Paweł Rajba
pawel@cs.uni.wroc.pl
http://itcourses.eu/

Information Systems Security

Threat Modeling

Agenda

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

Introduction

- Weakness
  - Common Weakness Enumeration (CWE)
  - Example
    - CWE-326: Inadequate Encryption Strength
  - https://cwe.mitre.org/
- Vulnerability
  - Common Vulnerabilities and Exposures (CVE)
  - Example
    - CVE-2016-0800 – a security vulnerability that allows to weaken TLS encryption if a vulnerable server supports SSLv2
      - DROWN (Decrypting RSA with Obsolete and Weakened eNcryption)
  - https://cve.mitre.org/
- Attack patterns
  - Common Attack Pattern Enumeration and Classification (CAPEC)
  - Example
    - CAPEC-245 describes an XSS attack using doubled characters
      [related to „CWE-85: Doubled Character XSS Manipulations".]
  - https://capec.mitre.org/
- CVSS
  - Common Vulnerability Scoring System
  - https://www.first.org/cvss/calculator/3.0

https://infosec-handbook.eu/blog/cvss-cve-cwe-capec/

Introduction

- Threat: a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.
- Threat can be
  - Intentional
  - Accidental

Introduction

- Basic input to risk

Value of an asset	A	e.g. bike
Threat	T	e.g. someone will steal it
Vulnerability	V	e.g. you leave it without locking

- Usually we convert the above to

Business Impact	I	e.g. cost of the bike, consequence we don’t have it
Probability	P	e.g. how likely it is someone exploit the lack of lock, so threat will materialize

- Risk = f(I, P)

Introduction

- Threat modeling:
  - a repeatable process that helps to find and mitigate all of the threats to a solution
- Understanding threats and applying mitigations is a key to have a secured solution

Introduction

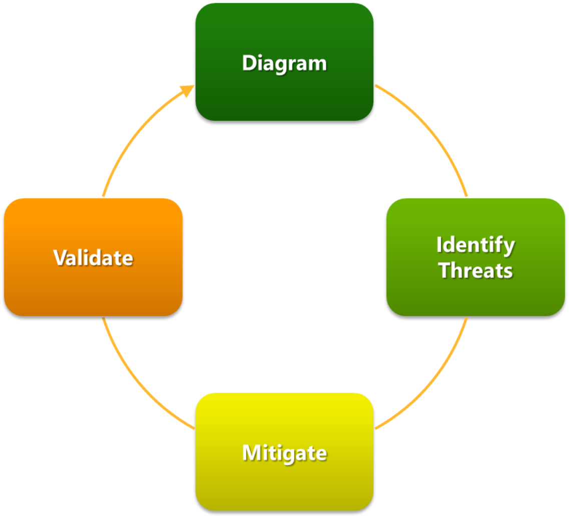
- The following items are very connected
  - Threat Model
  - Security Requirements
  - Information flows
  - Security Architecture
- Changes in any of them may affect others

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



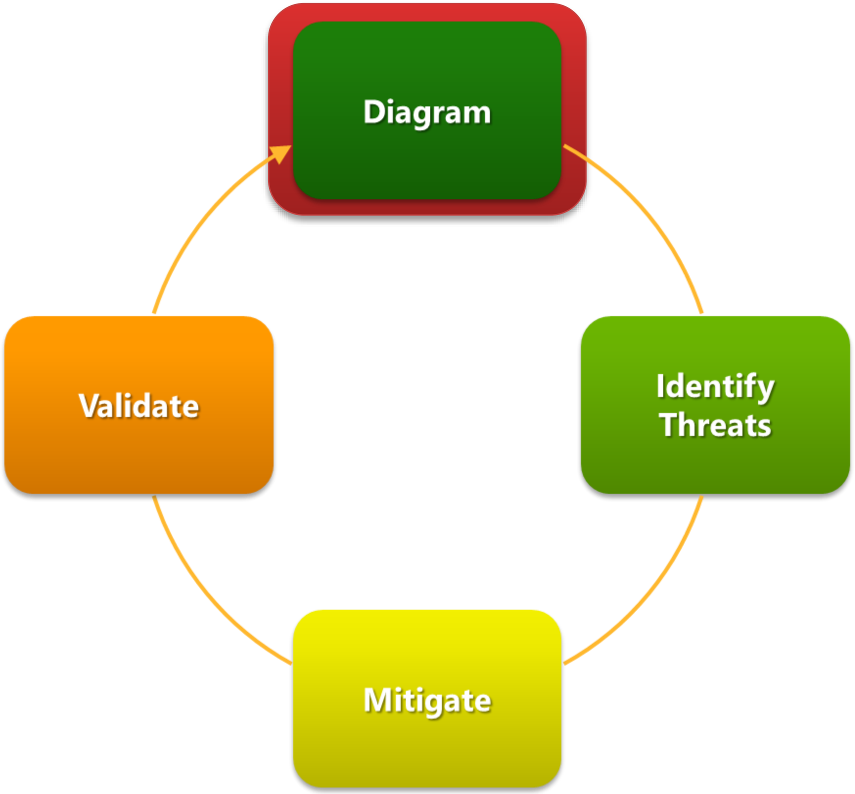


Diagram
Identify Threats
Mitigate
Validate

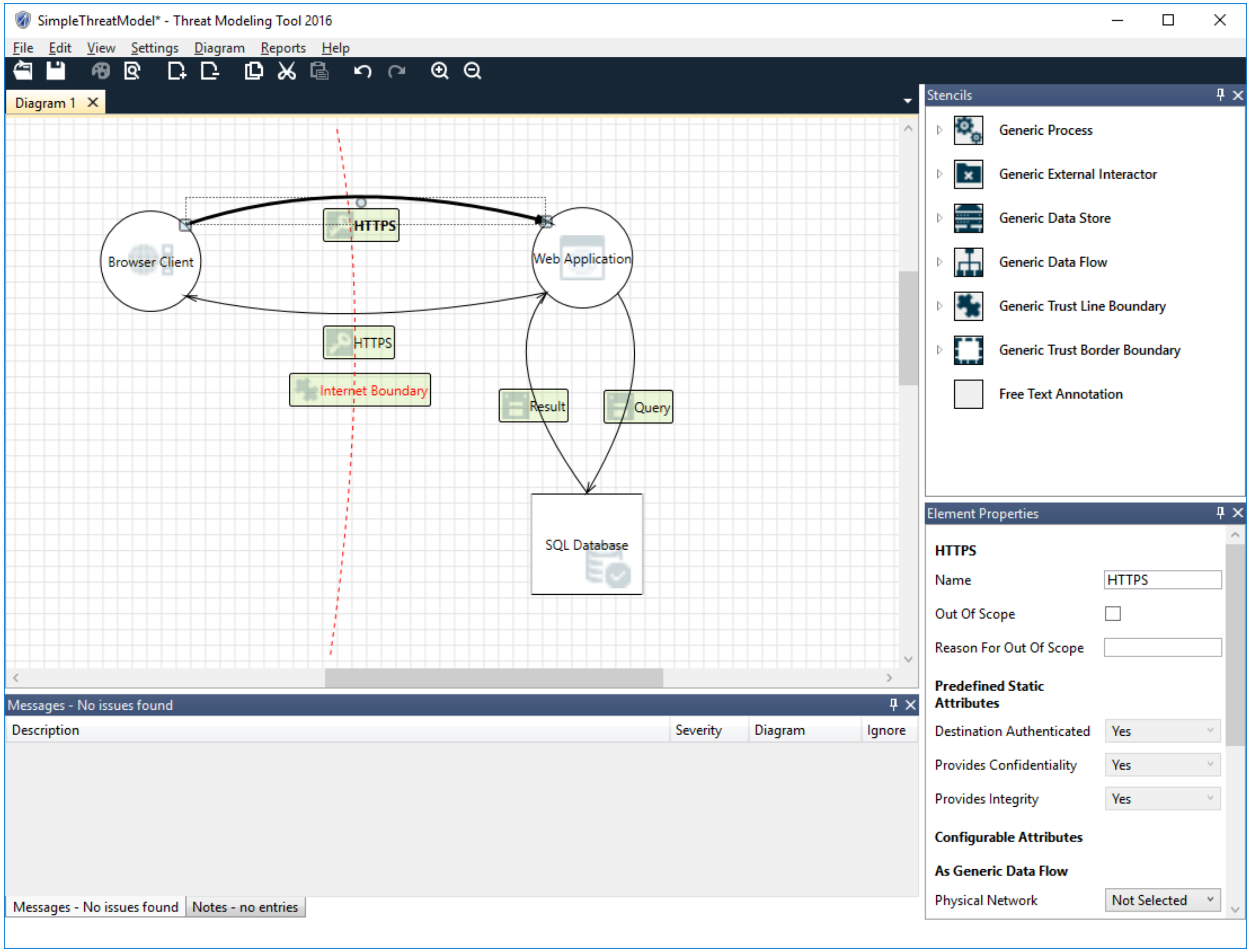
Create diagram

- 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



Description	Severity	Diagram	Ignore

HTTPS

Name: HTTPS

Out Of Scope: ☐

Reason For Out Of Scope:

Predefined Static Attributes

Destination Authenticated: Yes

Provides Confidentiality: Yes

Provides Integrity: Yes

Configurable Attributes

As Generic Data Flow

Physical Network: Not Selected

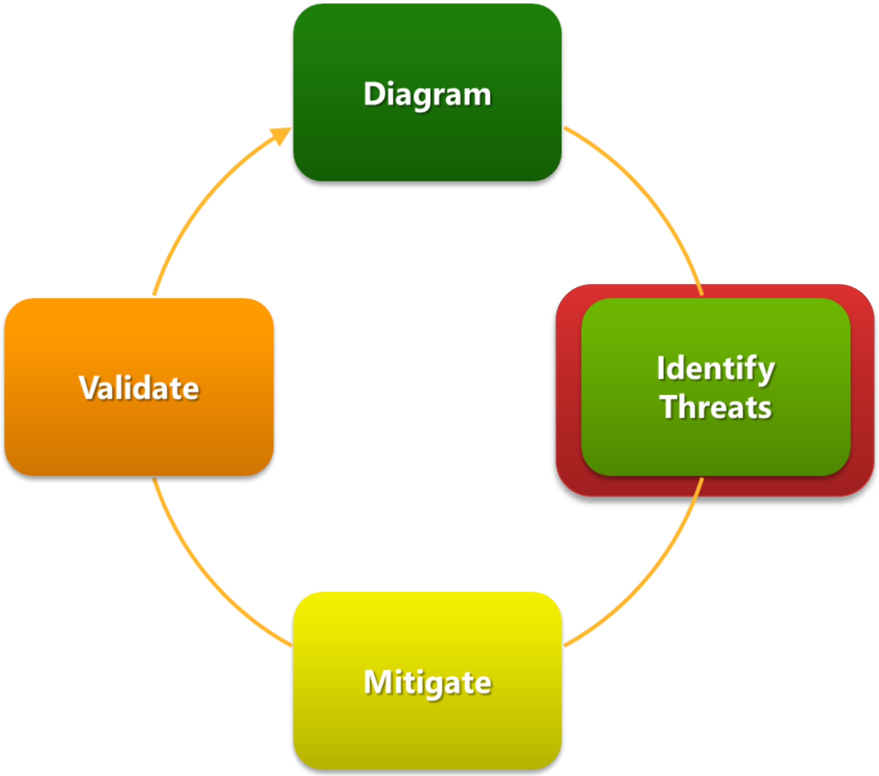
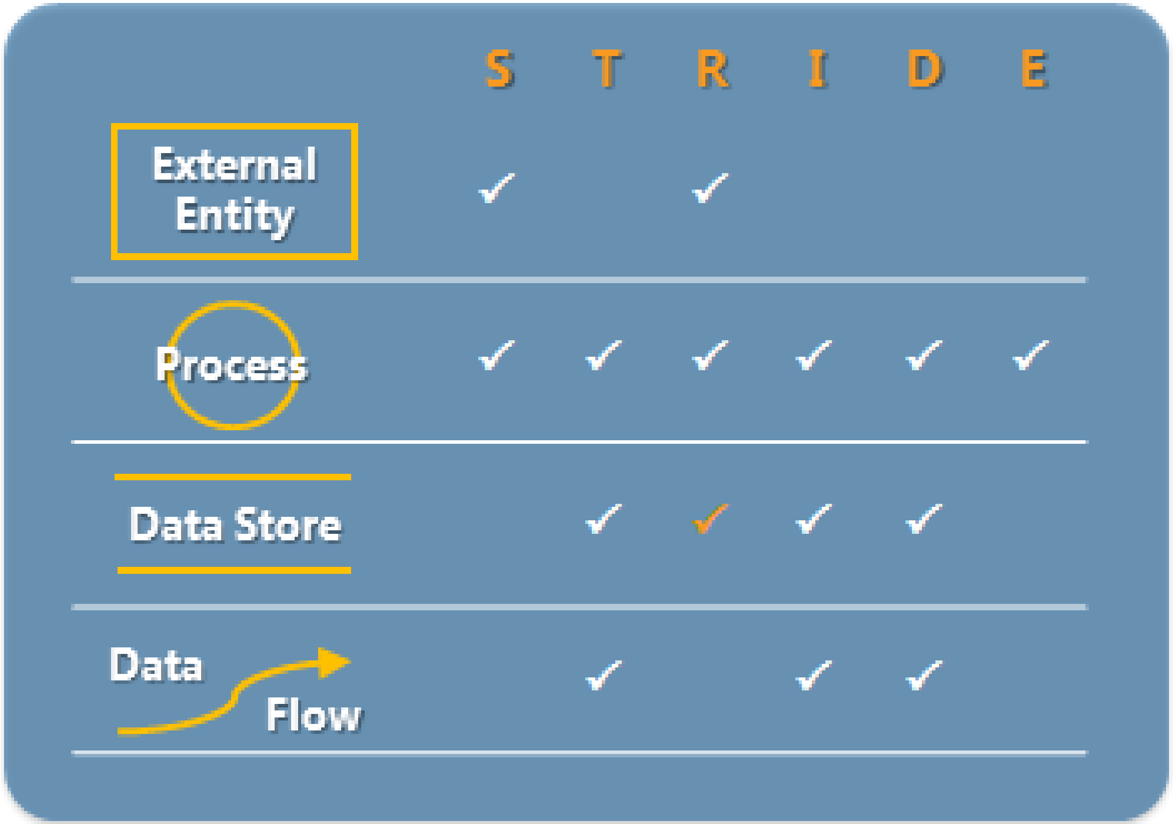


Diagram
Identify Threats
Mitigate
Validate

Identify threats

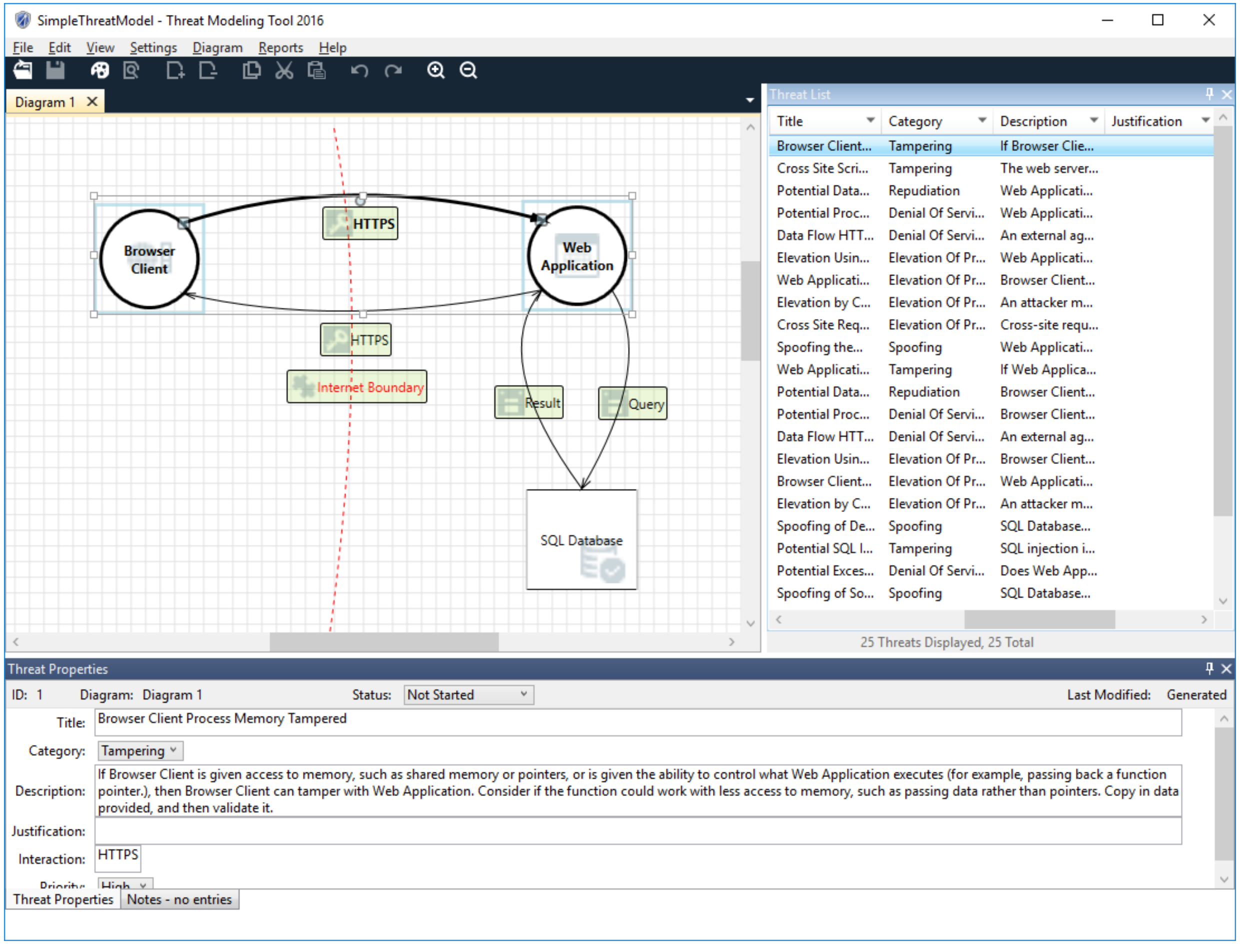
Threat	Property to secure
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Identify threats



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

Identify threats



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 Client...	
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 Client...	
Potential Proc...	Denial Of Servi...	Browser Client...	
Data Flow HTT...	Denial Of Servi...	An external ag...	
Elevation Usin...	Elevation Of Pr...	Browser Client...	
Browser Client...	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...	

25 Threats Displayed, 25 Total

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

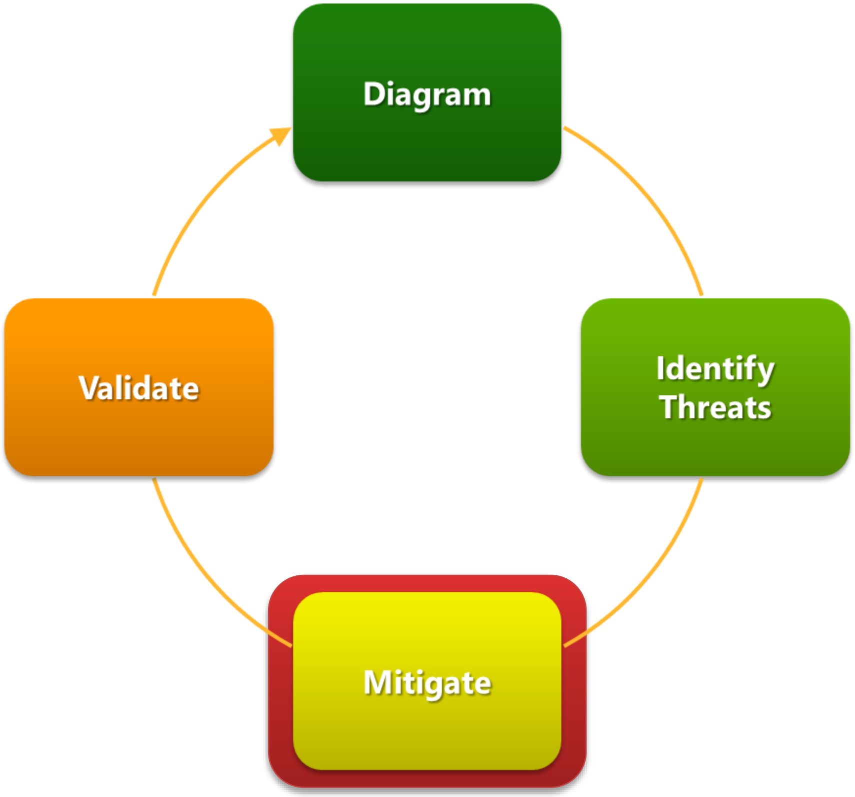


Diagram
Identify Threats
Mitigate
Validate

Mitigate threats

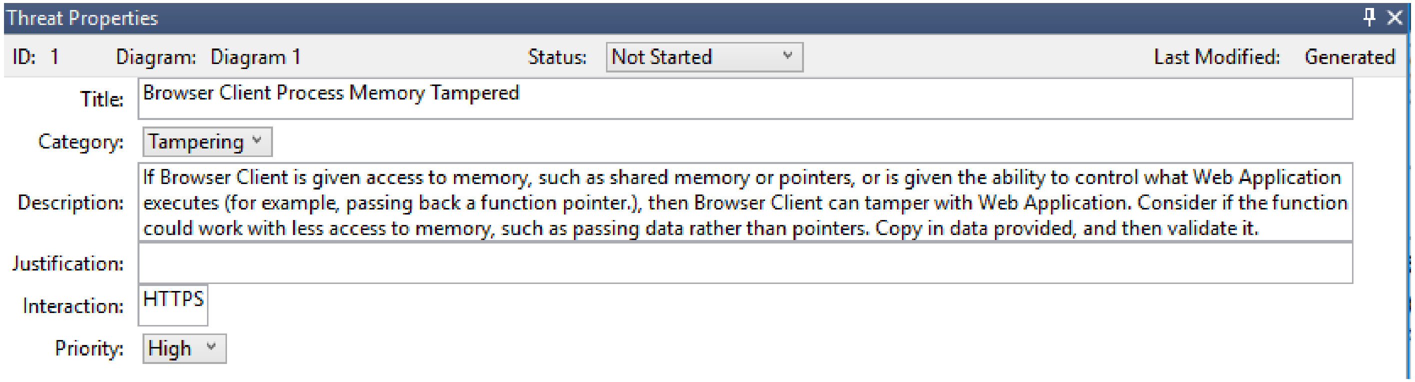
- Mitigation is the goal of Threat Modeling
- Every threat needs to be addressed
- Common ways to address threats:
  - Redesign to eliminate
  - Apply security controls
  - Accept vulnerability (permanently or temporary)
- Criticality of the asset is a crucial factor in any assessments and mitigations

Common mitigations

Threat	Property to secure	Mitigations examples
Spoofing	Authentication	• Cookie-based authN, CAS, SAML2 • Kerberos • PKI, SSL/TLS certificates • Digital signatures
Tampering	Integrity	• Message Authentication Codes (MAC) • Digital signatures
Repudiation	Non-repudiation	• Auditing • Digital signatures
Information Disclosure	Confidentiality	• Encryption • ACLs
Denial of Service	Availability	• Filtering • Quotas, timeouts • High-availability design, load balancers
Elevation of Privilege	Authorization	• 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



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

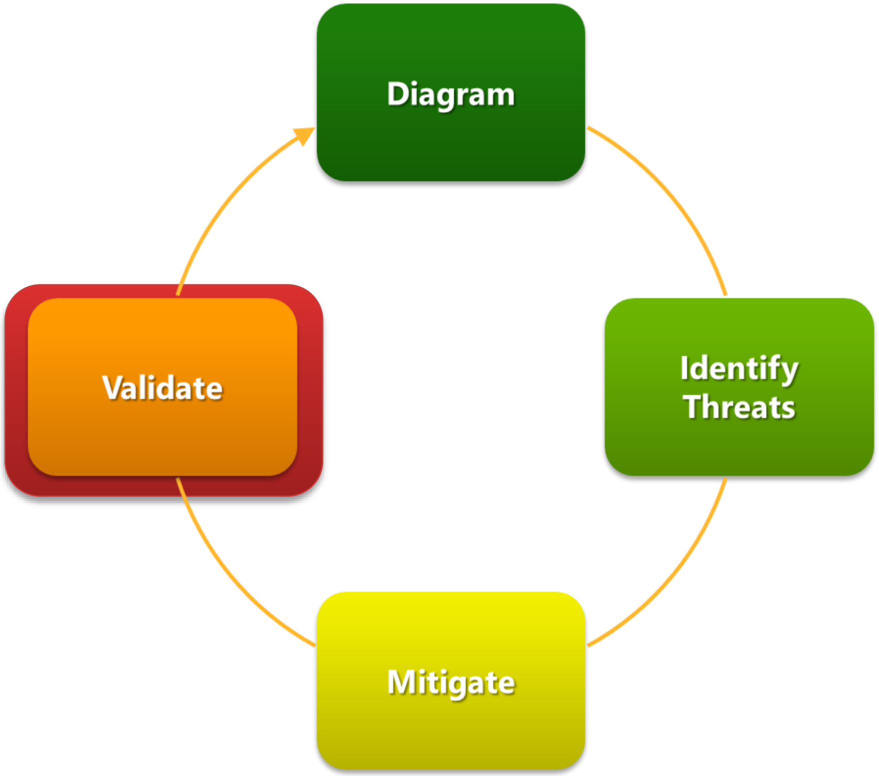
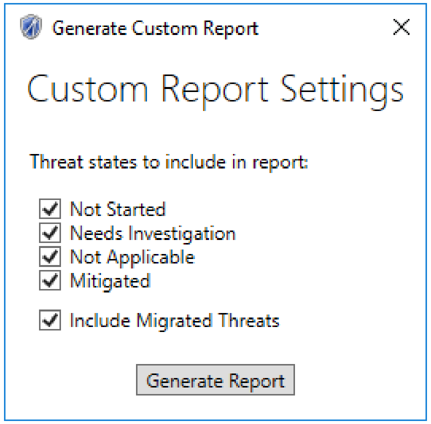


Diagram
Identify Threats
Mitigate
Validate

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



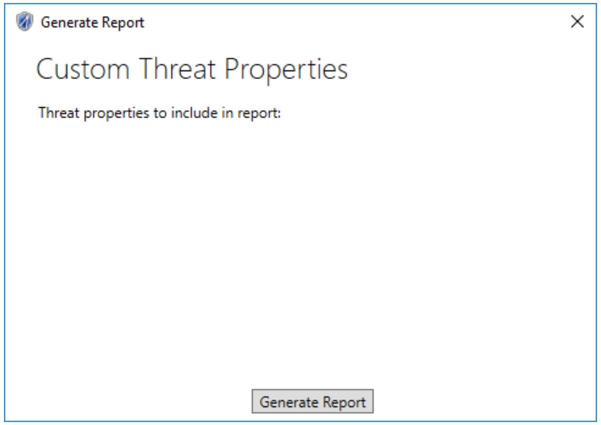
Generate Custom Report

Custom Report Settings

Threat states to include in report:

- ☑ Not Started
- ☑ Needs Investigation
- ☑ Not Applicable
- ☑ Mitigated

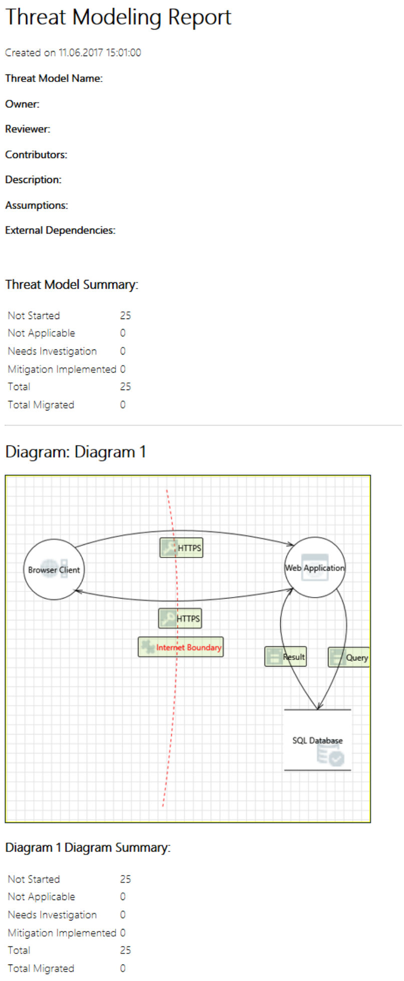
☑ Include Migrated Threats



Generate Report

Custom Threat Properties

Threat properties to include in 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:

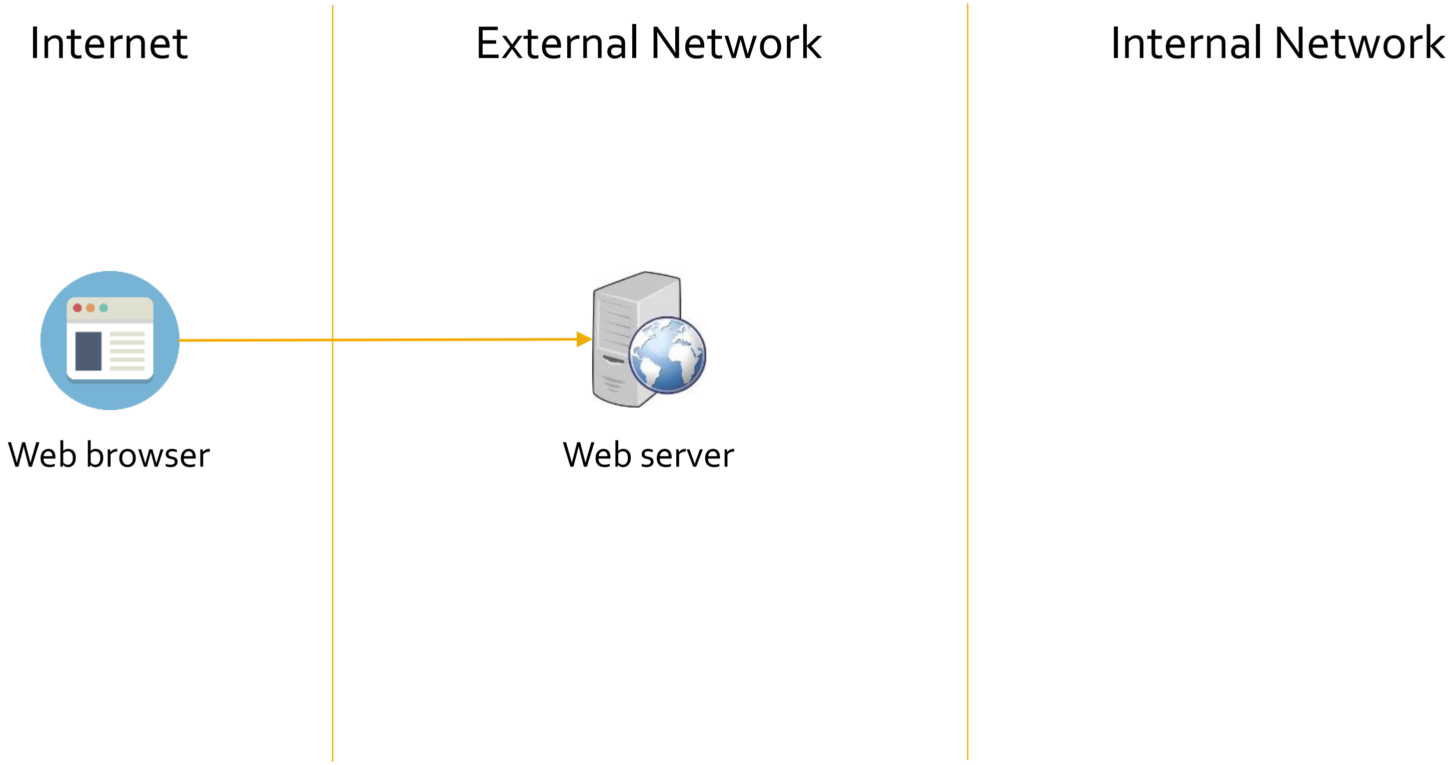
Not Started	25
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	25
Total Migrated	0

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

Examples

- Simple scenario



Internet

External Network

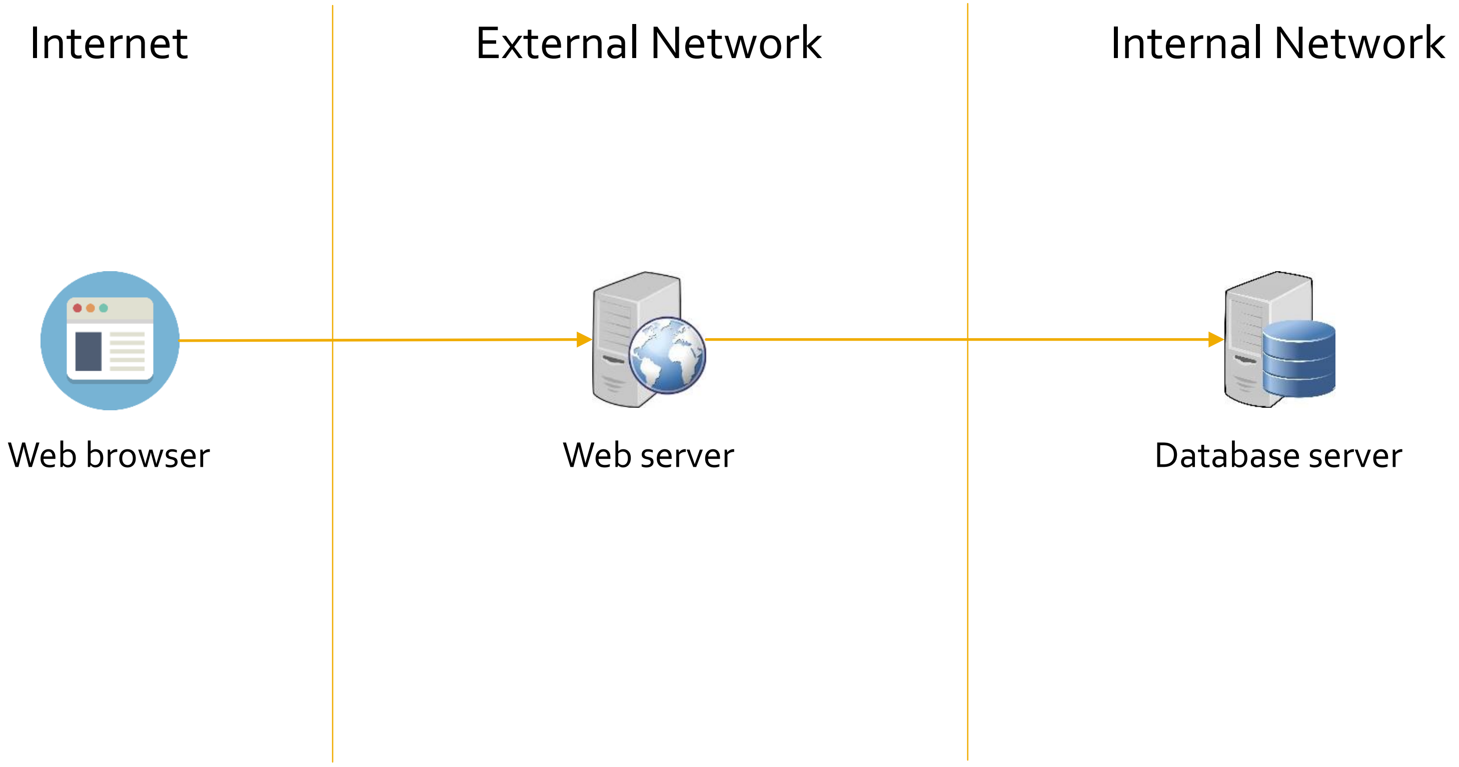
Internal Network

Web browser

Web server

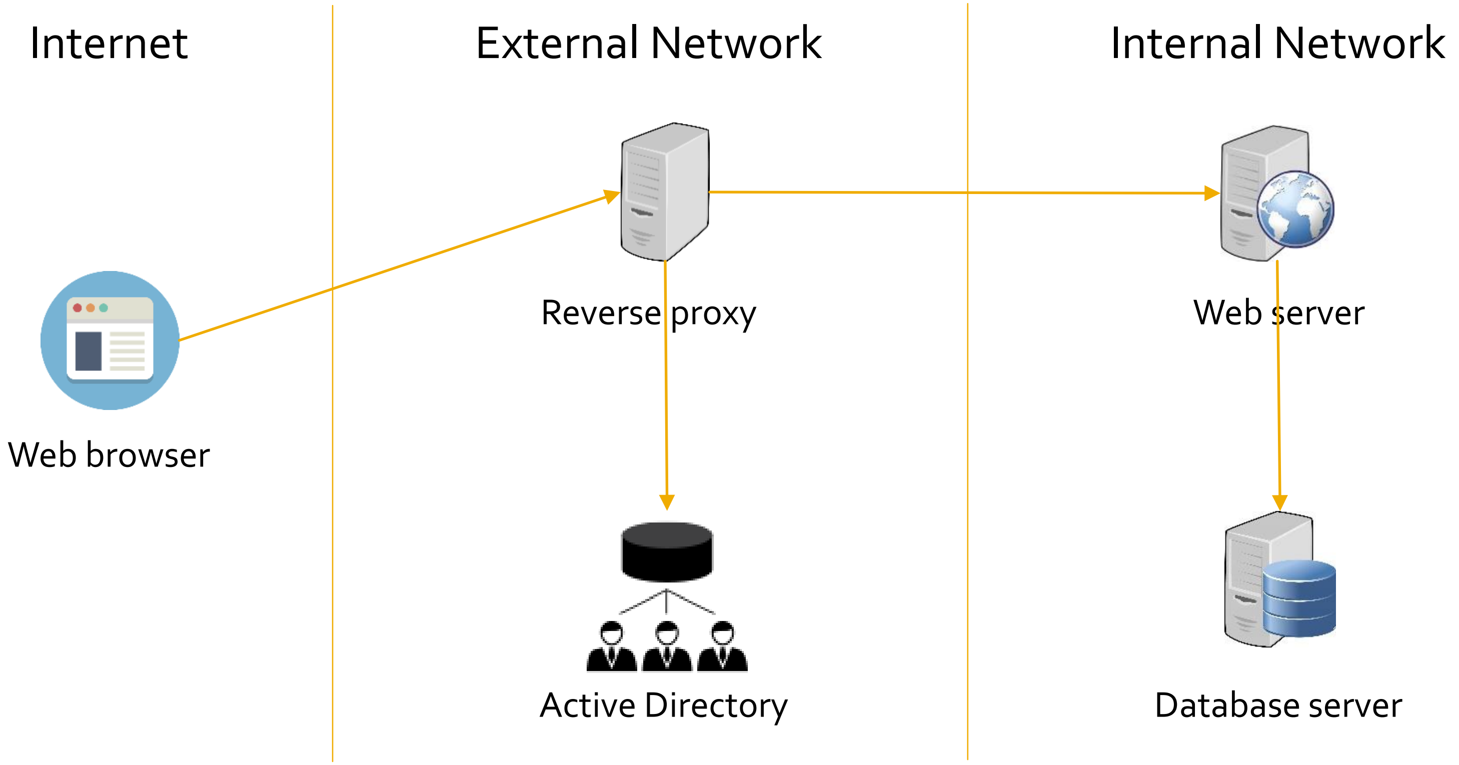
Examples

- Simple scenario with a database



Examples

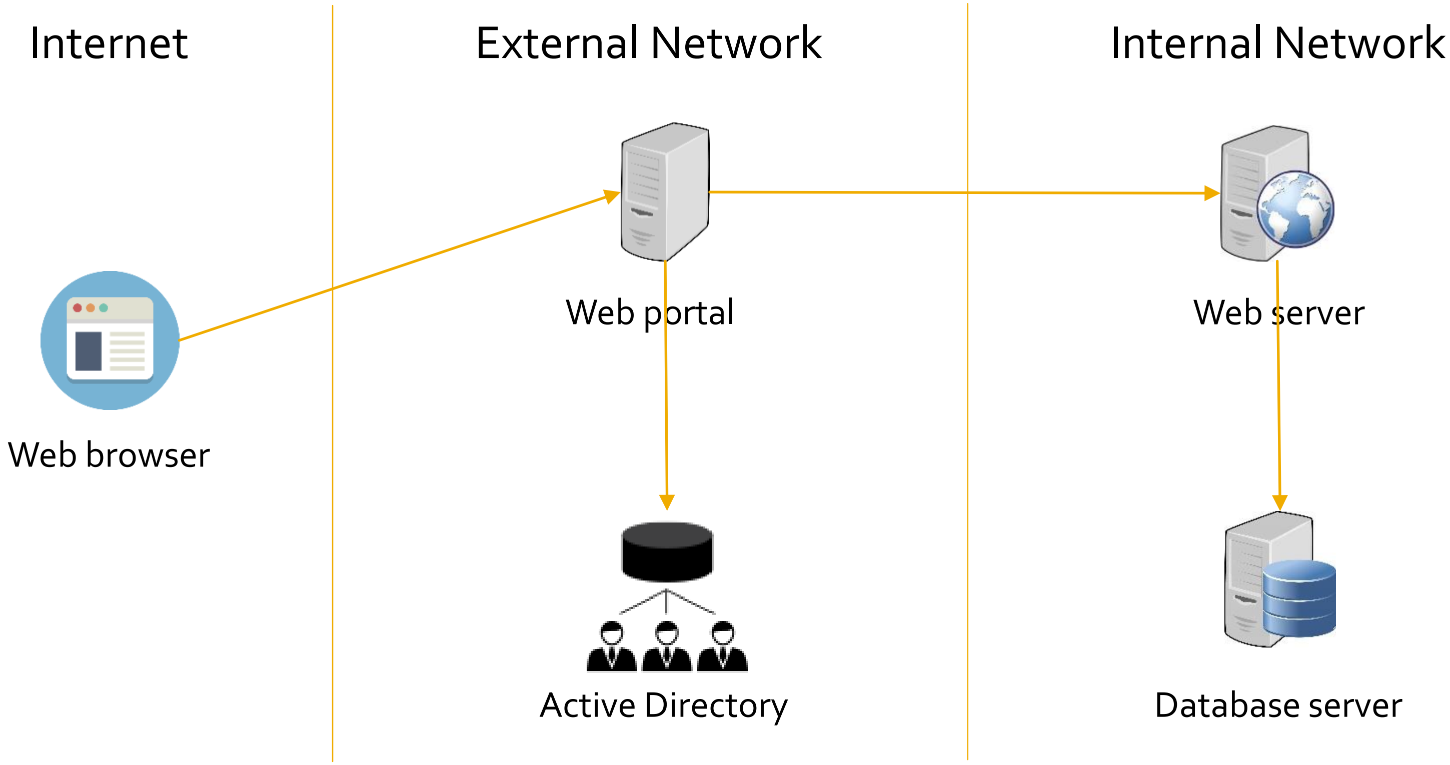
- Scenario with a reverse proxy



Q: Where is the EP? What is the split between Reverse Proxy and Web server?
Role of Web Access Management

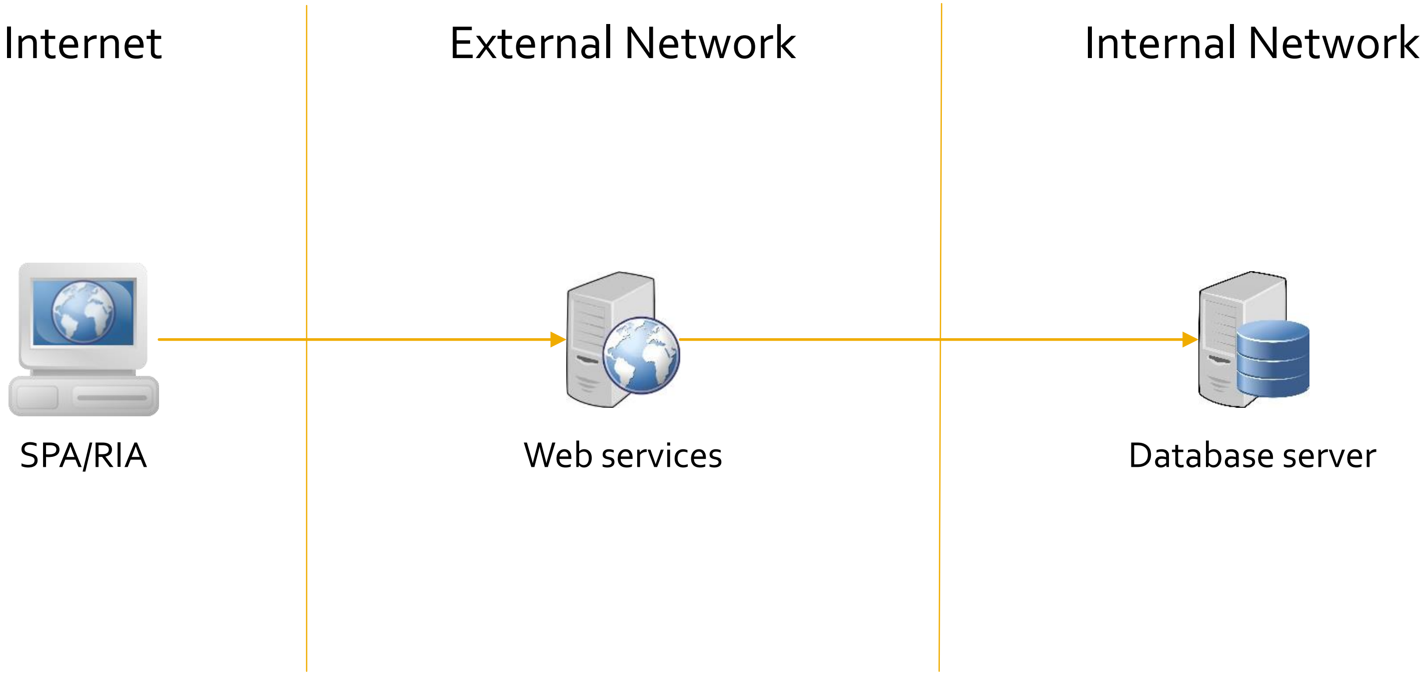
Examples

- Scenario with a web portal (including SSO)



Examples

- Simple scenario with a SPA/RIA



Q: What if client needs to support offline mode?