Logics for Security and Privacy

Leendert van der Torre

Computer Science and Communication, University of Luxembourg, Luxembourg

Abstract. In this presentation I first review new developments of deontic logic in computer science, then I discuss the use of dynamic epistemic deontic logic to reason about privacy policies, and finally I discuss the use of modal logic for access control. This presentation is based on joint work with Guillaume Aucher, Guido Boella, Jan Broersen, Dov Gabbay and Valerio Genovese.

1 Introduction

In the past two decades, a number of logics and formal frameworks have been proposed to model and analyse interconnected systems from the security point of view. Recently, the increasing need to cope with distributed and complex scenarios forced researchers in formal security to employ non-classical logics to reason about these systems. I believe that logicians have a lot to benefit from specifying and reasoning about real-world scenarios as well as researchers in security can apply recent advances in non-classical logics to improve their formalisms.

2 Deontic logic in computer science [3]

Over the past two decades, research in deontic logic has changed due to the participation of computer science. Broersen and van der Torre [3] discuss many traditional and new questions, centered around ten problems of deontic logic and normative reasoning in computer science. Five of these problems were discussed as philosophical problems in deontic logic by Hansen, Pigozzi and van der Torre [11], and five problems are addressed in particular in computer science.

Problem 1 - In what sense are obligations different from norms? Traditionally, people wondered whether there can be a deontic logic, given that norms do not have truth values. Nowadays, many people identify logic with reasoning, and the question is how *norms* and *obligations* are related. Instead of saying that a set of norms is consistent, two sets of norms are logically equivalent, a norm is implied by a set of norms, we have to define when a normative system is coherent, two normative systems are equivalent, or a norm is redundant in a normative system. Moreover, a new meta theory has to be developed, and relevant meta theoretic properties have to be identified.

Problem 2 - How to reason about contrary to duty norms? A difference between norms and other kinds of constraints is that norms can be *violated*, and the most discussed challenge to normative reasoning is the formalization of the *contrary-to-duty* paradoxes such as the Chisholm and Forrester paradoxes. These paradoxes receive less attention nowadays, also because they are not confined to contrary-to-duty reasoning but also contain other challenges such as according to duty reasoning associated with deontic detachment, and reasoning about time and action. But the challenge to reason about and recovering from violations is alive and kicking.

Problem 3 - How do norms change? Though *norm change* has been discussed since the early eighties, only during the last decade it has become one of the most discussed challenges. For example, researchers in normative multiagent systems identified that it is essential for a normative system application in computer science not only that norms can be violated, but in addition that norms can be changed by the agents in the system. Moreover, belief merging and its relation to judgment aggregation and social choice is emerging only recently.

Problem 4 - What is the role of time in deontic reasoning? Norms and *time* have been intimately related from the start of deontic logic, but it seems that most problems discussed in the area are not restricted to the deontic setting, but problems about temporal reasoning in general. Also in computer science and artificial intelligence, issues like deadlines where addressed in planning before they were addressed in deontic logic. For practical problems, for example in computer science, we now know that temporal references are the most elusive part of norms. However, it seems that little progress is made in understanding the challenges in the role of time in deontic logic.

Problem 5 - How to relate various kinds of permissions? In a sense, the relation between obligation and *permission* is the oldest problem in deontic logic, since Von Wright wrote his seminal paper in 1951 after he observed a similarity between the relation between necessity and possibility on the one hand, and obligation and permission on the other hand. The general opinion is that there are several kinds of permission, and it is not so easy to disentangle them. However, since permission plays a much less central role than obligation, it has received also less attention. By itself the notion of permission is also simpler than the notion of obligation, because permissions cannot be violated. The main challenge is the interaction between permission and obligation. The main interest nowadays seems to be in related legal concepts like rights and authorizations.

Problem 6 - What is the role of action in deontic reasoning? Von Wright considered his deontic *action* logic as his main contribution to the field of normative reasoning, and the first work of significance in the area was the use of dynamic deontic logic to model obligations on actions. Moreover, this is the rst problem where the agents subject to the norms come to the forefront, raising the questions how agents make decisions based on norms, or how norms are interpreted. Nevertheless, it seems that only few challenges have emerged.

Problem 7 - What is the role of constitutive norms? Constitutive norms have been used to dene meaning postulates and intermediate concepts, to define the creation of social reality using counts-as conditionals, to dene legal and institutional powers of agents, to dene the way normative systems can change, to define the interpretation of norms, and so on. However, their logical analysis has not achieved much attention. It may be expected, however, that more attention will be given to them in the future. They play a central role in many applications, for example in legal texts, there are often (much) more constitutive norms than regulative norms.

Problem 8 - How do norms influence, solve, or control games? One of our favorite challenges is to understand the relation between norms and *games*. On the one hand, it is now common to see norms as a mechanism to influence, solve, or control the interaction among agents, in particular in the area of multiagent systems. Thus, norms are useful tools in a wider context. Moreover, many problems of normative reasoning, such as norm creation, norm acceptance and norm compliance can be viewed as games, and existing game theoretic theories apply in the normative context. On the other hand, games may be seen as the foundation of deontic logic itself, defining norms as descriptions of violation or norm creation games.

Problem 9 - How do we check norm compliance? If you want to make money with deontic logic or normative reasoning, there is only one candidate: the challenge of norm *compliance*, i.e. the development of tools for automated checking of compliance to formalized sets of rules, laws and policies.

Problem 10 - How do norms interact with other modalities? How to represent and reason about boid agents and knowledge-based obligations? Traditionally norms and obligations have been studied by themselves, but nowadays the focus is on the interaction between them and *other modalities*. Some obligations hold only if you know something, and there are obligations and permissions about what you know or belief. For example, privacy policies are often expressed in what knowledge may be disclosed to who. In decision making in normative settings, there may be a trade off between fulfilling your obligations or your desires, and it may depend on your personality how you resolve such conflicts. Some interactions, such as between obligations and intentions, have hardly been studied thus far.

Finally, Broersen and van der Torre note that deontic logic has inherited from its philosophical origins the emphasis on conceptual and semantic issues, and only a few questions have actually addressed *computational* issues. This in contrast to, for example, decision theory, game theory and social choice, where new interdisciplinary disciplines of computational decision theory, computational game theory, and computational social choice have emerged over the past years. For further information on deontic logic in computer science, see:

http://www.deonticlogic.org

3 Dynamic epistemic deontic logic for privacy compliance [1]

In general, privacy policies can be defined either in terms of permitted and forbidden *knowledge*, or in terms of permitted and forbidden *actions*. For example, it may be forbidden to know the medical data of a person, or it may be forbidden to disclose these data. Both of these approaches have their advantages and disadvantages. Implementing a privacy policy based on permitted and forbidden *actions* is relatively easy, since we can add a filter on the system checking the outgoing messages. Such a filter is an example of a security monitor. If the system attempts to send a forbidden message, then the security monitor blocks the sending of that message. However, the price to pay for this relatively straightforward implementation is that it is difficult to determine privacy policies using permitted and forbidden actions only, in the sense that it is difficult to decide which actions are permitted or forbidden so that a piece of information is not disclose. For example, it is a well known database problem that you may be able to find out my identity without asking for it explicitly, for example by asking a very detailed question (all the people who are born in Amsterdam on September 11 1986, who drive a blue Mercedes, and who are married to a person from Paris on November 9, 2009), or by combining a number of queries on a medical database [12]. Aucher, Boella and van der Torre [1] are therefore interested in privacy policies expressed in terms of permitted and forbidden knowledge.

Expressing a privacy policy in terms of permitted and forbidden knowledge is relatively easy, since it lists the situations which should not occur. These situations are typically determined by the fact that it may not be permitted to know some sensitive information. In many cases it is more efficient or natural to specify that a given piece of information may not be known, than explicitly forbidding the different ways of communicating it. The policies are more declarative, more concise and therefore easier to understand by the user. They may also cover unforeseen sequences of actions leading to forbidden situation. However, implementing a privacy policy based on permitted and forbidden knowledge is relatively difficult, since the system has to reason about the relation between permitted knowledge and actions. The challenge is that the exchange of messages changes the knowledge, and the security monitor therefore needs to reason about these changes.

To express privacy policies in terms of permitted and forbidden knowledge, we use modal logic, since both knowledge and obligations (and permissions) are traditionally and naturally modeled in branches of modal logic called epistemic and deontic logic respectively. Cuppens introduced in 1993 a modal logic for a logical formalization of secrecy [4], and together with Demolombe he developed a logic for reasoning about confidentiality [5] and a modal logical framework for security policies [6]. The logic models the knowledge of the users of the system, and allows the security monitor to reason about them. It expresses formulas such as 'the user knows the address of someone', and epistemic norms, i.e. norms regulating what is permitted to know. The security monitor is able to foresee the inferences that the users can do by combining their knowledge. For example, if the user knows street name, number, town and state of a person, then he knows his address. Moreover, since privacy policies are specified in terms of knowledge that the recipient of information is permitted/forbidden to have, we can represent violations. This is an advantage over privacy policy languages modeling

norms as strict constraints that cannot be violated, because in some situations it is necessary to cope with violations. These violations can be due for example to occasional and unintentional disclosures, or to the creation of new more restrictive norms.

The main task of a security monitor reasoning about a situation given a privacy policy is to check compliance – regardless of whether these policies are expressed in terms of permitted and forbidden actions or permitted and forbidden knowledge. In our approach, to check compliance one has therefore to be able to derive the permitted, obligatory and forbidden actions in a given context, just like a decision maker needs to know whether his alternative actions do not violate norms and may therefore be subject to sanctions. In this paper, we further distinguish between regulatory compliance and behavioural compliance. Regulatory compliance checks whether the permissions and obligations set up by the security monitor of an organization (e.g., company, web-service ...) are compliant with respect to the privacy policies set up by the law/policy makers. Behavioural compliance checks whether these very obligations and permissions are indeed enforced in the system by the security monitor of the organization.

Despite its strengths, the Cuppens-Demolombe logic cannot express whether the situation is (regulatory or behaviourally) compliant with respect to a privacy policy. The problem is that the logic can define privacy policies in terms of the permitted and forbidden knowledge of the resulting epistemic state of the recipient of information, but it cannot derive the permitted messages nor the obligatory messages by combining and reasoning on this knowledge. Our modal logic addresses these problems and extends the Cuppens-Demolombe logic with dynamic update operators inspired from the ones of dynamic epistemic logic [13]. These dynamic operators model both the dynamics of knowledge and of privacy policies. They can add or remove norms from the policy, and we add constants expressing whether the system is regulatorily and behaviourally compliant with a policy, i.e., there is no violation.

Aucher, Boella and van der Torre [1] discuss the following scenario of privacy policies. They consider a single agent (Sender) communicating information from a knowledge base to another agent (Recipient), with the effect that the Recipient knows the information. The Sender is subject to privacy policies which restrict the messages he is permitted to send to the Recipient. The Sender is therefore a security monitor. They illustrate the distinction between norms of transmission of information and epistemic norms with an example:

Example 1. Consider a Sender s, e.g., a web server, which is subject to a privacy regulation: he should not communicate the address a of a person to the Recipient r. We could write this as a norm of transmission of information, regulating the sending of a message: $\neg P_s(Send\ a)$, which denotes the denial that the Sender sends message a. Instead, in an epistemic norm perspective, this prohibition can be derived from the prohibition for the Sender that the Recipient comes to know the address: $K_r a$. This is expressed by a deontic operator indexed by the Sender and having as content the ideal knowledge K_r of the Recipient: $\neg P_s K_r a$.

This distinction is bridged by modelling sending actions performed by the Sender which update the knowledge of the Recipient.

Example 2. The action of sending the message, $[Send\ a]$, expresses that the Sender sends to the Recipient the address a. The result of this action is that the Recipient

knows a: $K_r a$. Since $K_r a$ is not permitted by the epistemic norm $\neg P_s K_r a$, the Sender during his decision process derives that also the action $[Send\ a]$ is not permitted: $\neg P_s(Send\ a)$. Analogously, all other possible actions leading to the forbidden epistemic state $K_r a$, if any, are prohibited too. For example, if the address is composed by street m, number n and town t such that $(m \wedge n \wedge t) \leftrightarrow a$, then the sequence of messages $[Send\ m][Send\ n][Send\ t]$ leads to the forbidden epistemic state $K_r a$.

4 Modal logic for access control [2]

Boella *et al.* [2] study access control policies based on the says operator by introducing a logical framework called Fibred Security Language (FSL) which is able to deal with features like joint responsibility between sets of principals and to identify them by means of first-order formulas. FSL is based on a multimodal logic methodology. They first discuss the main contributions from the expressiveness point of view, they give semantics for the language (both for classical and intuitionistic fragment), they then prove that in order to express well-known properties like speaks-for or hand-off, defined in terms of says, they do not need second-order logic (unlike previous approaches) but a decidable fragment of first-order logic suffices. They propose a model-driven study of the says axiomatization by constraining the Kripke models in order to respect desirable security properties, they study how existing access control logics can be translated into FSL and they give completeness for the logic.

Genovese *et al.* [10] study the applicability of constructive conditional logics as a general framework to define decision procedures in access control logics. They formalize the assertion A says ϕ, whose intended meaning is that principal A says that ϕ, as a conditional implication. They introduce Cond_{ACL}, which is a conservative extension of the logic ICL recently introduced by Garg and Abadi. They identify the conditional axioms needed to capture the basic properties of the "says" operator and to provide a proper definition of boolean principals. They provide a Kripke model semantics for the logic and they prove that the axiomatization is sound and complete with respect to the semantics. Moreover, they define a sound, complete, cut-free and terminating sequent calculus for Cond_{ACL}, which allows them to prove that the logic is decidable. They argue for the generality of our approach by presenting canonical properties of some further well known access control axioms. The identification of canonical properties provides the possibility to craft access control logics that adopt any combination of axioms for which canonical properties exist.

Genovese and Garg [9] present a new modal access control logic ACL^+ to specify, reason about and enforce access control policies. The logic includes new modalities for permission, control, and ratification to overcome some limits of current access control logics. They present a Hilbert-style proof system for ACL^+ and a sound and complete Kripke semantics for it. They exploit Kripke semantics to define Seq-ACL^+: a sound, complete, cut-free and terminating calculus for ACL^+, proving that ACL^+ is decidable. They point at a Prolog implementation of Seq-ACL^+ and discuss possible extensions of ACL^+ with axioms for subordination between principals.

The same authors [8, 7] introduce also labeled sequent calculi for access control logics.

References

1. Guillaume Aucher, Guido Boella, and Leendert van der Torre. A dynamic logic for privacy compliance. *Artif. Intell. Law*, 19(2-3):187–231, 2011.
2. Guido Boella, Dov M. Gabbay, Valerio Genovese, and Leendert van der Torre. Fibred security language. *Studia Logica*, 92(3):395–436, 2009.
3. Jan Broersen and Leendert van der Torre. Ten problems of deontic logic and normative reasoning in computer science. In *ESSLLI 2010/2011 Lecture Notes in Logic and Computation*, 2012.
4. F. Cuppens. A logical formalization of secrecy. In *IEEE Computer Security Foundations Workshop CSFW'93*, Los Alamitos (CA), 1993. IEEE Computer Society.
5. F. Cuppens and R. Demolombe. A deontic logic for reasoning about confidentiality. In *Deontic Logic, Agency and Normative Systems, Third International Workshop on Deontic Logic in Computer Science (DEON 1996)*, Berlin, 1996. Springer.
6. F. Cuppens and R. Demolombe. A modal logical framework for security policies. In Z.W. Ras and A. Skowron, editors, *Foundations of Intelligent Systems, 10th International Symposium, ISMIS '97*, volume 1325 of *LNCS*, pages 579–589, Berlin, 1997. Springer.
7. D. Garg, V. Genovese, and S. Negri. Countermodels from sequent calculi in multi-modal logics. In *27th Annual ACM/IEEE Symposium on Logics in Computer Science - LICS 2012*, 2012.
8. V. Genovese, D. Garg, and D. Rispoli. Labeled sequent calculi for access control logics: Countermodels, saturation and abduction. In *25th IEEE Computer Security Foundations Symposium - CSF 2012*, 2012.
9. Valerio Genovese and Deepak Garg. New modalities for access control logics: Permission, control and ratification. In Catherine Meadows and M. Carmen Fernández Gago, editors, *STM*, volume 7170 of *Lecture Notes in Computer Science*, pages 56–71. Springer, 2011.
10. Valerio Genovese, Laura Giordano, Valentina Gliozzi, and Gian Luca Pozzato. A conditional constructive logic for access control and its sequent calculus. In Kai Brünnler and George Metcalfe, editors, *TABLEAUX*, volume 6793 of *Lecture Notes in Computer Science*, pages 164–179. Springer, 2011.
11. Jörg Hansen, Gabriella Pigozzi, and Leendert W. N. van der Torre. Ten philosophical problems in deontic logic. In Guido Boella, Leendert W. N. van der Torre, and Harko Verhagen, editors, *Normative Multi-agent Systems*, volume 07122 of *Dagstuhl Seminar Proceedings*. Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany, 2007.
12. L. Sweeney. k-anonymity: a model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):557–570, 2002.
13. H. van Ditmarsch, W. van der Hoek, and B. Kooi. *Dynamic Epistemic Logic*, volume 337 of *Synthese library*. Springer, Berlin, 2007.