

Semantic Web Policies for Security, Trust Management and Privacy in Social Networks

Daniel Olmedilla, Telefónica R&D

Invited Talk at the Workshop on

Privacy and Protection in Web-based Social Networks, June 8, 2009, Barcelona



Index

- 01 **Introduction**
- 02 **Semantic Web Policies**
- 03 **Protune Policy Framework**
- 04 **- Natural Language Policy Specification**
- 05 **- Natural Language Policy Explanations**
- 06 **Conclusions**
- 07 **References**

01 Introduction

Why do we care?

- A Texas family has sued Australia's Virgin Mobile phone company, claiming it caused their teenage daughter grief and humiliation by plastering her photo on billboards and website advertisements without consent. [...]
- The picture of 16-year-old Chang flashing a peace sign was taken in April by Alison's youth counsellor, who posted it that day on his Flickr page. [...]
- In the ad, Virgin Mobile printed one of its campaign slogans, "Dump your pen friend", over Alison's picture.
- The ad also says "Free text virgin to virgin" at the bottom.
- The experience damaged Alison's reputation and exposed her to ridicule from her peers and scrutiny from people who can now Google her, the family said in the lawsuit.

01 Introduction

Current Privacy Control in Social Platforms



Who can download your stuff	Anyone (<i>but no-one can download the original files, because you have a free account</i>)	edit
Who can share your photos or video?	Any Flickr member	edit
Who can print your photos	Only you	edit
Who can blog your stuff	Any Flickr member	edit
Hide your EXIF data [?]	No	edit
Hide your stuff from public searches [?]	No	edit
Hide your profile from public searches	Yes	edit
Who can see what on your profile	Your profile page will be hidden from public searches (unless your email address is known, or the person who's searching for you is a contact)	edit

01 Introduction

Current Privacy Control in Social Platforms

ions of your Profile. Visit the [Applications](#) page in order to change settings for
racy p

ile: S

Wall Posts

Who can see this?

Everyone on Facebook

Friends

- Friends of Friends
My friends and their friends can see this.
- Only Friends
Only friends can see this.
- Some Friends**
Choose specific friends who can see this.
- Only me
Only you can see this.

photos

ideos

WORK INFO

Only Friends [?]

Only Friends [?]

Only Friends [?]

Only Friends [?]

Only Friends [?]

Only Friends [?]

Only Friends [?]

Only Friends [?]

Only Friends [?]

Friends may post to my Wall [?]

Only Friends [?]

Everyone [?]

Friends of Friends [?]

Some Friends [?]

Only me [?]

No one [?]

Customise...

Save Changes

Cancel



01 Introduction

Current Privacy Control in Social Platforms

The image shows a screenshot of the Myspace privacy settings interface. The page is titled 'General Privacy:' and contains several sections of settings. A red rectangular box highlights the 'Profile on Mobile' section, which includes three radio button options: 'Anyone can view my profile on mobile' (selected), 'Anyone 18 and over can view my profile on mobile' (highlighted by the red box), and 'Only my friends can view my profile on mobile'. Below this, the 'Comments' section is visible, with 'Anyone can view my comments page' selected. Other sections include 'My Visitors', 'Online Now', 'Birthday', 'Status and Mood', and 'Block Users By Age'. A 'Save All Changes' button is located at the bottom of the page.

General Privacy:

- My Visitors:** Turn My Visitors on
- Online Now:** Show people when I am online
- Birthday:** Show my birthday to my friends
- Profile on Mobile:** Choose who can view your profile on mobile (e.g., m.myspace.com, iPhone, Sidekick, Helio, Blackberry and other apps).
 - Anyone can view my profile on mobile
 - Anyone 18 and over can view my profile on mobile
 - Only my friends can view my profile on mobile
- Comments:** Choose who can view your comments page.
 - Anyone can view my comments page
 - Anyone 18 and over can view my comments page
 - Only my friends can view my comments page
- Status and Mood:** Choose who can view your Status and Mood page.
 - Anyone can view my Status & Mood page
 - Anyone 18 and over can view my Status & Mood page
 - Only my friends can view my Status & Mood page
- Block Users By Age:** Allow users under 18 to contact me
- Block Users:** Block individual users by clicking "Block User" on their profile. [View list]



01 Introduction

Limitations

- Unflexible set of protection mechanisms
 - Fix set of (very simple and non-extendable) choices
- Lack of fine-grained protection
 - Focused on “whole collection” or “individual elements”
 - Difficult to independently protect sets of elements (overlapping groups)
- Static
 - Same policy for different groups → difficult to change
- No external evidences (proofs, external sources of information, etc.)

01 Introduction

Motivation

However, it is not possible to specify more flexible and powerful statements such as

- Only family members can see pictures geotagged at my house
- ESWC09 participants can see pictures tagged with 'eswc09' for two months starting now
 - Note that “ESWC09 participants” is not a group owned by me
- Members of my family are always also friends
- Only employees of my company can see my tutorial slides and only if their status is not “draft”



Typically, allowing users to specify these type of statements would make it too complex for common (non-computer expert) users

02 Semantic Web Policies

Problem Statement

Institutions, companies and people need to control the way they

- Make business, take decisions, offer their assets, etc.

Computers help us on our daily work performing tasks

- that we cannot perform (or we do it worse)
 - hard to control manually, time-consuming, expensive, error-prone
- automatically on our behalf

But generally, we need to control how decisions and actions are taken

02 Semantic Web Policies

What is a Policy?

Wikipedia:

- **Deliberate plan of action to guide decisions and achieve rational outcome(s)**
 - Not necessarily related to IT

In an IT setting:

- **Set of considerations designed to guide decisions of courses of actions**

Broad definition:

- **Set of statements defining the behaviour of an entity in a given situation**

02 Semantic Web Policies

Policies are everywhere (I)

Rules of ethics for robots

1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.
2. A robot must obey orders given to it by human beings, except where such orders would conflict with the First Law.
3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

[*Isaac Asimov. Runaround. 1942*]

02 Semantic Web Policies

Policies are everywhere (II)

The "3 Times" Policy

Always wait three times before doing something your advisor asks you to do.

AVOID GETTING BURIED IN POINTLESS AND UNNECESSARY TASKS TO THE DETRIMENT OF PRODUCTIVE ~~WEB SURFING~~ WORK



1st request

Translation: "I'm trying to come up with something for you to do."



2nd request

Translation: "The person who actually needs this keeps sending me e-mails."



3rd request

Translation: "I actually need it."

JORGE CHAM © 2007

WWW.PHDCOMICS.COM

02 Semantic Web Policies

Policies are everywhere (& III)

- B2B contracts
 - e.g. quantity flexible contracts, late delivery penalties, etc.
- Negotiation
 - e.g. rules associated with auction mechanisms
- Security
 - e.g. access control policies
- Privacy
 - Information Collection Policies (aka “ P3P Privacy Policies”)
 - Obfuscation Policies
- Workflow management
 - What to do under different sets of conditions
- Context aware computing
 - What service to invoke to access a particular contextual attribute
 - Context-sensitive preferences

[by *Norman Sadeh*, Semantic Web Policy Workshop panel, ISWC 2005]

02 Semantic Web Policies

The Goal

Build applications/agents where

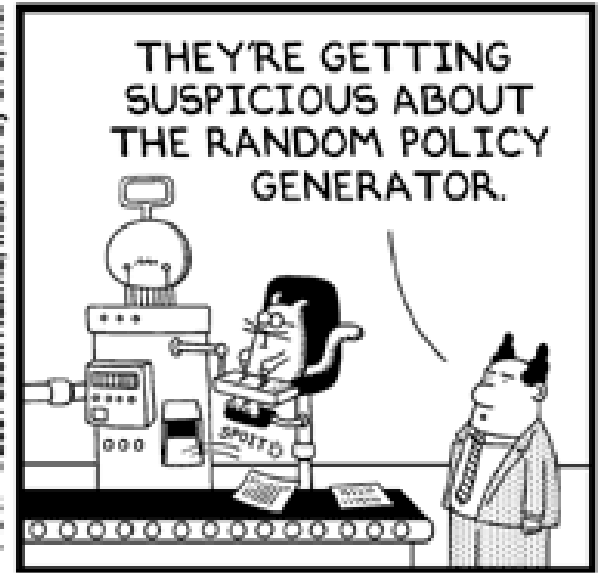
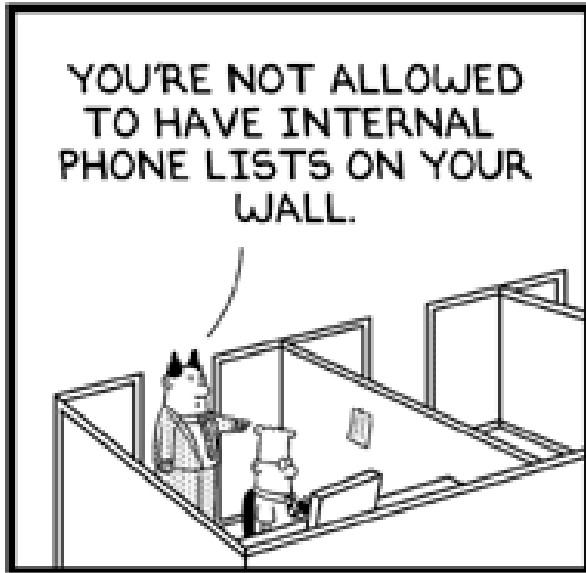
- Behaviour is flexible
 - Can be changed/updated dynamically
 - without re-coding, re-compiling, re-installing, etc...
 - In a costless manner
- Can be managed by administrators/users without needing to be computer experts
- Can be understood by normal users



**User Awareness
& Control**

02 Semantic Web Policies

User Awareness & Control



© Scott Adams, Inc./Dist. by UFS, Inc.

- Encourage people to personalize their policies
 - Make it easy for users to write their own rules
- Explain policies and system decisions
 - Make rules & reasoning intelligible to the common user

Natural Language Specification

Policy Explanations

03 Protune Policy Framework

Overview

- provides a **logic-based, declarative** policy language
- features include
 - **trust negotiation**
 - **external actions**
 - access to relational databases,
 - RDF stores,
 - file system requests,
 - time and location-aware packages
 - natural language policy **explanations**
 - *“You cannot access because ...”* (in contrast to just *“Access denied.”*)



03 Protune Policy Framework

Other policy frameworks

■ Ponder

- OO language, well established, focus on network management

■ XACML

- Standard by OASIS, it being taken up by companies

■ KAOS

- Based on DL reasoning

■ REI

- Combination of DL representation and LP semantics

■ PeerTrust

- Based on guarded distributed logic programs

And many others

04 Natural Language Policy Specification

How does a policy look like?

Policies (typically) are

- machine-understandable
- declarative
- formal syntax
- unintuitive and hard to grasp for users

An example:

$\text{allow}(\text{access}(\text{Requester}, \text{Resource})) \leftarrow$
 $\text{friend}(\text{Requester}), \text{family_picture}(\text{Resource}).$

What could be translated to

If the requester is a friend and the resource is a family-picture then the requester can access the resource.

04 Natural Language Policy Specification

Controlled Natural Language

Is a subset of natural language (NL)

- They are formal languages
 - CNLs have a formal, machine-understandable semantics that is unambiguous

“Bob sees the girl with the telescope.”

“Bob and John are friends. He is my friend, too.”

are always given the same semantics.

- But They do not look like formal languages
 - They are more user-friendly

We use ACE (Attempto Controlled English)

04 Natural Language Policy Specification

ProACE: a Controlled Natural Policy Language

- A subset of the controlled natural language ACE
- Each ProACE can be translated into a Protune policy
 - *“If the requester is older than 18 and she is Bob’s friend then she can access everything which is in ‘adult-content-folder’.”*
 - *“If the requester is a friend and the resource is a family-picture then the requester can access the resource.”*
 - *“If the company of a credit-card is “VISA” then the credit-card is accepted.”*

04 Natural Language Policy Specification

ProACE Mapping Examples

John waits.	<code>wait('John').</code>
John greets Sue.	<code>greet('John', 'Sue').</code>
John is old.	<code>old('John').</code>
Every resource is private.	<code>private(X).</code>
John is the murderer.	<code>murderer('John').</code>
The murderer is John.	<code>murderer('John').</code>
John is in London with Sue.	<code>inWith('John', 'London', 'Sue').</code>
John is with Sue in London.	<code>inWith('John', 'London', 'Sue').</code>
John is as old as Sue.	<code>asOldAs('John', 'Sue').</code>
John is fond-of Sue.	<code>fondOf('John', 'Sue').</code>
John is the son of Sue.	<code>'Sue'.son:'John'.</code>
John is the son of Sue with Bill.	<code>sonOfWith('John', 'Sue', 'Bill').</code>
John's mother waits.	<code>'John'.mother:X, wait(X).</code>
If the user is the owner of the file then the user can read the metadata of the file.	<code>allow(read(User, X)) :- File.metadata:X, File.owner:User.</code>

04 Natural Language Policy Specification

ProACE Editor (I)

Accepted partial sentence

Field for direct text input

Lists for one-by-one word insertion

ACE Text Editor

A

< Delete

text

function word	noun	adjective
more	account	active
most	address	angrier
	age	angriest
	aircraft	angry
	airline	authenticated
	ancestor	automatic
	animal	average
	ape	bad
	apple	best
	approach	better
	article	big
	asset	bigger
	ball	biggest
	bank	blue
	bed	bluer
	beer	bluest

OK Cancel

04 Natural Language Policy Specification

ProACE Editor (& II)

ProACE Editor

Every requester **1**

< Delete

text **2**

can access every|

properName

Alice
Bob
John
Mary **3**

presentIntransitivePredicate

certifies
sees

presentTransitivePredicate

accesses
certifies
contains
retrieves
sees
sends

presentDitransitivePredicate

certifies
retrieves
sends

variable

X
Y
Z

function word

's
a
an
can
is
of
some



OK Cancel

04 Natural Language Policy Specification

LearnWeb 2.0: Natural Language Policies in a social platform

LearnWeb 2.0

Title of the policy	Policy text
Family photos and videos rule	Everyone who is a relative can see everything which is a photo. Everyone who is a relative can see everything which is a video.
Work documents	If a file is related to "job" then everyone who is a colleague can access the file.
Student rule	If a document is protected then if the requester sends a student-id and the student-id's issuer is "uni hannover" then the requester can access the document.
Employee rule	Every requester can access everything which is an employee-credential.

		Edit Delete
Employee rule	Every requester can access everything which is an employee-credential.	  Edit Delete

03 Natural Language Policy Explanations

Motivation

Current problems include that the user has

- Lack of awareness
 - Users ignore the policies applied by the systems they use
- Lack of control
 - Users don't know how to personalize their policies
- Lack of technical competence

Therefore, it is needed to explain policies and policy decisions

- Crucial for the success of a service
- Especially failures: Why not?
 - Never say (only) “no”!

03 Natural Language Policy Explanations

Widespread Security and Privacy

A recent experiment:

- Several computers connected to the network
 - Different platforms and configurations
- With default policies: intrusion in **<5 min**
 - Bias towards functionality
- With personalized policies: safe for **2 weeks**
 - Till the end of the experiment

[Avantgarde. <http://www.avantgarde.com/xxxxttln.pdf>]

03 Natural Language Policy Explanations

Solution: User Awareness & Control

Explain why it is not allowed to download paper_0123.pdf - Mozilla

REVERSE
WG I2 - policy language

PROTUNE Why-Not Explanations

it is not allowed to download paper_0123.pdf because:

- Rule [3] cannot be applied:
 - paper_0123.pdf is not public [[details](#)]
- Rule [4] cannot be applied:
 - I find no User such that the User is authenticated [[details](#)]
- Rule [5] cannot be applied:
 - I find no User such that the User is authenticated [[details](#)]
 - I find no User such that the User paid for paper_0123.pdf [[details](#)]

[Policy file](#)

Done

03 Natural Language Policy Explanations

Solution: User Awareness & Control

Explain why the User is not authenticated - Mozilla

REVERSE
WG I2 - policy language

PROTUNE Why-Not Explanations

the User is not authenticated because:

- Rule [7] cannot be applied:
 - I find no Credential such that the Credential is an id [\[details\]](#)
- Rule [8] cannot be applied:
 - I find no Form such that the Form is a declaration [\[details\]](#)
- Rule [9] cannot be applied:
 - the procedure on <http://lol.com/register.php> has not (yet) been successfully completed [\[details\]](#)

[Policy file](#)

03 Natural Language Policy Explanations

Solution: User Awareness & Control

Explain why the Card is not a valid credential - Mozilla

REVERSE
WG I2 - policy language

PROTUNE Why-Not Explanations

the Card is not a valid credential because:

- Rule [19] cannot be applied:
 - c012 is a credential whose *issuer* is Open University
 - but**
 - I find no Key such that the Key is the public key of Open University

[\[details\]](#)

[Policy file](#)

03 Natural Language Policy Explanations

Solution: User Awareness & Control

I CAN'T PROVE THAT

it is allowed to download paper14.pdf

BECAUSE

Rule [r3] is not applicable:

THERE IS NO User SUCH THAT

User is authenticated

[details]

AND

Rule [r4] is not applicable:

THERE IS NO User SUCH THAT

User is authenticated

[details]

MOREOVER

THERE IS NO User SUCH THAT

User has paid for paper14.pdf

[details]

FILTERED POLICY

[r3]: allow(download(Resource)) ←
authenticated(User),
blurred(hasSubscription(User)).

[r4]: allow(download(Resource)) ←
authenticated(User),
paid(User,Resource).

METAPOLICY

allow(download(Resource)).explanation:
“It is allowed to download “ &
Resource.

public(Resource).explanation:
Resource & “ is public”.

authenticated(User).explanation:
User & “ is authenticated”.

hasSubscription(User).explanation:
User & “ has subscription”.

paid(User,Resource).explanation:
User & “ has paid for “ &
Resource.

[Bonatti, Olmedilla, Peer. Advance policy explanations on the web.

ECAI 2006, pages 200-204, Riva del Garda, Italy, Aug-Sep 2006. IOS Press.]

03 Natural Language Policy Explanations

Solution: User Awareness & Control

**“authenticated” depends on a credential.
“hasSubscription” depends on “authenticated”**

I CAN'T PROVE THAT

it is allowed to download paper14.pdf

BECAUSE

Rule [r3] is not applicable:

THERE IS NO User SUCH THAT

User is authenticated

[details]

AND

**Pruning: User is not authenticated so it
makes no sense to inspect her subscriptions**

Rule [r4] is not applicable:

THERE IS NO User SUCH THAT

User is authenticated

[details]

MOREOVER

THERE IS NO User SUCH THAT

User has paid for paper14.pdf [details]

FILTERED POLICY

[r3]: allow(download(Resource)) ←
authenticated(User),
blurred(hasSubscription(User)).

[r4]: allow(download(Resource)) ←
authenticated(User),
paid(User,Resource).

METAPOLICY

allow(download(Resource)).explanation:
“It is allowed to download “ &
Resource.

public(Resource).explanation:
Resource & “ is public”.

authenticated(User).explanation:
User & “ is authenticated”.

hasSubscription(User).explanation:
User & “ has subscription”.

paid(User,Resource).explanation:
User & “ has paid for “ &
Resource.

06 Conclusions

Summary

Privacy protection in social platforms needs to be

- More flexible
- More powerful
- Dynamically adjustable

Semantic Web policies can offer that but they need to also offer user awareness and control, i.e.,

- Natural language policy specification
- Natural language policy explanations

06 Conclusions

Summary

Using Natural Language Policies for Privacy Control in Social Platforms

- allows the user to create arbitrary conditions for access of resources or profile
 - not restricted to predefined groups or attributes
- may access external information about the requestors outside the social platform
 - e.g., if he is enrolled at your university or at another social platform
- natural language policies are more intuitive to the reader
 - definitely more than formal syntax

07 References

Demonstration & Prototype

- Demonstration
 - <http://policy.L3S.uni-hannover.de/>
- Prototype available
 - <http://skydev.L3S.uni-hannover.de/gf/project/protune/>
 - Freely distributed
 - All in java
 - Easily configurable, multi-thread
 - Legacy systems integration: RDBMS, LDAP, RDF repositories, ...

07 References

Some Publications

- Bonatti, Olmedilla. **Driving and monitoring provisional trust negotiation with metapolicies.** In *6th IEEE Policies for Distributed Systems and Networks (POLICY 2005)*. IEEE, 2005.
- Bonatti, Olmedilla, Peer. **Advanced policy explanations on the web.** In *17th European Conference on Artificial Intelligence (ECAI 2006)*. IOS Press, 2006.
- Antoniou et al., Rule-based policy specification. **Secure Data Management in Decentralized Systems.** Springer, 2007.
- Bonatti, Olmedilla. **Rule-based policy representation and reasoning for the semantic web.** In *Reasoning Web, Third International Summer School 2007*. Springer.

Thanks!

Questions?

*<http://www.olmedilla.info/>
danieloc@TID.es*

Work performed in collaboration with

Juri L. De Coi, Philipp Kärger, Sergej Zerr - L3S Research Center, Germany

Piero A. Bonatti, Luigi Sauro - Naples University, Italy

Telefonica
