TomTom Forensik

Fachgebiet: IT-Security
Betreuer: Dr. Endre Bangerter
Experte: Armin Blum (BAKOM)

Navigationssysteme erfreuen sich grosser Beliebtheit und gewinnen somit auch in der forensischen Analyse an Bedeutung. Die Geräte zeichnen oft den zurückgelegten Weg eines Fahrzeuges auf, oder versenden die Position via Mobilfunk. Die Analyse der Geräte ist jedoch sehr komplex, da es sich um proprietäre, undokumentierte Geräte handelt. Somit verlangt die forensische Analyse die Extraktion und das Reverse Engineering der Firmware und der Daten. Dies setzt wiederum oft die Demontage und Hardwareeingriffe am Gerät voraus.

Ausganslage

Moderne Navigationsgeräte, wie das TomTom GO LIVE 1000, senden per Mobilfunk Daten an TomTom, um daraus z. B. das Verkehrsaufkommen zu berechnen. Es wird vermutet, dass die gefahrenen Routen zur Verbesserung der TomTom eigenen Dienste auf den Geräten gespeichert werden. Die forensische Analyse ist bis heute nicht möglich, da die Geräte gut vor unerwünschtem Zugriff geschützt sind.

Ziele

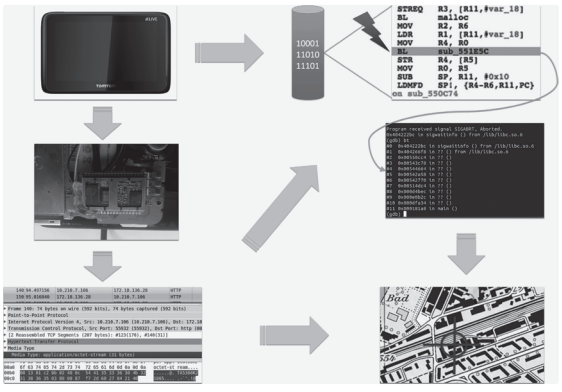
Das Ziel dieser Arbeit ist das Erarbeiten von forensischen Analysemethoden für die Geräte der TomTom GO LIVE 1000 Serie. Dabei interessiert natürlich, ob forensisch relevante Daten versendet oder auf den Geräten gespeichert werden. Der nötige Aufwand, um an diese Daten zu gelangen, wenn überhaupt möglich, ist nicht vorherzusagen. Darum ist die Arbeit als Forschungsarbeit aufgebaut, mit dem Fokus auf die systematische Vorgehensweise.

Resultate

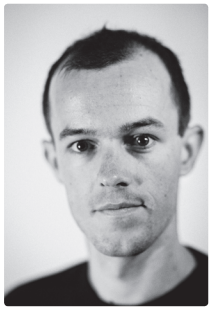
Mit Hilfe einer Hardwareanpassung und einer entsprechenden Filter- und Analysesoftware auf dem Computer können die über GSM gesendeten Daten live aufgezeichnet und mitverfolgt werden. Ein Merkmal der binären Daten fällt auf: jede Meldung an TomTom trägt zu Beginn der Daten die Device-ID mit sich. TomTom ist so theoretisch in der Lage, komplette Bewegungsprofile ihrer Geräte zu erstellen. Die Interpretation der gesamten Meldung gestaltet sich jedoch schwierig, da die Daten entweder codiert oder verschlüsselt sind. Um die vermutete Position in den Meldungen entziffern zu können, ist ein Reverse Engineering der Firmware notwendig.

Das Reverse-Engineering der Geräte-Firmware soll zwei Fragen beantworten: wie werden die Meldungen an TomTom codiert und wie, wenn überhaupt, werden die Positionsdaten auf dem Gerät gespeichert? Aufgrund der Komplexität der Firmware ist nur eine dynamische Analyse sinnvoll. Ist der Zugriff auf das Gerät nicht möglich, muss dazu ein virtueller Nachbau der ARM basierten Hardware erstellt werden.

Auf der Basis von QEMU, den quelloffenen Teilen der TomTom-Firmware und mit Anpassungen an der Firmware selber ist es uns gelungen, ein lauffähiger Nachbau der relevanten Teile der Firmware für eine Analyse zu erstellen. Aus Zeitgründen konnten bis zum Schluss die zwei offenen Fragen nicht beantwortet werden. Unsere Resultate liefern umfassende Informationen, eine erste Analyse und eine komplette virtuelle Umgebung für eine weiterführende Arbeit zu diesem Thema. Gerade die virtuelle Umgebung bietet gute Voraussetzungen, um die noch offenen Fragen zu beantworten.



Das Vorgehen der Analyse



Florian Badertscher
f.badertscher@gmail.com

Mathias Schneuwly
mathias.schneuwly@gmail.com