The MonIKA-Framework - A Trial Balloon of a Cooperative Monitoring Framework for Anomaly Detection

Arnold Sykosch <sykosch@cs.uni-bonn.de>

SPONSORED BY THE

Federal Ministry
of Education
and Research

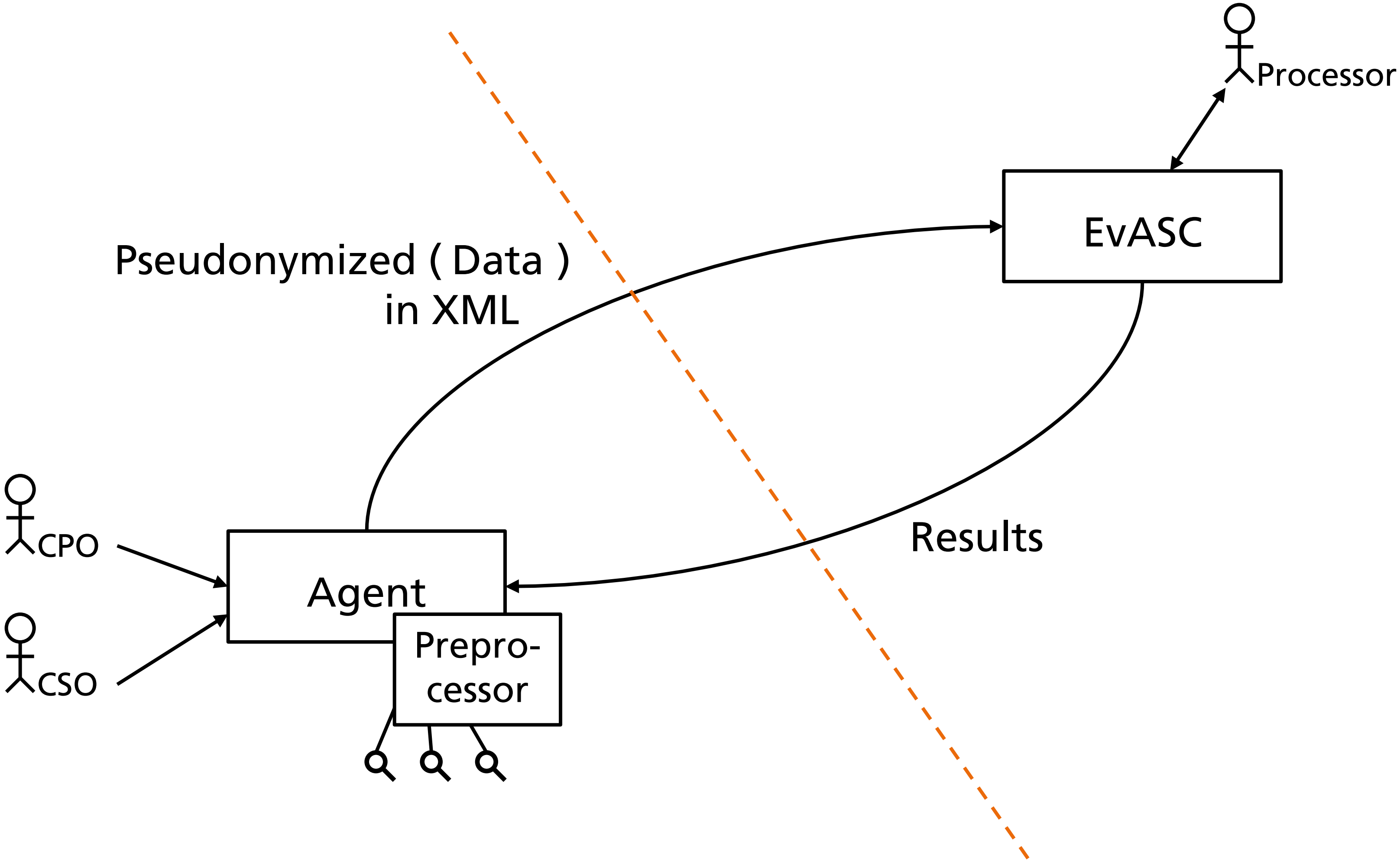
1. Key Requirements
A Recapitulation

- Information fusion
  - Gathering of information to one place
  - A global data schema

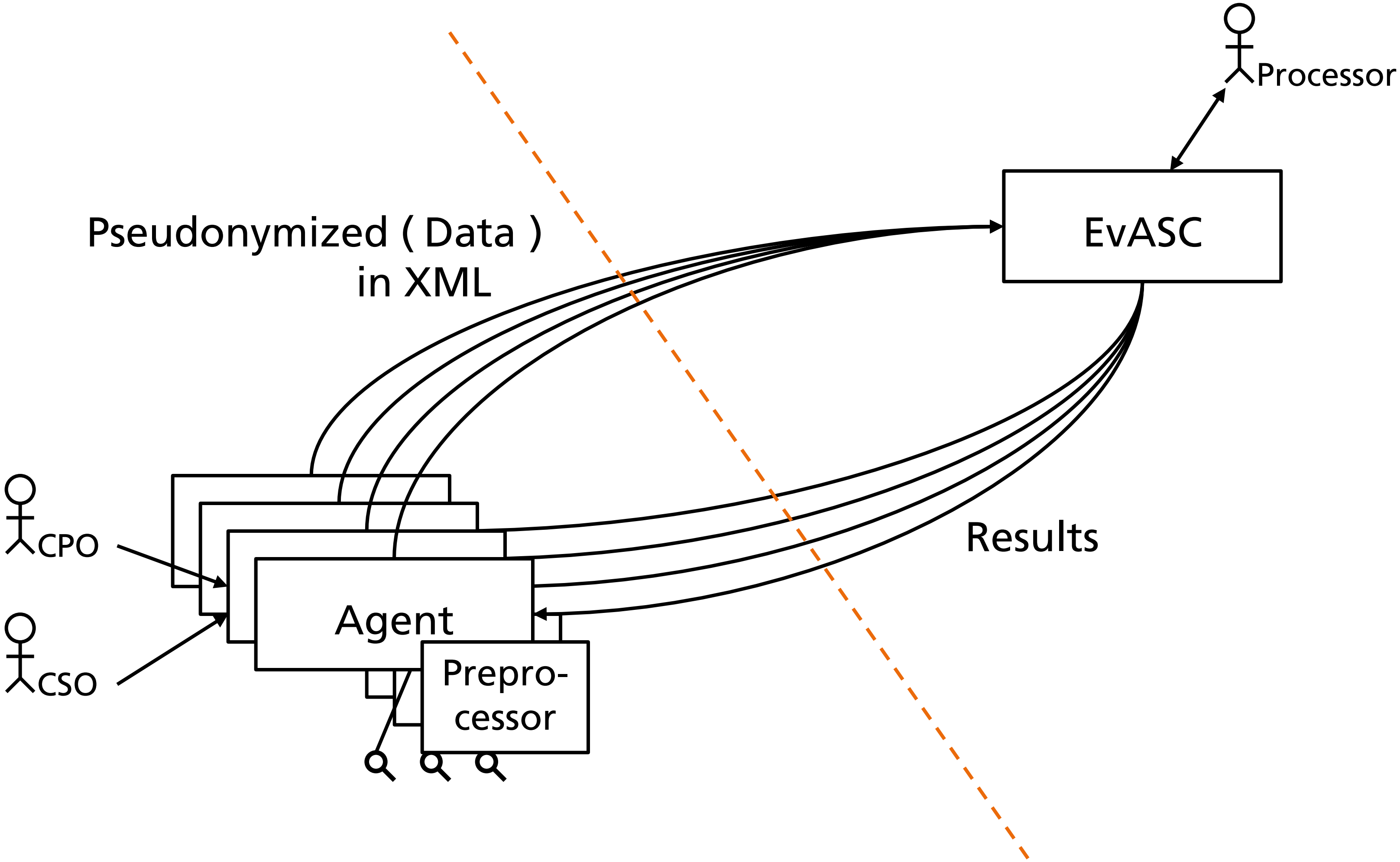
- Privacy protection
  - Pseudonymization
  - Purpose limitation

- Anomaly detection
  - Access for classification algorithms
  - Result management

2. The Basic Architecture



2. The Basic Architecture



1. Key Requirements
A Recapitulation

- Information fusion
  - Gathering of information to one place
  - A global data schema

- Privacy protection
  - Pseudonymization
  - Purpose limitation

- Anomaly detection
  - Access for classification algorithms
  - Result management

3. Pseudonymization by Policy
Availability and Confidentiality Requirements

- Requirements against the data

- Availability Requirements
  - *Laid down by:* the Processor.
  - *If not met:* The classification algorithm can not work.

- Confidentiality Requirements
  - *Laid down by:* the CPO
  - *If not met:* No agreement from CPO, therefore no data from one party.

- FLAIM[1] *(data from multiple sources can not be correlated)*

3. Pseudonymization by Policy
Parts & Pieces

`<pseudonym>`

What should the output in the global schema be called?

`<data>`

What is the input?

`<link>*`

How should the generated pseudonym be linkable?

`<revocation>*`

Should pseudonymety be revocable?

3. Pseudonymization by Policy
Parts & Pieces

`<pseudonym>`

What should the output in the global schema be called?

`<data>`

What is the input?

`<link>*`

How should the generated pseudonym be linkable?

`<revocation>*`

Should pseudonymety be revocable?

3. Pseudonymization by Policy

An Example - The Data

```
...
<alert>
   <type>
      ICMP-Redirect
   </type>
   <receiver>
      <ip>
         11000000101010000000000100001101
      </ip>
   </receiver>
...
```

3. Pseudonymization by Policy
An Example - The Policy

```
<pseudonym name=“ipaddr” application=“app” sensor=“snort”>
  <data>
    tokenize(replace(ip, '(.)', '$1&#xE0F1;'), '&#xE0F1;')
  </data>
  <link>
    <type>prefix</type>[2]
    <relation>app.ipaddr</relation>
    <condition salt=“...”>type==“ICMP-Redirect”</condition>
    <group>//ip/..</group>
  </link>
</pseudonym>
```

3. Pseudonym Generation
What does a pseudonym look like?

```
...
<alert>
   <type>
      ICMP-Redirect
   </type>
   <receiver>
      <ip>
         11000000101010000000000100001101
      </ip>
   </receiver>
...

...
<ipaddress condition="1"  group="fhDuek23DH83kdg">
  01111011001001000000110001010101
</ipaddress>
...
```

4. Conclusions

- MonIKA - Pseudonymization by Policy
  - Extends the concept of limited linkability in a very flexible way.
  - Allows modelling a best available fit between availability and confidentiality requirements.
  - Fits a multi-user scenario.

5. References

[1] Slagell et al.: *Flaim: A multi-level anonymization framework for computer and network logs* - Proceedings of the 20th USENIX Large Installation System Administration Conference, 2006

[2] Fan et al.: *Prefix-preserving IP address anonymization: measurement-based security evaluation and a new cryptography-based scheme* - Computer Networks 46-2, 2004

Q & A