Policy-Based Regulation of Internet Communication

Andreas Kasten

Universität Koblenz-Landau,
Universitätsstraße 1, 56070 Koblenz, Germany
andreas.kasten@uni-koblenz.de

Abstract. The Internet is a global communication medium which interconnects several content consumers and content providers of different countries. Since these countries have their own jurisdictions, the Internet can also be considered an interconnection of such. Although every content consumer is generally able to access any content from any content provider, the jurisdiction of its own country may prohibit her from doing so. This paper outlines the research towards a policy language for regulating Internet communication. The language allows for modeling such regulations on a technical level and also covers their legal and organizational background.

1 Problem Statement

The Internet provides different categories of content which can generally be accessed by any content consumer from any country. However, access to specific content may be considered illegal in some countries while still being legal in other countries. For example, the distribution of neo-Nazi material is legal in the USA but illegal in Germany according to §86 of the German Criminal Code [1]. Since the Internet interconnects different countries and jurisdictions, it also provides content for those consumers who are not allowed to access it according to their local law. A web server which is located in the USA and hosts neo-Nazi material can also be accessed by German content consumers although they are not allowed to do so. Although each Internet regulation is ultimately based on a set of laws issued by a country's government, its implementation is generally carried out by private organizations such as Internet access providers. If these organizations interpret the laws themselves, their implementations may differ between each other which leads to inconsistent and possibly contradicting results [2]. In order to reduce such unintended side-effects, the regulation should be described as precisely as possible including all details for its technical implementation. Such a description can be achieved by using a formal policy language. A policy consists of several rules which follow the same purpose.

Existing approaches for regulating the access and the processing of Internet content cover access control, usage control, and policy-based network management. However, all of these approaches focus on a particular application and are

not suited for regulating Internet communication. Access control languages such as XACML [3] regulate the access to content at the content provider's side. The content provider also creates and enforces access control policies which define the parties who are able to access the content. In the Internet, however, the party compiling the regulation's rules is often a country's government while the content provider may be located in a different country. Policy-based network management languages like DEN-ng [4] focus on regulating the communication flow within a closed network environment like that of an organization. It mainly requires low-level regulation systems such as routers or switches and does not allow for regulations on the application layer. This makes it difficult to use such languages for regulating global Internet communication. Usage control languages such as ODRL [5] allow for regulating which actions a content consumer may perform on a digital resource. The enforcement of usage control policies is carried out by the content consumers' systems since these systems are able to detect what actions the consumer wants to perform on the resource. However, usage control policies are rather abstract and cannot directly be interpreted by the enforcing system. Compared to network management policies, usage control policies require more human interaction for interpreting and enforcing them.

Since none of the existing approaches is suited for regulating Internet communication, the research outlined in this paper focuses on developing a policy language specifically designed for this issue. The language allows for describing flow control policies on a technical level and links them to their legal authorization. It is embedded into a workflow which covers the creation and processing of policies for regulating Internet communication.

2 Research Goal

The main research goal is to define and implement a workflow for regulating Internet communication which is transparent to all involved parties. These parties include among others the legislator who issues the laws on which an Internet regulation is based, the party who implements the regulation on a technical level, and the content consumers who are affected by the regulation.

The achievement of this main goal covers several different steps and aspects. In order to minimize any misinterpretation of a particular regulation, the workflow shall be based on a formal policy language. This language shall be able to describe the technical regulation details as well as its superior purpose such as a country's law or the code of conduct of the enforcing party. The workflow must cover the creation, distribution, and technical implementation of a particular policy. Each step in a policy's lifetime must be transparent for all involved parties. According to these steps, the following research questions can be formulated:

What parties are involved in an Internet communication? Parties in this case are considered legal or natural persons including organizations, governments, and individuals. A party is involved in an Internet communication if it directly participates in the communication process between two or more communicating parties.

What are their respective communication systems? A party participates in an Internet communication via its corresponding communication nodes such as web servers, web browsers, or routers. The specific communication nodes used by a party highly depend on the function that the party fulfills in the communication process.

What are possible mechanisms for technically regulating Internet communication? The mechanisms cover both abstract descriptions of a regulation and its technical implementation. A description is considered abstract if it does not rely on a particular implementation system but can be used for several systems instead.

How can a technical regulation be linked to its legal and organizational background? Internet regulations are based on the jurisdictions of the countries in which they are active and/or on the code of conduct of the enforcing organization. An Internet regulation can therefore be linked to its background which covers its superior purpose as well.

How can the reasons for an Internet regulation be presented to the affected Internet users? Since each regulation is based on an legal and/or organizational background, this background should be presented to the affected Internet users. In doing so, the regulation itself becomes more transparent for the users.

In order to evaluate the practicability of the policy language, prototypical systems shall be developed covering the different aspects of its corresponding workflow. Such systems include routers, name servers, and application-level proxy servers which are usually used for enforcing Internet regulations [6].

3 Current Results

An ontology-based policy language for regulating Internet communication has already been developed. The language defines a policy as a collection of rules following the same purpose. Each rule describes the technical details for regulating one particular communication flow. A policy links several rules to their legal authorization and/or their organizational motivation. The language is called InFO (short for Information Flow Ontology) and covers the basic regulation aspects independent from any enforcing system. Domain-specific extensions of InFO provide further details for a policy's implementation. There are currently three different extensions available for routers, name servers, and application-level proxy servers. A prototypical name server implementation is also available which interprets and enforces policies created with InFO's name server extension.

A rudimentary workflow for creating and processing flow control policies has been developed as well. A dedicated rule creator interprets the country's laws by collecting the technical regulation details and transforming them into a corresponding rule. This rule is then transfered to the rule enforcer who collects several rules from different rule creators and compiles them into a policy. The enforcer associates this policy with the rule's legal background and its own code

of conduct. It then implements the policy on the enforcing system. If a content consumer tries to access blocked Internet content, she receives a corresponding message and can obtain further information about the regulation's legal and organizational background.

The specification of the policy language and its domain-specific extensions is available at `http://icp.it-risk.iwvi.uni-koblenz.de`.

4 Open Issues

In order to allow for a better validation and verification of Internet regulations, the workflow outlined above has to be further refined. For example, digitally signing the rules and their corresponding policies allows for identifying the parties who are responsible for creating a policy and its rules. This provides for more transparency in the process of Internet regulation.

In order to create rules and policies, corresponding software tools must be developed. Since the process of creating such rules and policies involves several different parties, the software tools must also provide for such a collaborative creation process.

Content consumers, who are affected by an Internet regulation, must be able to understand the reasons for this regulation. This requires that the regulation's policy is presented to the consumer in a format which is easy to understand. A rather technical policy description must therefore be transformed into a more human-readable representation.

References

1. Bundesrepublik Deutschland: §86 StGB: Verbreiten von Propagandamitteln verfassungswidriger Organisationen (1975) `http://www.gesetze-im-internet.de/stgb/__86.html` (last accessed: 27/08/12).
2. Dornseif, M.: Government mandated blocking of foreign web content. In von Knop, J., Haverkamp, W., Jessen, E., eds.: Security, E-Learning, E-Services: Proceedings of the 17. DFN-Arbeitstagung über Kommunikationsnetze. Lecture Notes in Informatics, Düsseldorf (2004) 617–648
3. Moses, T.: eXtensible Access Control Markup Language (XACML) version 2.0. Oasis standard, OASIS (2005) `http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf` (last accessed: 27/08/12).
4. Strassner, J.: Policy-Based Network Management: Solutions for the Next Generation. Morgan Kaufmann (2004)
5. Iannella, R., Guth, S., Pähler, D., Kasten, A.: ODRL version 2.0 core model. Specification, W3C ODRL Community Group (2012) `http://www.w3.org/community/odrl/two/model/` (last accessed: 27/08/12).
6. Murdoch, S.J., Anderson, R.: Tools and technology of Internet filtering. In Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., eds.: Access Denied: The Practice and Policy of Global Internet Filtering. The MIT Press (2008) 57–72