

Paweł Rajba

pawel@cs.uni.wroc.pl

<http://itcourses.eu/>

Application Security

Threat Modeling

Agenda

- Introduction
- Drivers for threat modeling
- STRIDE methodology
 - Create diagram
 - Identify threats
 - Mitigate threats
 - Validate model
- Reporting

Introduction

- Understanding threats and applying mitigations is a key to have a secured solution
- Threat modeling is a method to achieve that
- Key terms: Risk, Vulnerability, Threat
- Threat modeling:
 - a repeatable process that helps to find and mitigate all of the threats to a solution

Introduction

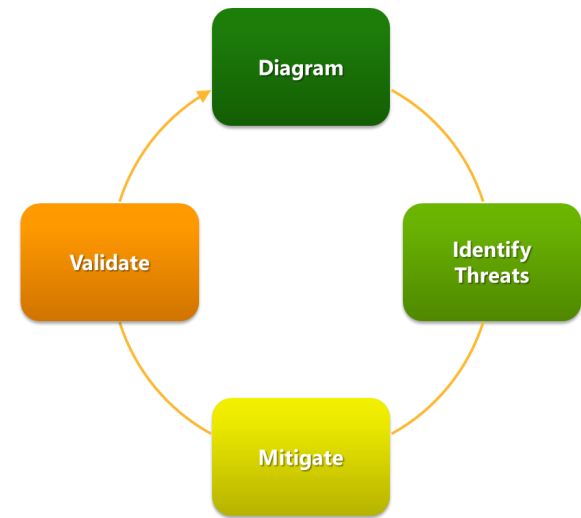
- The following items are very connected
 - Threat Model
 - Security Requirements
 - Information flows
 - Security Architecture
- Changes in any of them may affect others

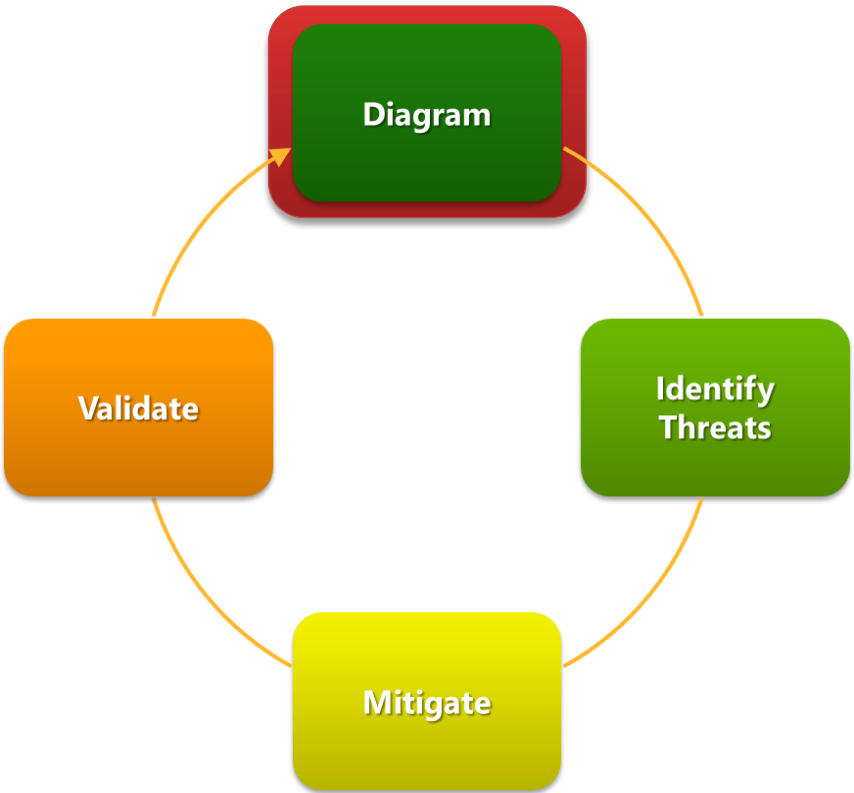
Drivers for threat modeling

- Address risks by applying appropriate and relevant security mechanisms
- Find potential problems with security in early stages
- Build security into architecture and design

STRIDE Methodology

- STRIDE stands for
 - Spoofing
 - Tampering
 - Repudiation
 - Information Disclosure
 - Denial of Service
 - Elevation of Privilege
- Every iteration follows 4 stages
- Supported by Threat Modeling Tool from MS





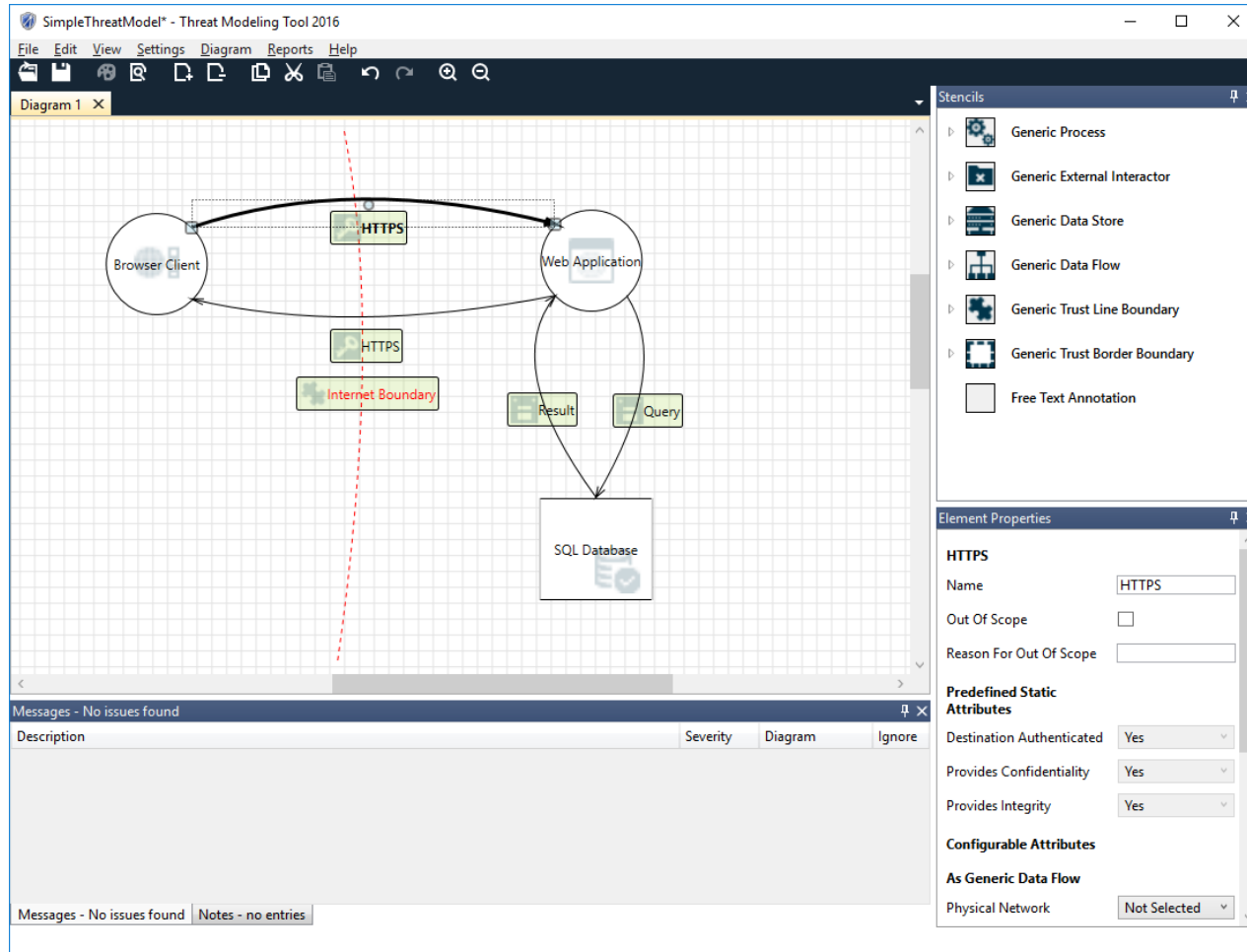
Create diagram

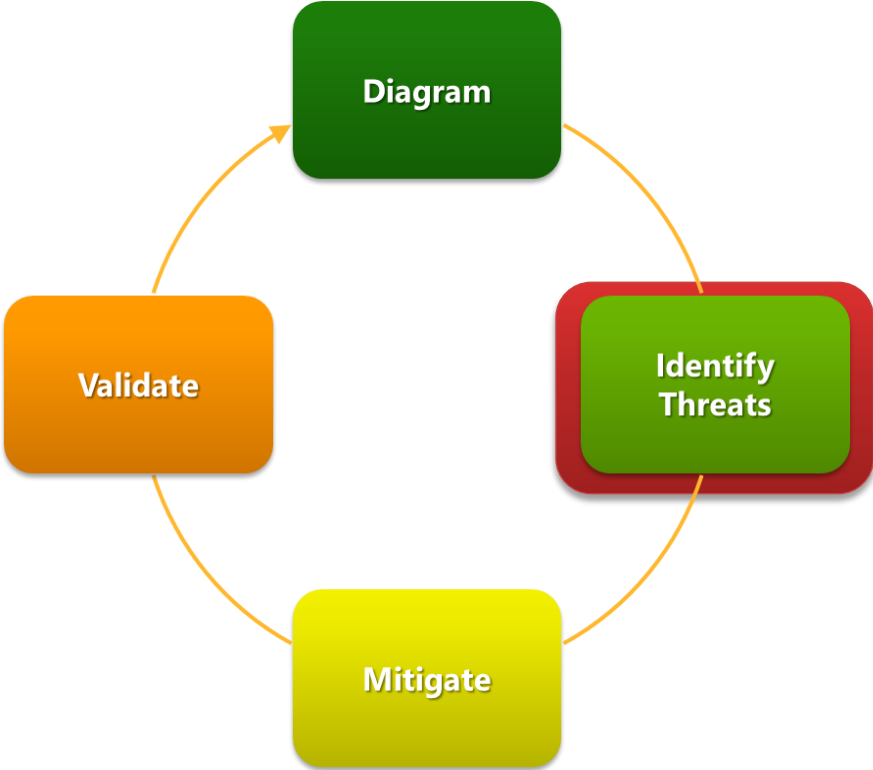
- Start with a diagram based on high-level architecture (context diagram)
- Break down specific parts if needed
- What to put on diagram?
 - Everything what transport or store data
 - Level of details depend on criticality

Create diagram

- Main categories of stencils
 - Process: components, applications, web services
 - External entity: human, system, service
 - Data store: SQL DB, configuration file, HTML5 storage, cookies, file system
 - Data flow: HTTP, Binary, IPSec, RPC, SMB
 - Trust boundary: line or border (Internet boundary)

Create diagram





Identify threats

Threat	Property to secure
S poofing	Authentication
T ampering	Integrity
R epudiation	Non-repudiation
I nformation Disclosure	Confidentiality
D enial of Service	Availability
E levation of Privilege	Authorization

Identify threats

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

Identify threats

The screenshot displays the SimpleThreatModel - Threat Modeling Tool 2016 interface. The main window shows a threat diagram with the following components:

- Browser Client** (left)
- Web Application** (right)
- SQL Database** (bottom)
- Internet Boundary** (dashed red line)
- HTTPS** (two boxes, one above the Browser Client and one above the Web Application)
- Result** and **Query** (two boxes between the Web Application and the SQL Database)

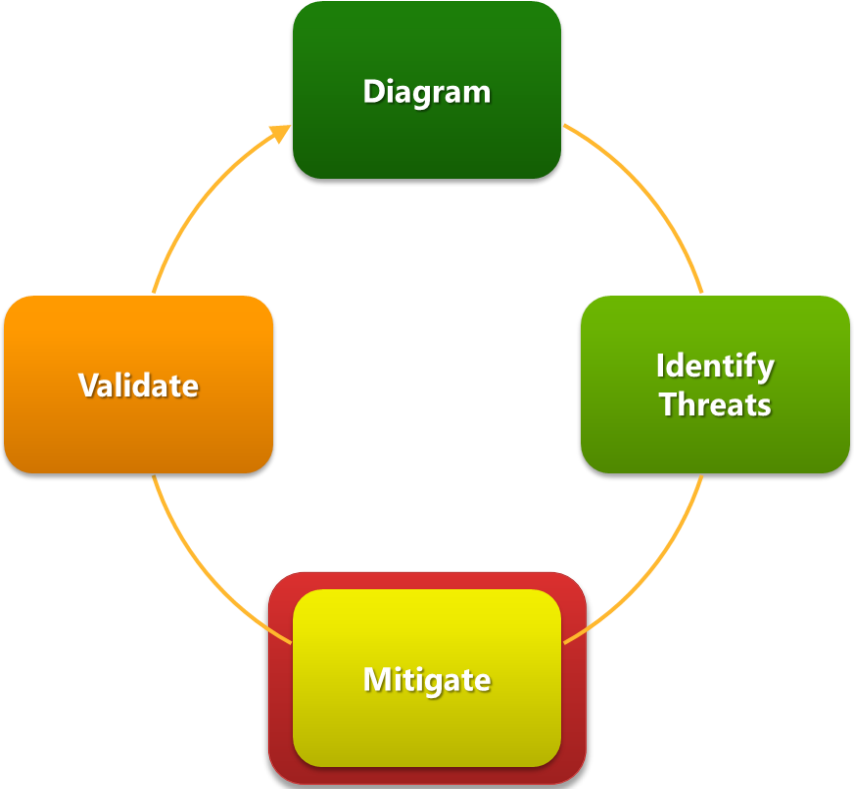
The diagram shows a flow from the Browser Client to the Web Application via HTTPS, and from the Web Application to the SQL Database via Query and Result. The Internet Boundary is positioned between the Browser Client and the Web Application.

The **Threat List** panel on the right displays a list of 25 threats. The first threat is highlighted:

Title	Category	Description	Justification
Browser Client...	Tampering	If Browser Clie...	
Cross Site Scri...	Tampering	The web server...	
Potential Data...	Repudiation	Web Applicati...	
Potential Proc...	Denial Of Servi...	Web Applicati...	
Data Flow HTT...	Denial Of Servi...	An external ag...	
Elevation Usin...	Elevation Of Pr...	Web Applicati...	
Web Applicati...	Elevation Of Pr...	Browser Clie...	
Elevation by C...	Elevation Of Pr...	An attacker m...	
Cross Site Req...	Elevation Of Pr...	Cross-site requ...	
Spoofing the...	Spoofing	Web Applicati...	
Web Applicati...	Tampering	If Web Applica...	
Potential Data...	Repudiation	Browser Clie...	
Potential Proc...	Denial Of Servi...	Browser Clie...	
Data Flow HTT...	Denial Of Servi...	An external ag...	
Elevation Usin...	Elevation Of Pr...	Browser Clie...	
Browser Clie...	Elevation Of Pr...	Web Applicati...	
Elevation by C...	Elevation Of Pr...	An attacker m...	
Spoofing of De...	Spoofing	SQL Database...	
Potential SQL I...	Tampering	SQL injection i...	
Potential Exces...	Denial Of Servi...	Does Web App...	
Spoofing of So...	Spoofing	SQL Database...	

The **Threat Properties** panel at the bottom shows the details for the selected threat:

- ID:** 1
- Diagram:** Diagram 1
- Status:** Not Started
- Title:** Browser Client Process Memory Tampered
- Category:** Tampering
- Description:** If Browser Client is given access to memory, such as shared memory or pointers, or is given the ability to control what Web Application executes (for example, passing back a function pointer.), then Browser Client can tamper with Web Application. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.
- Justification:**
- Interaction:** HTTPS
- Priority:** Link
- Threat Properties:** Notes - no entries



Mitigate threats

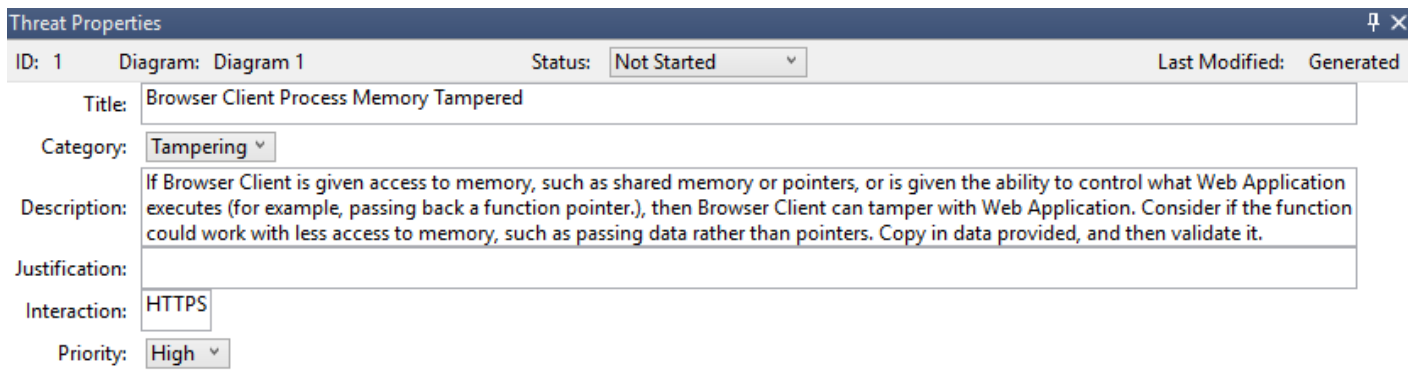
- Mitigation is the goal of Threat Modeling
- Every threat needs to be addressed
- Common ways to address threats:
 - Redesign to eliminate
 - Apply security controls
 - Accept vulnerability (permanently or temporary)
- Criticality of the asset is a crucial factor in any assessments and mitigations

Common mitigations

Threat	Property to secure	Mitigations examples
Spoofing	Authentication	<ul style="list-style-type: none">• Cookie-based authN, CAS, SAML2• Kerberos• PKI, SSL/TLS certificates• Digital signatures
Tampering	Integrity	<ul style="list-style-type: none">• Message Authentication Codes (MAC)• Digital signatures
Repudiation	Non-repudiation	<ul style="list-style-type: none">• Auditing• Digital signatures
Information Disclosure	Confidentiality	<ul style="list-style-type: none">• Encryption• ACLs
Denial of Service	Availability	<ul style="list-style-type: none">• Filtering• Quotas, timeouts• High-availability design, load balancers
Elevation of Privilege	Authorization	<ul style="list-style-type: none">• Group or role membership• Privilege ownership

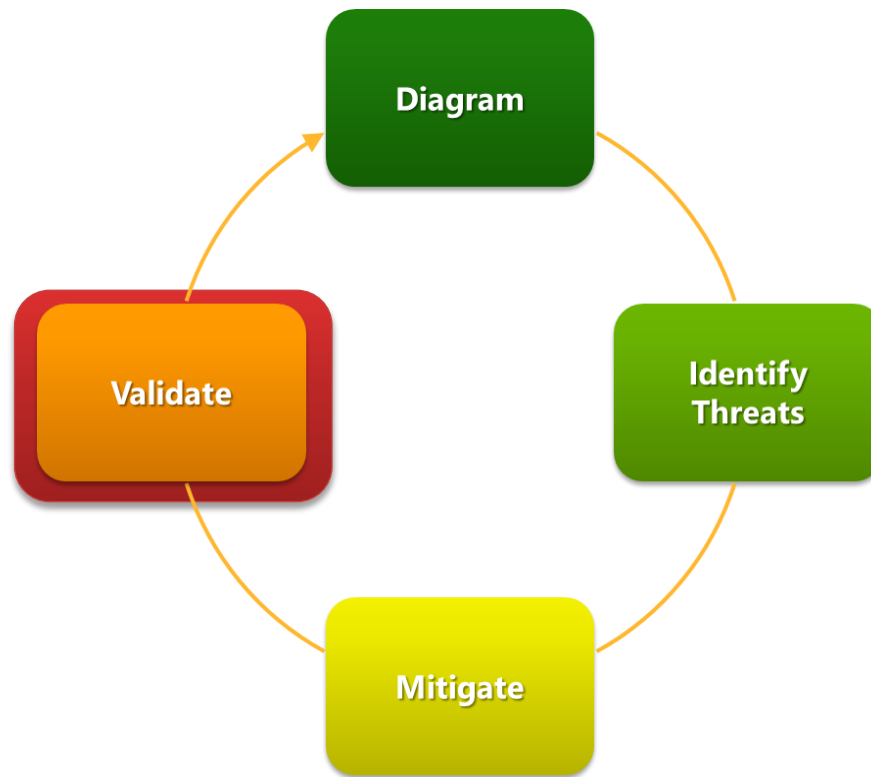
Tool support

- Switch to analysis view
- Work with:
 - Statuses: Not Started, Needs Investigation, Not Applicable, Mitigated
 - Priorities: High, Medium, Low
- Put Justification



The screenshot shows a 'Threat Properties' dialog box with the following fields and values:

Field	Value
ID	1
Diagram	Diagram 1
Status	Not Started
Last Modified	Generated
Title	Browser Client Process Memory Tampered
Category	Tampering
Description	If Browser Client is given access to memory, such as shared memory or pointers, or is given the ability to control what Web Application executes (for example, passing back a function pointer.), then Browser Client can tamper with Web Application. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.
Justification	
Interaction	HTTPS
Priority	High



Validate Threat Model

- Do diagrams match the current state?
 - Are changes in requirements and architecture applied in threat model?
- Are threats enumerated and mitigated?
 - Are mitigations associated with threats correctly?

Reporting

Generate Custom Report [X]

Custom Report Settings

Threat states to include in report:

- Not Started
- Needs Investigation
- Not Applicable
- Mitigated
- Include Migrated Threats

Generate Report

Generate Report [X]

Custom Threat Properties

Threat properties to include in report:

Generate Report



Threat Modeling Report

Created on 11.06.2017 15:01:00

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	25
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	25
Total Migrated	0

Diagram: Diagram 1

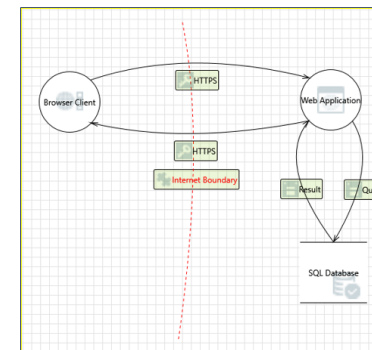


Diagram 1 Diagram Summary:

Not Started	25
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	25
Total Migrated	0

Final questions

- How to connect threat modeling in the SDL?
- How to make connection between Threat Modeling Tool and other tools?
 - Create tasks in TFS or Jira
 - Update mitigations