Da geht was!

Smartphones mit PinMe auch ohne Standortfreigabe tracken

GPS aus, WLAN aus – schon lässt sich ein Smartphone nicht mehr verfolgen. Falsch! Forscher zeigten, dass man auch anders herausfinden kann, wo Smartphone-Nutzer waren.

Von Michael Link

Jeden Tag muss man eines der angeblich ganz sicheren Lebensrezepte aussortieren. Aktuell dieses: Wer die Ortsbestimmung per WLAN und GPS an seinem Smartphone ausschaltet, wird nicht mehr geortet – außer vielleicht von der Polizei über Mobilfunk-Masten.

Das war mal richtig. Jetzt nicht mehr, denn nun hat ein Forscherteam um den Postdoktoranden Arsalan Mosenia an der Universität Princeton, USA, mit der PinMe-Methode gezeigt, dass man die Wege von Smartphone-Benutzern auch anders rekonstruieren kann – und zwar mit verblüffender Treffsicherheit [1].

Was zuvor geschah

Es hat schon einige Versuche gegeben, aus anderen Daten als dem Standortverlauf zu schließen, welchen Weg ein Smartphone-Nutzer genommen hat. Beispielsweise erriet die Powerspy-Attacke schon 2015 nur aufgrund der Stromverbrauchsdaten eines Smartphones auf einer Anzahl bekannter Strecken einen Standort mit einer Trefferquote von rund 45 Prozent [2].

Nach ähnlichen Versuchen mit weiteren Sensordaten musste man sich mit dem Gedanken anfreunden, dass Angreifer Standortinformationen auch mit solchen, scheinbar unkritischen Daten erlangen können. Alle Angriffsmethoden brauchten aber wenigstens eine der drei Voraussetzungen. Erstens: Der Startort des Opfers musste bekannt sein. Zweitens musste der Angreifer Zugriff auf Messdaten von Sensoren haben. Und: Deren Daten mussten mit sehr viel höherer Erfassungsrate aufgezeichnet werden als für alle üblichen Smartphone-Anwendungen üblich. Deswegen ist diese Angriffsmethode etwa so verbreitet wie andere erdähnliche Planeten im Sonnensystem.

„PinMe“ verfolgt einen breiteren Ansatz. PinMe ist keine App, sondern ein Verfahren. Es sammelt sehr viel mehr Sensordaten als bei bisherigen Studien und ergänzt sie durch externe Quellen. Die Forscher haben das Verfahren mit einem Apple iPhone 6 und 6S sowie mit einem Samsung Galaxy S4 durchgespielt. Die Geräte haben auf ihren Wegen Sensordaten eingesammelt und die Forscher konnten damit den Standortverlauf fast genauso gut nachvollziehen wie mit einem aufgezeichneten GPS-Track. PinMe erkennt unterschiedliche Aktivitäten wie Gehen, Autofahren, Zugfahren und Fliegen.

Die Stecknadel unterm Mikroskop

PinMe nutzt mehrere Quellen, einige im Smartphone, einige extern. Während ein Opfer normalerweise bemerken würde, wenn Apps Ortungswünsche hegen, kommt PinMe mit Informationen aus, die das Smartphone auch ohne Rückfrage beim Benutzer weitergeben darf. Sie sammelt den Netzstatus, die IP-Adresse, die Menge des verbleibenden Speichers sowie die Zeitzone. Hinzu kommen Sensordaten wie der Luftdruck und die Kompassrichtung und Beschleunigungswerte.

Die PinMe-Methode verbindet solche Daten mit allgemeinverfügbaren OpenStreetmap-Karten und Elevationsdaten für die Höhenangaben. Letztere spuckt das Google Maps API bequem für jeden Punkt der Erde aus.

PinMe zapft auch die Flugdaten von 9541 Flughäfen weltweit an und nutzt deren Höhen- und Lageinformation sowie Zeitzonen-Angaben; außerdem seine An- und Abflugdaten. Wertvoll sind auch Streckenpläne von Zugverbindungen. Die Forscher haben aus Google-Maps-Daten eine Datenbank erzeugt, welche die Fahrtrichtungen der Züge enthält. Durch Vergleich mit der Kompassrichtung in Verbindung mit dem Lagesensor im Smartphone fin-

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

det man heraus, in welche Richtung jemand mit dem Zug fährt. Fahrpläne verfeinern das Raster weiter, denn sie enthalten An- und Abfahrten für den Start- und Zielbahnhof sowie für alle Zwischenhalte. Dafür gibt es ebenfalls APIs zum Datenabruf übers Netz.

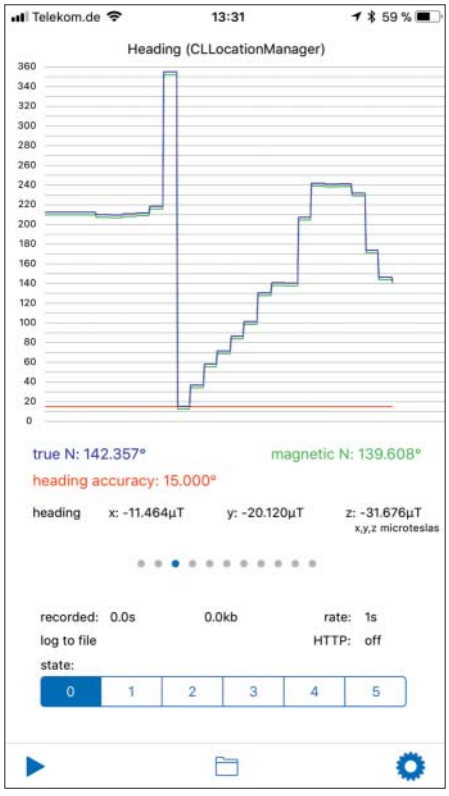
Fährst du noch oder gehst du schon?

PinMe durchläuft drei Schritte. Zunächst versucht der Algorithmus zu erkennen, in welcher Stadt man zuletzt mit einem WLAN verbunden war. Sowohl iOS als auch Android erlauben es Apps abzufragen, ob sie mit einem Mobilfunknetz oder einem WLAN verbunden sind. Dazu verwertet PinMe die Networkstatus-Daten. PinMe sucht die letzte IP-Adresse einer WLAN-Verbindung und füttert damit die „IP-Geolocation"-Datenbank. Sie wirft als Ergebnis aus, in welcher Stadt das Smartphone zuletzt mit einem WLAN verbunden war. Das ist zwar noch kein zwingender Hinweis auf den momentanen Standort, aber ein guter Startpunkt für die weitere Recherche.

Danach zerschneidet PinMe den gesammelten Datenwust in handlichere Portionen. Dazu verwendet es Muster der Bewegungserkennung als Schneidepunkte, zum Beispiel größere Änderungen beim Beschleunigungs- oder Lagesensor.

Im nächsten Schritt versucht PinMe, aus den Bewegungsmustern zu erkennen, ob der Nutzer zu Fuß unterwegs war, mit dem Auto fuhr, im Zug saß oder per Flugzeug reiste. Dazu nutzen die Forscher aus dem maschinellen Lernen stammende Modelle der Bewegungserkennung und weitere Daten, etwa den Luftdruckverlauf und Wechsel der Zeitzone. Für jede Art der Bewegung gibt es typische Merkmale. Bei einer Zugfahrt beispielsweise ändert sich die Bewegungsrichtung über lange Strecken nicht oder nur sehr langsam. Vom Fliegen lässt sich das auf den ersten Blick ähnliche Datenmuster durch den sich in kurzer Zeit stark ändernden Luftdruckverlauf unterscheiden. Beim Autofahren sind hingegen häufige Beschleunigungs- und Bremsvorgänge typisch, ebenso zahlreiche Richtungswechsel von 90 Grad beim Abbiegen. Fußgänger wiederum enttarnen sich durch häufige Beschleunigungsänderungen unabhängig von der räumlichen Lage des Smartphones.

Der dritte Schritt ist, daraus und aus den externen Quellen den Standortverlauf abzuleiten. Er ist der aufwendigste.



Apps wie Sensorlog zeichnen Rohdaten für die Richtung, den Luftdruck und andere Parameter auf.

Ene, mene, muh – da bist du!

Kurz rekapituliert: Die letzte Stadt mit WLAN-Kontakt ist bekannt, die Bewegungsart ebenfalls. Beides zusammen bestimmt, mit welchen Algorithmen und mit welchen Startinformationen PinMe den Datenpaketen zu Leibe rückt.

Hat man anhand der Daten erkannt, dass ein Opfer Auto gefahren ist, versucht PinMe mit einer Karte zunächst, ein Gitternetz zu konstruieren. Das enthält alle markanten Punkte im Zielgebiet, beispielsweise alle Einmündungen und Kreuzungen, außerdem deren exakte Höhenwerte. Die gefahrene Route ermittelt der PinMe-Ansatz unter anderem mithilfe der Abbiegevorgänge. Wann jemand abbiegt, verraten die Kompassdaten des Smartphones.

Die Höhe des Smartphones am Abbiegepunkt (H_{turn}) berechnet PinMe nicht einfach mit der barometrischen Höhenformel aus den Daten des Luftdrucksensors (P_{turn}). Und zwar deshalb nicht, weil das Barometer im Smartphone durch die Temperatur und Luftfeuchte beeinflusst wird. PinMe holt sich stattdessen den lokalen Luftdruck (P_{turn}) sowie die Höhe der

Kommentar

Von Michael Link

Was die PinMe-Forscher zeigten, war keine Raketentechnik, sondern bloß simples Auswerten offener Quellen. Erst die verräterischen Strava-Heatmaps, nun die Standortverfolgung von Smartphones ohne aktive Lokalisierungsfunktion – beides zeigt, wie leicht sich mit scheinbar harmlosen Bausteinen private Dinge offenbaren lassen.

Dass es so einfach ist, an solche Daten zu kommen, sollte die Politik zum Handeln zwingen. Die informationelle Selbstbestimmung ist nämlich ein Grundrecht. Die Datenschutzgrundverordnung (DSGVO) wird Besserungen bringen, aber auch mehr ellenlange Datenschutzerklärungen. Es bleibt unwahrscheinlich, dass alle App-Anbieter im Ausland ihre Apps DSGVO-konform programmieren.

Wie schön wäre es, wenn man als Nutzer nicht mehr jede App misstrauisch selbst nachprüfen muss. Die Politik könnte das regeln, indem sie Betriebssystem-Anbieter sanktioniert, wenn sie in ihren Ökosystemen intransparente Datenabflüsse von Apps nicht verhindern.

Statt aber solche verbraucherfreundlichen Signale zu setzen, plädiert die neue Digitalministerin für einen „smarten Datenschutz". Heißt: eine Aufweichung. Und sie nennt gleich ein Beispiel, nämlich den weltweiten Abgleich ausgerechnet von Patientendaten. Ich darf also nie mehr krank werden, sonst kommt alles, alles raus!

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

Wetterstation ($H_{station}$) als Vergleichsnormal aus lokalen Wetterdaten. Welche Stadt infrage kommt, weiß PinMe durch die in Schritt 1 ermittelte IP-Adressen-Zuordnung. Ebenso zieht sich PinMe die Werte für die Temperatur (T) und die Luftfeuchte (C). Die Höhe am Abbiegepunkt ergibt sich zu:

$$H_{turn} = H_{station} + \frac{T}{C} \ln\left(\frac{P_{turn}}{P_{station}}\right)$$

Damit ist die Höhenlage des Smartphones an jedem Abbiegepunkt jeweils bekannt, aber nicht die Geschwindigkeit. PinMe schließt nach einer Abbiegung alle theoretisch möglichen Wege aus, bei denen die Höhendaten und die Richtung für die anderen Abbiegevorgänge des Datenpaketes nicht mehr passen. Je mehr Fahrtrichtungsänderungen für die Analyse bereitstehen, desto weniger mögliche Routen bleiben übrig – von einigen Tausend nach wenigen Abbiegungen sind es selbst in ungünstigen Fällen nach rund sieben Richtungswechseln nur noch eine Handvoll. Mathematische Verfahren ergänzen danach weitere mögliche Routen und bewerten, wie wahrscheinlich sie sind. Ganz unsinnige Routen fallen dann raus.

Für Flüge zieht PinMe mehrere Datenstränge heran: Die Flugdaten für Start und Landung, die Zeitzone und Höhe von Start- und Zielflughafen. PinMe kann zwischen den einzelnen Flugphasen unterscheiden, also die Beschleunigung beim Start, Steig- und Sinkflug sowie das Landen erkennen – sogar Rollfeld-Fahrten. Ebenfalls erfasst sind Luftdruckdaten. Eine Suche in einer Datenbank fischt alle Flughäfen heraus, bei denen die Höhe sowie die Flugdaten und die Zeitzonen passen.

Bei Zugfahrten läuft es ähnlich: Beschleunigungsdaten – positive bei der Abfahrt, negative beim Bremsen – erzeugen mit den Fahrtdauern ein Muster, das zusammen mit einer Datenbank Züge mit passenden Fahrtverläufen ausspuckt.

Bleibt das Tracken von Fußgängern. Wie zuvor bei den Autofahrern bildet ein Netz der möglichen Wege mit allen Abbiegemöglichkeiten die Grundlage. Der Beschleunigungsmesser und der Kompass lassen auf die Schrittzahl sowie die Richtung schließen. Anders als beim Auto-Tracking ergibt sich durch die Schrittzahl auch eine Distanz. Der Rest ist aus der guten alten Koppelnavigation bekannt.

Ergebnisse

Alles in allem ergaben sich beim Rekapitulieren von Autofahrten Fehlerraten von weniger als 1,5 Prozent bei Tests in Princeton, Philadelphia und Trenton. Für die Flugverfolgung lagen nicht so viele Daten vor, doch PinMe erkannte alle vier Flüge der Probanden richtig und fand die jeweiligen Start- und Zielflughäfen. Auch das Verfolgen von Zugfahrten ergab bei 30 ausgewerteten Datenpaketen keinen einzigen Fehler. Mehr Unsicherheit gibt es naturgemäß beim Verfolgen von Fußgängern, weil sich diese nicht an Wege halten müssen und beispielsweise ein Überqueren der Fahrbahn auch als Abbiegen gedeutet werden kann. Dennoch lag der Annäherungsfehler ab einer Schrittzahl von rund 1500 Schritten bei weniger als 1 Prozent – und selbst bei nur 500 erfassten Schritten nur bei 2,5 Prozent.

Mögliche Einfallstore

Die Forscher haben zum Sammeln der Sensordaten fürs iPhone die App Sensorlog aus dem App Store benutzt und eine ähnliche für Android selbst geschrieben. Einen „PinMe“-Trojaner haben sie hingegen nicht entwickelt. Man braucht aber nicht viel Fantasie dazu, sich auszumalen, dass das keine Hexerei ist. Angreifer könnten ihren Opfern Apps unterjubeln, die dem Augenschein nach anderen Zwecken dienen, zum Beispiel Online-Spiele. Da das Auslesen bestimmter Sensor- und weiterer Daten in gängigen Betriebssystemen derzeit keine Nutzerfreigabe erfordert, ließ sich das gewünschte Material leicht unbemerkt abschöpfen.

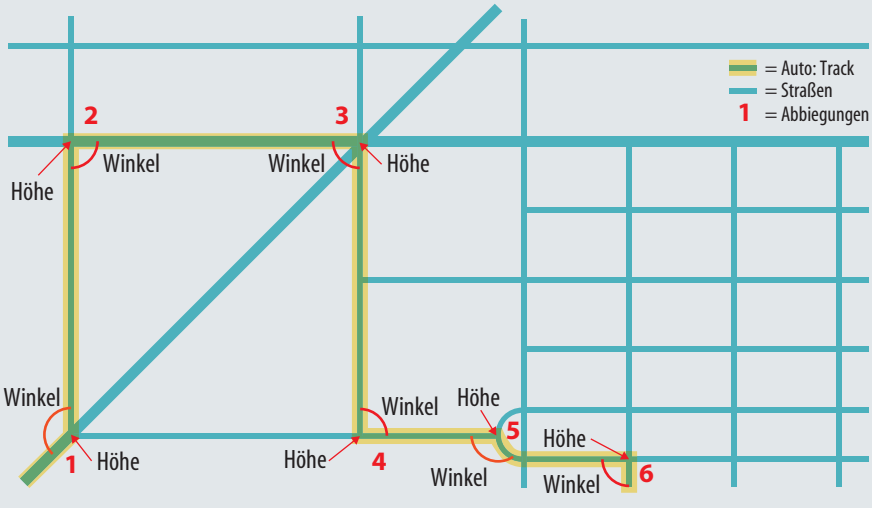
Wie man einen Korken auf die Flasche mit den üppig perlenden Daten bekommt, haben die Forscher ebenfalls eruiert. Die Erfassungsrate der Sensoren pauschal zu begrenzen wäre nach Ansicht des Forscherteams keine gute Idee, denn darunter würden auch Navi- und Sport-Apps sowie Online-Spiele wie Pokémon Go leiden. Ein Wachhund im Smartphone, der Alarm schlägt, wenn Daten heimlich abfließen, ist zwar denkbar, treibt aber den Teufel mit dem Beelzebub aus. Denn dazu muss jeder Datenstrom durch eine Überwachungsinstanz, was Angreifern weitere Möglichkeiten eröffnet. Die Sensordaten künstlich ungenauer zu machen löst das Problem auch nicht, denn das torpediert wieder gewünschte App-Funktionen.

Der letzte von den Princeton-Forschern vorgeschlagene Lösungsvorschlag wäre derzeit der nächstliegende: ein Knopf, der alle Sensoren ausschaltet.

(mil@ct.de) c't

Tracking von Autos

Fahrzeug-Tracking durch Höhen- und Winkelangaben: Während nach den ersten vier Abbiegevorgängen im ungünstigsten Fall noch mehrere zurückgelegte Routen möglich sind, sorgen spätestens die Daten nach dem fünften Abbiegen für einen eindeutigen Routenverlauf.



Literatur

[1] A.Mosenia et. al., PinMe: Tracking a smartphone user around the world, IEEE Trans. Multi-Scale Computing Systems

[2] Y. Michalevsky et. al., Powerspy: Location tracking using mobile device power analysis, Proc. Usenix Security Symposium 2015, pp. 785

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover