Threat modeling state of practice in Dutch organizations

Twentieth Symposium on Usable Privacy and Security

August 11-13, 2024

Stef Verreydt, Koen Yskout, Laurens Sion, Wouter Joosen

stef.verreydt@kuleuven.be

DistriNet

Threat modeling?

THREAT MODELING MANIFESTO

"Threat modeling is analyzing representations of a system to highlight concerns about security and privacy characteristics."

- Four key questions
  - What are we working on?
  - What can go wrong?
  - What are we going to do about it?
  - Did we do a good enough job?

https://www.threatmodelingmanifesto.org/

Goal: investigate how organizations apply threat modeling

- In collaboration with NCSC (NL)
- Semi-structured interviews
- 13 practitioners
  - Directly involved with threat modeling
- 7 large organizations
- Critical sectors

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Sector	Focus	Participants
Energy	OT Systems	1
Finance	Software development	4
Marine	IT Infrastructure	1
Public sector	Software development, advice	3
Transport	Software development	4

Research questions

RQ4
Experiences

RQ1
How is threat modeling embedded in the organization?

RQ2
Which organizational roles are involved in threat modeling activities?

RQ3
How is threat modeling performed within the organization?

Research questions

RQ4
Experiences

RQ1
How is threat modeling embedded in the organization?

RQ2
Which organizational roles are involved in threat modeling activities?

RQ3
How is threat modeling performed within the organization?

Purpose of threat modeling

- Finding potential **vulnerabilities**
- Raising security **awareness**

“a way for [developers] to discuss information security in a practical way within their team”

Motivation for threat modeling

- Seldom mandated, except for critical applications
- Focus on **internal motivation**

"[…] the moment you start forcing threat modeling, people naturally lose enthusiasm, and do it because they have to and not because they see the usefulness and necessity of it."

Research questions

RQ4
Experiences

RQ1
How is threat modeling embedded in the organization?

RQ2
Which organizational roles are involved in threat modeling activities?

RQ3
How is threat modeling performed within the organization?

Who participates in threat modeling activities?

- **Security team** 'markets' threat modeling
- Participants: Developers, Product owner, Architect, Facilitator (security team)
- Usually **not involved**: testers, information security officers, IT admins, business management, …

"[…] they don't have the capacity [(time) to attend threat modeling sessions]"

Involvement of business management roles

- Not always aware of threat modeling and its benefits
- Challenging to demonstrate effectiveness
- **Difficult to get support**

"management, according to me, does play a role in accepting [threat modeling], seeing the added value of it and being able to translate that back to their stakeholders as well"

Research questions

RQ4
Experiences

RQ1
How is threat modeling embedded in the organization?

RQ2
Which organizational roles are involved in threat modeling activities?

RQ3
How is threat modeling performed within the organization?

Planning

- Continuous refinement over a single delivery.

Preferably **early on** in the development lifecycle and **periodic** re-assessment

➔ But this is **difficult** in practice:

- **Scope** may not be clear early on
- **Mitigating** threats may be difficult later on
- Security team lacks resources
- Finding a hole in everyones **schedule**

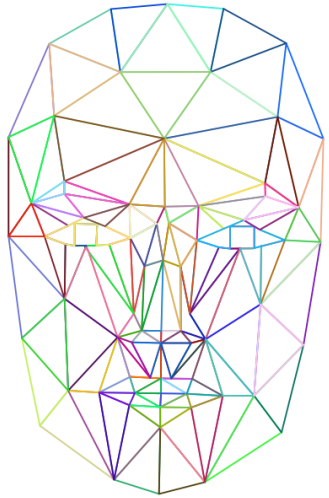
" [the security team] simply doesn't have the capacity for that yet, because we just have so many development teams."

Modeling an application

1. What are we working on?

- Ranging from white board drawings to structured notations like data flow diagrams
- Input (architectural documentation) not always available

  ➔ Creating a model may be **time-consuming**
- Advantage: create **mutual understanding** of the architecture



“there is no single record, with the truth, not even on a conceptual level”

Identifying threats

2. What can go wrong?

- Mostly STRIDE, other methodologies depending on the context
- Prefer pragmatism over strict methodologies

"[…] it's really not so much about whether it's done very well. The point is that we do it, and that we learn from it together and gain knowledge […]."

Output and follow-up

- Report includes the system model, identified threats, existing mitigations and mitigation advice.
- Preferably **limited reporting overhead**
- **Follow-up** is limited (team's responsibility)

"writing takes a lot of time, and I don't know if it's always worth the effort. Going through the process is perhaps the most fruitful."

Conclusion

- Main findings
  - **Benefits**: uncover threats, but also raise awareness
  - **Challenges**: preparation, scaling, following up
  - **Success factors**: intrinsic motivation and pragmatism
- Future research
  - Repeat and extend similar studies: BE/EU, SME, other sectors, …
  - Effectiveness of threat modeling

Threat modeling state of practice in Dutch organizations

Twentieth Symposium on Usable Privacy and Security

August 11-13, 2024

Stef Verreydt, Koen Yskout, Laurens Sion, Wouter Joosen

stef.verreydt@kuleuven.be

DistriNet