

DPP Risks and mitigations

Discussion of the CIRPASS2 D4.1 companion by
David Roefs, MSc *et al.*

Dr. ir. Rik Rurup

Background

- DPP systems [add value](#)
- But a DPP system can introduce [risks](#) that may [decrease value](#)
- Negative effects should not:
 - [Outweigh](#) the positive effects of the DPP system
 - Disproportionally [harm](#) the interest of an entity
- To prevent negative effects:
 - Possible [negative effects](#) have been [inventoried](#)
 - [Mitigations](#) for high-risk negative effects are [implemented](#)
- [Other talks](#) present positive effects
- [This talk](#) presents possible negative effects, and countermeasures based on CIRPASS2 Risks and mitigations report

Scope

- The risks and mitigations discussed in the CIRPASS2 report are **both technical and non-technical**
- Example of risks that cause **loss of confidential information**:
 - **Technical risk**: an entity eavesdrops the internet connection and stores confidential information
 - **Non-technical risk**: an entity commits fraud to get access to an account, then reads confidential information
- For CIRPASS2, **most risks** are non-technical
 - Making something mandatory introduces risks: not all users will like using the system
- zenodo.org – 15389457 - “Risks and mitigations: a companion to D4.1 Reference Architecture”, Roefs et al.



Risks and mitigations

Threat actors 1/3

- Threat actors:
 - are individuals, groups or entities
 - are the source of threats to a systems
 - attack systems relevant to their **motivations** and **capabilities**
- Only a capable **and** motivated threat actor is a threat to a system.
- Non-exhaustive example:

Target \ Threat actor	High School Student (resources: low)	Nation state (resources: high)
High school teacher	High risk: little resources but motivated	Low risk: much resources, little motivation
Ministry of Defence	Low risk: little resources, little motivation	High risk: much resources, high motivation

Threat actors 2/3

- Conclusion:
 - The nation state is much more capable
 - Yet, the teacher should focus on the threat posed by students
- Why does this matter?
 - Different threat actors use different techniques
- From the example:
 - The student might place a physical keylogger (device to capture passwords from the keyboard)
 - The nation state might prefer exploiting a device that is not updated
- Consequently, the mitigations are different:
 - To mitigate risks of students: check the physical keyboard for suspicious devices
 - To mitigate risks of state actors: update all devices

Threat actors 3/3

- For CIRPASS2, the process of identifying threat actors has been performed
- The results:
 - 9 threat **actors** identified
 - 52 main **actions** identified (action = something a threat actor could do, like the action of changing grades in the grading system by the student)
 - 78 main **risks** identified
 - 89 main **mitigations** proposed
 - many more **motivations** have been inventoried
- Note that most of these risk are **not applicable** to companies using DPP's, as the treat actors are different!

What can go wrong in the lifecycle of a DPP?

- DPP lifecycle:



- In every stage of the lifecycle, risks arise due to threat actors
- In the next slides, 2 main risks are highlighted

Risk: supplier provides DPP with incorrect info

- Context: a supplier delivers a **sub-product** (with DPP) that will be integrated into a product
- **Threat actor**: the sub-product supplier
- **Motivation**:
 - the supplier **dislikes** the mandatory DPP as it seems to introduce additional costs
 - therefore, the supplier wants to **fake complying** to the law: supply a plausible, but incorrect DPP
- Risk: the DPP contains **incorrect information**
- Possible **effects** are:
 - **The DPP** of the product that integrates the sub-DPP **is incorrect**, as it uses information from the sub-product DPP
 - **The product does not work correctly** as the sub-product does not live up to the specifications of the DPP
 - Recycling is impossible or poses health or environmental concerns

Mitigations: supplier provides DPP with incorrect info

- Technical mitigation:
 - the system [verifies](#) whether all required fields of the DPP are submitted
- Non-technical mitigation:
 - [the law requires](#) the supplier to provide correct information
 - [penalties are imposed](#) when inaccurate information is provided

Risk: public data from the DPP system is misused

- Public data can be [aggregated](#) in an automatic manner
- This might give [insight](#) on for example:
 - [Production capacity](#) of nations on product level
 - [Supply chain dependencies](#) of countries
- Example risks:
 - Perform [targeted sabotage](#) to decrease production levels
 - Pressure countries by [reducing export](#) of critical supply chain dependencies
- Is this a serious threat?
 - In the Chinese DPP system, there [will not be any](#) public data

Mitigations: public data from the DPP system is misused

- Technical mitigation:
 - the system does not expose an index to all information
 - DPP id's are not sequential, but random
 - the number of request that can be performed to the system are limited
 - etc.
- Together, these mitigations make it much harder to collect information



Conclusion

Conclusion

- DPP systems **create much value**, but risk might threaten that value
- DPP systems suffer both from **technical and non-technical risks**
- The specific **use case** of the DPP system **determines** the threat actors
- The threat actors determine the risks
- The risks determine which **mitigations** should be taken
- We saw example risks and mitigations:
 - supplier provides DPP with incorrect info
 - public data from the DPP system is misused
- These risks are important to identify and mitigate
 - Not only now, but **continuously**: as both the system and the world around us evolve
- Further reading: <https://cirpass2.eu/project-results/>