Threat Modeling

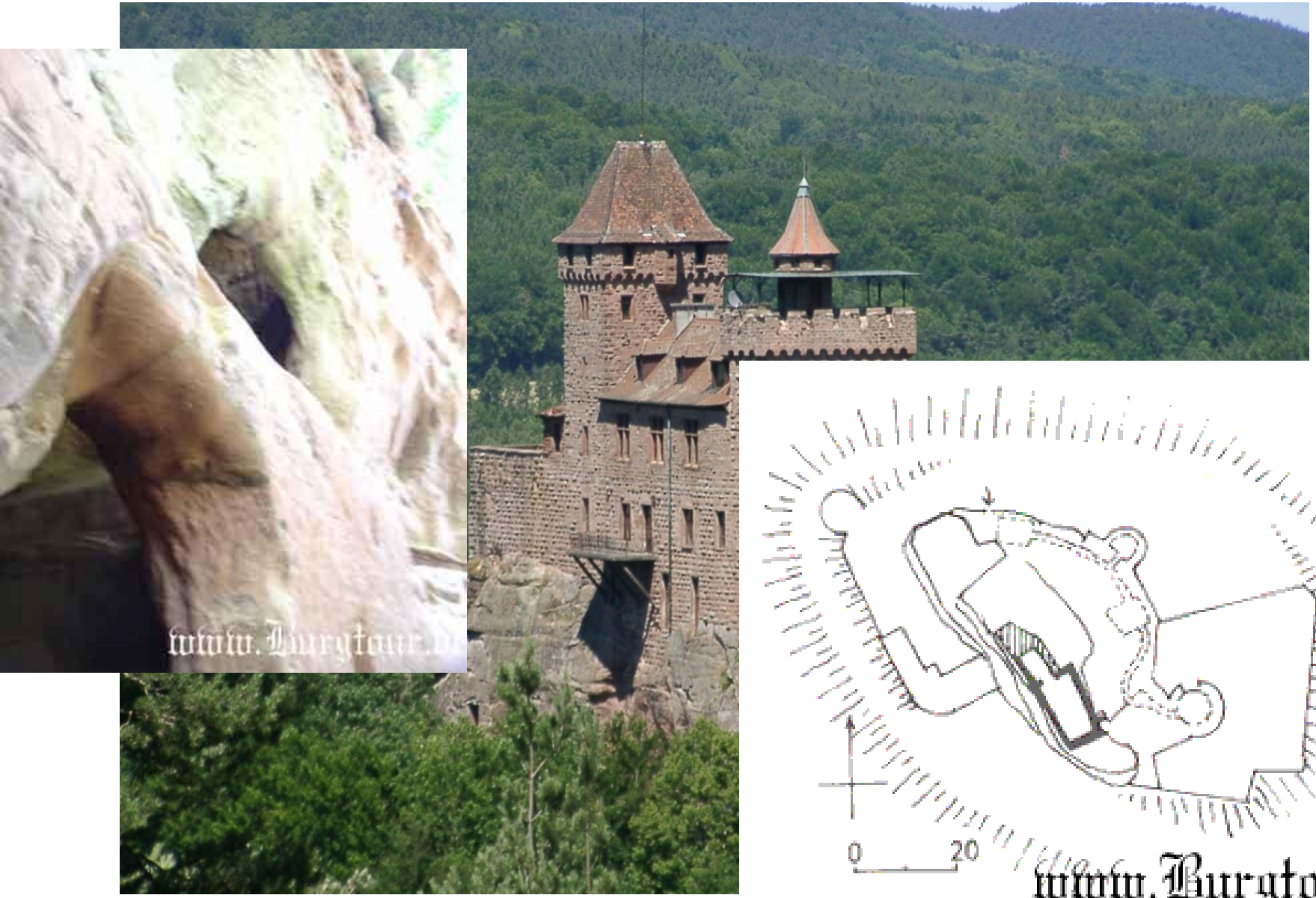
Martin Knobloch
martin.knobloch@owasp.org

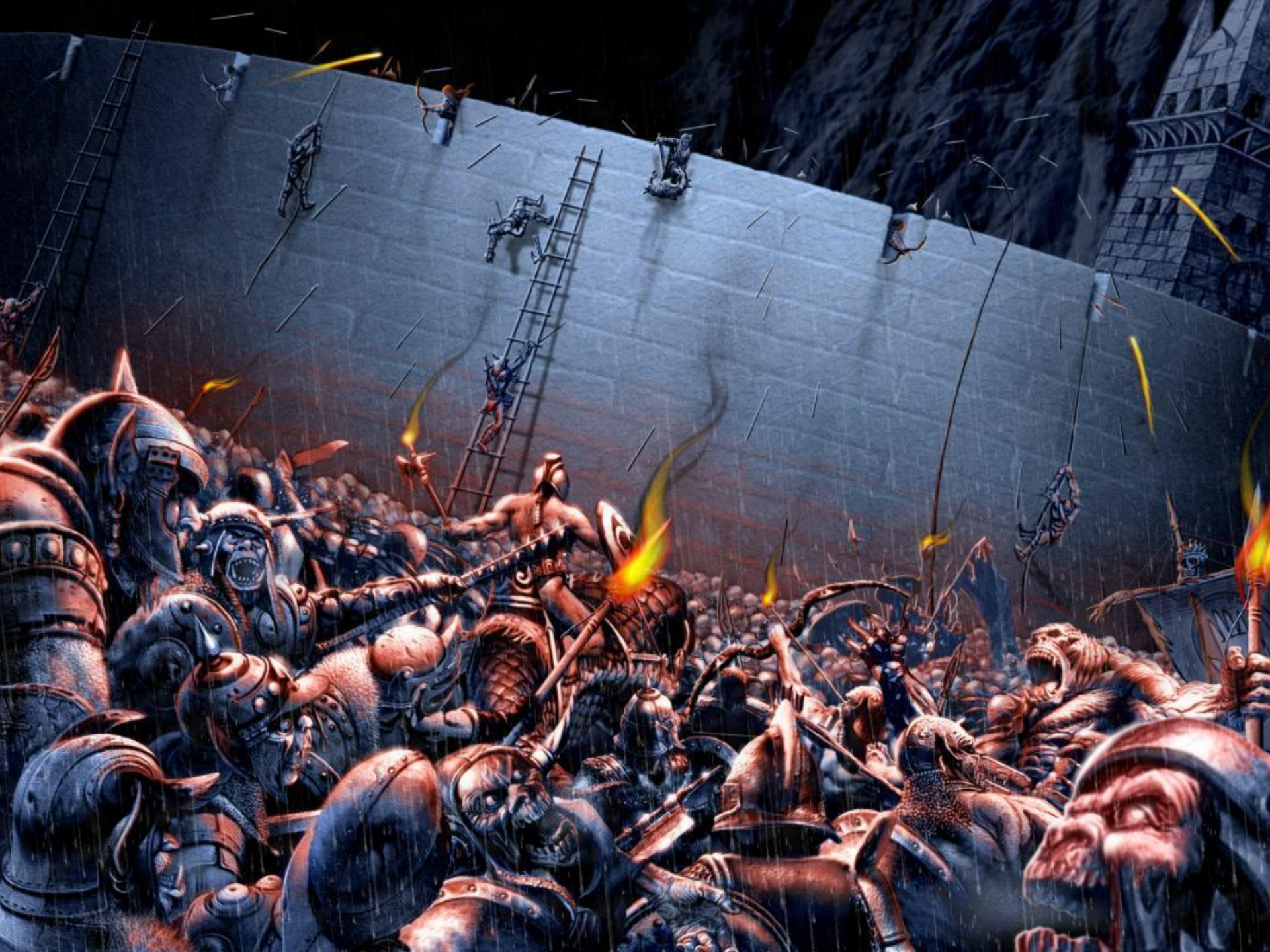
OWASP NL Chapter Board

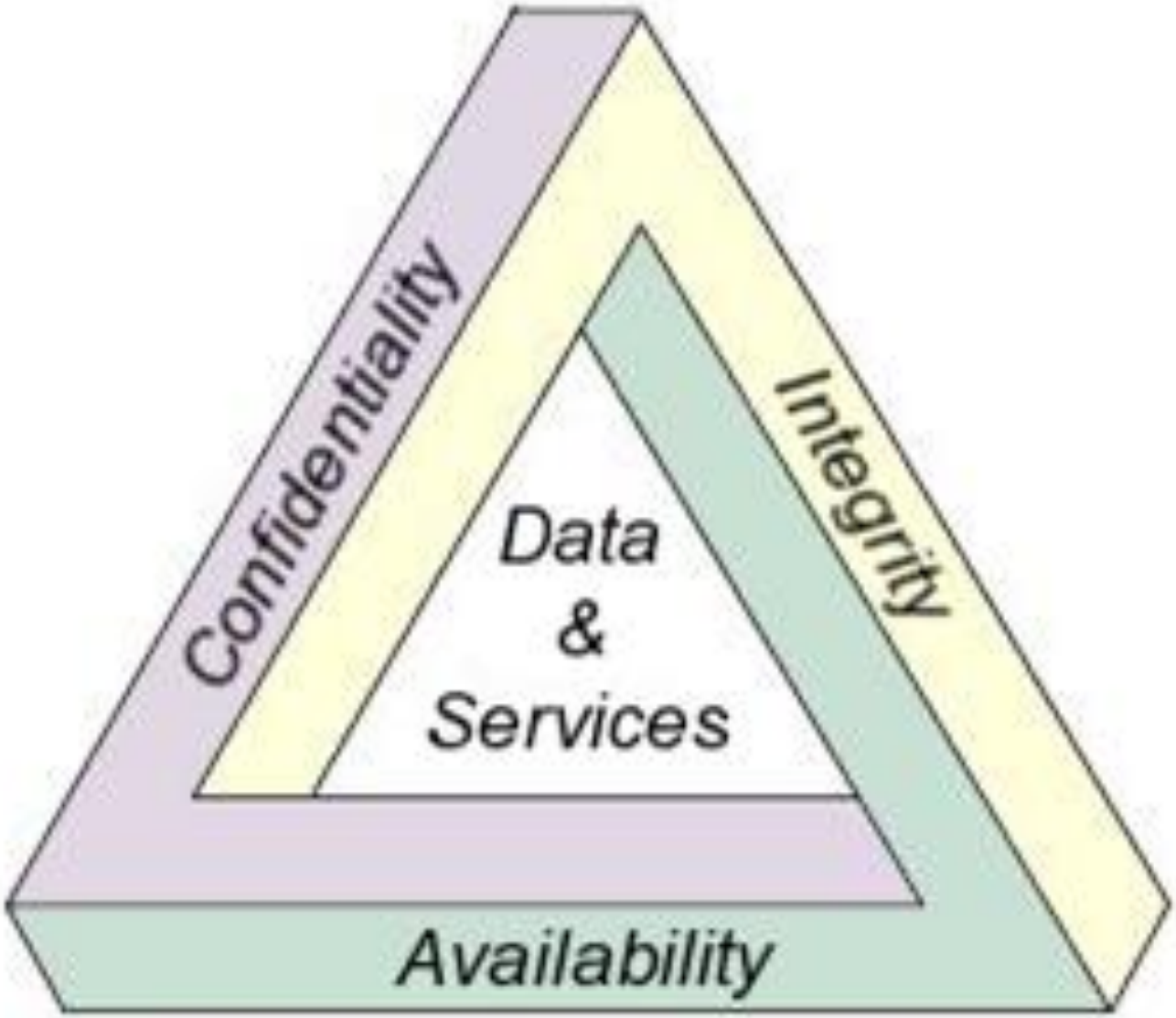
OWASP Global Education Committee
OWASP Education Project

OWASP

The OWASP Foundation
http://www.owasp.org


0
20
www.Burgtour.de




Confidentiality
Integrity
Data
&
Services
Availability

Threat Modeling Objectives

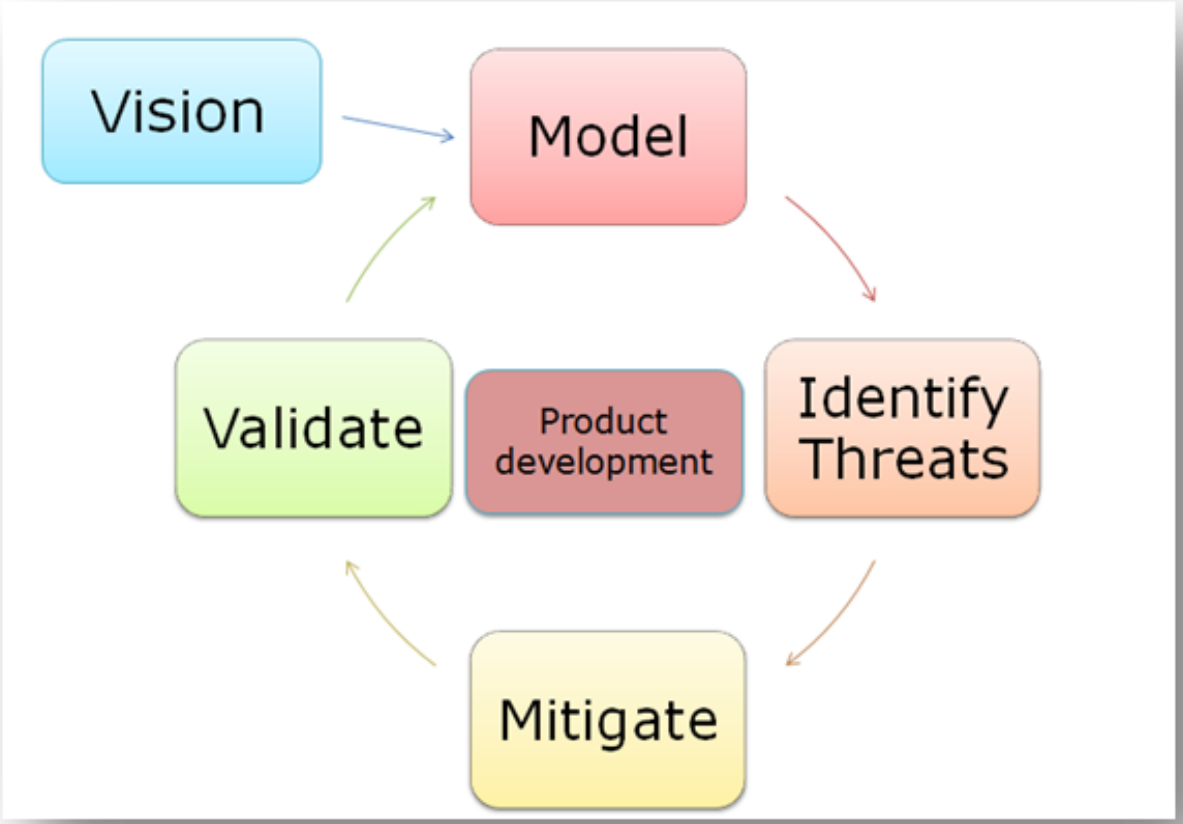
By performing Threat Modeling you can:

- Identify relevant threats to your particular application scenario.

- Identify key vulnerabilities in your application design.

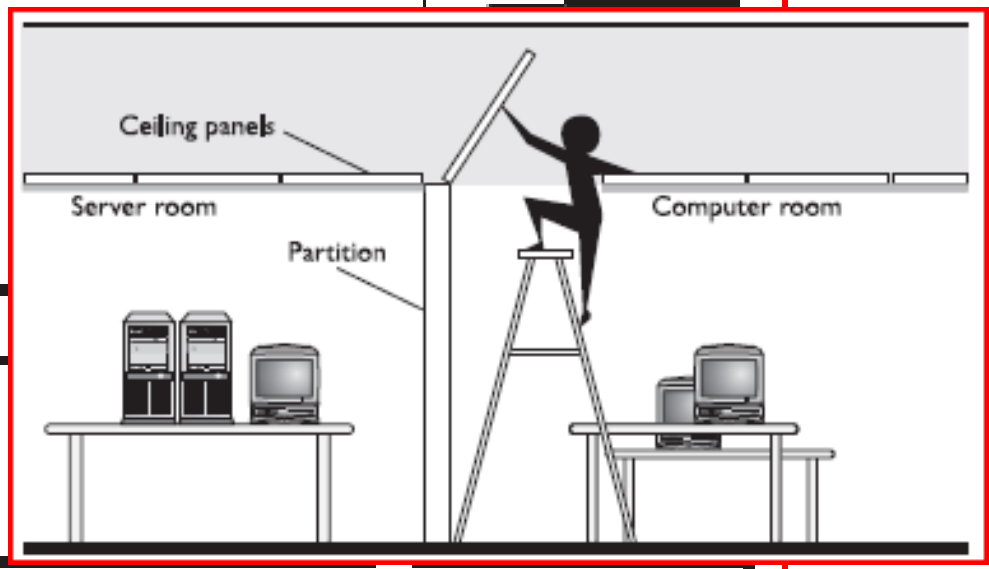
- Improve your security design.

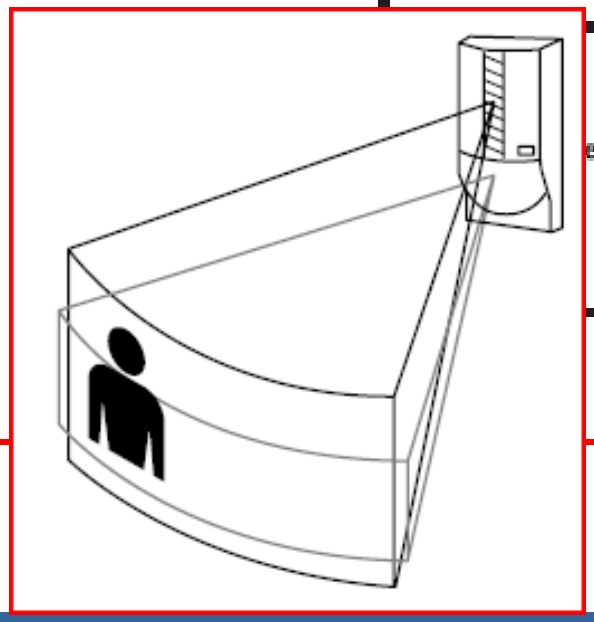
Threat Modeling – the proces



Threat Modeling – Terminology

- **Asset: Any resource with value**
  - > **Literal or perceived**
- **Vulnerability: Exploitable weakness**
  - > **Bugs and flaws**
- **Threat: Anything that can cause harm**
  - > **Intent is irrelevant**
- **Risk: Chance that a threat will cause harm**
  - > **Risk amount = (probability * impact)**
  - > **Risk will *always* be present in *any* system**
- **Countermeasure: Control to reduce risk**
  - > **Reduction to an acceptable level**
  - > **Must be balanced against both risk and asset**





Sensitive
zone

Restricted
zone

Security
zone

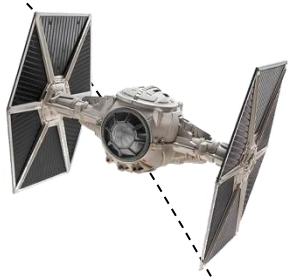
Public
zone

Public
zone

Threat Modeling – The Basics

Threat:
Causes harm

Risk:
Chance of harm occurring



Countermeasure:
Reduces risk

Asset:
Valuable resource

Vulnerability:
Exploitable weakness

Threat Categories:

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Service (Ddos)
- **E**levation of privilege

Threat Categories:

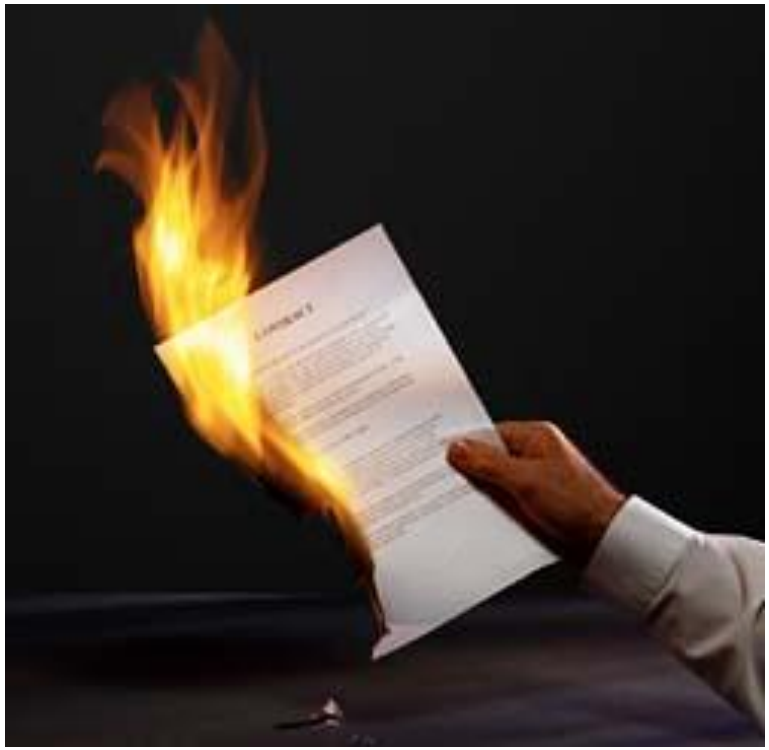
- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service (Ddos)
- Elevation of privilege

Threat Categories:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service (Ddos)
- Elevation of privilege

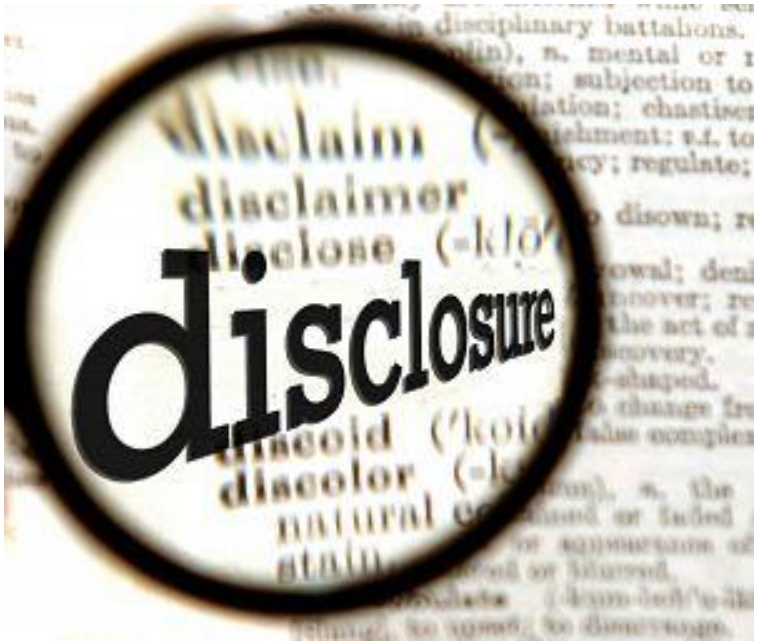
Threat Categories:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service (Ddos)
- Elevation of privilege



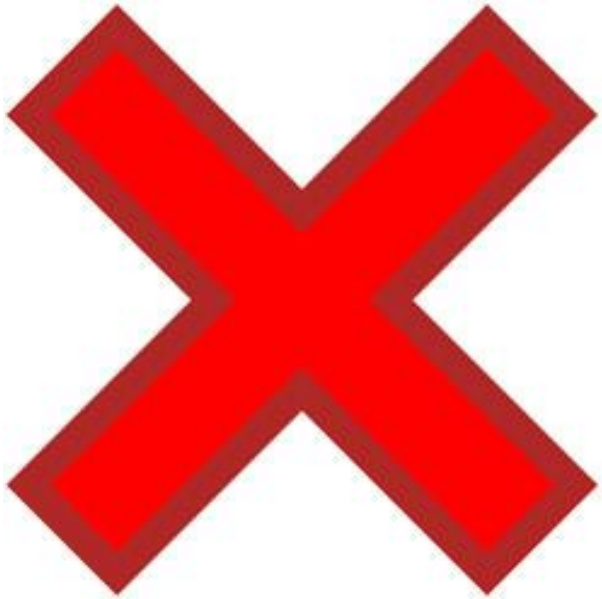
Threat Categories:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service (Ddos)
- Elevation of privilege



Threat Categories:

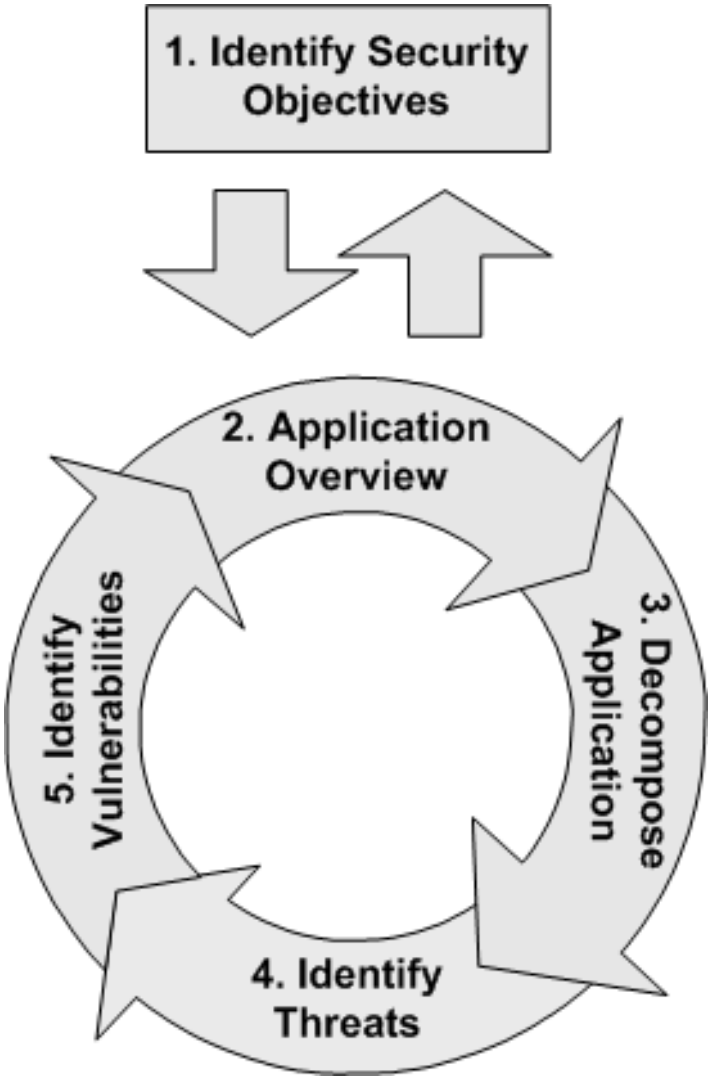
- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service (Ddos)
- Elevation of privilege



Threat Categories:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service (Ddos)
- Elevation of privilege

Threat Modeling Steps



The Threat Modeling Process

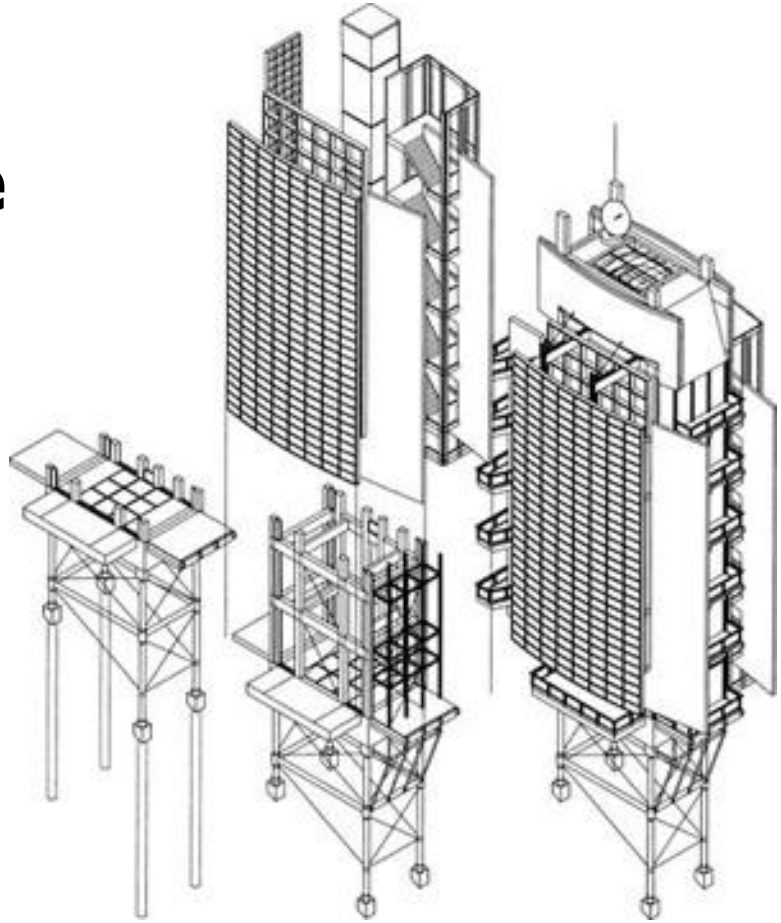
1. Identify Assests
2. Create an Architecture Overview
3. Decompose the Application
4. Identify Threats
5. Document the Threats
6. Rate the Threats

The Threat Modeling Process

1. **Identify Assests**
2. Create an Architecture Overview
3. Decompose the Application
4. Identify Threats
5. Document the Threats
6. Rate the Threats

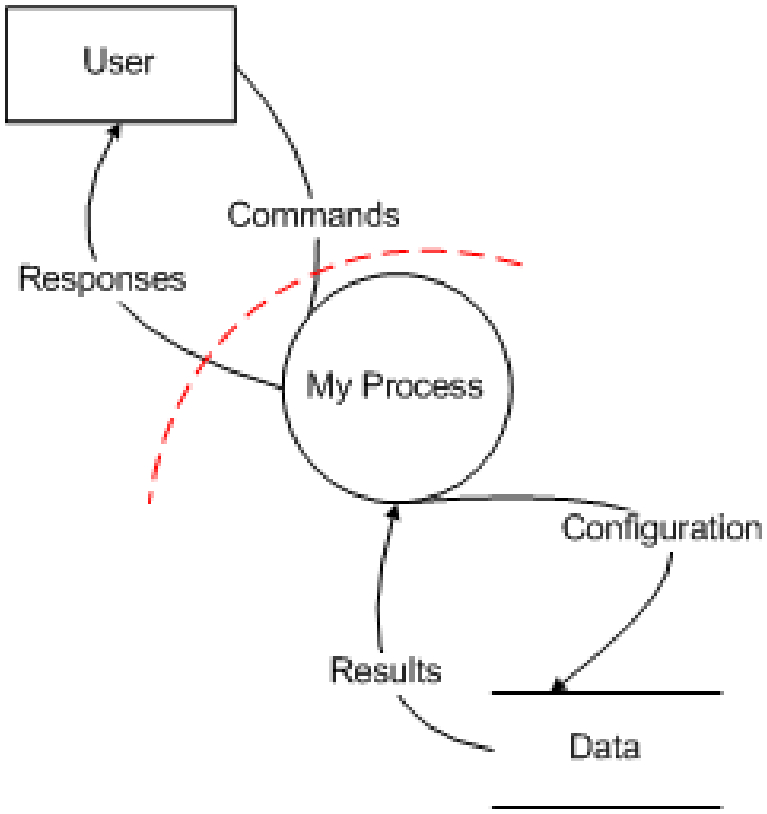
The Threat Modeling Process

1. Identify Assests
2. **Create an Architecture Overview**
3. Decompose the Application
4. Identify Threats
5. Document the Threats
6. Rate the Threats



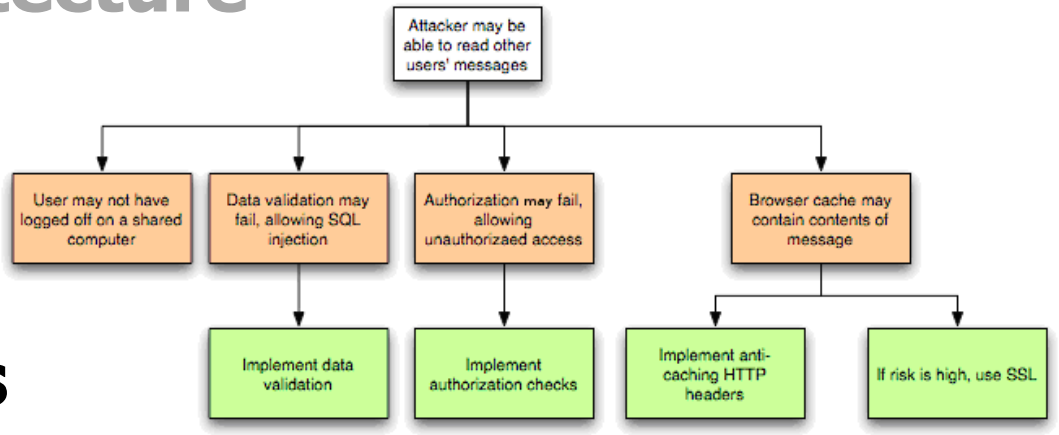
The Threat Modeling Process

1. Identify Assests
2. Create an Architecture Overview
3. **Decompose the Application**
4. Identify Threats
5. Document the Threats
6. Rate the Threats



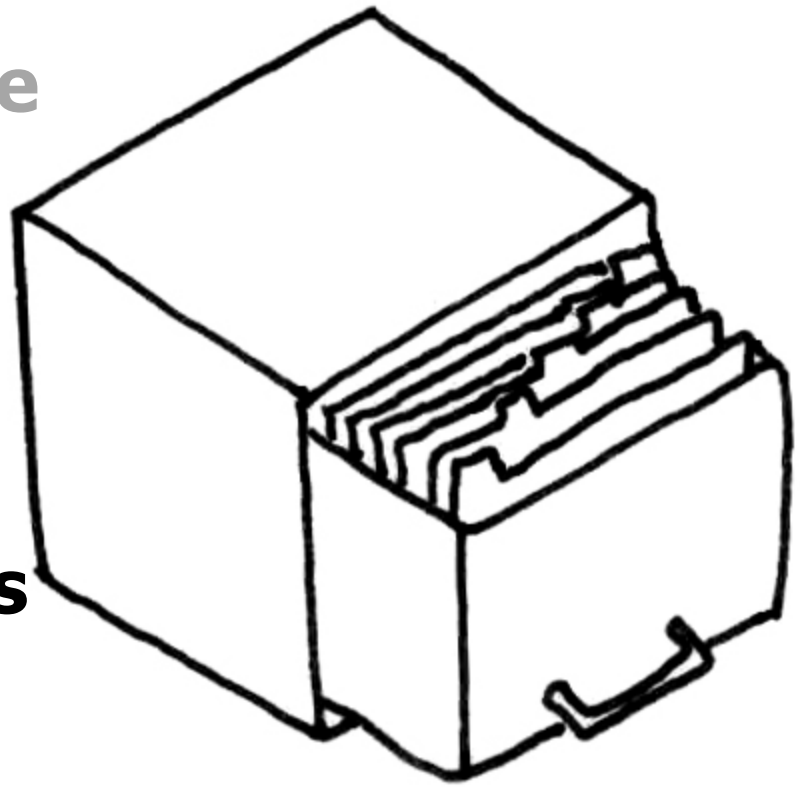
The Threat Modeling Process

1. Identify Assests
2. Create an Architecture Overview
3. Decompose the Application
4. **Identify Threats**
5. Document the Threats
6. Rate the Threats



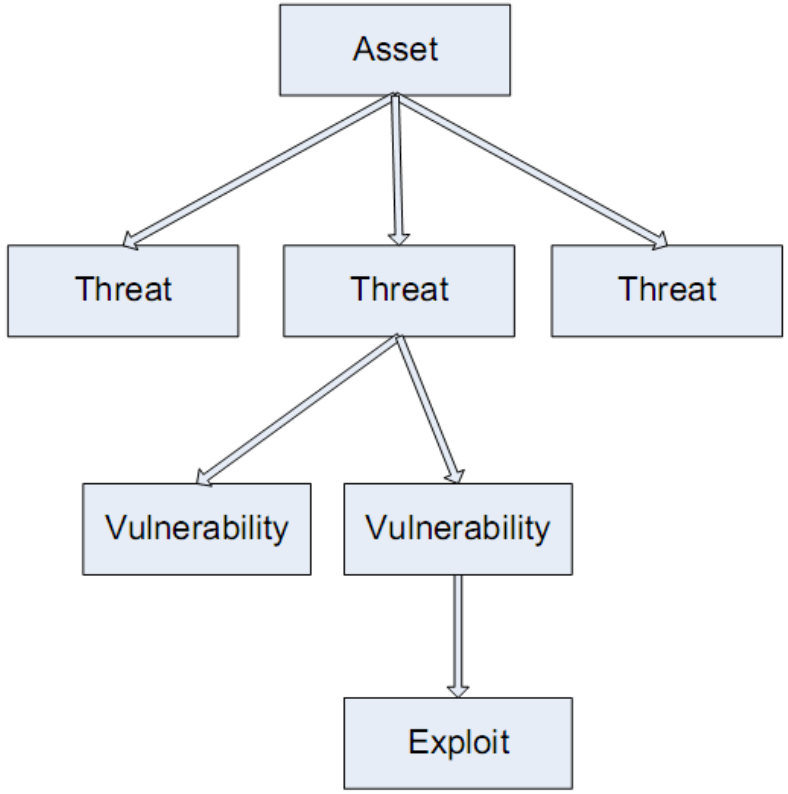
The Threat Modeling Process

1. Identify Assests
2. Create an Architecture Overview
3. Decompose the Application
4. Identify Threats
5. **Document the Threats**
6. Rate the Threats



The Threat Modeling Process

1. Identify Assests
2. Create an Architecture Overview
3. Decompose the Application
4. Identify Threats
5. Document the Threats
6. **Rate the Threats**



Threat Modeling – The process

1. **Assets / Vulnerabilties**
   1. Identify critical resources
   2. Their weaknesses
   3. How they could be harmed
2. **Threats / Risks**
   1. Best guess what would and could cause this harm
   2. How likely is it to happen
   3. The potential damage
3. **Countermeasures**
   1. Ways to prevent or reduce the damage
   2. Compare the cost of implementation
4. **Implementation**
   1. Choose and implement the best control
   2. Evaluate and document the results and lessons learned
   3. Start again

Why start again?

Threat

Risk is low

Asset

Countermeasure

Dependency's Threat

Dependency's Countermeasure

Dependency

That's it…

..thank you!

martin.knobloch@owasp.org

Remote weapons station

Loader's thermal sight

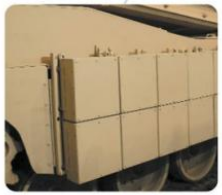
Loader's Armor Gun Shield

tank/infantry telephone

Thermal sight goggles

Rear protecting unit slat armor

Thermal sight components



Abrams Reactive Armore Tiles

OWASP