Threat Modeling Data Analysis in Socio-technical Systems

Tomasz Ostwald

SALIENT WORKS

Our decision-making becomes more and more data driven and dependent on systems of multiple technical components.

Data driven decision processes take place in socio-technical systems and require consistency between the decision level and the underlying data analysis.

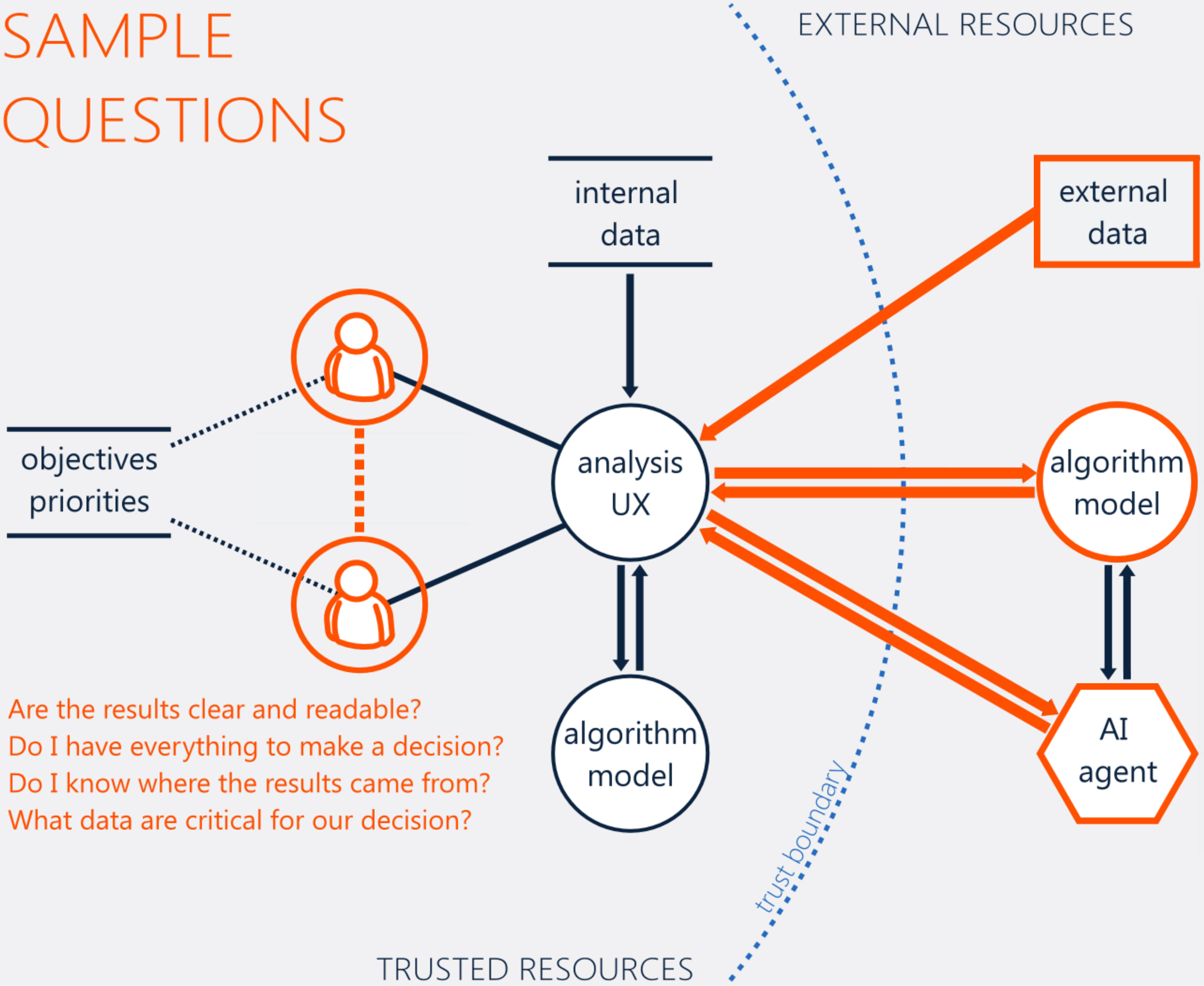
Threats against decision-making and data analysis can be defined as any activity aimed at disrupting these processes or changing their outcome.

Potential impact of successful attacks depends on scenarios and goals of decision processes.

Threat modeling methodologies are systemic approaches to evaluate the design of information processing systems in the security context.

We need to understand the system in order to mitigate the threats.

SAMPLE QUESTIONS



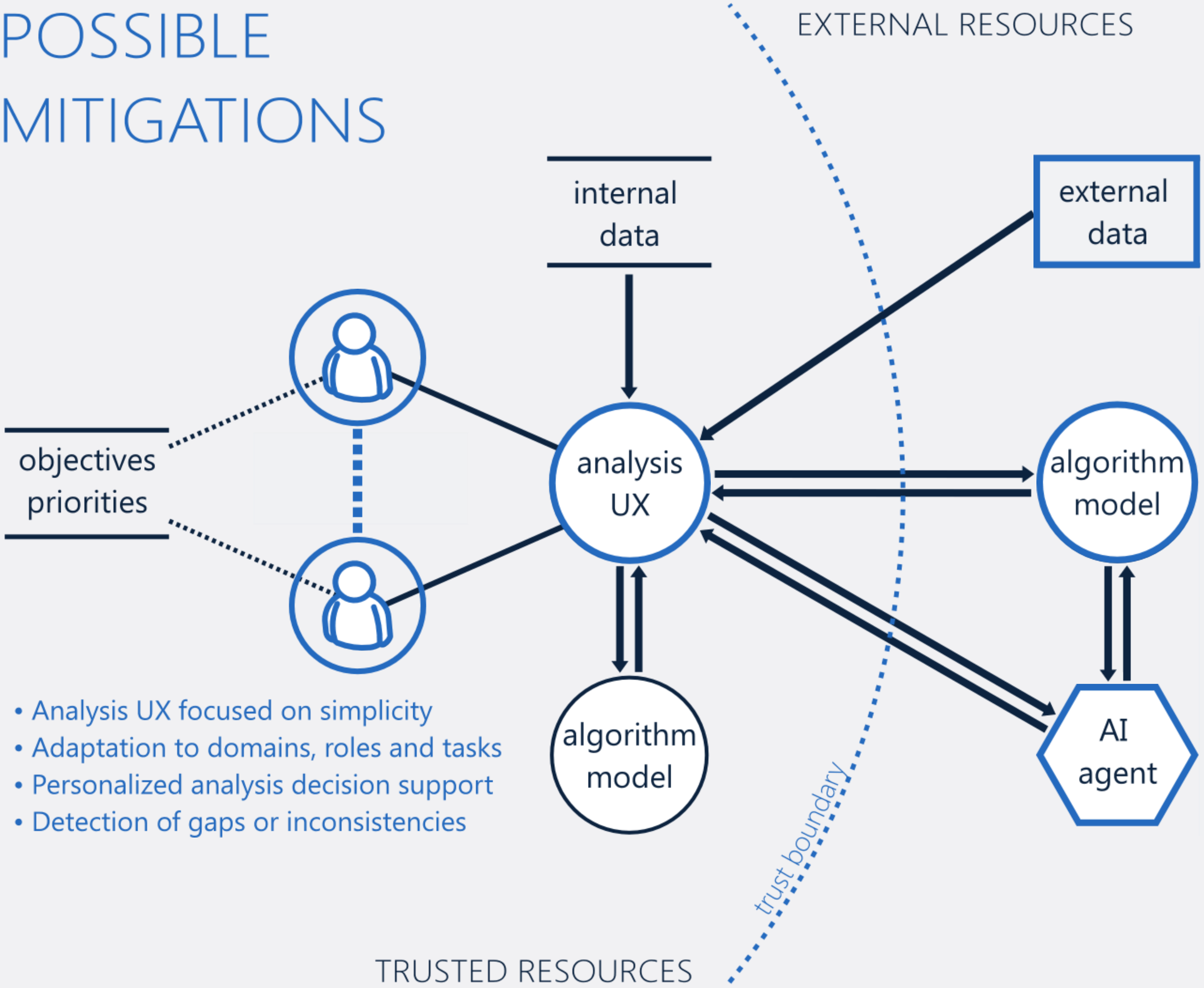
- Where are the data coming from?
- Correct, complete and up-to-date?
- Securely stored and transferred?
- What transformations were applied?

- Is the algorithm/model biased?
- How was the model trained?
- Applied configuration settings?
- Are results aligned with our needs?

- Do we know what the objectives and priorities of an AI agent we are talking with are?

- Are the results clear and readable?
- Do I have everything to make a decision?
- Do I know where the results came from?
- What data are critical for our decision?

POSSIBLE MITIGATIONS



- Verification of origin and integrity
- Data quality metrics, ownership
- Transformation logs
- Use data from different sources

- Use multiple algorithms in parallel
- Check results for anomalies
- Independent model validation
- Certifications & SLAs

- Historical records of interactions
- Non-repudiation mechanisms
- Specification of goals and priorities
- Limits on scope of cooperation

- Analysis UX focused on simplicity
- Adaptation to domains, roles and tasks
- Personalized analysis decision support
- Detection of gaps or inconsistencies

Threat modeling can be adapted to socio-technical systems and help us with designing decision processes that are more reliable, trustworthy and resistant to attacks.

Special requirements may be needed for decisions with shared goals and broad social impact.

1. Do not focus only on the opportunities and benefits of new solutions
2. Use the lessons from information security whenever possible
3. Understand the context and impact of decisions you are about to make
4. Think about the decision process as a system you are designing
5. Challenge the assumptions and ask uncomfortable questions
6. Pay close attention to things that are unexpected, unclear, or too shiny
7. Document the critical steps and decisions along the way

Data analysis technologies are changing our decision-making processes just as the Internet and mobile devices changed the nature of our interactions and communication patterns.

We cannot focus only on the benefits and opportunities of new technologies. If we do, we may soon find our decision processes to be very effective and accurate, but not necessarily aligned with our goals and priorities.

SALIENT WORKS