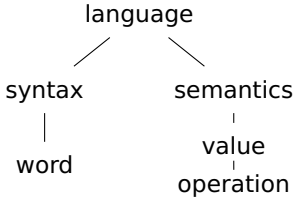
Towards a Formal Language for Privacy Options

Stefan Berthold

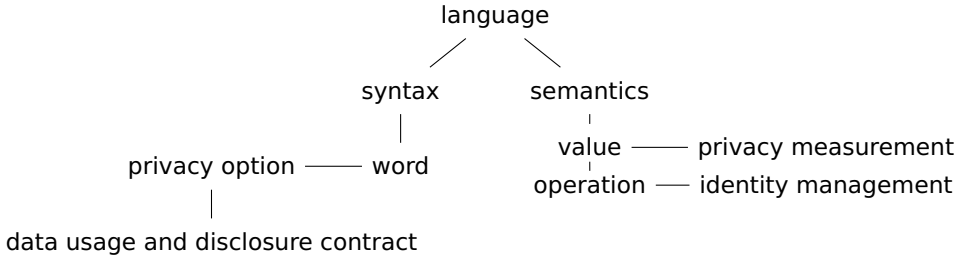
Karlstads universitet

2nd August 2010

Outline



Outline


language
syntax
semantics
privacy option
word
value
privacy measurement
operation
identity management
data usage and disclosure contract

Design Idea

$\underbrace{\text{predicate}\ \underbrace{c_1}_{\texttt{Contract}}}_{\texttt{Contract}}$ } simple extension of (basic) contracts

$\underbrace{c_1\ \text{`predicate'}\ c_2}_{\texttt{Contract}}$ } combination of contracts

Design Idea

$\underbrace{\text{predicate}\ \underbrace{c_1}_{\texttt{Contract}}}_{\texttt{Contract}}$ } simple extension of (basic) contracts

e. g., postponing of contract execution

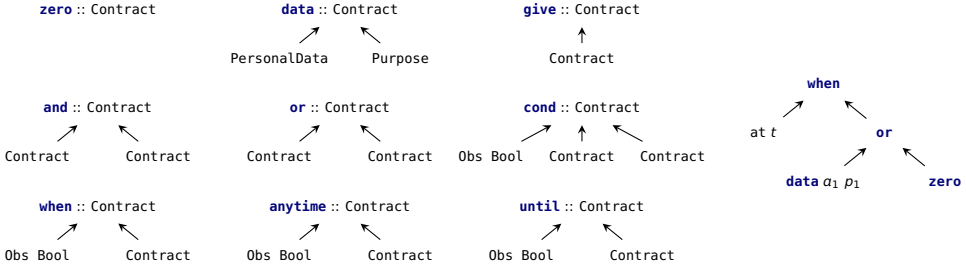
$\underbrace{c_1\ \text{`predicate'}\ c_2}_{\texttt{Contract}}$ } combination of contracts

e. g., Boolean operators

Examples

$c_1 = \texttt{zero}$	... no rights, no obligations
$c_2 = \texttt{data}\ a_1\ p_1$	... receive data and use it immediately
$c_3 = \texttt{give}\ c_2$	... send data which is used immediately
$c_4 = c_1\ \text{`}\texttt{or}\text{'}\ c_2$	... receive and use the data or do nothing
$c_5 = \texttt{when}\ (\text{at}\ t)\ c_4$	... postpone c_4 to time t

Syntax


zero :: Contract
data :: Contract
PersonalData
Purpose
give :: Contract
Contract
and :: Contract
Contract
Contract
or :: Contract
Contract
Contract
cond :: Contract
Obs Bool
Contract
Contract
when :: Contract
Obs Bool
Contract
anytime :: Contract
Obs Bool
Contract
until :: Contract
Obs Bool
Contract
when
at t
or
data a_1 p_1
zero

$$\mathcal{ACTION} = \texttt{Date} \to \mathcal{IO}\ \texttt{Contract}$$
$$\mathcal{O}_{\mathcal{E}}[\![\cdot]\!] : \texttt{Contract} \to \mathcal{ACTION}$$

$$\mathcal{O}_{\mathcal{E}}[\![\texttt{zero}]\!] = \text{return}(\texttt{zero})$$
$$\mathcal{O}_{\mathcal{E}}[\![\texttt{data}\ a\ p]\!] = \text{use}(a, p)$$
$$\mathcal{O}_{\mathcal{E}}[\![\texttt{give}\ c]\!] = \text{send}(c)$$
$$\mathcal{O}_{\mathcal{E}}[\![c_1\ \texttt{`and`}\ c_2]\!] = \mathcal{O}_{\mathcal{E}}[\![c_1]\!] \parallel \mathcal{O}_{\mathcal{E}}[\![c_2]\!]$$
$$\mathcal{O}_{\mathcal{E}}[\![c_1\ \texttt{`or`}\ c_2]\!] = \text{greedy}_{\mathcal{E}}(\mathcal{O}_{\mathcal{E}}[\![c_2]\!], \mathcal{O}_{\mathcal{E}}[\![c_1]\!])$$
$$\mathcal{O}_{\mathcal{E}}[\![\texttt{cond}\ o\ c_1\ c_2]\!] = \text{if}(\mathcal{V}[\![o]\!], \mathcal{O}_{\mathcal{E}}[\![c_1]\!], \mathcal{O}_{\mathcal{E}}[\![c_2]\!])$$
$$\mathcal{O}_{\mathcal{E}}[\![\texttt{when}\ o\ c]\!] = \text{when}'_{\mathcal{E}}(\mathcal{V}[\![o]\!], \mathcal{O}_{\mathcal{E}}[\![c]\!])$$
$$\mathcal{O}_{\mathcal{E}}[\![\texttt{anytime}\ o\ c]\!] = \text{stopping}'_{\mathcal{E}}(\mathcal{V}[\![o]\!], \mathcal{O}_{\mathcal{E}}[\![c]\!])$$
$$\mathcal{O}_{\mathcal{E}}[\![\texttt{until}\ o\ c]\!] = \text{absorb}'_{\mathcal{E}}(\mathcal{V}[\![o]\!], \mathcal{O}_{\mathcal{E}}[\![c]\!])$$

Comparison with PPL Sticky Policies

Motivation

- language with similar design goals: PPL Sticky Policies.
- POL $\not\subseteq$ PPL and POL $\not\supseteq$ PPL, thus no easy comparison.
- way out: POL$^-$ $\subseteq$ POL with POL$^-$ $\subseteq$ PPL.

Q: how to define POL$^-$?

- when and `anytime` *not* part of POL$^-$.
- points of time the *only* conditions of `until` and `cond`.
- new PPL action: ‘immediate usage’.

Language Extensions

- add new language primitives (experts only).
  - experts only.
  - risk for redundancy.
  - readjustment of semantics.
- combinators for common contract patterns (common user).
  - common user.
  - application of existing language primitives.
  - no readjustment of semantics.
  - ex def: `twice` $f\ c = (f\ c)$ `‘and‘` $(f\ c)$.
  - ex app: `until` (at t) `‘twice‘` c_1

Results & Summary

- def: language for describing privacy options (syntax, semantics).
- word in that language can be interpreted as:
  - (numeric) value – privacy measurement.
  - sequence of i/o action – identity management.
- comparision to existing languages (PPL).
- discussion: extending the language.

Q & A

Stefan Berthold

Karlstads universitet
stefan.berthold@kau.se

Recommended reading. Berthold, S., Böhme, R.: Valuating privacy with option pricing theory. In: Workshop on the Economics of Information Security (WEIS), University College London, UK (2009).