

Emily Kigel

Using Social Semantic Web Data for Privacy Policies

Bibliographic information published by the German National Library:

The German National Library lists this publication in the National Bibliography; detailed bibliographic data are available on the Internet at <http://dnb.dnb.de> .

This book is copyright material and must not be copied, reproduced, transferred, distributed, leased, licensed or publicly performed or used in any way except as specifically permitted in writing by the publishers, as allowed under the terms and conditions under which it was purchased or as strictly permitted by applicable copyright law. Any unauthorized distribution or use of this text may be a direct infringement of the author s and publisher s rights and those responsible may be liable in law accordingly.

Copyright © 2009 Diplomica Verlag GmbH
ISBN: 9783836644419

Emily Kigel

Using Social Semantic Web Data for Privacy Policies

Emily Kigel

Using Social Semantic Web Data for Privacy Policies

Emily Kigel

Using Social Semantic Web Data for Privacy Policies

ISBN: 978-3-8366-4441-9

Herstellung: Diplomica® Verlag GmbH, Hamburg, 2010

Zugl. Leibniz Universität Hannover, Hannover, Deutschland, Bachelorarbeit, 2009

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden und der Verlag, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

© Diplomica Verlag GmbH

<http://www.diplomica.de>, Hamburg 2010

Abstract

Social Web applications are steadily gaining popularity. At the same time, the open nature of such services leads to the exposure of an immense amount of personal data. Due to insufficient access control on nowadays Social Web applications problems in terms of privacy arise. This thesis focuses on the need for more flexible and fine-grained privacy restrictions. It analyses privacy problems of current Social Web applications and compares the privacy preferences such applications offer. Based on this analysis, this thesis extends the well-known principle of policy-based access control, which is a flexible and dynamic way to define who can get access to what content based on user preferences. The presented extension accommodates policies to the requirements of the Social Web. In particular, it describes how to exploit Social Semantic Web data for privacy reasoning. This includes the retrieval of Social and Semantic Web data from various information sources on the Web. It further includes its usage for the definition of privacy policies and its consideration during the policy evaluation. Consequently, using Social Semantic Web data for policy reasoning allows users to exactly define which social relationships and properties a requester has to have in order to access a particular resource. These conditions can cross the boundaries of a single Social Web application. Hence, a user can for example state that a friend on one application can access pictures stored on another application; thus bridging the walled garden of nowadays Social Web applications.

Contents

1	Introduction	1
2	Motivating Scenario and Problem Statement	4
2.1	Motivating Scenario	4
2.2	Problem Statement	5
3	Background	8
3.1	The Social Web	8
3.1.1	Social Networking Sites	8
3.2	The Semantic Web	9
3.2.1	The Resource Description Framework (RDF)	10
3.2.2	The SPARQL Protocol And Query Language	10
3.2.3	SPARQL Endpoints	11
3.2.4	The Social Semantic Web	11
3.3	Privacy Policies	12
3.3.1	Policy Languages	13
3.3.2	Policy Frameworks	13
3.3.3	The Protune Framework	14
4	The Social Web from a Privacy Perspective	16
4.1	Data Disclosure - Why Better Control is Needed	16
4.1.1	Privacy Issues	16
4.1.2	Information Overload	18
4.2	Privacy Protection on the Social Web - a State of Art	19
4.2.1	Twitter and its Privacy Options	19
4.2.2	Facebook and its Privacy Options	20
4.2.3	Flickr and its Privacy Options	27
4.3	Comparing Privacy Preferences on Social Platforms	30
4.3.1	Levels of Trust for Data Disclosure	30
4.3.2	Network Features and their Protection	33
4.4	Summary	35