Verteilte Nutzungskontrolle

Eine zukunftsgerichtete Kontrolle der Datennutzung als Enabler für existierende und zukünftige digitale Technologien

Manuel Hilty, ETH Zürich, Lehrstuhl für Informationssicherheit, Zürich
manuel.hilty@inf.ethz.ch

Alexander Pretschner, Dr., ETH Zürich, Lehrstuhl für Informationssicherheit, Zürich
alexander.pretschner@inf.ethz.ch

David Basin, Prof. Dr., ETH Zürich, Lehrstuhl für Informationssicherheit, Zürich
basin@inf.ethz.ch

Die Kontrolle über die Nutzung unserer Daten wird immer wichtiger. Die technische Umsetzung aber ist schwierig, die nötigen Mechanismen sind teilweise erst in Entwicklung.

Um seine Privatsphäre in einer zunehmend vernetzten Welt zu schützen, gibt es zwei Strategien. Eine Strategie besteht darin, die Menge anfallender persönlicher Daten zu minimieren und möglichst anonym zu bleiben. Dies ist jedoch häufig nicht möglich, etwa beim Einkaufen bei Online-Shops oder bei elektronischen Behördengängen, beim Verwenden von Mobiltelefonen oder Kreditkarten, oder bei der Beanspruchung medizinischer Leistungen. Weiterhin versprechen personalisierte Suchmaschinen viele Vorteile, bieten aber auch potenziell die Möglichkeit der Erstellung sehr detaillierter Nutzerprofile. Eine zweite Strategie besteht deshalb darin, die Verwendung der einmal angefallenen persönlichen Daten zu kontrollieren. Gesetze regeln, was mit persönlichen Daten geschehen darf, aber bisweilen werden diese Gesetze von den involvierten Informationssystemen und deren Benutzern nicht oder nur ungenügend befolgt (was nicht gezwungenermassen in böser Absicht geschehen muss). Die Disziplin der Verteilten Nutzungskontrolle befasst sich mit der technischen Umsetzung dieser zweiten Strategie, also damit, wie kontrolliert werden kann, was mit Daten geschieht, nachdem sie weitergegeben worden sind. Offensichtlich ist der Anwendungsbereich der Verteilten Nutzungskontrolle nicht auf den Datenschutz beschränkt, sondern umfasst unter anderem auch intellektuelles Eigentum und Amts- oder Firmengeheimnisse.

Wenn ein Datenkonsument bei einem Datenanbieter ein Datum anfordert, dann sind zwei Arten von Bedingungen relevant. Ob der Datenkonsument das Datum überhaupt erhalten kann, wird durch so genannte *Provisionen* beschrieben. Falls der Datenkonsument berechtigt ist, das Datum zu erhalten, dann beschreiben sogenannte *Obligationen*, was mit den Daten nachher passieren darf und was nicht. Provisionen und Obligationen werden in einer Policy des Datenanbieters zusammengefasst und regeln so die zukünftige Verwendung sensibler Daten.

Beispielszenario

Wir illustrieren das am Beispiel des Zusammenspiels zweier öffentlicher Verwaltungen. Verwaltung V_1 betreibt eine Datenbank mit persönlichen Daten. Verwaltungen V_2, V_3 und V_4 können unter bestimmten Umständen auf diese Daten zugreifen. Andere Verwaltungen haben nie Zugriff. Dies wird durch Provisionen geregelt, beispielsweise «V_2 kann an Werktagen zwischen 8:00 und 18:00 auf Dokument D_1 zugreifen» oder «V_3 kann auf alle Steuerdaten zugreifen». Diese Bedingungen umfassen die klassische Zugriffskontrolle. Was der Datenanbieter (in diesem Fall V_1) aber nach Herausgabe der Daten an eine andere Verwaltung auch spezifizieren kann und in vielen Fällen auch möchte, sind Bedingungen der Art «Dokument D_1 muss nach 30 Tagen wieder gelöscht werden», «V_1 muss bei jeder Verwendung der Daten benachrichtigt werden», oder «Dokument D_2 darf nur für statistische Zwecke verwendet werden».

Wenn nun zum Beispiel V_2 auf Dokument D_1 zugreifen möchte, dann wird zuerst geprüft, ob dieser Zugriff überhaupt möglich ist. Dies ist der Fall, wenn V_2 zu Arbeitszeiten darauf zuzugreifen versucht. V_2 wird dann über die damit verbundenen Obligationen in Kenntnis gesetzt, zum Beispiel dass das Dokument nach 30 Tagen wieder gelöscht werden und dass V_1 benachrichtigt werden muss, wofür die Daten tatsächlich verwendet werden. Falls V_2 diesen Bedingungen zustimmt, werden die Daten herausgegeben, zusammen mit einer sogenannten *Lizenz,* in der die damit verbundenen Obligationen aufgelistet sind. Wir illustrieren diesen Ablauf in ■■■■.

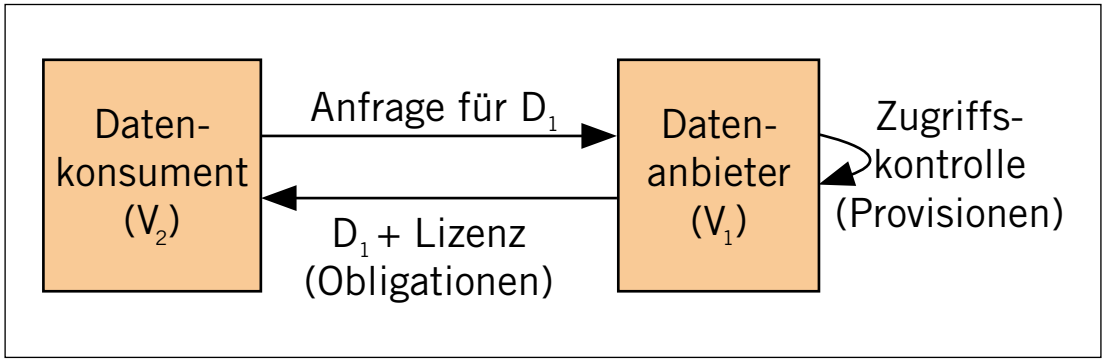

Abbildung 1: Beispielszenario

Mechanismen

Die Einhaltung von Provisionen zu garantieren, ist zumindest konzeptionell vergleichsweise einfach. Der Datenanbieter kann überprüfen, ob die geforderten Kriterien für eine Herausgabe der Daten erfüllt sind und entsprechend handeln. Zugriffskontrolle findet dann u.a. auf der Ebene von Datenbanken, Middleware, Applikationsservern oder Anwendungen statt. Die garantierte Einhaltung von Obligationen ist jedoch ungleich schwieriger. Der Grund dafür ist, dass ein Datenanbieter meist keine direkte Kontrolle über das Verhalten des Datenkonsumenten hat und deshalb nicht direkt verhindern kann, dass die Obligationen verletzt werden.

Grundsätzlich existieren zwei Methoden, um die Einhaltung von Obligationen zu erzwingen oder zumindest die Wahrscheinlichkeit dafür zu erhöhen. Beide Methoden unterscheiden sich in den zugrunde liegenden Vertrauensmodellen und Anforderungen sowie in den Garantien, die sie liefern können.

Kontrollmechanismen

Die erste Methode besteht darin, Kontrollmechanismen zu verwenden, die der Datenkonsument verwenden muss, um auf die Daten zugreifen zu können. Technisch erfolgt das üblicherweise durch Verschlüsselung der Daten, die ohne diese Mechanismen nicht lesbar sind. Die Kontrollmechanismen können dann Aktionen, die auf den Daten ausgeführt werden sollen, einschränken oder zusätzlichen Aktionen (z. B. das Verschicken einer Benachrichtigung) ausführen. Der Einsatz solcher Mechanismen kann somit dem Datenanbieter garantieren, dass bestimmte Obligationen eingehalten werden.

Kontrollmechanismen wurden bisher vor allem im Bereich des Digital Rights Management (DRM) entwickelt. Wir sind jedoch davon überzeugt, dass der Einsatz ähnlicher Mechanismen auch im Datenschutzbereich sinnvoll ist. Tendenzen in diese Richtung sind auch ersichtlich, wenn etwa Firmen wie Adobe und Microsoft Technologien für den Schutz von Dokumenten anbieten, die auf DRM-Technologien basieren. Diese Technologien sind jedoch noch nicht in der Lage, DRM-fremde Anforderungen wie Benachrichtigungen oder das Löschen von Daten nach einer gewissen Zeit zu unterstützen. Solche Anforderungen sind aber typisch für den Datenschutz.

Eine Strategie, seine Privatsphäre in einer zunehmend vernetzten Welt zu schützen, besteht darin, die Verwendung der einmal angefallenen persönlichen Daten zu kontrollieren.

Im Zusammenhang mit der Verwendung von Kontrollmechanismen gibt es zwei Probleme:

- Das erste Problem ist, dass solche Mechanismen nicht hundertprozentig sicher sind, wie die Erfahrung aus dem DRM-Bereich zeigt. Gerade softwarebasierte Mechanismen werden immer wieder geknackt. Dies schränkt die Verwendbarkeit solcher Mechanismen zwar ein, macht sie aber nicht nutzlos. Einerseits sind hardwarebasierte Sicherheitstechnologien in Entwicklung (z. B. im Bereich Trusted Computing), die das

Kurz&bündig

Unsere persönlichen Daten werden an verschiedenen Orten gesammelt und für diverse Zwecke verwendet. Online-Shops, Behörden, Telekommunikationsanbieter, Spitäler und viele andere Firmen und Institutionen geraten in den Besitz von persönlichen Daten, wenn wir mit ihnen interagieren. Auch bei der Verwendung des Internets, etwa bei der Benutzung von Suchmaschinen, werden potenziell Daten über uns preisgegeben. Da es schwierig ist, das Sammeln dieser Daten zu verhindern, sollte zumindest versucht werden, ihre Verwendung zu kontrollieren. Dies ist das Thema der «Verteilten Nutzungskontrolle». Die Autoren des Artikels geben einen Überblick über das Gebiet und diskutieren insbesondere, wie Anforderungen an die Verwendung von Daten in verschiedenen Umfeldern durchgesetzt werden können.

Potenzial haben, solche Mechanismen in Zukunft sicherer zu machen. Andererseits gibt es auch viele Anwendungsszenarien im Bereich des Datenschutzes, in denen die Benutzer im Gegensatz zum DRM nicht als bösartig angesehen werden, sondern eher als gutartig, aber nicht vor Fehlern gefeit. Solche Benutzer werden beim Einsatz von Kontrollmechanismen davor bewahrt, Daten unbeabsichtigt inkorrekt zu verwenden. Ausserdem sind bei der Anwendung von DRM-Mechanismen diejenigen Benutzer, die technisch nicht sehr versiert sind oder nicht viel kriminelle Energie aufbringen, auch nicht in der Lage, Daten absichtlich zu missbrauchen.

- Das zweite Problem im Zusammenhang mit Kontrollmechanismen ist, dass die Datenkonsumenten oft nicht wollen, dass eine andere Institution oder Firma über solche Mechanismen direkten Einfluss auf ihre Informationsverarbeitung ausüben kann. Das Risiko besteht, dass solche Mechanismen unbeabsichtigt auch andere Vorgänge beeinflussen und somit Fehler provozieren können. Zudem kann es sein, dass Kontrollmechanismen legitime Aktionen verhindern, weil sie sie für unrechtmässig erachten. Beispiele dafür sind Notfallsituationen, in denen Aktionen notwendig sind, die sonst nicht erlaubt wären. Solche Szenarien werden etwa von Povey (2000) beschrieben. In solchen Fällen ist die Verwendung von Beobachtungsmechanismen oft angemessener.

Wo der Einsatz von Kontrollmechanismen Probleme schafft, ist die Verwendung von Beobachtungsmechanismen oft angemessener.

Beobachtungsmechanismen

Solche Mechanismen bestehen aus zwei Teilen: Bei den Datenkonsumenten werden *Signalisierungsmechanismen* installiert, die den Datenanbieter davon in Kenntnis setzen, was mit bestimmten Daten passiert. Dieser benötigt einen *Monitor*, der die gesendeten Signale beobachtet und analysiert, wann Obligationen verletzt sind. Wenn dies der Fall ist, löst der Monitor Aktionen aus, etwa eine Bestrafung des Datenkonsumenten (zum Beispiel die Verminderung zukünftiger Leistungen oder rechtliche Schritte) oder, falls möglich, Aktionen, die die Verletzung rückgängig machen können.

Beobachtungsmechanismen sind, wie die Kontrollmechanismen, auch abhängig davon, dass vertrauenswürdige Plattformen bei den Datenkonsumenten verfügbar sind. Sonst kann sich der Datenanbieter nicht auf die Signale verlassen, die von den Signalisierungsmechanismen gesendet werden. Deshalb sind auch Beobachtungsmechanismen gegen technisch versierte und bösartige Benutzer nur bedingt wirksam, können in Umgebungen, in welchen ein gewisses Mass an Vertrauen vorhanden ist, aber einen grossen Beitrag zur vereinbarungsgemässen Verwendung von Daten leisten. Sie sind speziell in Firmenumgebungen und Behörden eine gute Lösung, weil sie die Informationsverarbeitung der Datenkonsumenten eher nicht behindern, aber trotzdem fehlerhafte Verwendungen von Daten zumindest detektieren können. Dies vermeidet zum Beispiel, dass grosse Datenbestände aus Versehen an Orten anfallen, an denen sie nie sein dürften.

Beobachtungsmechanismen können Auditierungsprozesse in geeigneter Form komplementieren. Die oben genannten Signalisierer können nämlich vergleichsweise einfach dahingehend angepasst werden, dass sie vertrauenswürdige Logs von Ereignissen erstellen. Ob die Verletzung von Obligationen schon zur Laufzeit detektiert wird oder erst über Nacht oder nur einmal im Quartal, ist offenbar eine Frage der Anwendungsdomäne und entsprechend der Dringlichkeit und des Datenaufkommens.

Ergänzung beider Mechanismen

Angesichts der nicht zu erwartenden hundertprozentigen Garantien von Kontroll- und Beobachtungsmechanismen können schliesslich beide Formen von Mechanismen um weiterführende Technologien wie etwa das Watermarking ergänzt werden.

Literatur

- Jaehong Park/Ravi Sandhu, The $UCON_{ABC}$ model. ACM Transactions on Information and System Security 7(1),128–174, 2004.
- Manuel Hilty/Alexander Pretschner/David Basin/C. Schaefer/T. Walter, A Policy Language for Usage Control. Proc. ESORICS, 531–546, 2007.
- Dean Povey, Optimistic security: a new access control paradigm. In Proceedings of New Security Paradigms Workshop, 40–45. ACM Press, 2000.
- Alexander Pretschner/ Susan Gauch, Ontology-Based Personalized Search. Proc. ICTAI, 391–398, 1999.
- Alexander Pretschner/Manuel Hilty/David Basin, Distributed Usage Control. Communications of the ACM 49(9), 39–44. ACM Press, September 2006.

Ausblick

Sicherzustellen, dass Daten nur vereinbarungsgemäss verwendet werden, ist angesichts der zunehmenden Digitalisierung unseres Alltags ein gesellschaftlich und ökonomisch relevantes sowie wissenschaftlich und ingenieurmässig höchst anspruchsvolles Problem. Die Heterogenität sowohl der zu kontrollierenden Daten (im Fall der Verwendung mobiler Telefone etwa Sensor-, Verbindungs-, Stamm-, Nutz- und Profildaten) als auch der technischen Infrastrukturen (Sensoren, mobile Telefone, geschäftliche Informationssysteme auf Netzbetreiber- und Dienstanbieterseite) stellen eine Vielfalt spannender Herausforderungen dar. An der ETH Zürich haben wir bisher insbesondere im Bereich der Policyspezifikation und -analyse, der Architekturen auf Datenkonsumenten- und Datenherausgeberseite, der Monitore, der Aushandlung von Policys und ersten Ansätzen im Bereich von Kontrollmechanismen auf Telefonen und Informationssystemen gearbeitet. Aktuelle Arbeiten liegen insbesondere im Bereich der Rechtedelegation und -propagation, und zukünftige Arbeiten umfassen Lösungen zu den schwierigen Problemen in Bezug auf das Design, die Implementierung und die Analyse vertrauenswürdiger Kontroll- und Beobachtungsmechanismen für weitere mobile Geräte und im Kontext serviceorientierter Architekturen u.a. auf der Basis virtualisierter Prozessoren und von Trusted-Computing-Technologien.

Die verteilte Nutzungskontrolle könnte der Enabler für viele aufregende bereits existierende und zukünftige digitale Technologien sein.

Wir sehen die verteilte Nutzungskontrolle als Enabler für viele aufregende bereits existierende – aber wegen mangelnden Datenschutzes noch nicht verbreitete – und zukünftige digitale Technologien.

Danksagung: Ein Teil der Konzepte und Technologien, welche wir in diesem Artikel vorstellen, wurde in Zusammenarbeit mit Dr. Thomas Walter und Christian Schäfer von DoCoMo Euro-Labs in München entwickelt.