NO THREAT, NO SWEAT: Privacy Threat Modeling in Practice – a Machine Learning Use Case

Kim Wuyts
imec-DistriNet, KU Leuven, Belgium

Isabel Barberá
BitnessWise

PEPR’21
PRIVACY
BY DESIGN
THREAT MODELING

- Tackled *proactively*
- *Systematically* analyzed
- *Integrated* in the development lifecycle
- Have an *impact on design* decisions
- Handled with a *risk-based* approach (~GDPR)
Threat Modeling is analyzing representations of a system to highlight concerns about security and privacy characteristics.
Threat modeling

What are you working on?
What can go wrong?
What are you going to do about it?
Did you do an acceptable job?
PROCESS SUPPORT

MODEL THE SYSTEM
- CREATE DFD

ELICIT THREATS
- MAP SYSTEM ELEMENTS
- IDENTIFY THREATS

MANAGE THREATS
- PRIORITIZE/ASSESS
- MITIGATE

REFLECT/REPEAT

KNOWLEDGE SUPPORT

LINKABILITY
IDENTIFIABILITY
NON-REPUTATION
DETECTABILITY
DISCLOSURE OF INFORMATION
UNAWARENESS
NON-COMPLIANCE

INCLUDED IN ISO27550 ON PRIVACY ENGINEERING
INCLUDED IN EDPS OPINION ON PRIVACY BY DESIGN
MAPPED TO NIST’S PRIVACY FRAMEWORK
SUPPORTED IN OWASP THREAT DRAGON

www.linddun.org
MODEL THE SYSTEM
- CREATE DFD

ELICIT THREATS
- MAP SYSTEM ELEMENTS
- IDENTIFY THREATS

MANAGE THREATS
- PRIORITIZE/ASSESS
- MITIGATE

REFLECT/REPEAT

PROCESS SUPPORT

KNOWLEDGE SUPPORT
- LINKABILITY
- IDENTIFIABILITY
- NON-REPUDATION
- DETECTABILITY
- DISCLOSURE OF INFORMATION
- UNAWARENESS
- NON-COMPLIANCE

INCLUDED IN ISO27550 ON PRIVACY ENGINEERING
INCLUDED IN EDPS OPINION ON PRIVACY BY DESIGN
MAPPED TO NIST’S PRIVACY FRAMEWORK
SUPPORTED IN OWASP THREAT DRAGON

WWW.LINDDUN.ORG
LEAN APPROACH TO PRIVACY THREAT MODELING

INTRODUCING LINDDUN GO

LOWERS THE THRESHOLD
REQUIRES LITTLE EXPERTISE AND LOW EFFORT
ENSURES THOROUGH ANALYSIS
What do you need to get started?

A system description

“It is better to create multiple threat modeling representations because there is no single ideal view, and additional representations may illuminate different problems.”

- Threat Modeling Manifesto anti-pattern Perfect representation

A deck of LINDDUN GO cards

“Allow for creativity by including both craft and science.”

- Threat Modeling Manifesto pattern Informed Creativity

A group of participants

“Assemble a diverse team with appropriate subject matter experts and cross-functional collaboration.”

- Threat Modeling Manifesto pattern Varied viewpoints
## LINDDUN GO cards

<table>
<thead>
<tr>
<th>Title</th>
<th>Origin of threat (organizational, external, receiving party)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Questions to check applicability</td>
</tr>
<tr>
<td>Example</td>
<td>Additional info</td>
</tr>
<tr>
<td>Impact/consequences (why is it important)</td>
<td>Card identifier</td>
</tr>
</tbody>
</table>

### IDENTIFYING INBOUND DATA

The data sent to the system can be used to identify the user (with a sufficient degree of likelihood).

1. Does the flow contain identifiable personal data (i.e., identified data, data that can be linked to already obtained identified data, or data that, when combined, become identified)? If unknown, assume it is.
2. Would it be a problem if the user is identified based on these data (i.e., do they need to remain anonymous)?

Data subject anonymously shares his preferences in a feedback form (of his employer, school, ...). When these preferences are unique, they can identify the user.

- Data subject can be identified by linking data to previously obtained data (from same or other source).
- Likelihood depends on previous knowledge of the organization.
- The data subject is not necessarily the sender.
- Combining several data items can lead to identification.
- Identifying credentials (I) and actions (II) are subtypes of this threat.
How it works

Take turns discussing each LINDDUN GO card

“Achieve thoroughness and reproducibility by applying security and privacy knowledge in a structured manner.”

- Threat Modeling Manifesto pattern
  Systematic Approach

The outcomes of threat modeling are meaningful when they are of value to stakeholders.”

- Threat modeling Manifesto principle

Document all identified threats
Theory into practice

Use successfully field-tested techniques aligned to local needs, and that are informed by the latest thinking on the benefits and limits of those techniques.

-Threat Modeling Manifesto pattern
From LINDDUN to LINDDUN-ML
PROJECT BACKGROUND

- Fraud detection & prediction
- Behavioural analysis
- Soft agile
THE VERY FIRST THING

Motivate stakeholders!

Explain what the purpose is and what they can expect
ADAPTATION OF LINDDUN

New threats & categories:

- Technical ML
- Ethics
- Accessibility
- Security ML

Linkability
Identifiability
Non-repudiation
Detectability
Disclosure of Information
Unawareness
Non-compliance
THE QUESTION APPROACH

- Brings focus
- Facilitates curiosity
- Facilitates engagement
- Easier to identify decisions
- Exchange information
THE RESULT

A Library

with new ML threats and categories &
with scenarios, elicitation questions & proposed mitigation measures
HOW DID WE MODEL THE PROCESS?
Simple!

<table>
<thead>
<tr>
<th>SAS</th>
<th>CRISP-DM</th>
<th>ASUM-DM</th>
<th>TDSP</th>
<th>MDM</th>
<th>Our DFD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask</td>
<td>Business Understanding</td>
<td>Analyze</td>
<td>Business Understanding</td>
<td>Problem formulation</td>
<td>Design</td>
</tr>
<tr>
<td>Prepare data</td>
<td>Data understanding</td>
<td>Design</td>
<td>Data acquisition &amp;</td>
<td>Data preparation</td>
<td>Input</td>
</tr>
<tr>
<td>Explore</td>
<td>Data preparation</td>
<td></td>
<td>understanding</td>
<td>Data understanding</td>
<td></td>
</tr>
<tr>
<td>Model</td>
<td>Modeling</td>
<td>Configure &amp; build</td>
<td>Modeling</td>
<td>Model assembly</td>
<td>Modeling</td>
</tr>
<tr>
<td></td>
<td>Evaluation</td>
<td></td>
<td></td>
<td>Model audit</td>
<td></td>
</tr>
<tr>
<td>Implement</td>
<td>Deployment</td>
<td>Deploy Operate &amp; Optimize</td>
<td>Deployment</td>
<td>Model delivery</td>
<td>Output</td>
</tr>
<tr>
<td>Act</td>
<td></td>
<td></td>
<td></td>
<td>Maintaining &amp;</td>
<td></td>
</tr>
<tr>
<td>Evaluate</td>
<td></td>
<td></td>
<td></td>
<td>decommissioning</td>
<td></td>
</tr>
</tbody>
</table>

SAS: Analytics Lifecycle, SAS Institute
CRISP-DM: Cross-industry standard process for data mining, ESPRIT
ASUM-DM: Analytics Solutions Unified Method, IBM
TDSP: Team Data Science Process, Microsoft
MDM: Model Development Process, Przemyslaw Biecek
HOW DID WE PUT IT IN PRACTICE?

Slides, video conference tool and taking notes :-}
Output

1. Will the output be used as input or will other sources of data be used?
2. Is human intervention needed?
3. Can the output have a negative impact for the organisation, individual and/or certain groups?
4. Can the output be linked to personal data?
A group of privacy champions is being trained in threat modeling
EXAMPLES OF IDENTIFIED THREATS

Does the model need to be explainable?
Avoid rework!

Do you use the output to feed the model?

Review the process!
FEEDBACK

“It is a journey that help us to be better, to improve processes, to keep sharp and focused. The whole organisation benefits from it and not only the project we are threat modelling”

“We have seen things we had not seen otherwise”

“It brings focus, the feeling we are working together towards a goal. We learn from the perspectives from others. And in the meantime risks are being documented”
NEXT STEPS

• Should we add Impact/Likelihood?
• How to prioritise risks? based upon session input?
• Should we assign a risk owner per threat or sprint?
• Should we establish some privacy acceptance criteria?
• Create a register of threats/status/owner
OPEN QUESTIONS

- Could we threat model feature selection?
- Is a privacy officer needed?
LESSONS LEARNED

- Avoid duplication of questions
- Facilitator is needed to guide discussion
- Online is more difficult to give voice to all participants
- Max. 2 hours per session
BENEFITS

• Improve processes - Maturity level
• Threats are effectively elicited and documented
• Bring focus and reduces endless discussions
• Reduce amount of rework
• Improve collaboration
• Output can be used to feed DPIA
Machine meets the human: by applying privacy threat modelling to ML we have learned to humanize the machine. The combination of human and machine learning benefits the creation of safe, respectful and privacy friendly products.
NO THREAT, NO SWEAT:
Privacy Threat Modeling in Practice
- a Machine Learning Use -

THANK YOU

GET IN TOUCH

Kim Wuyts
@wuytski
https://www.linkedin.com/in/kwuyts/

Isabel Barberá
@IsabBarb
https://www.linkedin.com/in/isabelbarbera/