New Models of System Behavior for Policy-based Access Control and Privacy Protection

Abstract

In the healthcare sector and other domains there is a trend towards patient-centric or user-centric data protection. This means that policies on who can use what in which way and for which purpose are not primarily constituted by general laws or the data processing institutions, but by the individuals concerned. Individuals are to be provided with means to individually and personally specify policies for data regarding themselves. The latter is politically wanted, but is also connected to technical issues.

A policy is commonly understood as a "[…] *constraint on a system specification foreseen at design time, but whose detail is determined subsequent to the original design, and capable of being modified from time to time* […]" (cf. RM-ODP). However, users are usually not capable to cope with the details of a system specification and to set the adjusting screws of a system in terms of a respective policy specification. Individuals should rather have the options to specify system behavior and its limitations regarding the processing of their data as a policy without knowing and considering system implementation details.

This presentation addresses a new approach to describe system behavior and proposes related models, e.g. for the concepts of act, communication, and protocol. On this basis, policies can be specified as a constraint on system behavior rather than constraints on a system specification. This shall allow for a combination of behavior-based policies with access and processing control standards, e.g. Digital Rights Management (DRM) according to ISO 21000-5 (MPEG-21) and e.g. allow for a better protection of an electronic health record in a cross-institution integrated care process according to a patient's provisions.

Abstract

Im Gesundheitswesen und anderen Bereichen gibt es einen Trend zu patienten- bzw. nutzerzentrierten Datenschutz. Das bedeutet, dass die Policies, wer was in welcher Weise oder zu welchem Zweck verwenden darf, nicht primär durch allgemeine Gesetze oder die datenverarbeitenden Institutionen bestimmt werden, sondern durch die Bertoffenen selbst. Individuen soll die Möglichkeit eingeräumt werden, Policies zur Verarbeitung von Daten, die sie selbst betreffenden, individuell und selbst zu spezifizieren. Letzteres ist politisch wünschenswert, aber mit technischen Schwierigkeiten verbunden.

Eine Policy wird in der Regel als eine „[…] *Einschränkung in Bezug auf eine Systemspezifikation verstanden, die bereits zur Entwurfszeit vorhergesehen wird, jedoch in ihren Details erst nach dem ursprünglichen Systementwurf festgelegt wird und von Zeit zu Zeit verändert werden kann* […]" (vgl. RM-ODP). Nutzer sind jedoch in der Regel nicht in der Lage, sich mit den Details einer Systemspezifikation auseinander zu setzen und die technischen Stellschrauben eines Systems im Rahmen einer entsprechenden Policy festzulegen. Vielmehr sollten Individuen in der Lage sein, ein Systemverhalten und seine Grenzen bei der Verarbeitung ihrer Daten im Rahmen einer Policy zu spezifizieren, ohne Implementierungsdetails eines Systems zu kennen oder zu bedenken.

Der Vortrag präsentiert einen neuen Ansatz Systemverhalten zu beschreiben und schlägt damit verbundene Modelle z.B. für die Konzepte Handlung, Kommunikation und Protokoll vor. Auf dieser Basis können Policies als Einschränkung eines Systemverhaltens spezifiziert werden, anstatt als Einschränkung einer Systemspezifikation. Dies soll ermöglichen, verhaltensbasierte Policies mit Zugriffs- und Verarbeitungskontrollverfahren, z.B. mit Digital Rights Management (DRM) gemäß ISO 21000-5 (MPEG-21), zu verbinden, und z.B. eine elektronische Patientenakte in einem institutionsübergreifenden integrierten Behandlungsprozess besser nach Maßgabe des Patienten schützen zu können.