Modeling wizard for confidential business processes

...and why it might be interesting.
Our business process

submit insurance claim

collect further information

suspicious claim

initiate fraud investigation

prepare payment

normal claim
Outsourcing tasks...

-suspicious claim
-initiate fraud investigation
-normal claim
-prepare payment

...considering confidentiality

-suspicious claim
-initiate fraud investigation
-normal claim
-prepare payment

Some tasks may be confidential.
Some tasks may be **confidential**. Those tasks shall **remain inhouse**.

Some tasks may be **confidential**. Those tasks shall **remain inhouse**. Others may be **outsourced**.
Confidentiality

What can be outsourced without revealing confidential tasks?

Confidentiality

How to express confidentiality?
How to express confidentiality?

Assign the tasks.

How to check confidentiality?
Outsourced tasks may not learn anything about confidential tasks.

Assumptions

Whole process is known and outsourced tasks are observable.
Non-Interference

Assumptions
Whole process is known and outsourced tasks are observable.

How to learn anything:

Possible Interference

Outsourced depends on confidential.
Possible Interference

Confidential excludes outsourced.

Back to mission.
**Mission accomplished?**

**Outsource everything?**
- submit insurance claim
- collect further information
  - suspicious claim
    - initiate fraud investigation
    - prepare payment
  - normal claim

**Keep everything confidential?**
- submit insurance claim
- collect further information
  - suspicious claim
    - initiate fraud investigation
    - prepare payment
  - normal claim

**Mission accomplished?**
Mission still open!

Submit insurance claim → Collect further information

Suspicious claim → Initiate fraud investigation

Normal claim → Prepare payment

Mission still open!

Submit insurance claim → Collect further information

Suspicious claim → Initiate fraud investigation

Normal claim → Prepare payment

Mission still open!

Submit insurance claim → Collect further information

Suspicious claim → Initiate fraud investigation

Normal claim → Prepare payment

2^t possible assignments
2ᵗ possible assignments
most task assignments are
uninteresting

Model support
1. Assign all tasks.

2. Press „Verification“.
1. Assign all tasks.
2. Press „Verification“.
3. Evaluate result.

Problem: stupid and nerving (2^t options)

1. Assign confidential tasks.
1. Assign **confidential** tasks.
2. Assign restricted tasks.

1. Assign **confidential** tasks
2. Assign restricted tasks.
3. Assign all (other) tasks.
1. Assign confidential tasks.
2. Assign restricted tasks.
3. Assign all (other) tasks.
4. Press „Verification“.

Problem: still nerving (\(\sim 2^t\) options)
1. Assign **confidential** tasks.
2. Get all implied assignments.

3. **Outsource** as much as possible.

**Confidentiality by design**
Confidentiality by design

Problems:
too many assignments
Confidentiality by design

Problems:
too many assignments

Confidentiality by design

Problems:
too many assignments
too many checks for them
Solve problems

Checks are independent.

Depends „collect“ on „submit“?

Solve problems

Save contraints.

❌ submit = high ∧ collect = low

Constraint:
NOT (submit = high ∧ collect = low)
Solve problems

Checks are independent.

Mutual exclusion of „prepare“ and „initiate“?

Solve problems

Checks are independent.

Depends „initiate“ on „collect“?
Checks are independent.

Depends „prepare“ on „collect“?

5 of 20 checks necessary

4 of 16 assignments are valid
Solve problems

Represent assignments symbolically.

Submit
Collect
Fraud
Pay
Valid
Invalid

Submit
Collect
Fraud
Pay
Valid
Invalid
Confidentiality model support for 559 business processes

<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Average</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasks</td>
<td>1</td>
<td>20</td>
<td>100</td>
</tr>
<tr>
<td>Assignments</td>
<td>2</td>
<td>1,048,576</td>
<td>&gt; $10^{30}$</td>
</tr>
</tbody>
</table>
### Confidentiality model support for 559 business processes

#### Tasks
<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Average</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasks</td>
<td>1</td>
<td>20</td>
<td>100</td>
</tr>
</tbody>
</table>

#### Assignments
<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Average</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignments</td>
<td>2</td>
<td>1,048,576</td>
<td>&gt; $10^{30}$</td>
</tr>
</tbody>
</table>

#### Checks
<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Average</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checks</td>
<td>3</td>
<td>38</td>
<td>282</td>
</tr>
</tbody>
</table>

### Confidentiality model support for 559 business processes

#### Nodes in BDD
<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Average</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nodes in BDD</td>
<td>7</td>
<td>107</td>
<td>1,090</td>
</tr>
</tbody>
</table>
### Confidentiality model support for 559 business processes

<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Average</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasks</td>
<td>1</td>
<td>20</td>
<td>100</td>
</tr>
<tr>
<td>Assignments</td>
<td>2</td>
<td>1,048,576</td>
<td>&gt; $10^{30}$</td>
</tr>
<tr>
<td>Checks</td>
<td>3</td>
<td>38</td>
<td>282</td>
</tr>
<tr>
<td>Nodes in BDD</td>
<td>7</td>
<td>107</td>
<td>1,090</td>
</tr>
<tr>
<td>Time (sec)</td>
<td>0,00</td>
<td>0,09</td>
<td>2,14</td>
</tr>
</tbody>
</table>

### Take-Home Points

1. **Confidentiality** is relevant. Protects sensitive assets.

2. **Confidentiality** by design. Avoids subsequent verification steps.

3. **Confidentiality** is practicable. Model and tool support.
Take-Home Points

1. **Confidentiality** is relevant. Tomorrow
   Tool-Demo!

2. **Confidentiality** by design
   The day after tomorrow
   Verification background

3. **Confidentiality** is practicable
   Model and tool support

Backup
Formalism: Petri nets

Formalism: Noninterference

Positive Place Based Noninterference
A potential causal place...

...is an active causal place:

High marks causal place. Other transitions may fire. (except those marking causal place)

Low is activated.

A potential conflict place...

...is an active conflict place:

High is activated in m. Other transitions may fire from m. (except those marking conflict place)

Low is activated.