netidee

STIPENDIEN

Active Measurements in Cellular Networks

Zwischenbericht | Call 19 | Stipendium ID 7308

Inhalt

1 Einleitung

Seit dem Start meines Netidee-Stipendiums ist viel passiert. Ich hatte einen echten Lauf, was Publikationen und Konferenzreisen angeht: Insgesamt habe ich drei weitere Erstautor-Paper veröffentlicht, auf zwölf verschiedenen Konferenzen präsentiert und wurde dafür sogar mit einem Best Paper Award sowie einem Best Poster Award ausgezeichnet.

Obwohl ich die Kriterien (Anzahl der Publikationen) für den Abschluss meiner Dissertation schon seit Längerem erfülle, habe ich zwischen all diesen Erfolgen die formalen Schritte zur Einreichung meiner Dissertationsschrift etwas vernachlässigt. Dadurch liege ich gegenüber meinem ursprünglichen Zeitplan etwas zurück.

Auch wenn mich weiterhin viele neue Paper-Ideen in den Fingern jucken, möchte ich meine Dissertation bis zum Jahresende an die Gutachter schicken, damit ich im Frühjahr 2026 promovieren kann.

2 Status

1.1 Meilenstein 1 - Paper zu Privacy Leaks bei Mobile Instant Messengers

Dieses Paper markierte den Beginn einer längeren Forschungsreihe zu Instant-Messengern wie WhatsApp und Signal. Obwohl wir diese Apps täglich für einen Großteil unserer digitalen Kommunikation nutzen, gibt es bis heute nur wenig Forschung zu Security und Privacy auf diesen dominanten Plattformen in der Praxis. Um das zu ändern, habe ich mögliche Side-Channels in WhatsApp und Signal genauer untersucht. Diese Artefakte im Nachrichtenprotokoll können für die gezielte Überwachung beliebiger Personen missbraucht werden.

Mehrzähligen Paper-Rejections der ersten Publikation haben für etwas Verzögerung gesorgt, im Endeffekt wurden die Bemühungen aber sogar mit dem Best Paper Award auf der RAID 2025 in Gold Coast belohnt (mehr dazu gibts im entsprechenden Blogbeitrag). Außerdem lieferten die Ergebnisse genug Stoff für ein zweites Paper das auf der USENIX WOOT 2025 in Seattle präsentiert wurde. Auch in Las Vegas auf der DEF CON 33, der weltweit größten Hacking-Konferenz durfte ich einen Vortrag zum Thema halten.

Publikationen:

- Careless Whisper: Exploiting Silent Delivery Receipts to Monitor Users on Mobile Instant Messengers, *RAID 2025*
- Prekey Pogo: Investigating Security and Privacy Issues in WhatsApp's Handshake Mechanism, *USENIX WOOT 2025*

1.2 Meilenstein 2 - Paper zu Stalking Defense bei Offline Tracker Devices

Offline-Tracker-Geräte wie Apple AirTags sind im Alltag äußerst praktische Helfer, werden jedoch immer wieder auch für Zwecke wie Stalking missbraucht. Um wirksame Abwehrtechnologien zum Schutz der eigenen Privatsphäre und Sicherheit entwickeln zu können, ist es entscheidend, Wissen über die Funktionsweise dieser kommerziellen Produkte und ihrer proprietären Protokolle zu sammeln.

Obwohl ich dieses Thema bereits vor meiner Forschung zu Instant-Messengern begonnen habe, hat es aufgrund begrenzter zeitlicher Resourcen im vergangenen Jahr etwas weniger Aufmerksamkeit erhalten und ist somit noch zu keiner vollständigen Publikation gereift. Umso mehr freut es mich, dass ich nun trotzdem erste Ergebnisse im Dezember 2025 im Rahmen einer Poster-Präsentation auf der ACSAC-Konferenz in Hawaii vorstellen kann.

Publikationen (Poster):

- A Relay a Day Keeps the AirTag Away: Practical Relay Attacks on Apple's AirTags, ACSAC *2025*

1.3 Meilenstein 3 - Paper zu Phone Number Enumeration über WhatsApp

In den ersten beiden Publikationen zu Instant Messengern zeigte sich, dass WhatsApp kein effektives Rate-Limiting für Nachrichten besitzt, die über die App an den Server geschickt werden. Nachdem WhatsApp auf unsere Hinweise im Rahmen einer Responsible Disclosure nicht reagiert hatte, haben wir selbst untersucht, ob sich diese Schwachstelle für groß angelegte „Enumeration Attacks" missbrauchen lässt – also für das systematische Durchprobieren aller möglichen Telefonnummern, um aktive WhatsApp-Accounts zu identifizieren.

Zu unserer Überraschung wurden wir nicht gestoppt und konnten ungehindert 3,5 Milliarden Telefonnummern inklusive zusätzlicher Metadaten extrahieren. Trotz sehr langwieriger Kontaktaufnahme haben wir zum Glück doch noch eine Rückmeldung von

Meta/WhatsApp bekommen und konnten sogar aktiv beim Beheben der Schwachstelle helfen. Es war sehr spannend einblicke in ein Unternehmen dieser Größenordnung zu bekommen und ich bin froh dass meine Forschungsarbeit dazu geführt hat, die Sicherheits- und Privatsphäre aller weltweiten WhatsApp Nutzer:innen zu verbessern.

Aufgrund des beachtlichen Umfangs der Daten, die man abfragen konnte, wurden auch viele Medien darauf aufmerksam. Ein Highlight war ein Artikel im WIRED Magazine, insgesamt gab es sogar mehrere Hundert Medienberichte (darunter Printmedien, Onlinezeitungen, Radio und sogar Fernsehen) über meine Publikation.

Publikationen:

- Hey there! You are using WhatsApp: Enumerating Three Billion Accounts for Security and Privacy, *NDSS 2026*

3 Zusammenfassung Planaktualisierung

Die Milestones zur Verfassung der Dissertationsschrift konnten leider nicht vollständig abgeschlossen werden und sind daher für die kommenden Monate (Dezember und Jänner) vorgesehen. Außerdem habe ich bereits mit mehreren potenziellen Gutachter:innen Kontakt aufgenommen und befinde mich derzeit in der finalen Abstimmung. Die Erstellung der Gutachten sowie die Terminfindung mit den Reviewer:innen meiner Dissertation könnten noch zu gewissen Verzögerungen führen; auf solche administrativen Prozesse habe ich jedoch leider nur begrenzten Einfluss.

Insgesamt bin ich aber zuversichtlich, im ersten Halbjahr 2026 erfolgreich promovieren zu können. Da ich plane, der akademischen Forschung treu zu bleiben, wird der Übergang voraussichtlich fließend verlaufen.