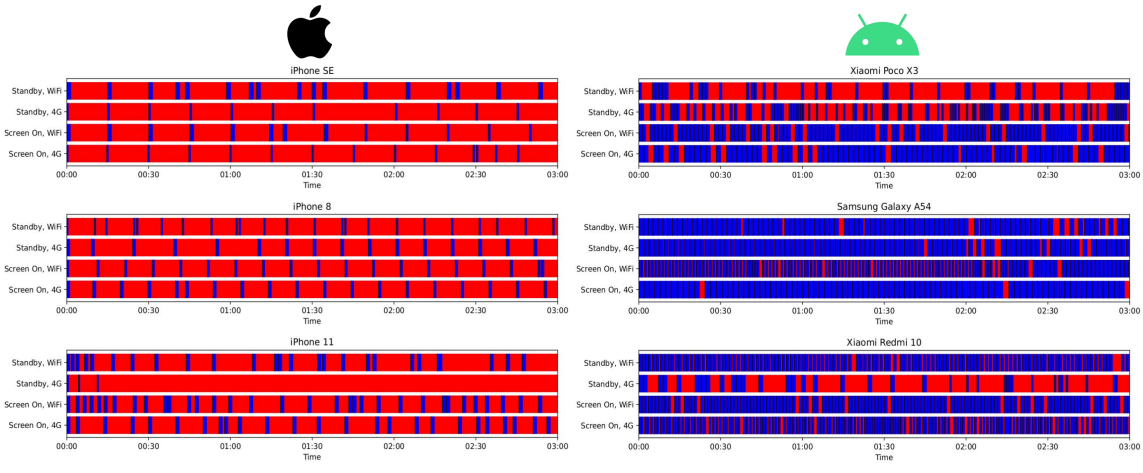
Prekey Depletion

- Usually client only requests one prekey bundle
- WhatsApp **does not enforce rate-limits**
- Attacker can consume all available prekeys of the victim



Tracking Device Online Status



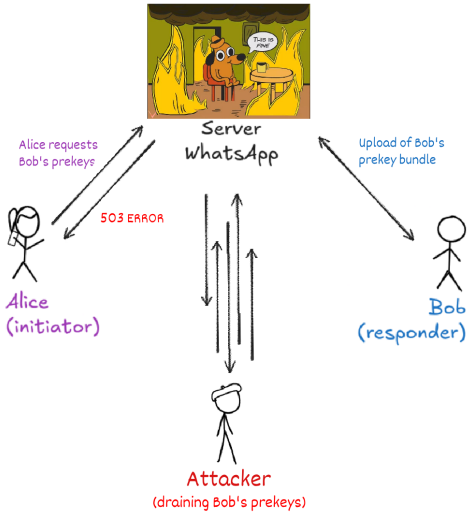

iPhone SE
Xiaomi Poco X3
iPhone 8
Samsung Galaxy A54
iPhone 11
Xiaomi Redmi 10
Standby, WiFi
Standby, 4G
Screen On, WiFi
Screen On, 4G
00:00
00:30
01:00
01:30
02:00
02:30
03:00
Time
keys available
keys depleted

PFS Downgrade

- Depletion of one-time prekeys leads to **PFS downgrade**
  - One-time prekey skipped in retrieved prekey bundles
  - New conversations are only encrypted with identity key and signed-prekey
- **PFS now depends on lifetime of the signed prekey**
  - Signed prekey rotated once **a month**
  - Only relevant for conversation start (until Bob responses to the message)

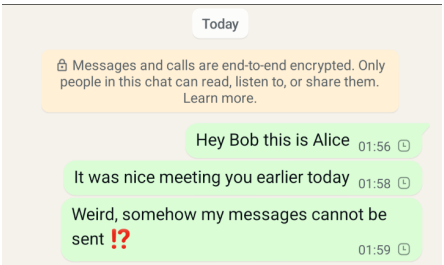
Prekey Retrieval Clogging

- Rapidly (asyncronously) **spamming prekey requests** to the server
- Server needs to synchronize all requests
  - Every request has to return a distinct one-time prekey
- Attacker can **clog prekey retrieval for all users** -> server returning `[503 Service Unavailable]`



Denial of Service

- Vulnerability hinders anybody from getting the victim's encryption keys
- Third party is **not able to start a new conversation**



universität wien SBA Research

Responsible Disclosure

- Reported findings to Meta on March 28, 2025
  - Issue closed on March 30, 2025
  - **Flagged as duplicate** to one of our previous reports about abusing delivery receipts to monitor users
    - *Careless Whisper: Exploiting Silent Delivery Receipts to Monitor Users on Mobile Instant Messengers*, RAID 2025

universität wien SBA Research

Mitigations

- Server-side rate limiting
- Unifying Android/iOS implementations
- Visual indication of missing PFS

universität wien SBA Research

Conclusion

- Some issues **inherent to E2EE**, thus hard remove entirely
  - Focus on making exploitation harder
- Multi-device setups amplify issues
  - Privacy leaks
  - More security-relevant attack surface (e.g., PFS downgrade), longer offline periods
- Complex deployment environment vs. verification of isolated parts

Questions?

- Contact
  - Mail: gabriel.gegenhuber@univie.ac.at
  - Twitter: @GGegenhuber
  - Bluesky: @ggegenhuber.bsky.social

Paper Link

github.com/sbaresearch/prekey-pogo