Identitätsmanagement und das Risiko der Re-Identifikation

Sebastian Clauß, Stefan Schiffner, Sandra Steinbrecher
{sc2, ss602038, ss64}@inf.tu-dresden.de

Dogan Kesdogan, Tobias Kölsch, Lexi Pimenidis
{kesdogan, koelsch, lexi}@i4.informatik.rwth-aachen.de

Abstract: Ein essentieller Bestandteil zukünftiger Informationstechnologien ist das nutzerzentrierte Identitätsmanagement zum Schutz der Privatsphäre. Es muss die verschiedenen Anforderungen von mehreren Parteien erfüllen und weist deshalb eine hohe Komplexität auf. In dieser Arbeit geben wir einen Überblick über vorhandene Systeme und zeigen die damit verbundenen Probleme. Insbesondere wird der Frage nachgegangen, inwieweit die Privatsphäre durch solch ein System geschützt werden kann. In erster Linie wird dabei die Gefahr der Re-Identifikation diskutiert. Mögliche Gegenmaßnahmen zu den erkannten Angriffen werden im Anschluss kurz skizziert.

1 Einführung

Wer im realen Geschäft die Beratung eines Verkäufers sucht, gibt diesem zumeist nur Informationen, die für den geplanten Kauf relevant sind. Aber der Nutzer eines Internetshops bietet diesem zumeist ein umfangreicheres Persönlichkeitsprofil. Hier kann Identitätsmanagement (IDM) Nutzern bei der Kontrolle der Datenmenge helfen, die sie zu Servern übertragen. Dabei werden verschiedene Nutzerprofile (oder partielle digitale Identitäten) verwendet. IDM-Systeme können in nutzer- und serverzentrierte Systeme unterteilt werden, je nachdem, wo die Kontrolle über die Daten liegt.

In fast allen technischen Bereichen ist Anonymität nicht perfekt realisierbar. Daher sollte der Nutzer über den erreichten und erreichbaren Grad an Anonymität informiert werden. Hierzu ist eine Schätzung der Anzahl der Nutzer verschiedener Anwendungen und deren Verteilung notwendig. Serverzentrierte IDM-Systeme erlauben eine einfache Berechnung dieser Zahlen, erreichen aber zumeist keine Anonymität des Nutzers gegenüber dem Systembetreiber während nutzerzentrierte Ansätze dies bieten, dafür aber nur eine Schätzung dieser Zahlen erlauben.

Bisher konzentrierte sich die Anonymitätsforschung im Bereich von Protokollen, Designoptionen und Angriffen auf die IP-Ebene. In dieser Arbeit präsentieren wir einen strukturellen Ansatz zur Klassifikation von Angriffszielen, Angreifern und Angriffen auf IDM-Systeme. Die meisten Techniken stammen aus dem Bereich der Anonymität auf IP-Ebene und der Datenbanksicherheit. Die Klassifikation ist auf alle bekannten Arten von IDM-Systemen anwendbar.

2 Identitätsmanagement

In der digitalen Welt können Personen durch Mengen von maschinenlesbaren Daten (Attribute) repräsentiert werden, sogenannte digitale Identitäten. Abhängig von Situation und Kontext werden nur Teilmengen dieser Daten zu ihrer Repräsentation benötigt, sogenannte Teilidentitäten. Ein IDM-System stellt die technischen Möglichkeiten zur Verwaltung dieser Teilidentitäten zur Verfügung, die an unterschiedliche Namen (Pseudonyme) gebunden sind. Nutzer können je nach Beziehung zum Kommunikationspartner zwischen den Pseudonymen wählen. IDM Systeme müssen dabei sowohl Techniken für Anonymität als auch für Authentizität unterstützen, um folgende Sicherheitsziele zu erreichen:

Kontrollierbare Pseudonymität von Nutzern: Diese besteht aus zwei Aspekten: *Unverkettbarkeit von Pseudonymen und ihren Inhabern (bzw. Inhaberanonymität)* und *Unverkettbarkeit zwischen Pseudonymen*.

Kontrollierbare Zurechenbarkeit von Nutzern: Ein Pseudonym kann auf sichere Art authentisiert werden und basierend darauf zur Nutzung gewisser Dienste autorisiert werden. Die unter dem Pseudonym begangenen Handlungen sind diesem zurechenbar und der Inhaber soweit erforderlich aufdeck- und/oder haftbar.

IDM-Systeme zur Verwaltung von Accounts oder Profiling von Nutzerdaten sind *serverzentriert* und werden zentral implementiert. Ihr Hauptziel ist die vertrauenswürdige Identifikation von Personen oder Zuschreibung von Eigenschaften zu diesen. Die kontrollierte Pseudonymität wird hingegen zumeist vernachlässigt, da alle Daten serverseitig gespeichert werden. Die einfachste Umsetzung ist ein stand-alone-System mit einer Datenbank zur Speicherung der partiellen Identitäten, das von diesem Server und den dem Nutzer angebotenen Anwendungen genutzt wird.

Ein *nutzerzentriertes* IDM soll dem Nutzer die Kontrolle über die Herausgabe seiner Daten ermöglichen. Es soll sowohl kontrollierte Pseudonymität des Nutzers als auch Verlässlichkeit der übermittelten Daten erreicht werden. Der Nutzer kann entscheiden, ob, an wen und für welchen Zweck er personenbezogene Daten herausgeben möchte.

Um Unverkettbarkeit zwischen mehreren Pseudonymen zu erreichen ist es notwendig, Attribute zwischen Pseudonymen transferieren zu können. Attribute, die für ein Pseudonym a zertifiziert wurden, sollen auch unter dem Pseudonym b verwendet werden können, ohne einen Zusammenhang mit Pseudonym a herstellen zu müssen. Um dies zu erreichen, müssen die Attribute in Form von *anonymen Credentials* vorliegen. Ein Credentialsystem mit solchen Eigenschaften wurde in [CL00] veröffentlicht.

Weitere Unterstützung erhält ein nutzerzentriertes IDM durch Treuhänder für Werteaustausch (Wertetreuhänder) und Treuhänder zur vertrauenswürdigen Verwaltung von Identitätsdaten (Identitätstreuhänder). Hiermit können Datensparsamkeit und Rechtssicherheit unterstützt werden. Privacy Emergency Response Teams (PERT) können analog zu den bereits bestehenden Computer Emergency Response Teams (CERT) Informationen über Sicherheits- und Datenschutzrisiken an Identitätsmanagementsysteme der Nutzer weitergeben, um dort die Herausgabe personenbezogener Daten zu beeinflussen.

3 Angriffe

Das IDM-System soll Individuen vor einer Analyse und Aufzeichnung ihrer Daten schützen, selbst wenn ein Angreifer große Teile des Systems kontrollieren kann. Der Angreifer versucht aus den verfügbaren Daten die partiellen Identitäten zu rekonstruieren. Hierfür kann er auf zwei Datenquellen zurückgreifen: Der Angreifer gewinnt seine Informationen entweder aus dem Pool der Daten, die ein Nutzer ihm bereits preisgegeben hat, oder er kennt den Nutzer als Person und beobachtet ihn, bzw. interagiert mit seinem Umfeld. Zustandsänderungen in IDM-Systemen, die durch den Nutzer verursacht wurden, können ebenfalls durch den Angreifer ausgewertet werden. Schließlich können die unterschiedlichen Organisationen, die verschiedene partielle Identitäten eines Nutzers kennen, diese untereinander abgleichen.

Angreifer können in mehrere Kategorien eingeteilt werden: aktive und passive Angreifer, Insider (Angreifer, die legitime Rechte missbrauchen) und Outsider (Angreifer, die nicht oder nur teilweise am Geschehen beteiligt sind). Passive Angreifer sammeln die gewünschten Informationen durch Beobachtung, hierunter fällt z.B. das Aufzeichnen einer Kommunikation oder die Suche in öffentlich zugänglichen Datenbanken, z.B. eine Internetrecherche. Passive Angreifer handeln oft unbemerkt und aus beliebiger Entfernung. Im Gegenzug versuchen aktive Angreifer Informationen durch Manipulationen beliebiger Art zu gewinnen, deren einfachste Art es ist, Nutzer direkt nach den Daten zu fragen. Insider haben bereits eine größere Datenmenge über den Nutzer zur Verfügung, während Outsider Aktionen durchführen müssen, um an weitere Daten zu gelangen. Das kann durch den Kauf von kommerziellen Datensammlungen geschehen, das Überwachen einer Datenleitung, oder durch die Bereitstellung der Daten durch Dritte.

Durch die interaktive Natur des Identitätsmanagement ergeben sich einige IDM-spezifische Angriffe: Bei *Timing Attacks* nutzt der Angreifer sein Wissen über zeitliche Abfolgen von Ereignissen. Kann er mehrere Datenbanken beobachten, dann kann er Änderungen untereinander oder mit Beobachtungen außerhalb verketten. Eine *Wait and Seek Attack* liegt vor, wenn der Angreifer weiß, wann sein Opfer auf eine Datenbank zugreift. Dann kann er vor und nach diesem Zugriff die Datenbank abfragen und aus den Veränderungen Rückschlüsse ziehen. In einer *Linking Attack* hat ein Angreifer Zugriff auf mehrere Datenbanken und kann die Informationen miteinander verketten. Ein *Selective Information Request* liegt vor, wenn ein Dienstleister seine Anfragen verändert, je nach dem welche Informationen er schon hat. Dadurch können gezielt Informationen erfragt werden, die zur Re-Identifizierung des Opfers führen.

Anonymität ist auf Netzwerkebene nur bedingt erreichbar [KP04]. Diese Erkenntnis kann aus einer allgemeinen Beschreibung gewonnen werden, die auf einer Beobachtung von Anonymitätsmengen basiert. Damit kann man diese Analysen und insbesondere Schnittmengenangriffe entsprechend verändert auch auf IDM-Systeme anwenden.

4 Schutzverfahren

Schutzverfahren basieren darauf, dass Nutzer bei der Übermittlung ihrer Attribute lügen, die Genauigkeit reduzieren oder Attribute nicht übermitteln, d.h. es werden Merkmale entfernt, die eindeutige Zuordnung und leichte Kontaktierung von Individuen ermöglichen.

Besonders Ausreißer lassen sich leicht re-identifizieren, da sie in einer Datensammlung problemlos wieder zu erkennen sind. Schutz bietet hier die Vergröberung der Skalen. Diese Methode ist allerdings nur bedingt hilfreich, wenn ein Individuum durch die seltene Kombination einiger Attribute zum Ausreißer wird. Hier kann durch Aggregation Abhilfe geschaffen werden. Eine Reihe von Individuen wird zu einer Gruppe zusammengefasst, deren Attribute aus den Einzelattributen berechnet werden.

Ein Verfahren, das bei nutzerzentrierten IDM Ansätzen leichter angewandt werden kann, ist das Verrauschen der Attributwerte. Allerdings ist zu beachten, dass die Daten zu einem bestimmten Zweck übermittelt wurden, der durch das Rauschen gefährdet werden könnte. Effektiver wird der Schutz, wenn verhindert wird, dass der Angreifer weiß, ob das Opfer überhaupt in der Datenbank vorkommt [Pom91].

5 Zusammenfassung

In dieser Arbeit wurde ein kurzer Überblick über Identitätsmanagement und die an es gestellten Anforderungen der gleichzeitigen kontrollierbaren Zurechenbarkeit und Pseudonymität von Nutzern gegeben. Es wurde ein Klassifikationsschema bzgl. der möglichen Angriffe auf die Pseudonymität vorgeschlagen. Aus drei verschiedenen Gebieten (statistische Datenbanken, Anonymität im Netz, und Interaktivität) konnten konkrete Angriffe auf IDM-Systeme abgeleitet werden. Schutzmöglichkeiten gegen die angeführten Angriffe wurden kurz skizziert. Eine genauere Ausführung ist in [CKK$^+$] zu finden.

Literatur

[CKK$^+$] Sebastian Clauß, Dogan Kesdogan, Tobias Kölsch, Lexi Pimenidis, Stefan Schiffner, and Sandra Steinbrecher. Privacy Enhancing Identity Management: Protection Against Re-identification and Profiling. ACM CCS2005 Workshop on Digital Identity Management, November 2005, George Mason University, Fairfax, VA, USA.

[CL00] Jan Camenisch and Anna Lysyanskaya. Efficient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation. Research Report RZ 3295 (# 93341), IBM Research, November 2000.

[KP04] Dogan Kesdogan and Lexi Pimenidis. The Hitting Set Attack on Anonymity Protocols. In *Proceedings of Information Hiding, 7th International Workshop*. Springer Verlag, 2004.

[Pom91] Klaus Pommerening. *Datenschutz und Datensicherheit*. BI-Wissenschaftsverlag, Mannheim, Wien, Zürich, 1991. ISBN 3-411-15171-4 (in German).