POSEIDON

Risk Management and Data Analysis in PoSeID-on

Presenters:
Paulo Silva
Rui Casaleiro

July 11th, 2019

Funded by Horizon 2020
Framework Programme of the European Union
INDEX

1. The PoSeID-on platform
2. R&D Challenges
3. Risk Management Approach
4. Data Analysis
PoSeID-on

Protection and control of Secured Information by means of a privacy enhanced Dashboard
PoSeID-on Goals

- Empower data subjects
- Safeguard personal data
- Data minimization and data quality
- Detection of unexpected and potentially harmful behaviours
Our challenge

Detection of unexpected and potentially harmful behaviours
Approach

- Model normal behaviour of PoSeID-on
- Analyse contents of PII related operations
Risk Management Module Goals

• **Model normal system behavior**
  • While being as decoupled and less intrusive as possible

• **Generate warnings each time a possible privacy risk is happening**
  • By identifying anomalous patterns in system operations

• **Manage data processor reputation**
  • According to previous good risk generating behavior
RMM Approach

Model system behaviour based on:

- Type of operations performed in the system
  - PII Permission Request, PII Access, PII Permission Revocation…
- Logs generated by each component in the system

Notify system administrators and data subjects when the pattern extracted from such info deviates from the regular pattern
T4.3 RMM – Anomaly Detection

**Log collection**
- Messages from components

**Log parsing**
- Generate log event templates
- Fit each log into one of the template events

**Feature extraction**
- Count number of events happening within a window (e.g. hourly window)
- Count number of PII operations of each type happening within a window

**Anomaly detection**
- Create a model from regular event count per window using clustering algorithms
- Predict cluster for upcoming logs
- Determine distance from predicted cluster and clusters with small number of entries in order to identify anomalies
- Update model according to new values
T4.3 RMM – Anomaly Detection

Output:
A window (sequence of events) which has been flagged as anomalous or in other words, not fitting in the regular behavior of the system. This might be:

- A privacy risk
- A system malfunction
- A non-malicious but rare pattern of logs

Further analysis of the identified anomalies is needed to determine if a risk is real or not.
T4.3 RMM – Anomaly Detection

Identifying which Data Subjects and Data Processors are involved in the anomalous window allows:

- Updating data processor reputation accordingly
- Notifying involved data subjects
**T4.3 RMM – Log Anomaly Detection**

1. **Log Collection**

1. 2008-11-09 20:55:54 PacketResponder 0 for block blk_321 terminating
2. 2008-11-09 20:55:54 Received block blk_321 of size 6708864 from /10.251.195.70
4. 2008-11-09 20:55:54 Received block blk_321 of size 6708864 from /10.251.126.5
5. 2008-11-09 21:56:30 10.251.126.5:5000:0:Got exception while serving blk 321 to /10.251.127.243:
6. 2008-11-10 08:58:04 Verification succeeded for blk 321

2. **Log Parsing**

**Event Templates:**
- Event 1: PacketResponder * for block * terminating
- Event 2: Received block * of size * from *
- Event 3: *Got exception while serving * to *
- Event 4: Verification succeeded for *
- Event 5: Deleting block * file *

**Log Events:**
- Log 1 → Event 1
- Log 2 → Event 2
- Log 3 → Event 3
- Log 4 → Event 4
- Log 5 → Event 5
- Log 6 → Event 5

3. **Feature Extraction**

**Fixed windows:**

**Event Count Matrix**
- [0 2 1 1 1 1 2 1 2 1 0 0 1 2 0 1 1 0 2 1 0]

4. **Anomaly Detection**

RMM Architecture

Simplified Lambda Architecture

- Speed layer returns results in real-time by analysing the stream
- Batch layer stores incoming data, performs analysis over a larger dataset and trains models
- Service layer handles results, involved data subject identification and reputation metric requests
T4.3 RMM – Current status

Detailed design and architecture - 100%

Implementation - 50%

- Communication protocol (Libsodium + Protobuf)
- Integration of RabbitMQ with Spark Streaming
- Log analysis for anomaly detection pipeline
  - Extracting parameters from messages and format them to proper data structure
  - Java implementation of Drain Log Parser algorithm, adapted to work on Spark Streaming Pipeline
  - Creation of feature vector to feed clustering algorithms
T4.3 RMM - Next Steps

• Dataset Generation
• Development
  • Implementing anomaly detection
  • Implementing storage for parsed data
  • Adapting stream pipeline to batch layer
• Configuration
  • Distributed deployment
  • Security aspects
• Testing and validation
Personal Data Analyser - PDA

- **Control personal data in a transaction**
  - Personally Identifiable Information (PII)

- **Natural Language Processing & Understanding**
  - Extracting and processing information from transactions

- **Artificial Intelligence**
  - Analyze and evaluate the extracted information
PDA Goals

- **Control personal data in a transaction**
  - Detect or prevent anomalies on misbehaved transactions

- **Generate warnings each time a transaction contains non-identified PII**
  - Discovering PII and making sure existing PII is compliant with permissions

- **Generate privacy risks warnings**
  - PII analysis based on its unique degree of sensitiveness
  - PII analysis based on the correlation with other PII fields
PDA Approach

- **Analysis requests**
  - Transactions performed within PoSeID-on
  - Connection to PoSeID-on’s central messaging protocol

- **Request Handling**
  - Messaging protocol
    - Protocol Buffers (protobuf)
    - Libsodium (PyNaCl)
    - RabbitMQ (pika)

- **Data extraction and parsing**
  - NLP tools
    - NLTK, Stanford CoreNLP, SpaCy

- **Data analysis**
  - ML Models for Named Entity Recognition
  - Regular Expressions

- **Privacy risks analysis**
  - PII sensitiveness
  - PII correlation
  - DP’s reputation
# PDA PII Analysis

<table>
<thead>
<tr>
<th>PII Fields</th>
<th>MEF</th>
<th>Softeam</th>
<th>Santander</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>First name</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Last name</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Email address</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Street name</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Street number</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Post code</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>City</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Country</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Social security number</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Bank details</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employment contract and salary information</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>License plate number</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>National ID numbers</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Passport number</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>
PDA Architecture

- **Incoming Requests**
  - Dashboard
  - RMM
  - Data Processor API

- **Pipeline**
  - Request Handling
  - Data Extraction / Parsing
  - NLP Processing
  - Privacy Risks Analysis
**PDA Current Status**

- **Message Bus**
- **Message Handling**
- **Data Extraction / Parsing**
- **NLP Processing**
- **Integration**
  - Containerization
  - Minikube
T4.3 PDA - Next Steps

**Development**
- Tests and Validation
- Create in-house models
  - With information provided by partners
  - PII Specific Information
- Assessment and implementation of privacy metrics to be used in the analysis
- ML Reasoning Unit development

**Finalize first integration stage**
- Module communication, Minikube configuration

**Papaya collaboration**
- Privacy-preserving Neural Networks (NN)
- To allow a data owner either to:
  - Classify data
  - Collaboratively (with other data owners) train neural networks (NN) while ensuring data privacy
- Analyze the requirements and conclusions taken from today’s bilateral meeting
Final Considerations

- Development and integration progress
- State-of-the-art technologies
- GDPR compliance
- Public documentation available by the end of the month
THANK YOU