Practical Threat Modeling with Microsofts Threat Modeling Tool 2016

Matthias Rohr

Agenda

- Some Context on Threat Modeling
- Demo
- Conclusion

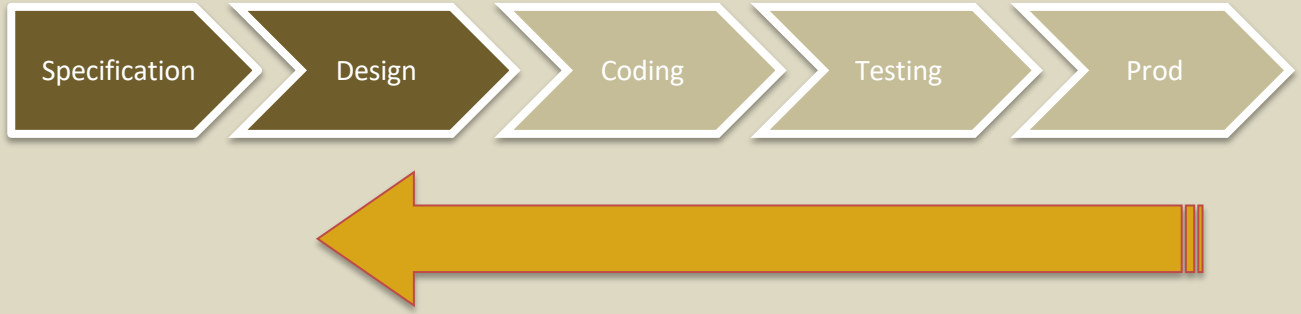
About Me

- Matthias Rohr
- Founder of Secodis GmbH
- Active in application security > 12 years
- Professional focuses:
  - Building secure web-based applications
  - Secure SDLC
  - Security test automation

ROMA MMXVI | APPSEC EUROPE


ROMA
MMXVI
APPSEC
EUROPE
MOTIVATION

Move Left to be More Secure!



Advantages:

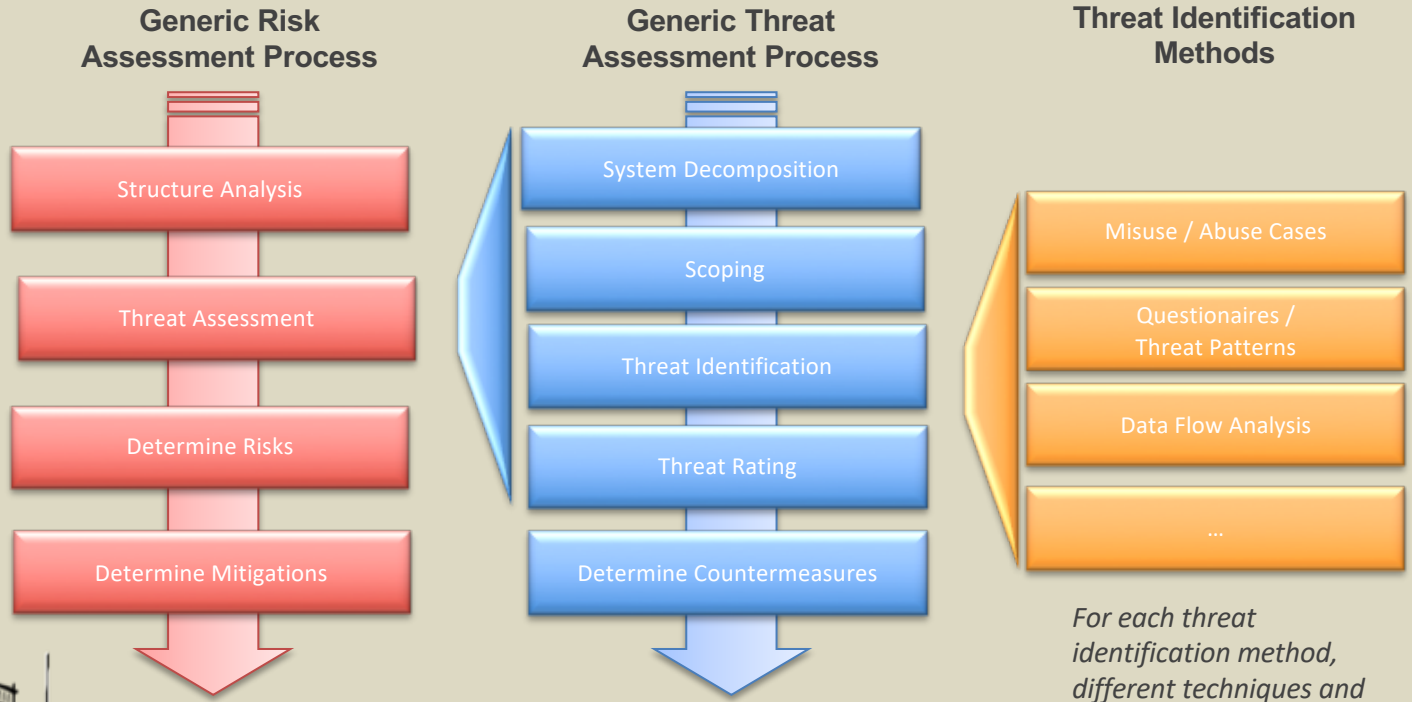
1. Relatively easy to fix / cost-effective
2. We can find a lot of (potential) security problems
3. Increases AppSec maturity of organization
4. Vital for meeting architectural security requirements
5. …

What is Threat Modeling?

1. **Threat modelling** is a structured approach for identifiying potential security problems (threats) within the software specification or design.

2. A **threat model** is a model of threats, not just a list of threats.

What is Threat Modeling?



For each threat identification method, different techniques and tools exist!

Common „Threat Modeling Tools“

Threat Identification Technique	Tool
Abuse and Misuse Case	▪ MS Visio*
Questionnaires / Threat Patterns	▪ MS Word* & MS Excel*
Data Flow Analysis	▪ MS Visio*

* or similar products

Challenges

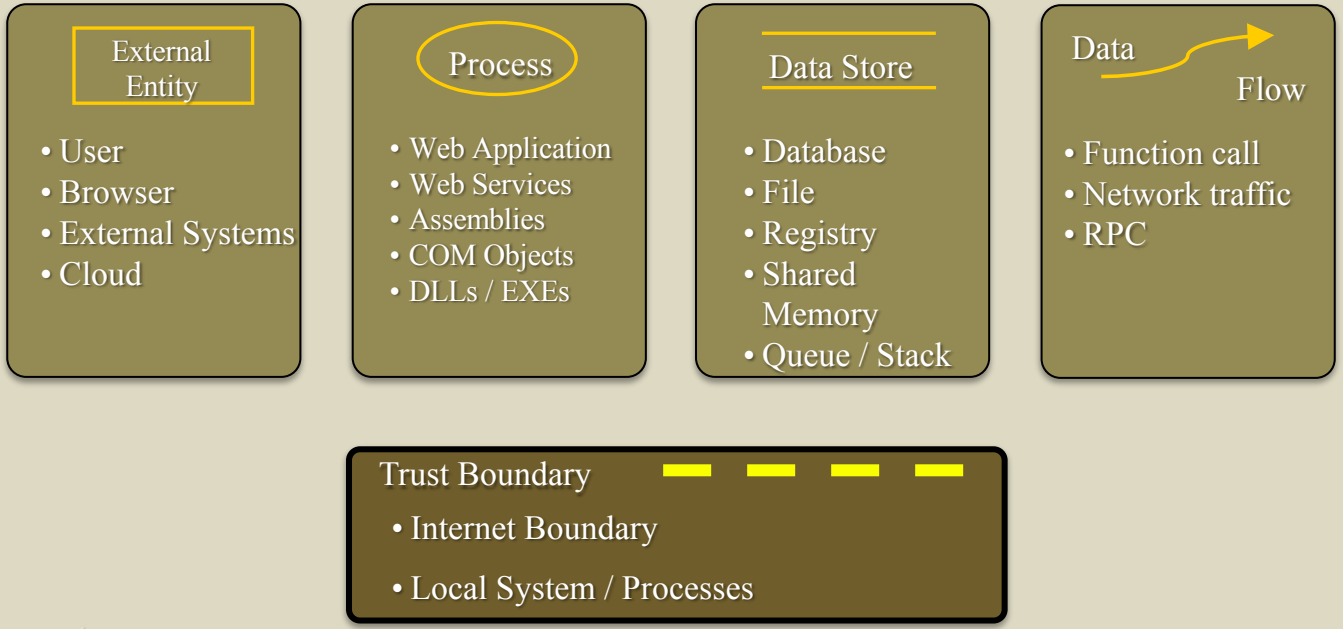
- Repeatability / Consistency (=> threat model)
- Ease of use (e.g. by non sec experts such as developers)
- Mapping of custom environments / threat intelligence

(Some) Threat Modeling Tools

Threat Identification Technique	Tool
Abuse and Misuse Case	• Microsoft's Elevation of Privilege (EoP) Card Game (Free)
Questionnaires / Threat Patterns	▪ IriusRisk (Free + $)
Data Flow Analysis	▪ ThreatModeler ($) ▪ MS Threat Modeling Tool (Free)

DATA FLOW BASED THREAT MODELING WITH MS THREAT MODELING TOOL

Data Flow (Threat) Analysis - Elements



ROMA MMXVI

APPSEC EUROPE

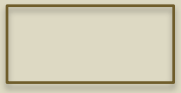
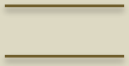
Source: Michael Howard

The STRIDE Approach

STRIDE is an acronym for these threat categories:

- **S**poofing
- **T**ampering — *Malicious data manipulation*
- **R**epudiation — *Dispute of actions*
- **I**nformation Disclosure — e.g. Stack Traces
- **D**enial of Service — *e.g. Application crash by malicious user input*
- **E**levation of Privilege

Mapping STRIDE to DfD Elements

Element	S	T	R	I	D	E
 External Entity	✓		✓			
 Process	✓	✓	✓	✓	✓	✓
 Data Store		✓	?	✓	✓	
 Data Flow		✓		✓	✓	

Source: Michael Howard

Mapping STRIDE to OWASP TOP 10

OWASP Top Ten 2013	STRIDE
A1 - Injection	Tampering, Spoofing
A2 – Broken Auth. & Session Management	Elevation of Privileges, Spoofing, Information Disclosure
A3 – Cross-Site Scripting (XSS)	Tampering, Spoofing
A4 – Insecure Object References	Privilege Escalation, Information Disclosure
A5- Security Misconfiguration	Information Disclosure (and others)
A6 – Sensitive Data Exposure	Information Disclosure
A7 – Missing Function Level Access Control	Privilege Escalation, Information Disclosure
A8 - Cross Site Request Forgery (CSRF)	Tampering, Spoofing, Elevation of Privileges
A9 - Using Components with Known Vuln.	All
A10 – Unvalidated Redirects and Forwards	Spoofing, Tampering

Microsoft Threat Modeling Tool 2016

- Free ☺
- Windows only ☹
- Version History
  - 2004, 2005: Threat Analysis & Modeling Tool (TAM) v1,v2: Windows GUI
  - 2011: SDL Threat Modeling Tool 3: Visio Plugin
  - …
  - 2014: Microsoft Threat Modeling Tool 2014: Windows GUI
  - **2015: Microsoft Threat Modeling Tool 2016: Windows GUI**

- Download: http://aka.ms/tmt2016


ROMA
MMXVI
APPSEC
EUROPE
DEMO

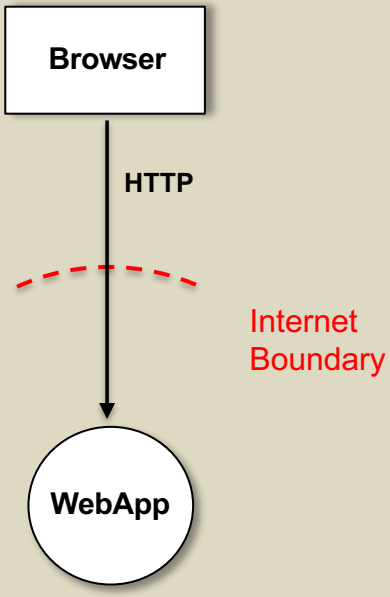
DFD Threat Modeling Logic

1. A **SOURCE**
   has a type („Browser“) and attributes
   has a parent („Generic External Interactor“) with attributes

2. Sends data via a **DATA FLOW**
   with a type („HTTP“) and attributes

3. That may crosses a **TRUST BOUNDARY**
   with a type („Internet Boundary“) and attributes

4. To a **TARGET**
   has a type („WebApp“) and attributes
   has a parent („Generic Process“) with attributes



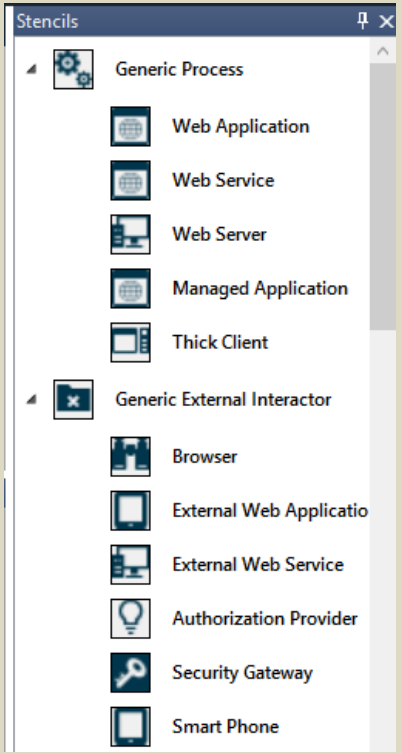
ROMA MMXVI

APPSEC EUROPE

Simplified Template for Web Apps

- Simplified Template for Web apps & examples available here: https://github.com/matthiasrohr/OTMT

- Some modifications I made:
  - Removed stencils & properties note related to any threat logic
  - Fixed some threat logic (e.g. XSS sanitization, DoS logic)
  - Added some useful stencils (e.g. security gateway)
  - Added threat logic (e.g. NoSQL Injection, XXE)
  - Added trust boundaries & network zones
  - Added properties for countermeasures and risk
  - …



Conclusion

- Microsoft Threat Modeling Tool 2016
  - Can be a great tool for technical threat modeling with strong customization capabilities that allows you to map your own environment & threats to it
  - With proper customized templates, usable for non-sec experts (e.g. architects)

- Limitations:
  - It is of course just a tool (requires processes, people using it, etc.)
  - System / Development centric approach (not suitable for everyone)
  - Threats related to business logic etc. cannot be identified
  - Combination with other approaches (e.g. questionairs) may really helpful

Thank you!

Questions?

Contact: m.rohr@secodis.com

Demo Templates & Model: https://github.com/matthiasrohr/OTMT