LINDDUN GO, Lightweight & Gamified Privacy Threat Modeling

European Cybersecurity Competence Centre (ECCC) ECCO

Community Group on Human Factors

23 July 2024

European Cybersecurity Competence Centre (ECCC) ECCO

Community Group on Human Factors

Kai Rannenberg / Narges Arastouei

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

Objectives

- Build a community of experts and "end users" for the WG domain by initiating work on a sequence of prioritized topics in the WG domain
- Support selected actions prioritised in the ECCC Strategic Agenda matching the WG domain, especially within
  - 1.1.4 Ensure the availability of easily accessible and user-friendly cybersecurity tools for SMEs
  - 1.2.3 Promote security and privacy 'by design'
  - 2.1.4 Promote security and privacy 'by design' approach in training and education

Methodology

- Start with actions related to one or several of the topics listed in the ECCO technical offer:
  - 5G applications, ICT in mobility, security of day-to-day tools like smartphones, web meeting systems and services, Internet access technologies, digital money.
- Deep dive on proposals for priorities for DEP or other appropriate support measures
- Build sub-groups as needed
- …

Matching: ECCC Strategic Agenda actions Topics from Technical Offer

Action/Topic	1.1.4 Ensure the availability of easily accessible and user-friendly cybersecurity tools for SMEs	1.2.3 Promote security and privacy 'by design'	2.1.4 Promote security and privacy 'by design' approach in training and education
5G applications			
ICT in mobility			
Security of day-to-day tools, e.g.			
Smartphones			
Web meeting systems and services			
Internet access technologies			
Digital money			
…			
…			

Work on topics within the matrix prioritized by the community of experts and "end users"

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

Activities and deliverables

- Identification of relevant achievements / best practices (e.g. developed in the ECCC pilots) to address the Strategic Agenda
  - 1st webinar (March 8): **A Footprint of CyberSec4Europe: two prominent cybersecurity tools (Keynotes: Vashek Matyas et al, Masaryk University Brno, CZ)**
  - 2nd webinar (May 22): **Security-by-design for SMEs exploiting trusted hardware (Keynote: Antonio Lioy, Politecnico di Torino, IT)**
  - **3rd webinar (19 June): Engaging Citizens and Civil Society in Cybersecurity (Dr. Michael Friedewald, Fraunhofer Institute for Systems and Innovation Research)**
  - **Today's webinar (23 July): LINDDUN GO, Lightweight & Gamified Privacy Threat Modeling (by Jonah Bellemans at the DistriNet Research Group of KU Leuven (Belgium)).**

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

Activities and deliverables

- Recommendations for future specific priority "Joint Actions" (e.g. DEP projects) and other actions for the ECCC
  - Based on matching of goals with action types also considering the ECCC action plan
- Possible cooperation in immediate Joint Actions
  - Deep dive on specific topics: e.g. stemming from the needs of SMEs for easily accessible and user-friendly cybersecurity tools considering privacy
- Knowledge sharing events: presentations for EC, NCCs, ECCC
  - Webinars on the progress including refinement of the topics

ECCO
European Cybersecurity COmmunity

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

How to join the CG

- Email: community_humanfactors-owner@list.cyber-ecco.eu with your
  - Contact details
  - Affiliation and role therein
  - Area of expertise

Keynote & Speaker

- **LINDDUN GO, Lightweight & Gamified Privacy Threat Modeling**

Privacy threat modeling plays an important role in the implementation of software according to the principle of privacy by design. However, performing an exhaustive and thorough analysis using methods such as LINDDUN PRO (per-interaction) is a time- and resource-intensive endeavour. To meet increasing demand from practitioners for more accessible methods with a lower barrier to entry, LINDDUN GO was developed. This lightweight 'flavour' of LINDDUN strives to draw a wider audience into privacy threat modeling by distilling the framework into a narrowed down set of concrete threats and representing the information with a deck of custom-made playing cards. The cards can be used to 'play' through a threat modeling session according to a set of rules, or simply serve as inspiration for the threat modeler.

- **Keynote Speaker: Jonah Bellemans**
  - He is a doctoral researcher at the DistriNet Research Group of KU Leuven (Belgium). As a key member of the team that develops the renowned LINDDUN privacy threat modeling framework, his work primarily focuses on privacy engineering in the early stages of software development, with specific attention to the interplay between software engineering methods and techniques, and the diverse regulatory aspects. Jonah holds a degree in both Computer Science Engineering and IT & IP Law.

ECCO
European Cybersecurity COmmunity

ECCO Community-driven Knowledge Sharing Events

Disclaimer

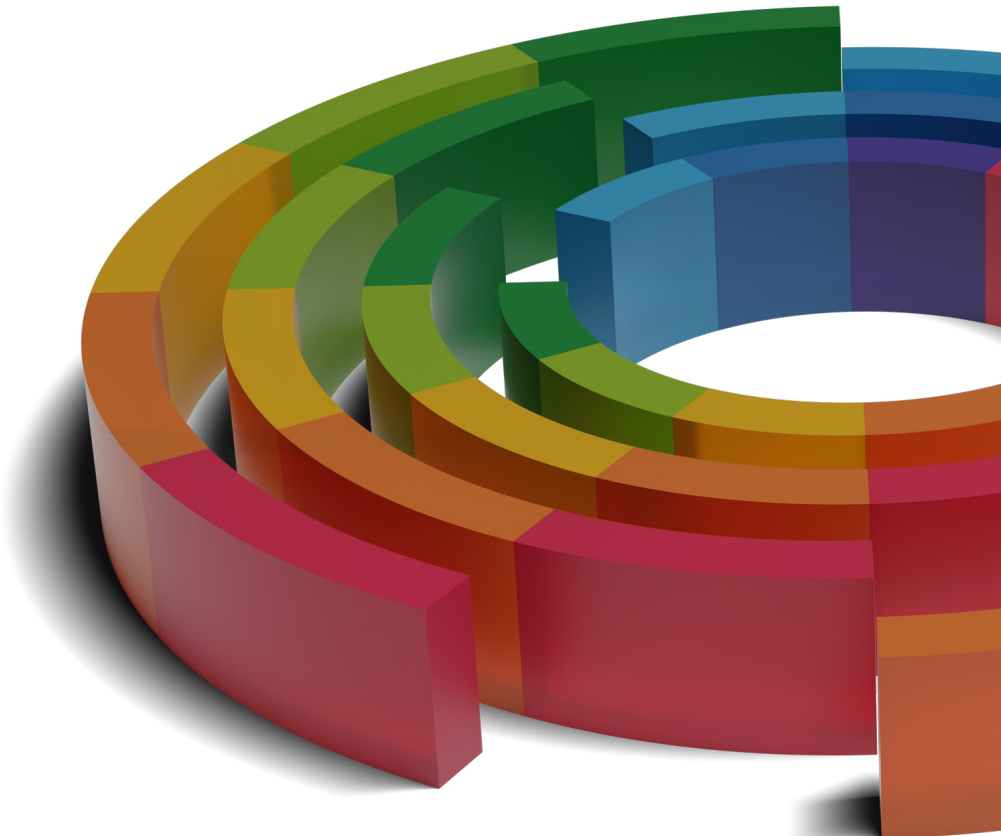
- *These sessions are ECCOcommunity-driven and expert-led, reflecting the collective knowledge and contributions of the members of the ECCO Community Groups. They are designed as knowledge-sharing events to build/animate the cybersecurity Community Groups on key topics and share valuable insights among stakeholders.*
- *The information and opinions in this document are provided "as is" for general purposes only.*
- *Experts are encouraged to ensure their presentations are accurate and up-to-date.*
- *The views expressed in this webinar are purely those of the experts and may not, in any circumstances, be interpreted as stating an official position of the European Commission (EC), the European Cybersecurity Competence Centre (ECCC), the ECCO project, or any other EU institution, body or agency. The European Commission does not guarantee the accuracy of the information included in this webinar, nor does it accept any responsibility for any use thereof.*
- *References to specific commercial products, processes, or services do not imply endorsement or recommendation, and this webinar should not be used for advertising purposes.*

LINDDUN GO

Lightweight and Gamified Privacy Threat Modeling

Jonah Bellemans – Distrinet Research Group, KU Leuven – 23 July 2024

Introduction



WHAT IS THREAT MODELING?

Analyzing representations of a system to highlight concerns about security and privacy characteristics

- Threat Modeling Manifesto

Tackled proactively

Systematically analyzed

Integrated in the development lifecycle

Have an impact on design decisions

LINDDUN

- **Supports** addressing **privacy threats** early in the development lifecycle
- Comprehensive **knowledge** base of **privacy threat** characteristics
- Rich set of (100+) concrete threat **examples** and **cases**
- **Aligned** with security threat modeling approaches (e.g. **STRIDE)**

www.linddun.org

ECCO
European Cybersecurity COmmunity

LINDDUN GO

FOR LEAN PRIVACY ANALYSIS

LINDDUN PRO

FOR SYSTEMATIC PRIVACY ANALYSIS

LINDDUN MAESTRO

FOR MODEL-DRIVEN ANALYSIS

ECCO
European Cybersecurity COmmunity

LINDDUN GO

FOR LEAN PRIVACY ANALYSIS

Lightweight & accessible

For low-risk applications, or as introduction to privacy threat modeling

LINDDUN PRO

FOR SYSTEMATIC PRIVACY ANALYSIS

Systematic & exhaustive

For higher-risk applications, supported with tooling

LINDDUN MAESTRO

FOR MODEL-DRIVEN ANALYSIS

Systematic & exhaustive

More extensive and complex system models enriched with additional information

LINDDUN Adoption

Institutions & Standards

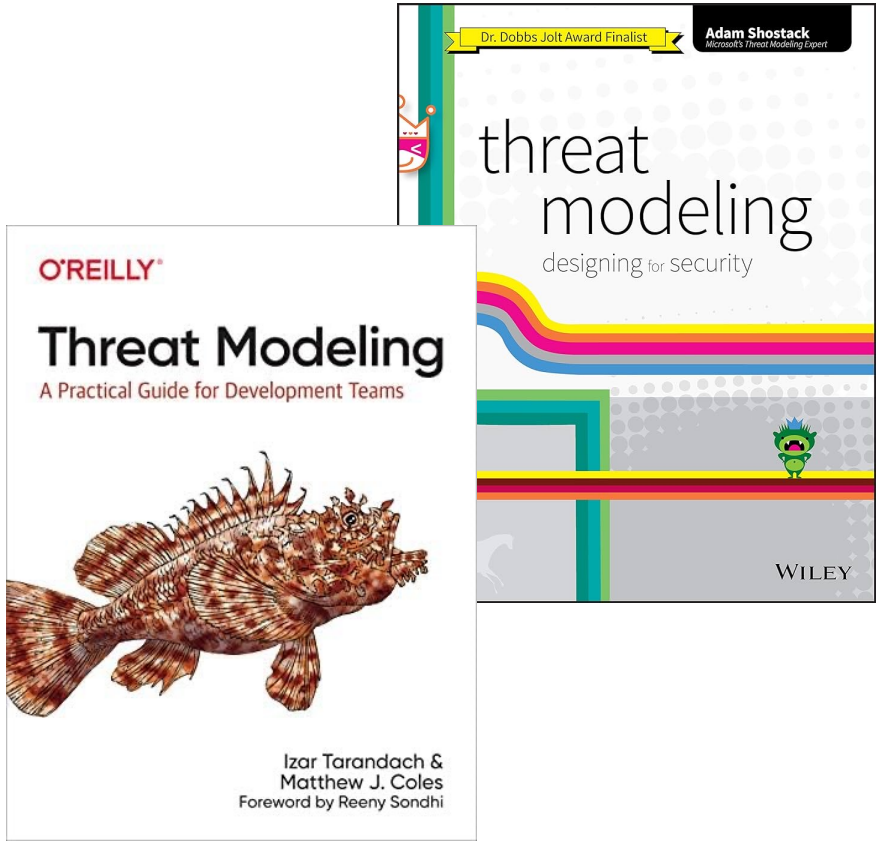
ENISA

ISO/IEC 27550

EDPS Opinion 5/2018

NIST Privacy Framework

Books



[1] Shostack, A. 'Threat Modeling. Designing for Security', 2014, ISBN 978-1118809990
[2] Tarandach, I. and Coles, M. J. 'Threat Modeling – A Practical Guide for Development Teams', 2020, ISBN 978-1492056553

LINDDUN Adoption

Received 19 January 2024, accepted 28 January 2024, date of publication 1 February 2024, date of current version 8 February 2024.
Digital Object Identifier 10.1109/ACCESS.2024.3360864

SURVEY

On the Evaluation of Privacy Impact Assessment and Privacy Risk Assessment Methodologies: A Systematic Literature Review

SAMUEL WAIRIMU[1], LEONARDO HORN IWAYA[1], (Member, IEEE), LOTHAR FRITSCH[1,2], AND STEFAN LINDSKOG[1]
[1]Privacy and Security (PriSec) Research Group, Department of Mathematics and Computer Science, Karlstad University, 651 88 Karlstad, Sweden
[2]Department of Computer Science, Faculty of Technology, Art and Design, Oslo Metropolitan University, 0130 Oslo, Norway
Corresponding author: Samuel Wairimu (samuel.wairimu@kau.se)

This work was supported in part by Region Värmland, Sweden, through the Digital Health Innovation (DHINO) Project under Grant RUN/220266; and in part by the Vinnova via the DigitalWell Arena Project under Grant 2018-03025.

ABSTRACT Assessing privacy risks and incorporating privacy measures from the onset requires a comprehensive understanding of potential impacts on data subjects. Privacy Impact Assessments (PIAs) offer a systematic methodology for such purposes, which are closely related to Data Protection Impact Assessments (DPIAs), particularly outlined in Article 35 of the General Data Protection Regulation (GDPR). The core of a PIA is a Privacy Risk Assessment (PRA). PRAs can be integrated as part of full-fledged PIAs or independently developed to support PIA processes. Although these methodologies have been identified as essential enablers of privacy by design, their effectiveness has been criticized because of the lack of evidence of their rigorous and systematic evaluation. Hence, we conducted a Systematic Literature Review (SLR) to identify published PIA and PRA methodologies and assess how and to what extent they have

*"Our analysis of PTMs shows that **LINDDUN has emerged as the most evolved research method** based on the published improvements of the method."*

Requirements Engineering (2023) 28:177–194
https://doi.org/10.1007/s00766-022-00382-8

ORIGINAL ARTICLE

Check for updates

Privacy requirements elicitation: a systematic literature review and perception analysis of IT practitioners

Edna Dias Canedo[1] · Ian Nery Bandeira[1] · Angelica Toffano Seidel Calazans[2] · Pedro Henrique Teixeira Costa[1] · Emille Catarine Rodrigues Cançado[1] · Rodrigo Bonifácio[1]

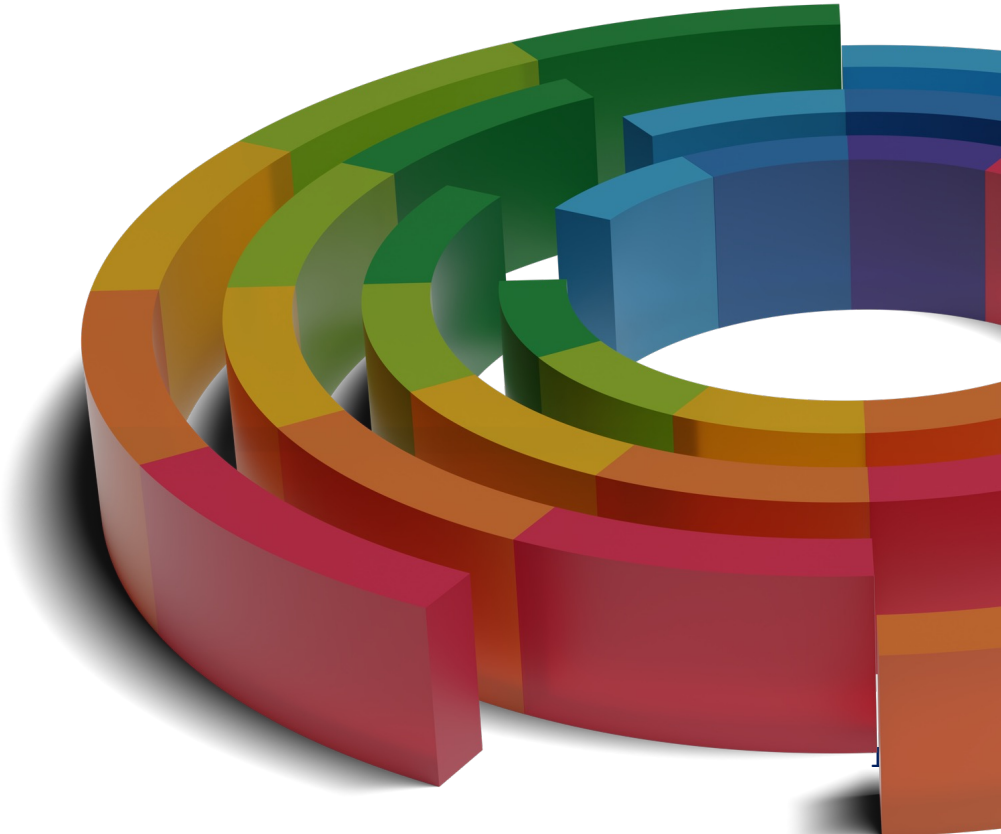
Received: 3 August 2021 / Accepted: 4 April 2022 / Published online: 11 June 2022

Abstract
During the software development process and throughout the software lifecycle, organizations must guarantee users' privacy by protecting personal data. There are several studies in the literature proposing methodologies, techniques, and tools for privacy requirements elicitation. These studies report that practitioners must use systematic approaches to specify these requirements during initial software development activities to avoid users' data privacy breaches. The main goal of this study is to identify which methodologies, techniques, and tools are used in privacy requirements elicitation in the literature. We have also investigated Information Technology (IT) practitioners' perceptions regarding the methodologies, techniques, and tools identified in the literature. We have carried out a systematic literature review (SLR) to identify the methodologies, techniques, and tools used for privacy requirements elicitation. Besides, we have surveyed IT practitioners to understand their perception of using these techniques and tools in the software development process. We have found several methodologies, techniques, and tools proposed in the literature to carry out privacy requirements elicitation. Out of 78 studies cataloged within the SLR, most of them did not verify their methodologies and techniques in a practical case study or illustrative contexts (38 studies), and less than 35% of them (26 studies) experimented with their propositions within an industry context. Th
su
a p
tec

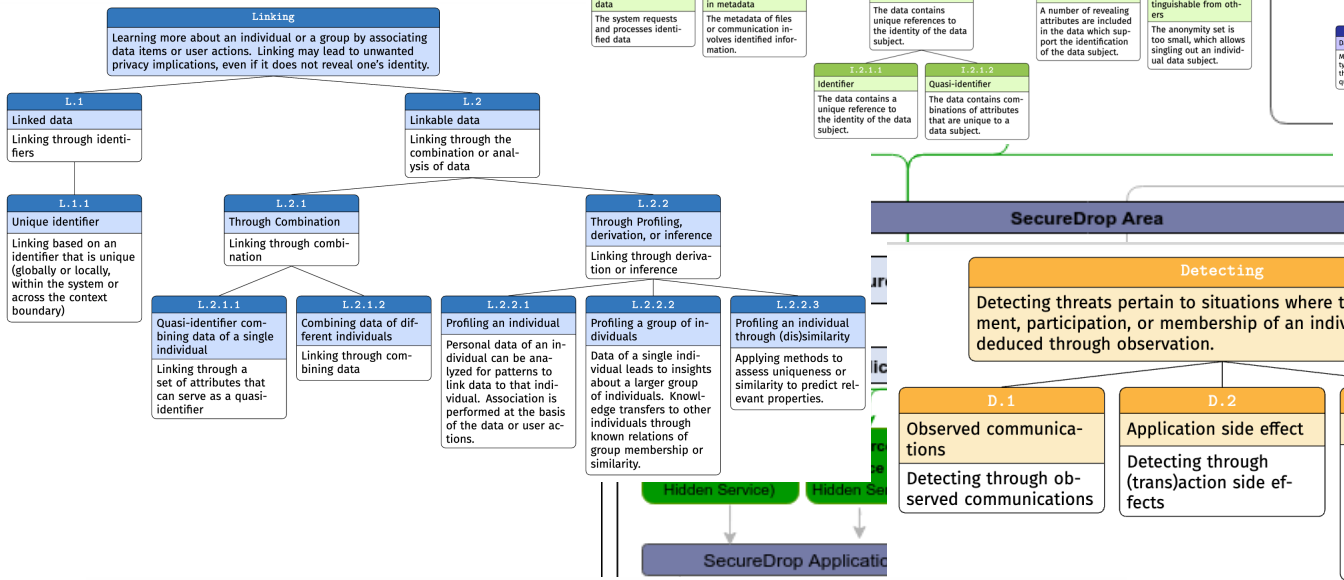
Ke

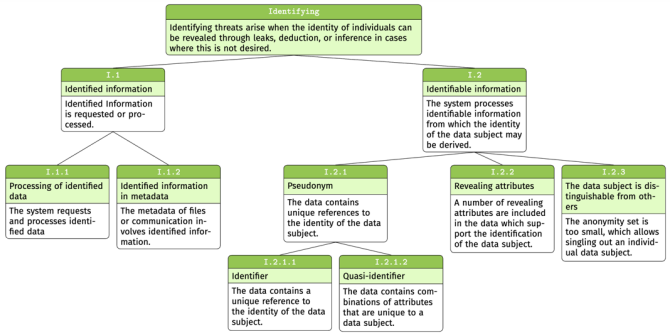
"An important finding is that the i Model and LINDDUN methodologies are **among the ten most used in the literature** and are **the two best known in the industry** by the IT practitioners in the requirements area."*

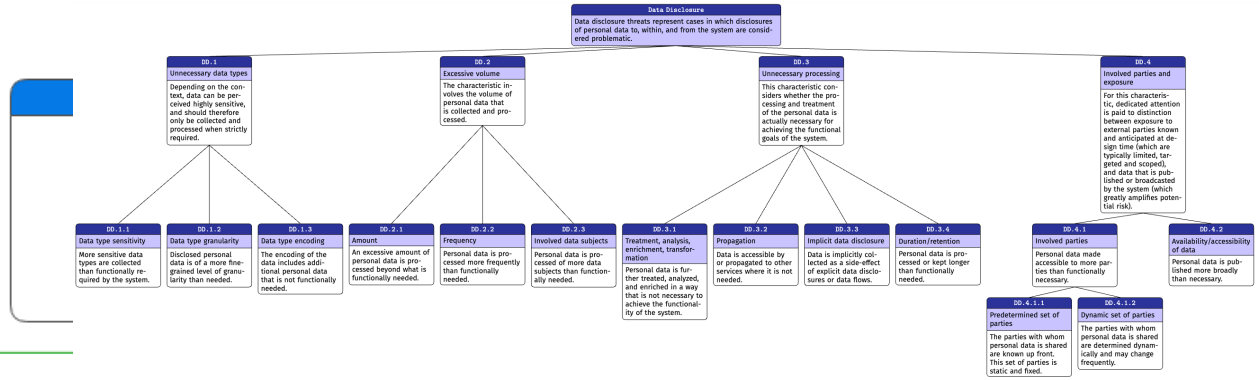
Why LINDDUN GO?

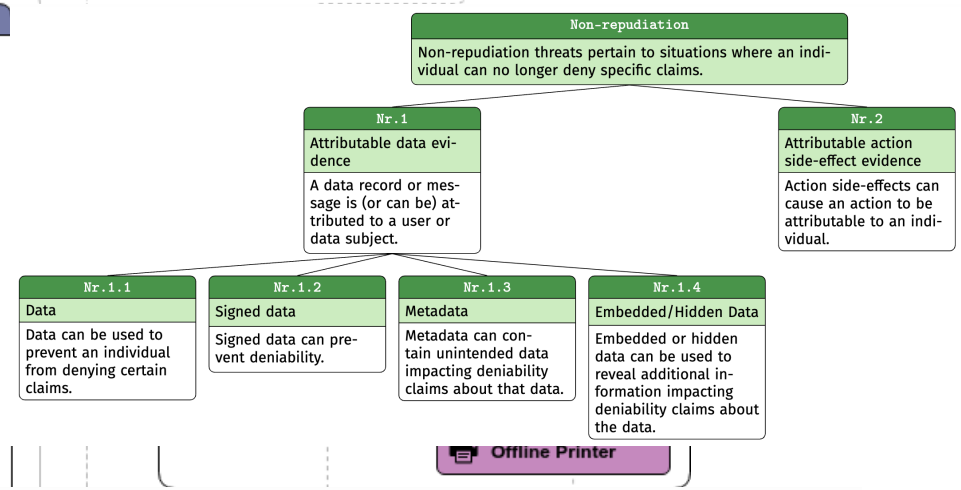


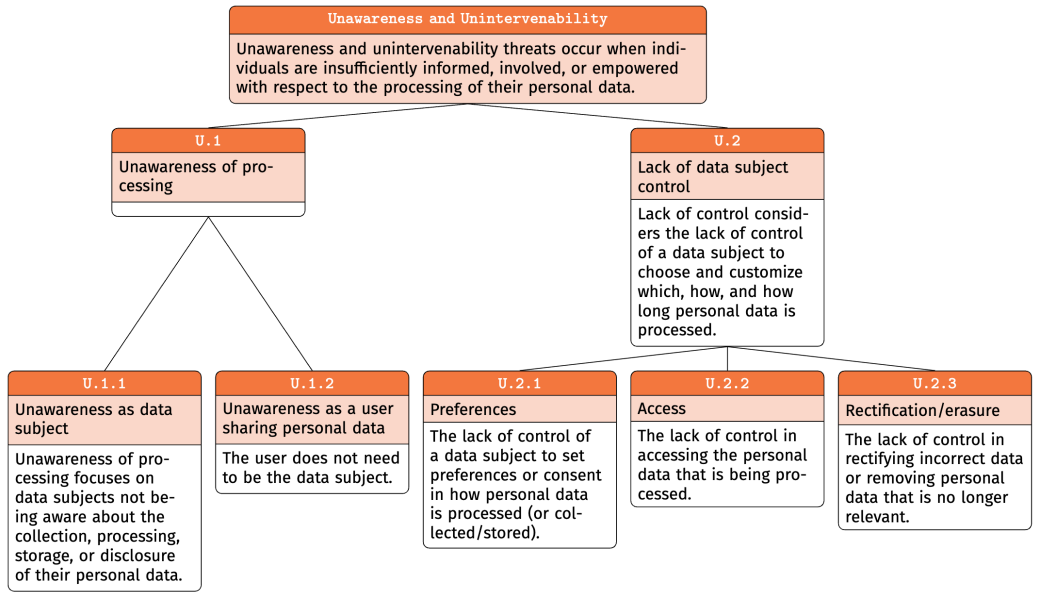
The Problen

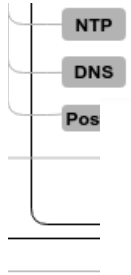


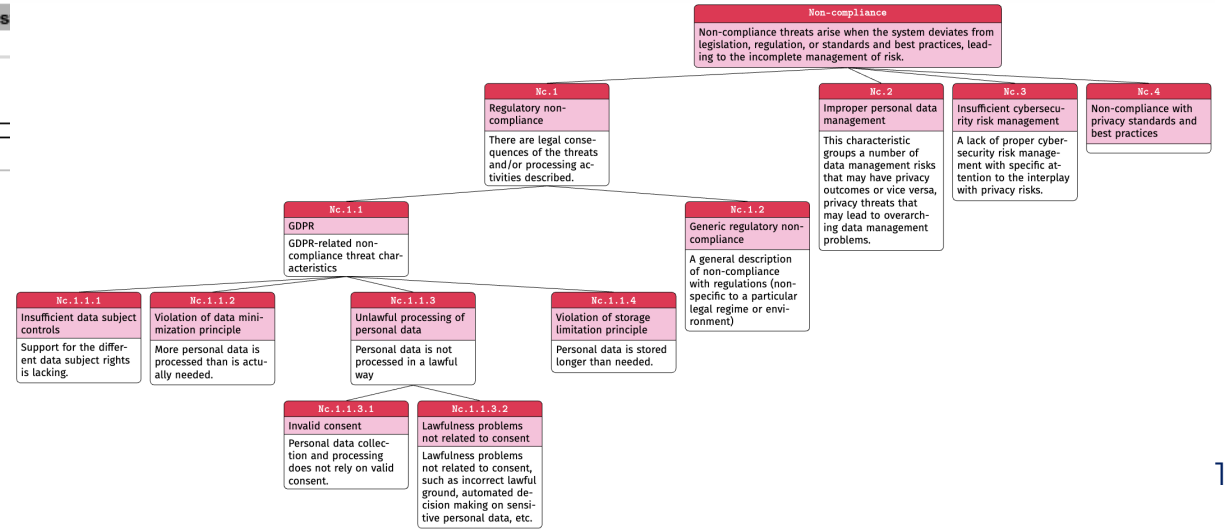












[1] Securedrop, https://docs.securedrop.org/en/stable/threat_model/dataflow.html

Lightweight

LINDDUN PRO

FOR SYSTEMATIC PRIVACY ANALYSIS

- Data Flow Diagram
- Threat Trees

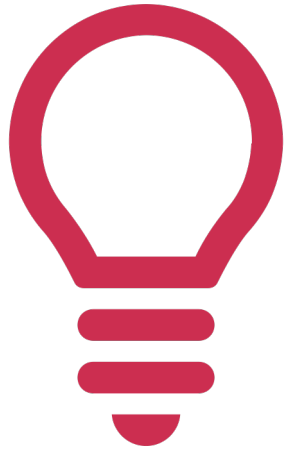
LINDDUN GO

FOR LEAN PRIVACY ANALYSIS

- Simple Sketch Suffices
- Limited set of 33 predefined threats

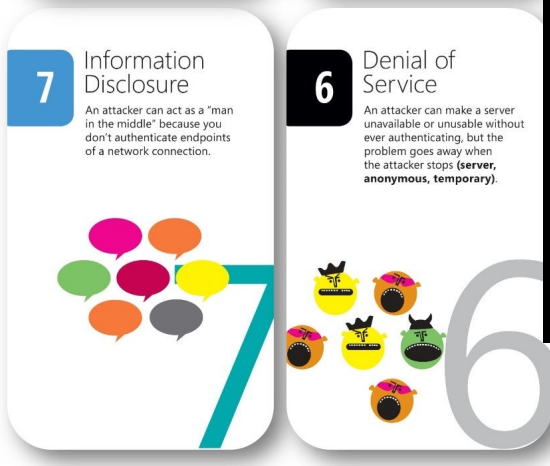
Accessible

Tangible & Clear
Threat Library



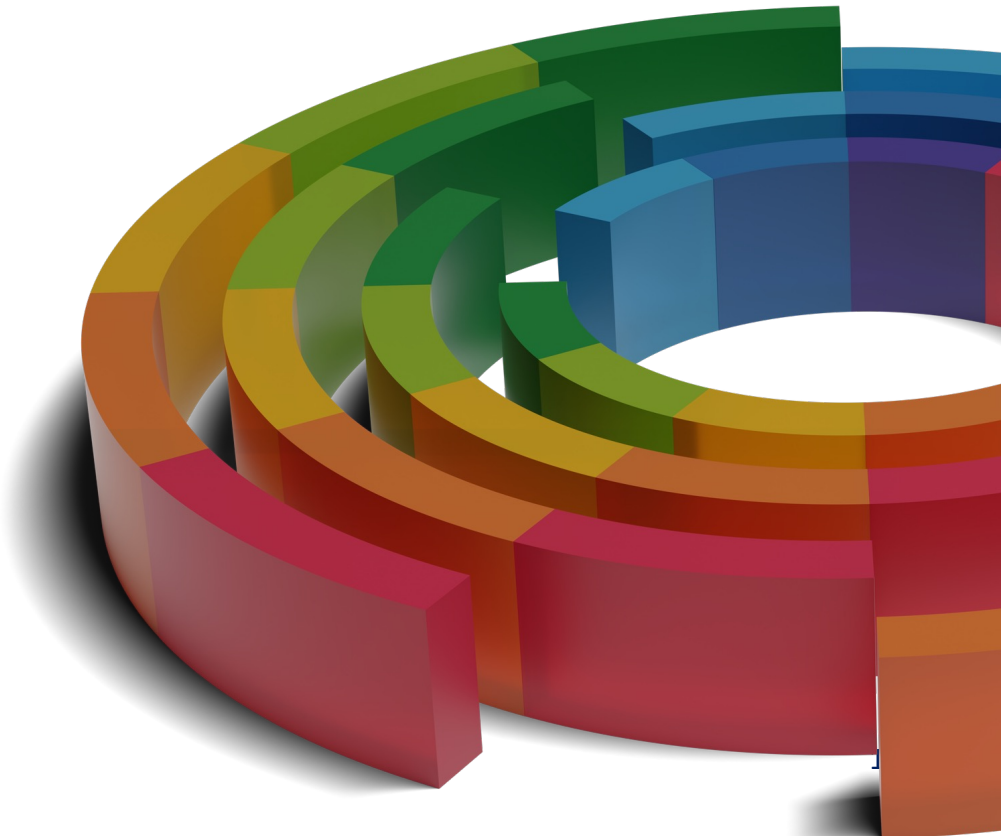
Concrete
Examples

Gamified



[1] Elevation of Privilege, https://shostack.org/games/elevation-of-privilege
[2] [d0x3d!], https://d0x3d.com/
[3] Control-Alt-Hack, https://www.controlalthack.com/

LINDDUN GO



LINDDUN GO cards

Element/ component where threat occurs in the system (~ DFD interaction + additional constraints)

Questions to check applicability

Impact/ consequences (why is it important)

Card identifier

IDENTIFIABLE DATA FLOWS

Hotspot: INBOUND PERSONAL DATA

Threat Source: ORGANIZATIONAL

Data sent to the system is sufficiently revealing to identify the user.

? Is there free-form user provided data that is received or processed by the system?
? Is data collected that may reveal the identifying information?

When an individual shares detailed data (such as location, employer, device type, etc.) in a feedback form, the provided information may be revealing enough to uniquely identify that person.

Inadvertently providing identifiable attributes in user-submitted data can lead to the unintentional identification of the individual.

The data subject is not necessarily the source of the provided data.

I3

LINDDUN

Title

Origin of threat (organizational, external)

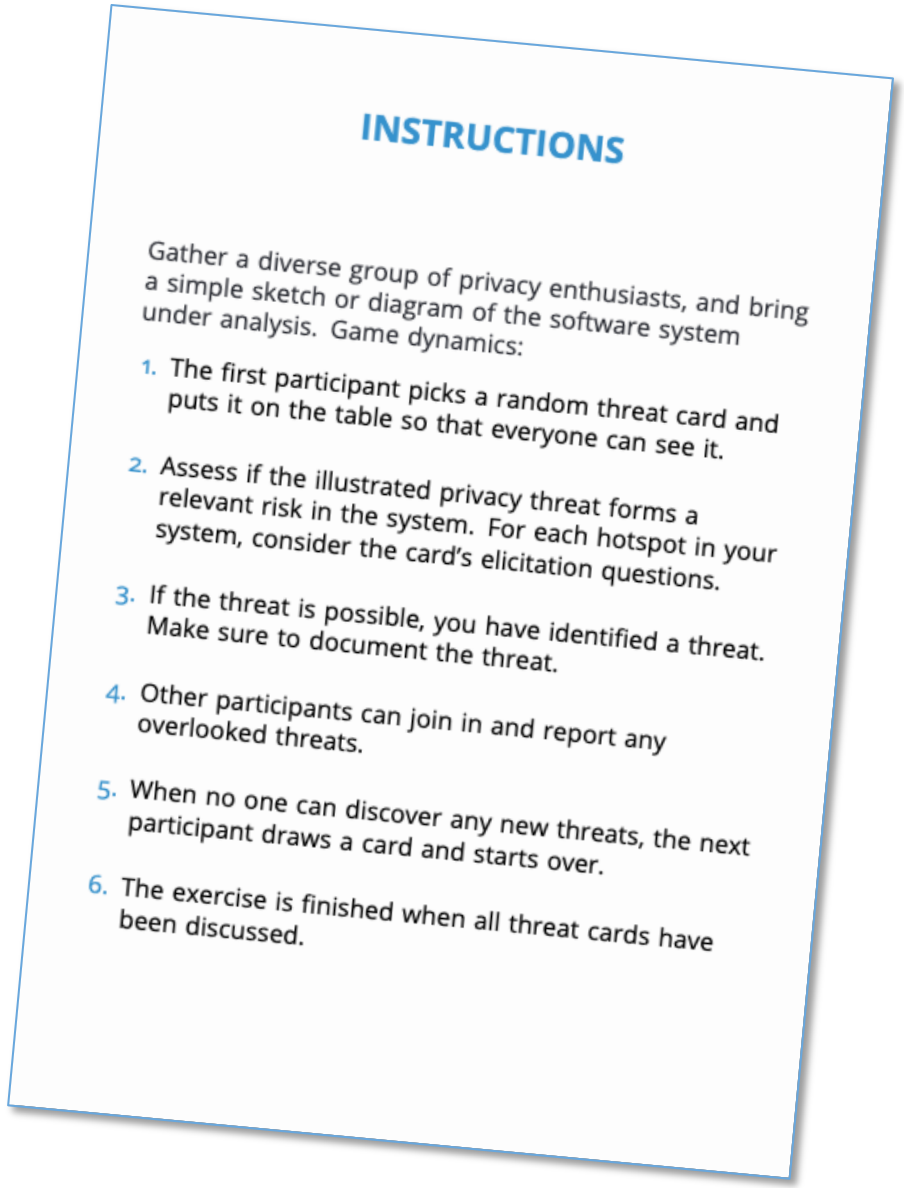
Summary

Example

Additional info

Highlighted LINDDUN type

LINDDUN GO Cards – How to play



INSTRUCTIONS

Gather a diverse group of privacy enthusiasts, and bring a simple sketch or diagram of the software system under analysis. Game dynamics:

1. The first participant picks a random threat card and puts it on the table so that everyone can see it.
2. Assess if the illustrated privacy threat forms a relevant risk in the system. For each hotspot in your system, consider the card's elicitation questions.
3. If the threat is possible, you have identified a threat. Make sure to document the threat.
4. Other participants can join in and report any overlooked threats.
5. When no one can discover any new threats, the next participant draws a card and starts over.
6. The exercise is finished when all threat cards have been discussed.

How to play ?

Gamified threat modeling in group…

or

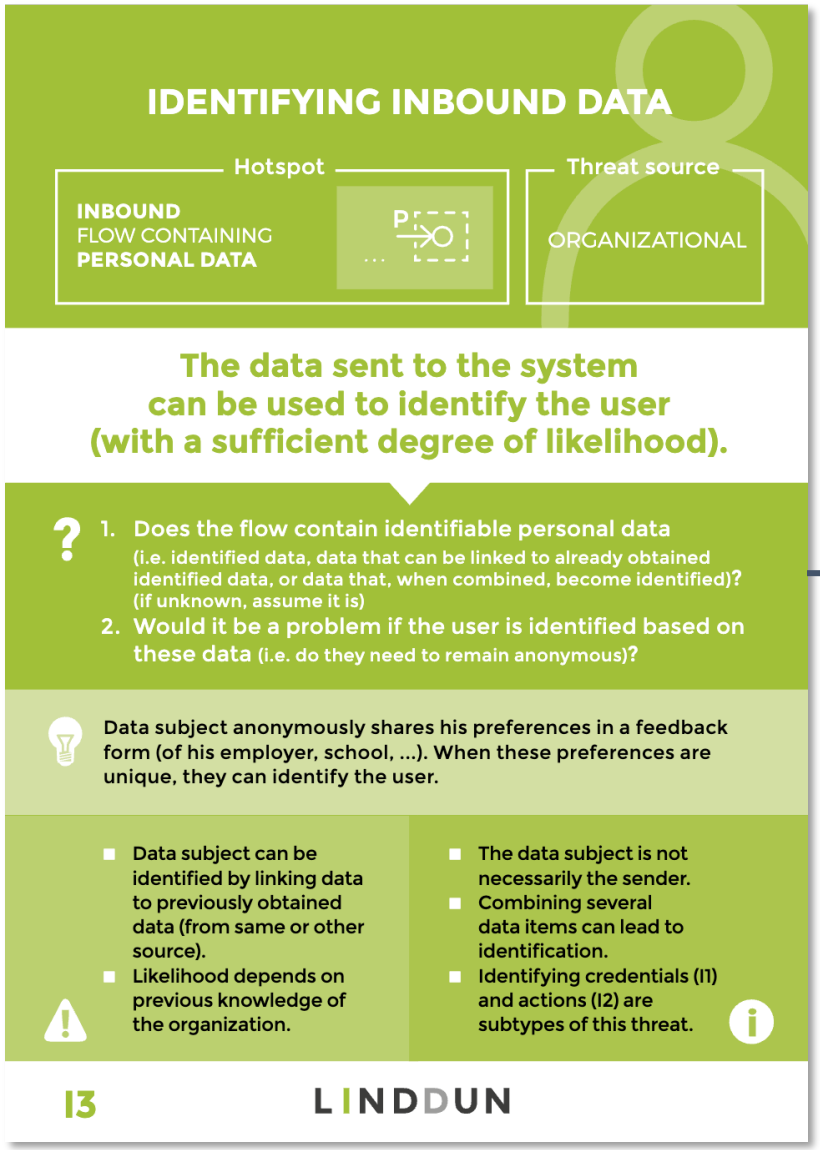
… cards serve as inspiration for (solo) threat modeler

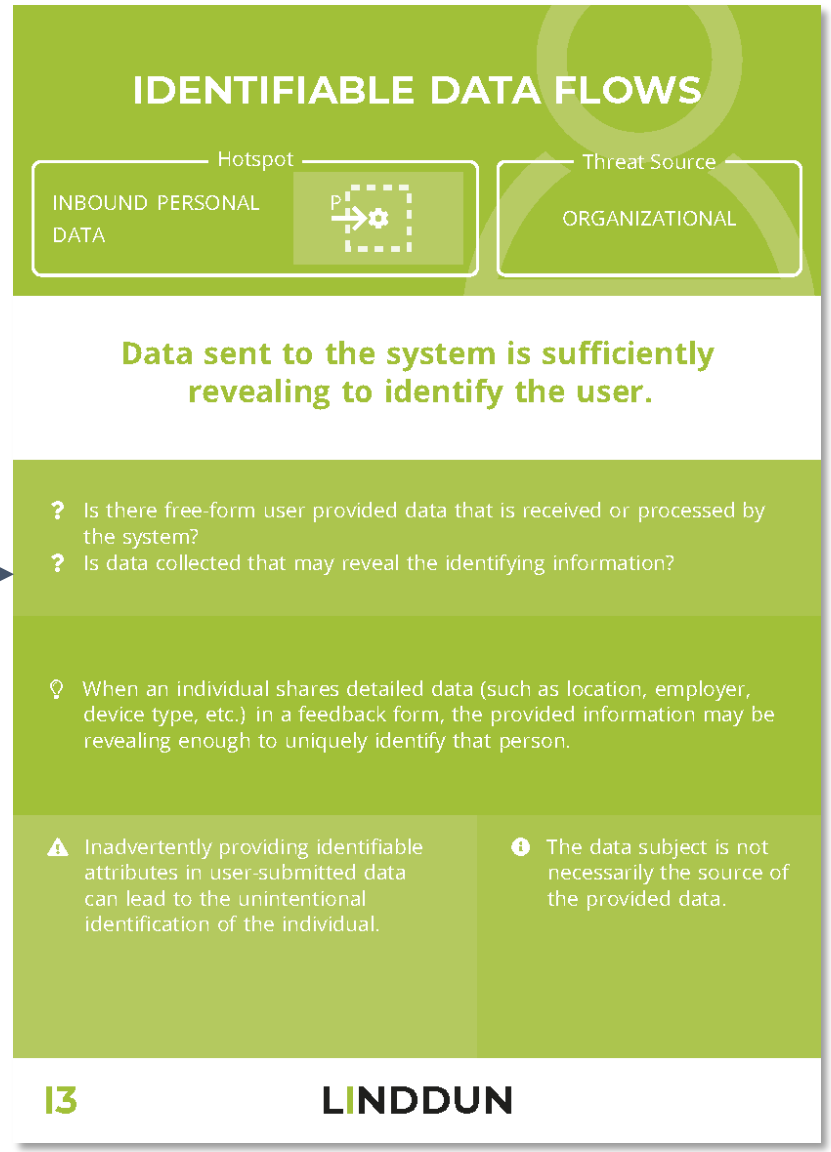
Variations

Competition

Time Pressure

LINDDUN GO Cards - Update





LINDDUN GO Cards - Update

Threat Type Cards

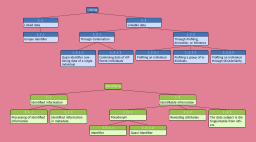
1. Short Description
2. Long Description
3. Why you should care

4. QR-code with link to more information on the website


LINKED USER DATA
Hotspot
INBOUND USER WITH PERSONAL DATA
Threat Source
ORGANIZATIONAL, EXTERNAL
The requests from a user to the system are linked through identifiers.
1. Is there an identifier (unique within the system or for the session) or dataset?
2. Is there other data associated with that identifier?
3. Is there previous data with the same identifier to which new data can be linked?
An email address as ID can be used to link all activity to the same user even across multiple services where that email address is used.
IP address can be used to link multiple visits to the same user.
All product views in a web shop are linked to the same user because they are logged in.
The use of unique identifiers enables the linking of new data items to a user profile to gather increasing amounts of personal data linked to this profile. This can later lead to identifying threats.
Linking is especially easy for authenticated users, as all requests in the same session are linked.
LINDDUN
Nc1
D1
Nr1
I1
L1

- Linking
  - L.1 Linked data
    - L.1.1 Unique identifier
  - L.2 Linkable data
    - L.2.1 Through Combination
      - L.2.1.1 Quasi-identifier combining data of a single individual
      - L.2.1.2 Combining data of different individuals
    - L.2.2 Through Profiling, derivation, or inference
      - L.2.2.1 Profiling an individual
      - L.2.2.2 Profiling a group of individuals
      - L.2.2.3 Profiling an individual through (dis)similarity

- Identifying
  - I.1 Identified information
    - I.1.1 Processing of identified information
    - I.1.2 Identified information in metadata
  - I.2 Identifiable information
    - I.2.1 Pseudonym
      - I.2.1.1 Identifier
      - I.2.1.2 Quasi-identifier
    - I.2.2 Revealing attributes
    - I.2.3 The data subject is distinguishable from others



LINDDUN Web Catalog

Linking / Linked data / Unique identifie

- **LINKING** (2)
  - Linked data (1)
    - Unique identifier
  - Linkable data (2)
- **IDENTIFYING** (2)
- **NON-REPUDIATION** (2)
- **DETECTING** (3)
- **DATA DISCLOSURE** (4)
- **UNAWARENESS AND UNINTERVENABILITY** (2)
- **NON-COMPLIANCE** (3)

Unique identifier

Description

Linking based on an identifier that is u

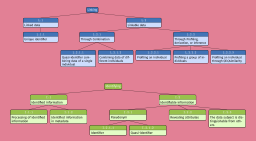
Unique identifiers make it trivial to link
interactions with a system) as belongi

Examples

- **Email address as ID**

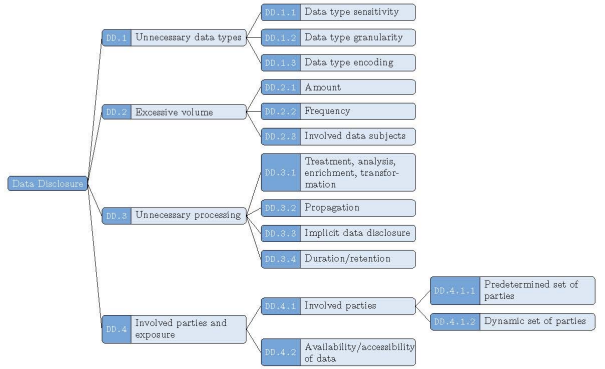
  An email address as ID can be used t
  address is used.

  Many services frequently rely on emai
  different services on which they use t



1 Data Disclosure

This threat tree concerns threats involving the excessive/unnecessary collection or disclosure of personal data. Personal data may be collected explicitly and intentionally as part of the system design, but also may implicitly collected as a side-effect of these data disclosures or data flows. These implicit data flows and disclosures must be investigated in an identical manner to explicit data flows.



DD.1 Unnecessary data types Depending on the context, data can be perceived highly sensitive, and should therefore only be collected and processed when strictly required.

DD.1.1 Data type sensitivity More sensitive data types are collected than functionally needed by the system.

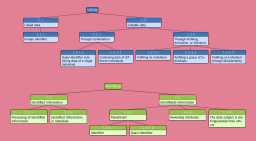
Examples:

Patient health monitoring: Tracking a patient's weight is relevant for dieting app but not for a contact tracing application.

DD.1.2 Data type granularity Personal data of a fine-grained level of granularity is dislosed than needed.

Examples:

Smart meter: A smart meter shares realtime measurements rather than the aggregated consumption.



LINDDUN Web Catalog

Linking / Linked data / Unique identifier

- LINKING (2)
  - Linked data (1)
    - Unique identifier
  - Linkable data (2)
- IDENTIFYING (1)
- NON-REPUDIATION (2)
- DETECTING (3)
- DATA DISCLOSURE (4)
- UNAWARENESS AND UNINTERVENABILITY (2)
- NON-COMPLIANCE (3)

Unique identifier

Description

Linking based on an identifier that is u

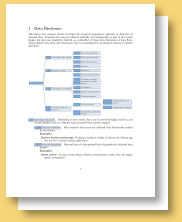
Unique identifiers make it trivial to link interactions with a system) as belonge

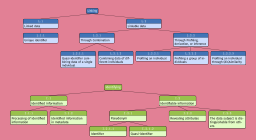
Examples

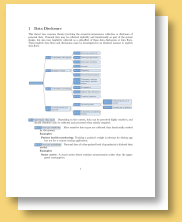
- Email address as ID

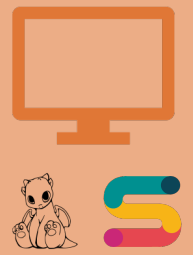
An email address as ID can be used t address is used.

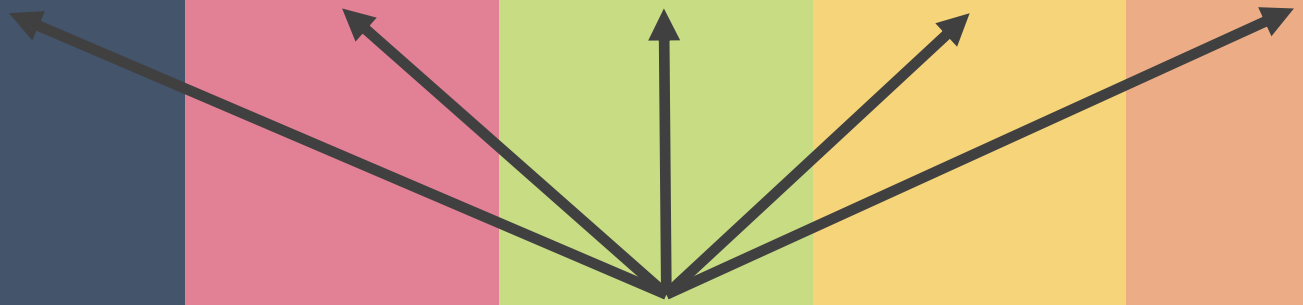
Many services frequently rely on ema different services on which they can't







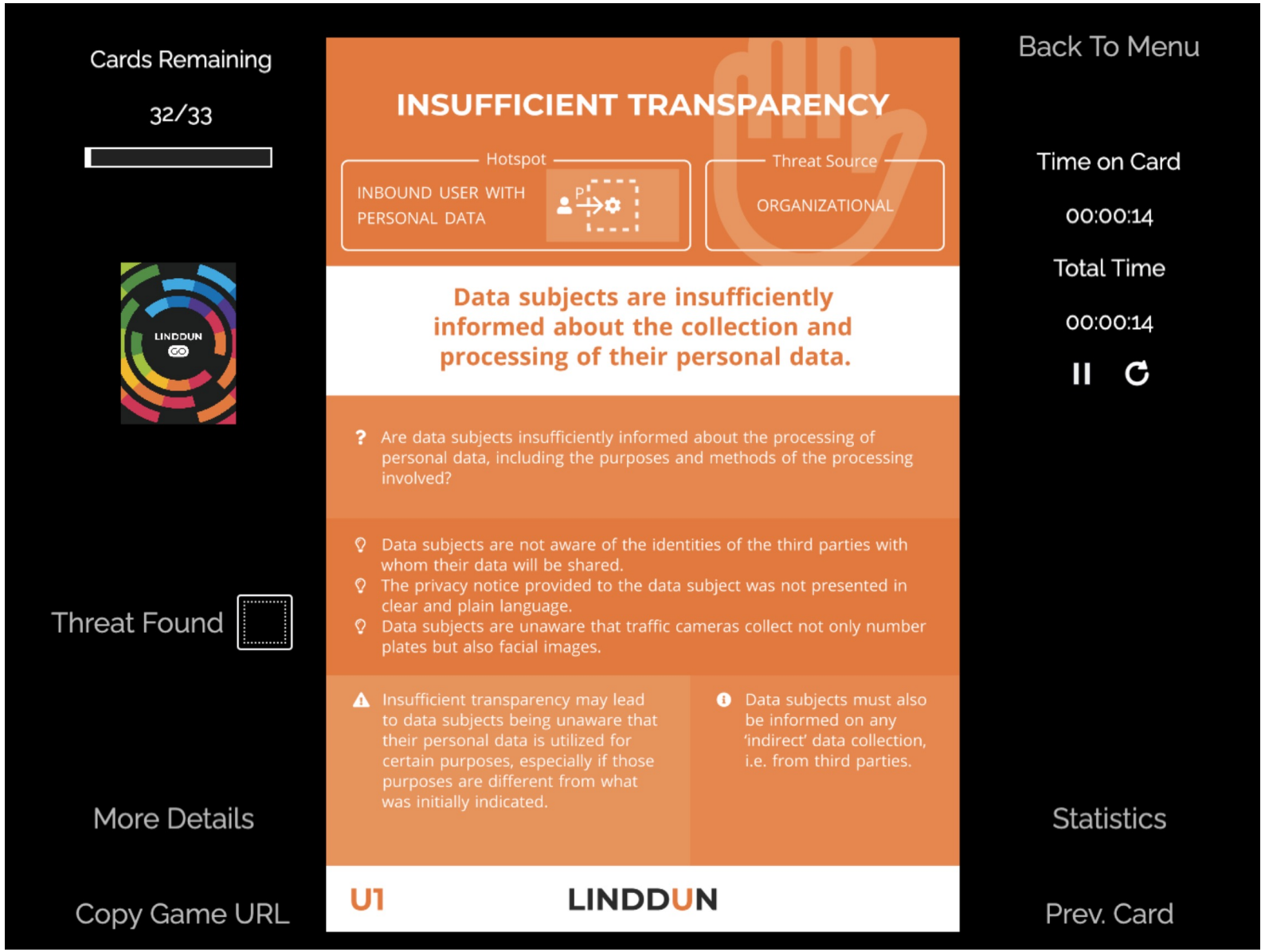




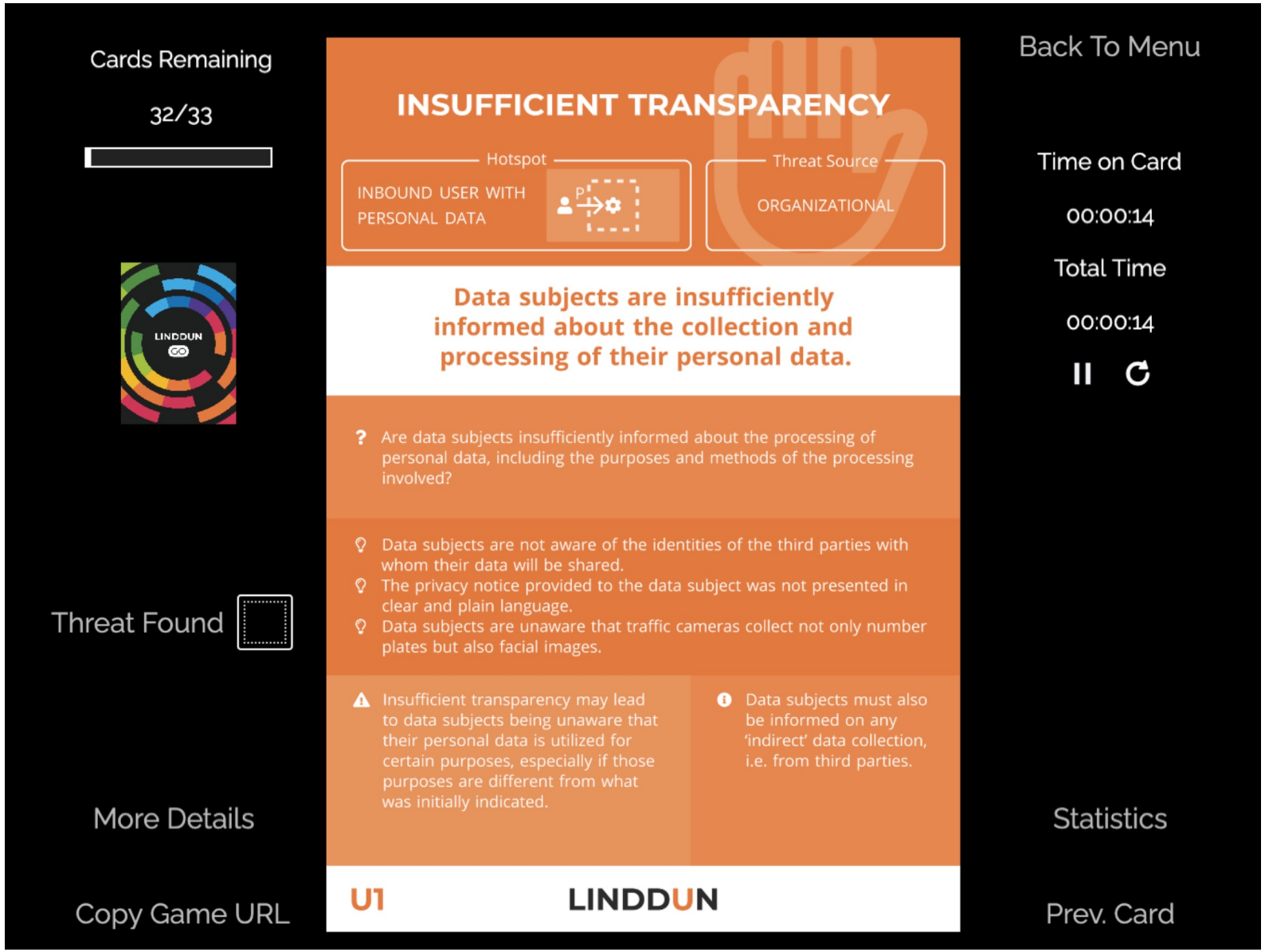
ECCO
European Cybersecurity COmmunity

LINDDUN

LINDDUN GO Digital



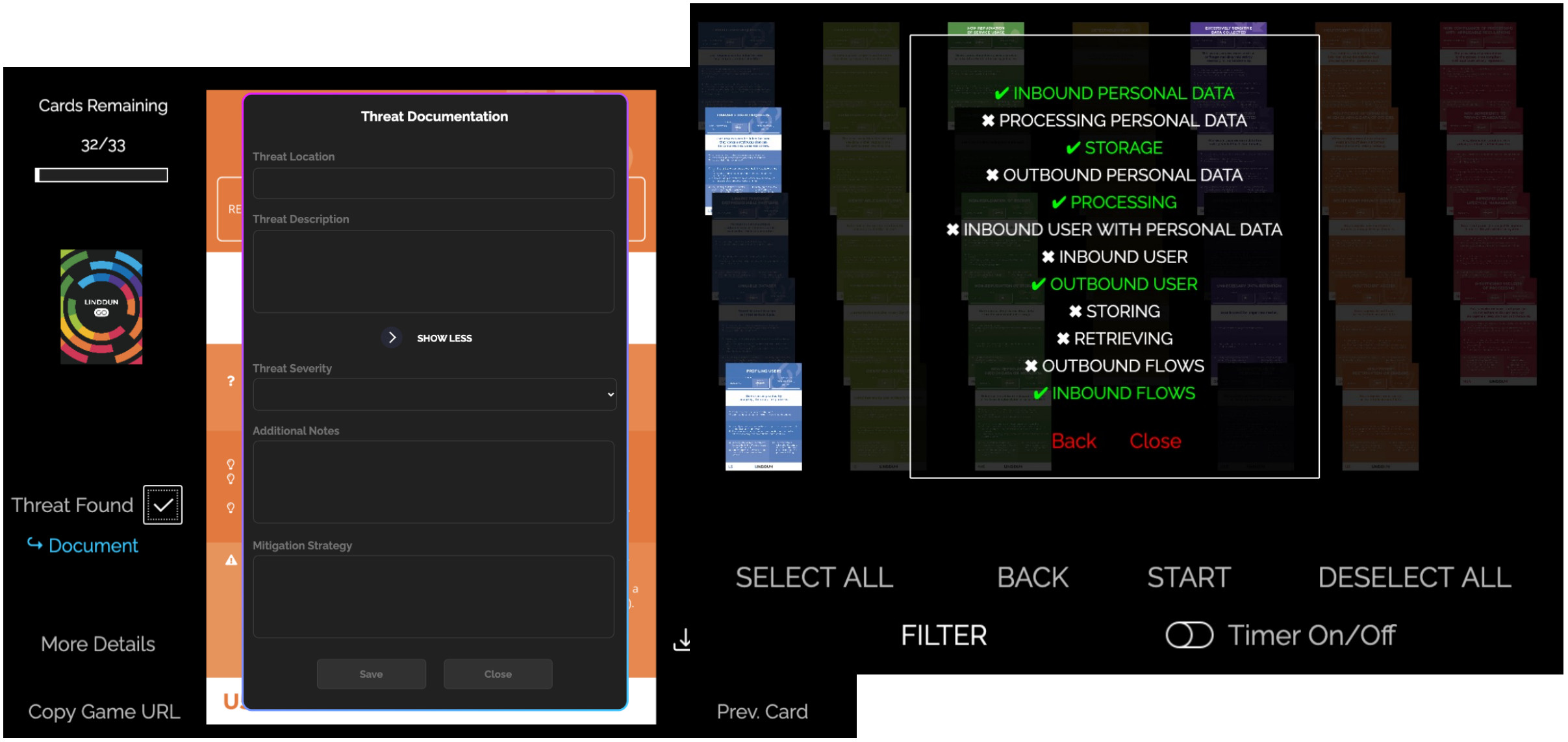
LINDDUN GO Digital



Features include:

- Interactive card library
- Choose which cards to play with
- Time keeping
- Document threats as you go
- Export documented threats
- Save and share progress
- Get additional information by clicking on a card element

LINDDUN GO Digital



Templates – Documenting

LINDDUN GO Threat Tracker

Introduction

Welcome to the LINDDUN GO Threat Tracker!

You can use this document to note down any threats you have elicited during your LINDDUN GO threat modeling session.
This tutorial explains the purpose of each tab in the document, as well as some tips and tricks on how to use it.

You can find more information about LINDDUN GO on our website: https://linddun.org.

How to use this document

Eliciting threats
separate system

For each step, th

Step 1. Sketch th
Step 2. Elicit app
Step 3. Follow-u

Important! Threa
It is important th
'mitigation track
sure that this do

Tab Explanati

System Information	The threat modeling process starts with creating a sketch of the system you want to assess. This tab helps you with this by providing a s the system itself. If you have one, you can also add a sketch of the design to this tab so that the reader of this document can find back l
Identified Threats	This is the tab of the document used for the main event in the process. Here, you can write down any threats you have identified by sele the appropriate column, and filling out the details of the threat in the other fields. For every threat you spot, you fill out one row in the populate itself based on the choice you made it in the dropdown. **Note:** it is possible to find multiple occurrences of the same threat in different places within the system! In this case, you have to note tackling all of them at once. **Note:** estimating the (potential) impact of a threat is strongly dependent on your organisational context and the sensitivity/criticality of already have pre-determined criteria to perform such assessments, it is best to base this assessment on the recommendations of the n of such criteria can be found on the website of the French Data Protection Authority (CNIL): https://www.cnil.fr/sites/cnil/files/atoms/

Threat	Threat Type	Relevant Threat Card	Threat Location	Detailed Description	Threat Severity
1	Non-Repudiation	Non-repudiation of Service Usage	Dataflow (Client -> Load balancer)	Communications from the user client to the load balancer are observable, possibly revealing the user is using the service.	High
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

General Information

System Name	ExAmPLE - Extra Amazing Privacy-Loving E-mail Application
System Owner / Primary Contact	Jane Doe, Principal Product Owner, jane.doe@corporation.com
Purpose Description	Web-based E-mail application that respects the user's privacy.
(Target) Commissioning Date	2024-02-03
System Design / Sketch	Link to the system design / sketch here, or paste an image of the system diagram/architecture to the right of this questionnaire.

Technical Information

Used Technologies / Programming Languages	Describe the technology stack the system will be built on. e.g., consider: Programming Languages / Datastore Technologies / ....
Networking	Describe the network environment in which the system will reside. e.g., consider: Load balancer(s) / DDoS protection / (Web-App) Firewall(s) / Segmentation / ...

Privacy & Data Protection Information

Will the system systematically store personal data?	Write your answer here.
Will the system systematically perform operations/analysis on personal data?	Write your answer here.
Will the system process (i.e., store or	

Templates - Reporting

Privacy Threat Report <System Name> LINDDUN

T.x. <Placeholder - Threat Title>

Affected Components		Relevant Threat Cards / Nodes	Priority
Data Flow:	<Placeholder>	<Placeholder>	<Placeholder>
Involved Data:	<Placeholder>		
Source:	<Placeholder>		
Destination:	<Placeholder>		

Detailed Description

<Placeholder>

Risk Assessment

Impact:	<Placeholder>
Likelihood:	<Placeholder>
Conclusion:	<Placeholder>

Mitigation Strategy

Summary:	<Placeholder>
Responsible:	<Placeholder>
Target Date:	<Placeholder>

Additional Notes

<Placeholder>

Privacy Threat Report <System Name> LINDDUN

T.1. Communications from the user client to the load balancer are observable by outsiders

Affected Components		Relevant Threat Cards / Nodes	Priority
Data Flow:	DF2	Nr1 – Non-repudiation of Service Usage	High
Involved Data:	Account Credentials	D2 – Detectable Service Usage	
Source:	User Client (Entity)		
Destination:	Load Balancer (Process)		

Detailed Description

Communications from the user client to the load balancer are observable, possibly revealing the user is using the service. These communications travel over an encrypted, yet untrusted and authenticated channel which means an outside observer can not only detect the communication, but also potentially identify the source and destination. The outcome would be that an attacker who observes the communications can see participation in the system by the user, and link this back to them with a high degree of confidence.

Risk Assessment

Impact:	Due to the sensitive nature of the system, the information of whether a user is a participant in the system may be used by an adversary to infer sensitive personal data about the user's health condition. Based on the impact assessment criteria of our organization, we assess the worst-case impact on the data subject to be **High**.
Likelihood:	Because an adversary would need to be able to intercept and observe the communications of the user with the platform, this threat is limited to adversaries in the vicinity of the data subject that are in a position to observe the communications with the platform. Regardless, isolated incidents of this nature cannot be excluded. In addition, observing such network communications is not particularly difficult to achieve. Therefore, in accordance with the likelihood assessment criteria of our organization, the likelihood is estimated to be **Medium**.
Conclusion:	An estimated **High** impact, combined with a **Medium** likelihood, corresponds to an overall **High priority** in our organization's priority/risk matrix.

Mitigation Strategy

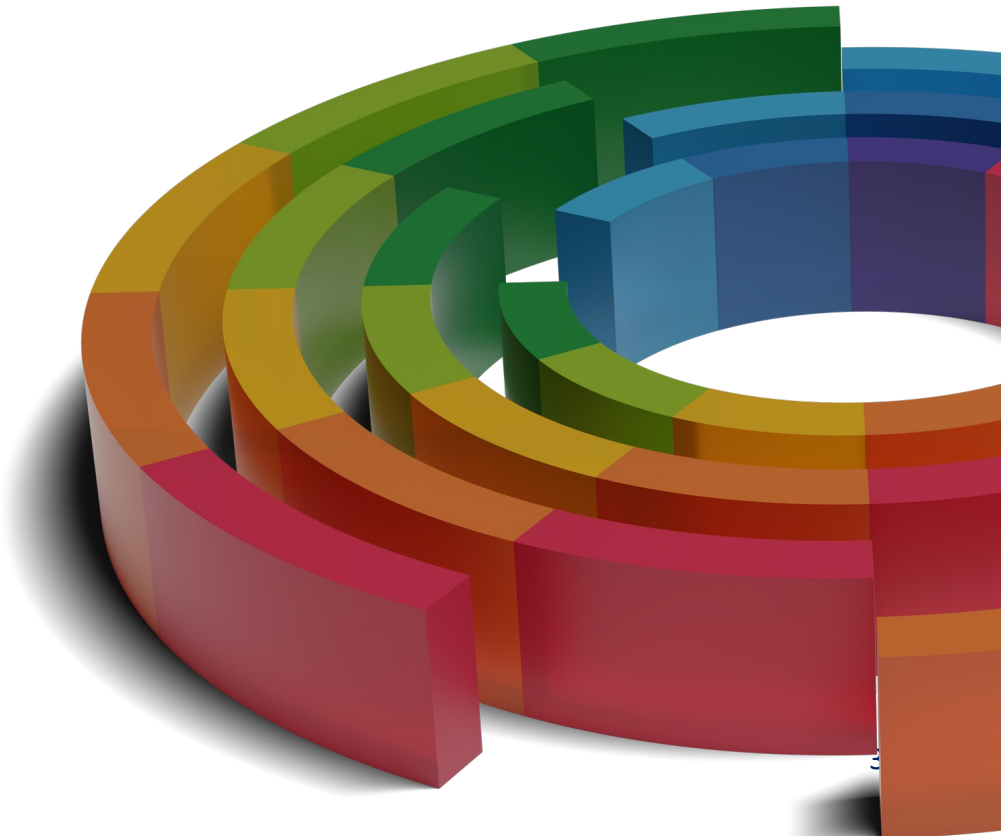
Summary:	Instead of connecting immediately to our own application network, employ an ubiquitous cloud-based network solution as an intermediary to mask the real destination of the traffic.
Responsible:	Jane Doe (System Owner)
Target Date:	End of Q2, 2025

Additional Notes

This entry is an example, feel free to remove it!

CO security COmmunity

Pipeline

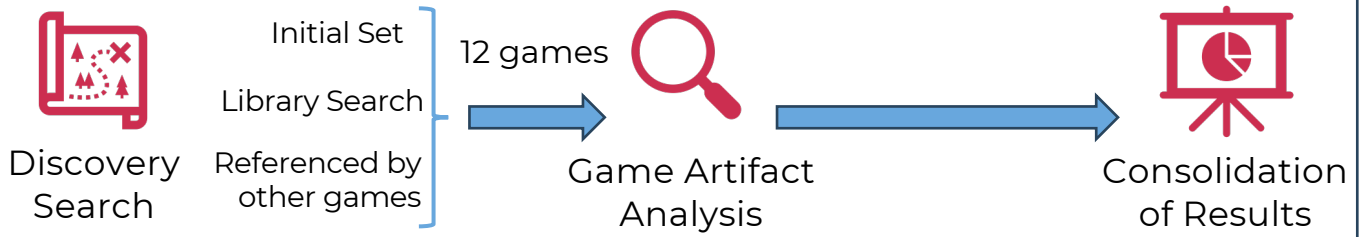


Research Track Gamification

Objectives

- Serious Game Landscape
- Gameful design elements
- Empirical Evaluation of Effectiveness

Method



Key Results & Conclusions

Serious Game Landscape

- Multi-stakeholder
- Industry practitioners
- Introduction to S&P activities
- Primarily RE & TM

Gameful design elements

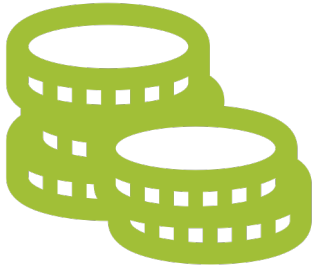
Despite the existence of serious game design frameworks and methodologies, **most games are designed in an ad-hoc manner.**

Empirical Evaluation of Effectiveness

Experiments gauge **participant opinion and experience** rather than outcome.

Domain-specific variants

ML / AI



Finance

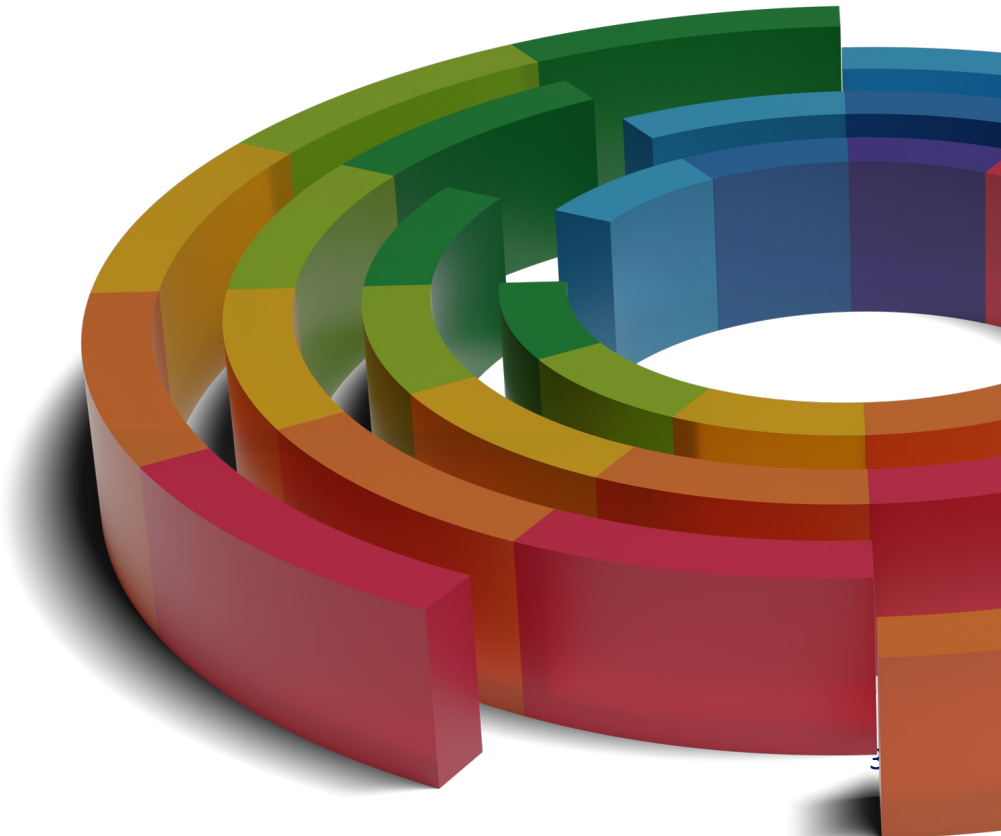
e-Health

User Studies

Cases with practitioners

Feedback to improve techniques

Conclusion



CLOSING REMARKS

Objectives

- ✓ Lightweight, accessible privacy threat modeling
- ✓ Fostering collaboration between stakeholders

Updated LINDDUN GO

- ✓ Revised threat cards with concise descriptions and clear examples
- ✓ Digital version available with built-in documentation functionality

Pipeline

- ✓ Research track on gamification
- ✓ Domain-specific variants
- ✓ User studies with industry

DistriNet KU LEUVEN ECCO European Cybersecurity COmmunity

Thank you.

Any questions?

Scan to get your own LINDDUN GO card deck!

...or visit our website at:

https://linddun.org/go