Evidential Authorization

Yuri Gurevich
with Andreas Blass, Michal Moskal, Itay Neeman
Future of Software Engineering, Zurich, Nov 2010
“The future ain’t what it used to be.”
Yogi Berra
§ MOTIVATION

Drawings by Hava Gurevich
You manage a public cloud

- Attracting fat customers
- The security problem
- A glorified blob store?
- The promise of cryptography
- The mystery of the world of brick and mortar
Example: Commerce

- An involved support system
  - Banks issue letters of credit
  - Insurance companies underwrite the transactions and transportation
  - ...
- Numerous policies are enforced.
Another example: Clinical trials

Here are some actors in that drama:

❖ Trial organizer
  ■ CRO = Contract Research Organization = Clinical Research Organization

❖ Trial sites
  ■ University hospitals for example.

❖ Physicians,
  also lab technicians, auditors, etc.
Yet another example

Compliance
Lifting to the cloud

In the case of a clinical trial, we’d like that all patient info is (properly guarded) in the cloud.

- There will be another actor:

Policies must high level.

- To allow comprehension and reasoning.

Policies must be stated formally.

- To allow automation.

Cryptography is indispensible in enforcing policies but first we need a policy language.
Enter DKAL

- Distributed Knowledge Authorization Language was created with such applications in mind.
- It required foundational logic investigation.
- It is in the process of tech transfer.
PROBLEM
Authorization used to be simple

The authorization matrix
- ACLs vs. the capability model

Problems
- Groups, exceptions and combinations of such
- From ACL’s to policies
- Security, in particular privacy
- Federated scenarios
Authz is only a tip of the policy iceberg

- Security policies beyond permit/deny
  - “Change you password every 6 weeks.”
- Policies beyond typical security
  - “The physician will not see you before you fill the questionnaire.”
  - Attire: business casual
- Organizations, including governments, are drowning in policies, laws, regulations, etc.
Engineering solutions

Decentralized and imperative

- XACML
- XrML

and weak in the semantics department
Logic-based solutions
centralized and declarative
How to bridge the gap?

There is a genuine tension between logic and federated scenarios.

- Logic is centralized and declarative.
- Federated scenarios are decentralized and imperative.
§ RELATIVITY
Infons

Real world statements are rarely true or false.
1. Turning right on red light is legal.
2. This picture is beautiful. Haggis is edible.

In case 1, as in relativity theory, the value (in this case the truth value) depends on observer’s place.
In case 2, the truth value may be ill-defined even for observers.

Forget about truth values and treat statements as pieces of information, *infons*.

It is not about whether the infon is true or false; it is about which parties know the infon and which don’t.
Infon logic

Infon logic happens to be a conservative extension of well-known constructive (aka intuitionistic) logic.

The extension is by means of connectives “p said x” and “p implied x”. (The first is essentially a special case of the second; we’ll return to the issue.)

“P is trusted on saying x” abbreviates “(P said x) → x”. And similarly for implying x.
Knowledge vs. information

Plato’s *Theaetetus*
- Infon logic is sort of an information theory.
- So called epistemic logics are really about information as well.

Infon logic is not an intuitionistic version of known knowledge logics.
- There you have “Yuri knows that Bertrand knows x”. But Yuri only knows what Bertrand said or implied.

Knowledge remains informal.
- The omniscience paradox
Algorithmics

- Primal infon logic
- The linear-time decision procedure
§ FEDERATION
Communicating principals

- The DKAL world consists of communicating principals.
- There is nothing else.
- Principals live in their own states, control their privacy and compute their knowledge.
The state of a principal

- Conceptually
  \[ \text{state} = \text{substrate} + \text{infostrate}. \]
- The substrate is a database (or a collection of such).
- For example, the substrate of a trial organizer may contain, for each trial, a relation where each row is an actual or potential trial site.
Infostrate

Knowledge assertions
- These are infons (syntactically, infon formulas)

Communication rules

Filters
What does principal know?

1. Knowledge assertions
   - He may have some knowledge assertions from birth
   - An incoming message may result in a new knowledge assertion.
   - Assertions may be deleted.

2. Results of infon-logic deductions from his valid assertions.
Remarks

- It is not necessary that every principal speaks DKAL.
  - Guido’s work on DKAL adjudication engine for XACML.
- Having communication in the language facilitates analysis of multiple policies.
§ COMMUNICATION
Declarative is too narrow

- This is really a separate lecture.
- Declarative vs. high-level
- The EU suit against Microsoft
Communication rules

if premise then send [justified] to recipient content

Here premise and content are infon formulas and recipient is a term.

How does it work?
One abbreviation

if premise
then say [justified] to recipient
  content
for

if premise
then send [justified] to recipient
  sender said content
Most fascinating is a feature that would make any journalist tremble. Tuyuca requires verb-endings to show how the speaker knows something. 

Diga ape-wi means “the boy played soccer (I saw him)”. Diga ape-hiyi means “the boy played soccer (I assume)”. English can provide such information, but for Tuyuca that is obligatory.

---The Economist, January 1, 2010 (slightly simplified)
Simple justifications of principal A

If $\varphi$ has the form

\[(A \text{ said } \alpha)\]

or

\[\beta \rightarrow (A \text{ implied } \alpha),\]

then a cryptographic signature of principal A under (a strong hash of) the $\varphi$ is a justification for $\varphi$.

(The first is essentially the special case of the second.)
A justification for an arbitrary infon formula $\varphi$ is a derivation of $\varphi$ in infon logic from

- simple justifications, and
- axioms of shared theories e.g. arithmetic.
§ CLINICAL TRIALS
To demo or not to demo

The demo requires

- internet connection (to use an SQL engine in the cloud),
- time.
Instead of the demo