Privacy-Aware Access Control

I

Eugenia I. Papagiannakopoulou
National Technical University of Athens, Greece

Maria N. Koukovini
National Technical University of Athens, Greece

Georgios V. Lioudakis
National Technical University of Athens, Greece

Nikolaos L. Dellas
SingularLogic S.A., Greece

Dimitra I. Kaklamani
National Technical University of Athens, Greece

Iakovos S. Venieris
National Technical University of Athens, Greece

INTRODUCTION

The advent of new technologies, such as Social Media and the Internet of Things, apart from the apparent advantages, has a huge impact on privacy. Thus, privacy protection has become a significant aspect of ICT, and a salient issue for stakeholders. Privacy-Enhancing Technologies (PETs) (Wang, 2009), such as privacy policies and preferences management, identity management, and techniques for anonymity and pseudonymity, have been subject to much research, whereas a recent trend is represented by the "Privacy by Design" philosophy (Cavoukian, 2009). Since any privacy violation certainly includes illicit access to personal data, access control constitutes a fundamental aspect of privacy protection. However, the traditional access control models, such as the Discretionary Access Control (DAC) and the Mandatory Access Control (MAC) (Samarati & de Capitani di Vimercati, 2001), as well as the family of Role-Based Access Control (RBAC) (Ferraiolo et al., 2001) models fail to meet the requirements stemming from the fundamental privacy principles, as laid down by milestone initiatives such as the seminal OECD guidelines (OECD, 1980), or the European legislation (European Parliament and Council, 1995). In that respect, the development of access control models specifically tailored towards privacy protection has been the focus of intense research in the last few years. This trend, usually referred to as privacy-aware access control (cf. e.g., Antonakopoulou et al., 2012), typically concerns the enhancement of RBAC in order to incorporate different criteria in access control decisions, rather than just *which user*, having *which role*, is performing *which action* on *which data object*.

In the following, privacy-aware access control is overviewed. First, background information motivating the need for privacy-aware access control is provided, along with the associated requirements. Next, the most important research approaches are outlined. Before providing views for prospective research and concluding, an abstract model is sketched, reflecting the fundamental requirements.

BACKGROUND

Privacy is recognized as a fundamental human right by the Universal Declaration of Human Rights of the United Nations (1948), as well as the Charter of Fundamental Rights of the European Union (European Parliament, Council & Commission, 2000). It is protected by relevant legislation in all the democratic countries throughout the world (cf., e.g., Greenleaf,

DOI: 10.4018/978-1-4666-5888-2.ch432

in press). A significant milestone in the privacy literature has been the codification of the fundamental privacy principles by the Organization for Economic Co-operation and Development (1980), as this codification lays out the basis for the protection of privacy. The OECD principles are reflected in the European Directive 95/46/EC (European Parliament and Council, 1995), "*on the protection of individuals with regard to the processing of personal data and on the free movement of such data*." The Directive 95/46/EC enforces a high standard of data protection and constitutes the most influential piece of privacy legislation worldwide (cf., e.g., Greenleaf, 2012), that seems to pull a general framework and has been characterized as an "engine of a global regime" (Birnhack, 2008), affecting many countries outside Europe in enacting similar laws. It is further particularized and complemented by subsequent Directives, as well as various Decisions, Recommendations, and Opinions of the Article 29 Data Protection Working Party, among others. Recently, a reform to the existing data protection framework has been proposed (European Commission, 2012); among the most significant features introduced, it will require companies to conduct privacy impact assessments, to implement "Privacy by Design" principles, and to ensure "Privacy by Default" in their applications, while individuals will have greater rights, such as the "Right to be Forgotten" and the "Right to Data Portability."

The legislation and accompanying documents and related policy-oriented best practice guidelines provide, and often codify, the fundamental principles surrounding the provision of privacy-aware services. These typically concern lawfulness of data collection and processing, purpose specification and binding, necessity, adequacy, proportionality and quality of the data processed, minimal use of personal information, application of security measures, special provisions regarding retention and protection of information, enforcement of data subjects rights, coordination with the competent authorities, etc. The elaboration of principles and requirements stemming from the legislation and fair information practices has been the subject of various studies and extensive research (e.g., Solove, 2006; Lioudakis et al., 2010; Gutwirth et al., 2013). Rethought from the point of view of access control, the corresponding principles converge to the following challenges.

Multi-aspect access rights definition: Given the inherent complexity of the notion of privacy and the underlying implications, the associated solutions should incorporate various criteria in access and usage control decisions, rather than just *which user* holding *which role* is performing *which action* on *which object*.

Purpose: The "purpose principle" is essential for privacy awareness, being a core part of data collection and processing lawfulness (European Parliament and Council, 1995); a privacy-aware access control framework should provide for purpose specification and binding.

Privacy-aware information flow: Beyond controlling access and usage, a privacy-aware access control model should provide for the specification of acceptable patterns as far as the flow of data is concerned; this implies, for instance, the prevention of some data to be communicated from a system to another, whereas the latter may be *per se* allowed to receive the same data by a third system.

Unlinkability: Along the same line, a privacy-aware access control model should provide support for preventing linkability. Whereas privacy-aware information flow refers to "direct" passing of data among systems, processes or people, the need for unlinkability reflects a generalization towards mutually exclusive availability or processing of data, either explicitly or implicitly.

Separation and Binding of Duty (SoD/BoD): Similarly, SoD and BoD constraints should be possible to be specified and enforced, since they hold an important position among authorization requirements (Joshi et al., 2003), serving, among others, conflicts avoidance and unlinkability.

Complementary actions: In several cases, access to the data should be accompanied by certain actions that should follow the collection and/or processing of information. These are often referred to in the literature as "privacy obligations" (Casassa Mont, 2004; Hilty et al. 2005) and may concern, for instance, the application of immediate protection measures, the interaction with the data subjects (e.g., in terms of information or request for consent), and the enforcement of data retention provisions.

Context-awareness: It has become apparent that effective security and privacy policies largely depend on contextual parameters (Cuppens & Cuppens-Boulahia, 2008; Kapitsaki et al., 2010). Therefore, a privacy-aware access control framework should incorporate the corresponding aspects, in terms of restrictions over contextual parameters and events, and be enabled to impose different access rights according to the applicable constraints.