Silke Holtmanns und Ian Oliver

Sicherheit und Privacy innerhalb des Mobilfunknetzwerks

Wie schützt man Nutzer im Mobilfunknetz?

Ziel dieses Artikels ist es, auf verständliche Weise die praktischen Schwierigkeiten und Herausforderungen darzustellen, die bei der Umsetzung von vielen verschiedenen Anforderungen, Richtlinien und Grundsätzen für die Handhabung persönlicher Daten im Mobilfunknetz entstehen.

Stellen Sie sich vor, Sie sind ein Programmierer und sollen ein Programm für einen Mobilfunk-Netzwerkknoten entwickeln, welches das Netz selbst und seine Benutzer vor Angriffen schützt. Durch Ihren Knoten gehen u. a. Informationen und Kommandos, die für Benutzermobilität gebraucht werden, zum Beispiel Logs für Handover zwischen Funkzellen, Anrufaufbau, Daten, Änderung von Benutzerprofilen etc. Sie haben sich eine Liste der ganzen Daten angelegt, die durch Ihren Knoten gehen oder dort gespeichert werden. Was machen Sie jetzt? Sie wollen Nutzer schützen und dafür sorgen, dass das Netz verfügbar bleibt, aber Sie haben keine genaue technische Beschreibung und wenden sich deshalb in Ihrer Ratlosigkeit an verschiedene interne Stellen.

Sie gehen erst einmal in die Kaffeeecke und denken darüber nach, was Sicherheit für das Netz, die Benutzer und Privacy eigentlich bedeutet. Ihre erste Idee ist, dass die Benutzer nicht abgehört werden möchten, und dass der ganze Service funktionieren sollte. Der Kollege am Nachbartisch von der *Radio Network Konfiguration* sagt, dass die Luftschnittstelle recht gut verschlüsselt ist mit A5/3, zumindest in den neueren Knoten, und dass die alten Knoten eh Auslaufmodelle bei den fortschrittlichen Netzwerkbetreibern seien. Er erklärt auch, wie schwierig die ordentliche Konfiguration des Netzes sei, um zu vermeiden, dass Gespräche und *Data Sessions* abbrechen, der Benutzer keine Verbindung mehr hat, dem Telefon die Batterie leer gesaugt wird oder manche Telefone nicht mehr funktionieren. Um das zu konfigurieren, schauen sich er und seine Kollegen die Logs, Fehlernachrichten und die ganzen Metadaten genauer an, um dann entsprechend die Fehler zu entdecken und zu beseitigen. Er rät Ihnen, alle Metadaten zu speichern, zumindest für eine Weile.

Sie gehen zurück zu Ihrem Arbeitsplatz und schauen in den Security Newsticker, wo Sie sehen, dass eine große Webseite gehackt worden ist und Tausende von Kundendaten nun im Internet liegen. Da ein Telefonnetzwerk ja eigentlich auch nur ein Netzwerk mit vielen Kundendaten ist, entschließen Sie sich mit der IT-Sicherheitsabteilung zu reden, die sollten doch wissen, wie man Benutzer schützt. Die IT-Abteilung ist gerade dabei, eine *Denial-of-Service*-Attacke von einem Botnet abzublocken, welche schon einen Hauptknoten überlastet hat und gerade dabei ist, auch die Backup-Knoten anzugreifen, und wenn der runtergeht, wäre das Netz vollständig lahmgelegt. Sie kriegen nur brüsk an den Kopf geworfen, dass Benutzer erwarten, dass der Netzwerkbetreiber sich um die Sicherheit kümmert, anstatt selbst was dafür zu tun. Dafür würde man alle Daten brauchen, die man kriegen kann. Sie schleichen leise aus dem Raum. In dem Moment ruft Ihr Vater an, er hätte da so eine merkwürdige Meldung beim Browsen gekriegt und wisse nicht, was er machen soll. Sie hatten schon im Newsticker gelesen, dass das neuste Security Update mit dem falschen Schlüssel unterschrieben war und der Browser eine Zertifikatswarnung rauswirft. Sie beruhigen also Ihren Vater und sagen, dass es in dem Fall in Ordnung ist und er *Erlauben* klicken kann.

Sie gehen zurück zu Ihrem Büro und grübeln. Auch wenn Sie die IT-Kollegen verstehen, scheint Ihnen das alles doch etwas viel der Datensammlung. Andererseits, dem Benutzer das Sicherheitsmanagement aufzubürden, nein, das scheint auch nicht richtig zu sein und funktioniert sicherlich auch nicht. Da es um Privacy und persönliche Daten geht, wenden Sie sich nun an die Abteilung *Ethics & Compliance*. Die schickt Ihnen eine 10 Seiten lange *Privacy Guidance* von ihrer Webseite, welche generisch und allumfassend beschreibt, wie gut und verantwortlich Ihr Arbeitgeber mit den Daten seiner Kunden umgeht, und dass er der *EU Privacy Regulation* streng folgt. Die Idee und der Tenor des Dokumentes sind gut, aber was sollen Sie jetzt mit den Log-Files und den Metadaten in Ihrem Knoten machen? Sollen Sie sie einfach löschen? Die Abteilung *Ethics & Compliance* setzt auch den Kollegen von *Legal Compliance* ins *cc*-Feld. Der meldet sich bei Ihnen und erklärt, dass wenn eine richterliche Anordnung vorliegt, ein Netzwerkbetreiber verpflichtet ist, die Kommunikationsdaten eines Kunden als Kopie an die entsprechende Behörde über eine spezifizierte Schnittstelle weiterzureichen. Diese Kommunikation muss natürlich lesbar sein für die Behörde, zumindest darf der Netzwerkbetreiber nicht die Kommunikation eines potenziellen Kriminellen oder Terroristen verstecken[1]. Diese gesetzliche Anforderung muss vom Netzwerkbetreiber erfüllt werden, sonst darf das Netz nicht betrieben werden. Da Sie an die Rechtstaatlichkeit Ihrer Regierung glauben und auch ganz gerne einen Job haben, haben Sie soweit kein Problem mit der Idee, dass nach einem richterlichen Beschluss Nutzerdaten an die Behörden gegeben werden.

Aber da war doch letztens noch was in den Nachrichten über NSA, Merkel und Benutzerortung. Sie werden neugierig und lesen nach, was da eigentlich los war. Mobilfunkbetreiber haben vor ungefähr 30 Jahren angefangen, die Netzwerke zu verbinden, um Benutzern *Roaming* zu ermöglichen. Damals waren es wohl nur eine Handvoll staatlicher Netzwerkbetreiber, welche sich gut kannten und vertrauten. Mittlerweile gehören Hunderte Netzwerkbetreiber zu dem Roaming-Netzwerk und obendrein diverse Service Provider. Da die EU den globalen Wettbewerb fördert und Netzwerkbetreiber ihre Zugänge auch vermieten, ist die Zahl sicher noch steigend. Diese Netze sind entweder direkt per Kabel miteinander verbunden, wenn es viele Benutzer gibt, die ständig zwischen zwei Netzen *roamen*, oder über *Roaming Hubs* für Netzwerk-Kombinationen, die etwas seltener sind. Roaming funktioniert weltweit, egal ob Deutschland, Malediven, Bangladesch, Russland oder China. Das Roaming läuft über ein Netzwerk, welches hauptsächlich die Protokoll-Suite SS7/

SIGTRAN verwendet, die aber keine Absenderauthentifizierung hat, da man sich vor 30 Jahren ja gut kannte und vertraut hat. Sie werden hellhörig und graben weiter. Die NSA hat zum Beispiel diese fehlende Authentifizierung benutzt, um Informationen aus den Netzen abzufragen. Und zwar über eben die Verbindung, welche eigentlich für das Roaming gedacht ist. Snowden-Dokumente behaupten, dass die NSA 701 der 985 Mobilfunknetzwerke weltweit mittels *Auroragold* gehackt habe[2]. Der prominenteste Privacy-Hack über das Roaming-Netzwerk ist die Benutzerortung[3], wobei das ursprüngliche Kommando (MAP_ATI) eigentlich für Mobilitätsmanagement netzwerkintern gebraucht wird. Solche Daten-Akquise in Wild-West-Manier verträgt sich nicht mit Ihrem Verständnis von Rechtsstaatlichkeit und Unschuldsvermutung. Sollen Sie die Metadaten einfach alle hashen? Sollen Sie einen Filter für solche externen Roaming-Anfragen entwickeln, um die Benutzer vor diesen Anfragen zu schützen? Sollen Sie Roaming unterbinden und das Interface schließen und alle externen Kommandos einfach blocken?

Sie sind verzweifelt und reden mit Ihrem Chef. Der fragt Sie, wie teuer so ein Filter sein wird, was ist das Return-on-Investment? Bald sind wieder Quartalsergebnisse und Shareholder-Meeting, jede Investition für die Softwareentwicklung wird von den Shareholdern auf ihren Wert hin geprüft. Werden die Benutzer mehr für ihren Mobilfunkvertrag zahlen, wenn wir die Filter installieren? Was ist der *Business Case*? Der Chef weist darauf hin, dass Shareholder-Meetings nicht für ihren Altruismus bekannt sind und Benutzer auch nicht mehr zahlen, bloß weil es sicher ist und die Privatsphäre schützt, die benutzen doch eh' alle Google und Facebook, kriegen Sie zu hören. Als Sie das Schließen des Roaming-Interfaces erwähnen, wird Ihr Chef blass und meint, dann sollten wir uns alle nach einer neuen Arbeit umsehen. Aber der Chef versteht auch Ihr Problem und hat einen guten Hinweis: Sie sollen mal mit der Forschungsabteilung reden, die machen „Privacy, Security und so 'n Gedöns". Sie wenden sich also mit wenig Hoffnung der Forschungsabteilung zu.

Die Forschungsabteilung hat mehrere Experten. Ein Experte erklärt Ihnen, dass das Sicherheitsproblem im Roaming-Netzwerk nicht nur ein Privacy-Problem ist, sondern auch zu großem finanziellen Schaden für den Netzwerkbetreiber führen kann. Über das Roaming-Netzwerk können nicht nur Kommandos für die Benutzerortung geschickt werden, sondern auch Kommandos, welche das Benutzerprofil im Hauptknoten ändern. Das Benutzerprofil enthält wichtige Daten, die festlegen, dass den Kunden ihre Netznutzung korrekt berechnet wird oder welche Premiumservices eine Benutzerin in ihrem Vertrag hat etc. Ändert man dort geschickt einige Felder, dann können Benutzer Services erhalten, ohne dafür zu zahlen, oder *Roaming Fraud* begehen, was zu großen finanziellen Einbußen führen kann. Sie gehen zusammen in die Kaffeeecke und setzen einen Business Case für einen Filter auf dem Roaming-Interface auf. Ein Mitarbeiter aus der Standardisierungsabteilung erwähnt, dass die Vereinigung der Netzwerkbetreiber GSMA an einer Spezifikation für SS7-Filter arbeitet. Sie präsentieren den Business Case Ihrem Manager, der damit zufrieden ist und die Ressourcen genehmigt, um einen Roaming-Filter für die eingehenden Kommandos zu entwickeln. Aber was ist mit den IT-Security-Problemen, polizeilichen Anfragen und den Log-Dateien?

Sie gehen zurück zu Research. Ein anderer Forscher erzählt etwas wirr von *non-Euklidean spaces, weighted distances* und *data distortion*. Sie wollen sich gerade höflich aus der Diskussion entfernen, als er Ihnen die Demo-Implementierung zeigt. Mit dieser Implementierung lassen sich stufenweise Network Traces und Logs anonymisieren. Die Daten werden entsprechend ihres Informationsinhalts mittels verschiedener Methoden anonymisiert, z. B. mit *k-anonymity, l-diversity* etc. Die Anonymisierung ist so angelegt, dass die Daten zwar *verzerrt* werden, aber *Malware* und *Radio Network Bug Tools* immer noch reagieren. Wenn so ein Fall eintritt, dann kann die Anonymisierung für diesen Traffic-Stream schrittweise heruntergefahren werden. Sie schleppen den Forscher zur IT-Abteilung und diese bestätigt, dass sie mit diesem Tool sicher noch die meisten Botnets und Malware finden werden. Die IT-Abteilung hat es geschafft, das Netz am Laufen zu halten und gibt zu, dass sie eigentlich ganz froh ist, nicht die heißen Rohdaten direkt zu haben. Deshalb schickt sie eine Mail an Ihren Manager, dass sie so ein Tool benötigen und wohl bei der Integration mit Ihnen und der Forschungsabteilung zusammenarbeiten würden. Da die Forschungsabteilung die Hauptarbeit der Entwicklung schon erledigt hat, steht Ihr Manager der Integration der stufenweisen Anonymisierungssoftware positiv gegenüber. Danach schauen Sie bei den Radio-Kollegen vorbei, die auch bestätigen, dass sie hauptsächlich bei Auffälligkeiten gewisse Details benötigen. Die Daten, die die Demo rausgibt, würden wahrscheinlich reichen. Nur bei dem *l-diversity* oder *k-anonymity,* da war der Kollege nicht sicher, welches Verfahren wohl besser wäre. Auf die Anfrage bei Ethics, ob sie für das Feld *Protokoll* im Header im Zusammenhang mit der Anonymisierung der Länge der Nachricht lieber *l-diversity* oder *k-anonymity* nehmen, erhalten Sie nur eine *Out-of-Office*-Antwort und beschließen, es einfach im Testnetzwerk mit ein paar alten Datensätzen auszutesten.

Silke Holtmanns und Ian Oliver

Dr. **Silke Holtmanns** arbeitet seit mehr als 15 Jahren im Bereich der Mobile Security und ist zurzeit als *Security Specialist* in der Thematik SS7/*Diameter Roaming Security* bei *Nokia Networks* tätig.

Dr. **Ian Oliver** ist seit 16 Jahren im Mobilfunkbereich tätig. Er ist Autor des Buches *Privacy Engineering* und als *Security Specialist* für *Privacy/Malware Data Analysis* bei *Nokia Networks* beschäftigt.

Nachdem Sie endlich die Ressourcen für Ihre Arbeit erhalten haben, Ihre Arbeit getan ist, die Filter hoffentlich vernünftig funktionieren, Malware erkannt wird, die Radio-Experten das Netzwerk am Laufen halten können und den Gesetzen genüge getan ist, trinken Sie erst mal einen großen Kaffee und grübeln darüber nach, ob die Sicherheit und Privacy der Benutzer jetzt wohl wirklich zu 100 % geschützt sind und ob wohl alles der *Privacy Policy* entspricht? Als Ihr Kaffeebecher leer ist, sieht es so aus, als hätte eine Pille auf dem Grund gelegen, manchmal scheint sie rot, manchmal blau …

Nachtrag

Die Autoren haben diese Geschichte natürlich komplett erfunden. Die Geschichte und die hier repräsentierten Meinungen sind die der Autoren und nicht notwendigerweise die von *Nokia Networks*. Und unser Manager hat ein gutes Sicherheitsverständnis. Wir haben einige technische Details verallgemeinert, um die Leser nicht mit 3-5-Buchstaben-Abkürzungen zu bombardieren. Falls aber Interesse an selbigen besteht, werden wir diese selbstverständlich auf direkte Anfragen genau erläutern. Das Thema Sicherheit der Luftschnittstellen haben wir bewusst nicht genauer erläutert, da es recht heterogen ist. In diesem Bereich gibt es viele Varianten die den Rahmen des vorliegenden Textes sprengen würden und einen eigenen Artikel verdienen.

Anmerkungen

1 *Wenn Benutzer HTTPS Ende-zu-Ende benutzen, ist das keine Maßnahme, die vom Netzwerkbetreiber angewandt wird*

2 *Status 2012, es geht nicht daraus hervor, ob diese Zahlen auch die Virtual Operator enthalten*

3 *Chaos Computer Club, Dez. 2014, Tobias Engel*

Max Maaß

Faire Algorithmen

In der öffentlichen Diskussion werden Algorithmen oft als objektiv oder gar unfehlbar dargestellt. Ein Algorithmus habe schließlich keine versteckten Vorurteile, er behandle alle gleich, und sei damit per definitionem *objektiv. Diese Einschätzung nutzen einige als Argument, um immer mehr Aufgaben von Menschen auf Algorithmen zu übertragen – von der Verkehrsplanung über die Auswahl von Bewerber.innen bis hin zur Strafverfolgung mittels* Predictive Policing.[1] *In diesem Artikel soll die Frage untersucht werden, ob Algorithmen tatsächlich objektiv sind, und welche Probleme sich ergeben können, wenn Algorithmen die Arbeit von Menschen übernehmen.*

Eine Geschichte unfairer Algorithmen

Die Untersuchung von Algorithmen auf Verfälschungen und Befangenheit[2] geht bereits mehr als 30 Jahre zurück. Schon in den 1980ern wurde dem Buchungssystem *Sabre* (betrieben von *American Airlines*) vorgeworfen, bestimmte Flüge bevorzugt anzuzeigen. Tatsächlich stellt [illegible] von American Airlines gezielt da [illegible] rierende Fluglinien systematisch z [illegible] hielt American Airlines einen Vort [illegible] der sich auch in den Bilanzen niederschlug.

In diesem Fall wurde der Algorithmus gezielt so entworfen, dass er bestimmte Ergebnisse bevorzugt. Schwieriger wird es beim anderen Extrem: Ein Algorithmus, der möglichst neutral sein soll, aber *trotzdem* befangen ist. Ein Beispiel dafür war ein Algorithmus, der in den 1970ern von einer englischen *Medical School* entwickelt wurde, um den Bewerbungsprozess um die limitierten Studienplätze zu beschleunigen. Das Programm sollte eine erste Auswahl der Kandidat.innen vornehmen, die für ein Bewerbungsgespräch eingeladen werden sollten. Es wurde über mehrere Jahre weiterentwickelt, bis es eine Übereinstimmung von bis zu 95 % mit den Ergebnissen der (menschlichen) Bewerbungskommission ergab.

Der Algorithmus war über fünf Jahre im Einsatz, bis sich herausstellte, dass er gegen Frauen und ethnische Minderheiten diskriminierte. Dieses Verhalten wurde ihm nicht explizit beigebracht, er hatte es aus den Entscheidungen der Kommission gelernt, die (bewusst oder unbewusst) eine solche Diskriminierung an den Tag gelegt hatte.[4]

Der Stand der Forschung

[illegible] gorithmen sowohl gezielt als auch [illegible] ken können. Während *analoge* [illegible] gerer Zeit wissenschaftlich untersucht wird, ist das Feld der Erforschung digitaler Diskriminierung vergleichsweise wenig erschlossen. Die erste Arbeit zu diesem Thema wurde 1987 von Huff *et al.* geschrieben und weist auf die Gefahr von Gender-Stereotypen in der Softwareentwicklung hin.[5] Diese Arbeit stammt allerdings aus der Psychologie, nicht der Informatik.

Die ersten Informatikerinnen, die sich mit diesem Themenkomplex beschäftigten, waren Batya Friedman und Helen Nissenbaum, die 1996 einen Artikel über die verschiedenen Formen von Verfälschungen in Computersystemen schrieben. Sie identifizierten drei Formen von Verfälschung: *preexisting bias* (Tendenzen, die aus der realen Welt übernommen werden), *technical bias* (Verfälschungen durch technische Limitationen), und *emergent bias* (Verfälschungen, die erst im Verlauf der Zeit entstehen, weil sich die Software nicht an neue Begebenheiten anpasst).[6] Der bereits diskutierte Fall des Bewerbungs-Algorithmus' wäre in diesem Modell ein Fall von *preexisting bias*. Ein Beispiel