Take CARE
Provenance, Policies and Your Obligations in the Future

Christoph Ringelstein & Steffen Staab
Do you remember?

- That Italian tax office published all tax data about citizens on its Web page...
- That CIA published a list of his agents on the internet....

Even in a friendly environment allowing/disallowing data handling is a big issue
Middle Rhine Hospital shares its Health Record for research.
1. I want to describe what **may** be done with my record

2. I want to define what **must** be done with my record (obligation)
Motivation

- **Provenance**
  - very general mechanism to represent
    - which past events may influence policy decisions

- **Provenance**
  - natural mechanism to consider the past and
  - extend this consideration into the future
Policies build on the Past and Affect the Future

No permission
allowed

Provenance

S₂ examination
S₃ asking permit
S₄ examination
S₅ discharge
S₆ transfer
S₁₀ prepare share
S₁₁ share
S₁₂ analysis

Future Provenance

S₇.a
S₈.a
S₈.b
S₈.c
WHAT MAY BE DONE?

**PAPEL**: A POLICY LANGUAGE USING PROVENANCE
WeST

Steffen Staab
staab@uni-koblenz.de

Steffen Staab
1. - 2. Provenance & Policies

3. Conditions based on Provenance

4. Hiding Information

5. Attributes

6. Interpreting Conditions
Middle Rhine Hospital

1. admission
2. examination
3. asking permit
4. examination
5. prepare share
6. share for research
7. research

Health Record

Policies

Provenance

You
Middle Rhine Hospital

1. admission

Health Record
create

Policies
create

Provenance
create
Syntax of Provenance in Sticky Logs:
step (Data, Actors, InvolvedAgents, Category, Purpose, ID, PIDs)

Sticky Log:
step (record, {mrh}, {}, create, patient_treatment, 1, {0})
(P1): ukob is allowed to process health records for research purposes. However, ukob is not allowed to transfer the health records of patients to other organizations.

(P2): The mrh demands that the record is only accessed by ukob after the sharing of the health records is approved by the patient and the approval must have been confirmed by a doctor.
(P1): ukob is allowed to process health records for research purposes. However, ukob is not allowed to transfer the health records of patients to other organizations.
PAPEL Syntax for Policies:

permit (ID) IF Condition.
deny   (ID) IF Condition.

XACML [2]

(P1): ukob is allowed to process health records for research purposes.

permit (ID) IF step (record, {ukob}, _, _, research, ID, _).

However, ukob is not allowed to transfer the health records of patients to other organizations.

deny (ID) IF step (record, {ukob}, _, transfer, _, ID, _).
**Middle Rhine Hospital**

**Health Record**

**Policies**

**Sticky Log**

1. **admission**

**Matches step(...) an element of the history?**

**(P1):** ukob is allowed to process health records for research purposes.

`permit (ID) IF step (record, {ukob}, _, _, research, ID, _).`

However, ukob is not allowed to transfer the health records of patients to other organizations.

`deny (ID) IF step (record, {ukob}, _, transfer, _, ID, _).`
(P1): **ukob** is allowed to process health records for research purposes.

\[
\text{permit (ID) IF step (record, \{ukob\}, _, _, research, ID, _).}
\]

However, **ukob** is not allowed to transfer the health records of patients to other organizations.

\[
\text{deny (ID) IF step (record, \{ukob\}, _, transfer, _, ID, _).}
\]

Allowed processing steps:

- All steps are denied, if not explicitly permitted by a permit rule and not explicitly prohibited by a deny rule.
Sticky Log:
step (record, {mrh}, {}, create, patient_treatment, 1, {0})
step (record, {mrh}, {}, update, examination, 2, {1})
Middle Rhine Hospital

Health Record

Policies

Sticky Log

Mapping the temporal structure to a graph structure!

Sticky Log:
step (record, {mrh}, {}, create, patient_treatment, 1, {0})
step (record, {mrh}, {}, update, examination, 2, {1})
(P2): The mrh demands that the record is only accessed by ukob after the sharing of the health records is approved by the patient and the approval must have been confirmed by a doctor.
The **mrh** demands that the record is only accessed by **ukob** after the sharing of the health records is approved by the patient and the approval must have been confirmed by a doctor.

\[
\text{permit (ID) IF (step (record, \{ukob\}, _, access, _, ID, _) AFTER (step (record, \{doctor\}, _, _, confirmation, _, _) AND step (record, \{patient\}, _, _, access_approval, _, _)))}
\]
Middle Rhine Hospital

1. admission
2. examination
3. asking
4. examination

Health Record
- create
- update

Policies
- create
- update

Sticky Log
- create
- update

Hiding Sensitive Information
Syntax for Sticky Logs:
step (Data, Actors, InvolvedAgents, Category, Purpose, ID, PID)

Syntax of Reduced Facts in Sticky Logs:
reduced (Data, [Actors, InvolvedAgents, Category, Purpose, ID, PID])
replace with hidden as required.
Syntax of Reduced Facts in Sticky Logs:

```
reduced (Data, Actors, InvolvedAgents, Category, Purpose, ID, PIDs)
```

replace with `hidden` as required.

Sticky Log:

```
step (record, {mrh}, {}, create, patient_treatment, 1, {0})
step (record, {mrh}, {}, update, examination, 2, {1})
reduced (record, hidden, hidden, update, hidden, 4, {2})
```
Using Attributes

Health Record
- create
- update
- update
- de-id.

Policies
- create
- update
- You
- fulfill

Sticky Log
- create
- update
- update
- encrypt
- update

Middle Rhine Hospital

1. admission
2. examination
3. asking permit
4. examination
5. prepare share

WeST
Steffen Staab
staab@uni-koblenz.de
Syntax of Attributes in Sticky Logs:
attribute (Data, Name, Value, ID)

Sticky Log:
step (record, {mrh}, {}, create, patient_treatment, 1, {0})
step (record, {mrh}, {}, update, examination, 2, {1})
reduced (record, hidden, hidden, update, hidden, 4, {2})
step (record, {mrh}, {}, de-identified, privacy, 5, {4})
attribute (record, de-identified, true, 5)
(P3): You demand that your record is shared only after de-identification.

permit (ID) IF (step (record, _, _, transfer, _, ID, _) AFTER step (record, _, _, update, de-identify, _, _))

permit(ID) IF (step (record, _, _, transfer, _, ID, _) AND attribute (record, de-identified, true, ID)).
(P3): You demand that your record is shared only after de-identification.

permit(ID) IF (step (record, _, _, transfer, _, ID, _) AND attribute (record, de-identified, true, ID)).

assignment(ID) IF step (record, _, _, _, de-identified, ID, _) DO set_attribute (record, de-identified, true, ID).

assignment(ID) IF step (record, _, _, _, re-identified, ID, _) DO set_attribute (record, de-identified, false, ID).
Middle Rhine Hospital

1. admission
2. examination
3. asking
4. examination
5. prepare
6. share for research

Health Record
- create
- update
- update
- de-id.
- transfer

Policies
- create
- update
- fulfill
- check
- transfer

Sticky Log
- create
- update
- update
- update
- encrypt
- update
- transfer

WeST
Steffen Staab
staab@uni-koblenz.de
WeST

Middle Rhine Hospital

Sticky Log:

```
step (record, {mrh}, {}, create, patient_treatment, 1, {0})
step (record, {mrh}, {}, update, examination, 2, {1})
reduced (record, hidden, hidden, update, hidden, 4, {2})
step (record, {mrh}, {}, de-identified, privacy, 5, {4})
attribute (record, de-identified, true, 5)
step (record, {mrh}, {ukob}, transfer, research, 6, {5})
```
Sticky Log:

<table>
<thead>
<tr>
<th>Step</th>
<th>Record</th>
<th>Action</th>
<th>Data</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>{mrh},</td>
<td>create</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>{mrh},</td>
<td>update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>hidden,</td>
<td>update</td>
<td>hidden</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>{mrh},</td>
<td>update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>{mrh},</td>
<td>update</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(P3): 

\[
\text{permit (ID) IF } \begin{cases} \text{step (record, \_\_\_, transfer, \_\_\_, ID, \_\_)} \land \\ \text{attribute (record, de-identified, true, ID)} \end{cases}.
\]

WeST

create examination

Middle Rhine Hospital

Health Record

Policies

Sticky Log

share for research

transfer

check

permit (ID)
Sticky Log:

- step (record, {mrh}, {}, create, patient_treatment, 1, {0})
- step (record, {mrh}, {}, update, examination, 2, {1})
- reduced (record, hidden, hidden, update, hidden, 4, {2})
- step (record, {mrh}, {}, de-identified, privacy, 5, {4})
- attribute (record, de-identified, true, 5)
- step (record, {mrh}, {ukob}, transfer, research, 6, {5})

P3:

\[
\text{permit (ID) IF (step (record, _, _, transfer, _, ID, _) AND attribute (record, de-identified, true, ID))}.
\]
Formal definition of semantics available.
WHAT MUST BE DONE?
OBLIGATIONS WITH CARE
Policies – Obligation

(P1): Staff members are permitted to transfer the record to Jane Doe after her discharge.

(P2): Staff members and the archive are permitted to transfer the record to staff members.

(O1): Jane Doe demands to receive her record after her discharge.

(O2): A nurse has to transfer the record to the archive if she received it after the patient’s discharge.

(D1): Jane Doe is denied to transfer her record.
(P1): Staff members are permitted to transfer the record to Jane Doe after her discharge.

(P2): Staff members and the archive are permitted to transfer the record to staff members.

(O1): Jane Doe demands to receive her record after her discharge.

(O2): A nurse has to transfer the record to the archive if she received it after the patient’s discharge.

(D1): Jane Doe is denied to transfer her record.
(P1): Staff members are permitted to transfer the record to Jane Doe after her discharge.

(P2): Staff members and the archive are permitted to transfer the record to staff members.

(O1): Jane Doe demands to receive her record after her discharge.

(O2): A nurse has to transfer the record to the archive if she received it after the patient’s discharge.

(D1): The archive is not allowed transferring records to non-staff.
(P1): Staff members are permitted to transfer the record to Jane Doe after her discharge.

(P2): Staff members and the archive are permitted to transfer the record to staff members.

(O1): Jane Doe demands to receive her record after her discharge.

(O2): A nurse has to transfer the record to the archive if she received it after the patient’s discharge.

(D1): The archive is not allowed transferring records to non-staff.
(P1): Staff members are permitted to transfer the record to Jane Doe after her discharge.
(P2): Staff members and the archive are permitted to transfer the record to staff members.

(O1): Jane Doe demands to receive her record after her discharge.
(O2): A nurse has to transfer the record to the archive if she received it after the patient’s discharge.

(D1): The archive is not allowed transferring records to non-staff.
Future Execution Graph

History

- $S_2$: examination
- $S_3$: asking permit
- $S_4$: examination
- $S_5$: discharge
- $S_6$: transfer

Now

- $S_{10}$: prepare share
- $S_{11}$: share
- $S_{12}$: analysis

Future Execution Graph

- $S_{7,a}$
- $S_{8,a}$
- $S_{8,b}$
- $S_{8,c}$

Invalid:

- $S_7.a$

Allowed:

- $S_8.a$
- $S_8.b$
- $S_8.c$
The Destiny

- $S_2$: examination
- $S_3$: asking permit
- $S_4$: examination
- $S_5$: discharge
- $S_6$: transfer
- $S_{10}$: prepare share
- $S_{11}$: share
- $S_{12}$: analysis
- $S_{7.a}$
- $S_{8.a}$
- $S_{8.b}$
- $S_{8.c}$

- invalid
- allowed
- closed
The Destiny

- S₂: examination
- S₃: asking permit
- S₄: examination
- S₅: discharge
- S₆: transfer
- S₁₀: prepare share
- S₁₁: share
- S₁₂: analysis
- S₁₃: Destiny

Statuses:
- invalid
- allowed
- closed
Which next steps have a destiny?
**Policies**

**Input:**
- History +
- Next Step +
- Policy Rules

```
...  
step (record_jd, bob, null, discharge, 5, {4})
step (record_jd, bob, alice, transfer, 6, {5,13})

```

```
+  
step (record_jd, alice, jane, transfer, 7, {6})

```

```
permit (ID) IF step (record_jd, S, jane_doe, transfer, ID, _) AFTER
  step (record_jd, _, _, discharge, _, _) AND
  instance_of (S, staff_member).
```

**Translation:**
- Axioms specifying possible steps.

```
+  
Translation to colored Petri nets.
```

**Decision:**
Reachability of a future state where all obligations are met.
Which next steps have a destiny?

discharge transfer

Alice (nurse)

transfer

archive

transfer

Jane Doe
Conclusion

- Policies with Obligations: ‘Business rules‘ may decide about what may/may not and must be done to your data

- Provenance Graph is core to store what has and will be done to data

- Formal underpinning of our approach makes it semantically sound and complete
Thank You!

Key Publications


They also link to a few more....