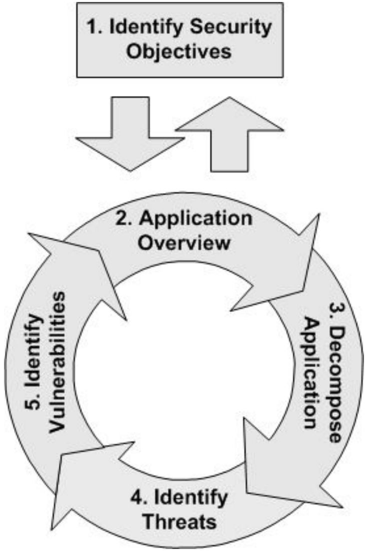
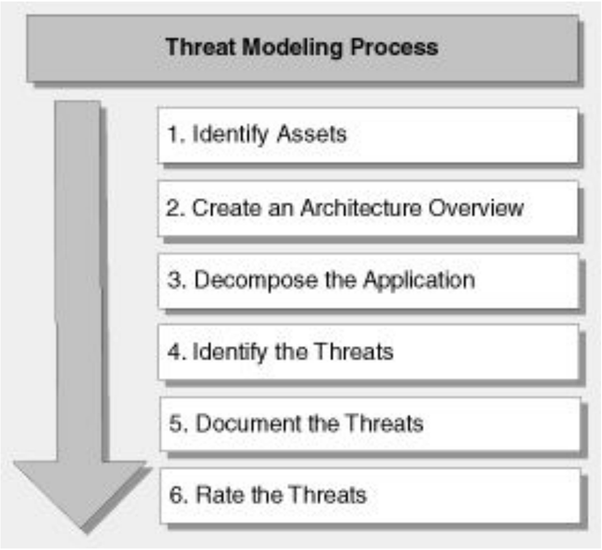
Recitation 11

Threat Modeling

Threat Modeling





Source: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN

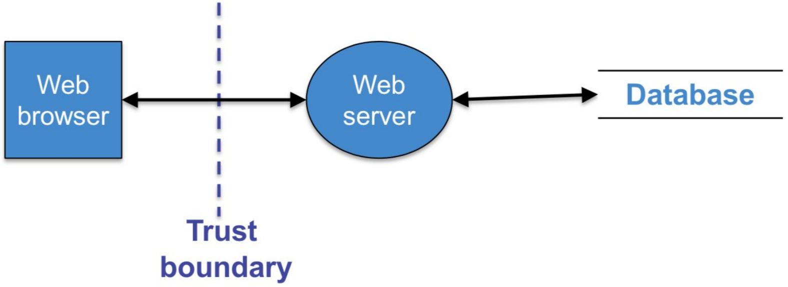
STRIDE

● S	- Spoofing	- violates authentication
● T	- Tampering	- violates integrity
● R	- Repudiation	- violates non-repudiation
● I	- Information disclosure	- violates confidentiality
● D	- Denial of service	- violates availability
● E	- Elevation of privilege	- violates authorization

Example - Web Application

- **Assets and security objectives**
  - User credentials, user profile
  - Maintain availability
- **Architecture overview**
  - Data flow diagram (DFD)
- **Decompose application**
- Identify threats
- Document threats
- Rate threats

Data Flow Diagram



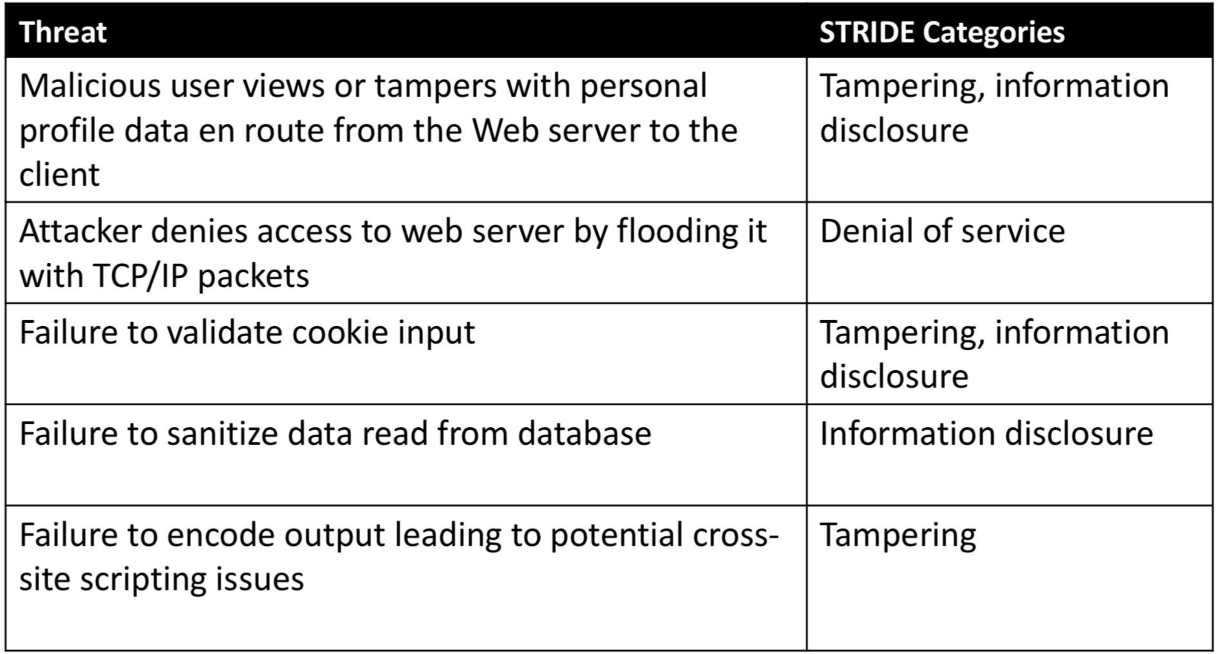
Item	Purpose	Symbol
Data flow	Data in motion over network	Arrow
Data store	File, database, etc.	Parallel lines
Process	Computation or program	Circle
Multi-Process	Multiple processes	Two circles
Trust boundary	Border between trusted/un-trusted entities	Dotted line
Interactor	System end points	Rectangle

http://msdn.microsoft.com/en-us/magazine/cc163519.aspx#S3

Example - Web Application

- Assets and security objectives
  - User credentials, user profile
  - Maintain availability
- Architecture overview
  - Data flow diagram (DFD)
- Decompose application
- **Identify threats**
- **Document threats**
- **Rate threats**

Threats



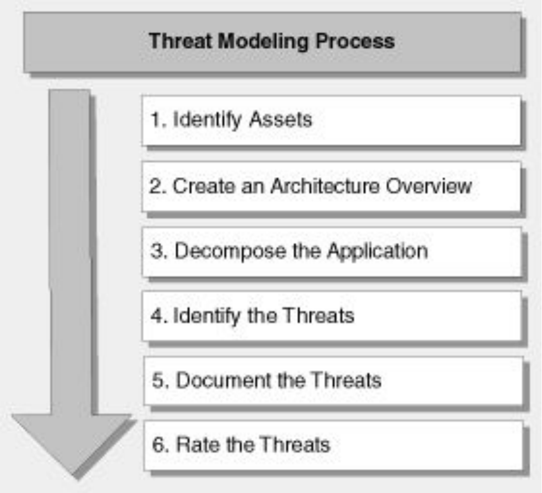
Threat	STRIDE Categories
Malicious user views or tampers with personal profile data en route from the Web server to the client	Tampering, information disclosure
Attacker denies access to web server by flooding it with TCP/IP packets	Denial of service
Failure to validate cookie input	Tampering, information disclosure
Failure to sanitize data read from database	Information disclosure
Failure to encode output leading to potential cross-site scripting issues	Tampering

Scenario

- **System**
  - Amazon-like online shopping platform
  - ML component recommends products based on user ratings
- **Context**:
  - Several vendors are in close competition for selling products of similar types
- **Attacker’s goal**
  - Favor certain vendor’s products to be recommended over the others

Steps 1-3

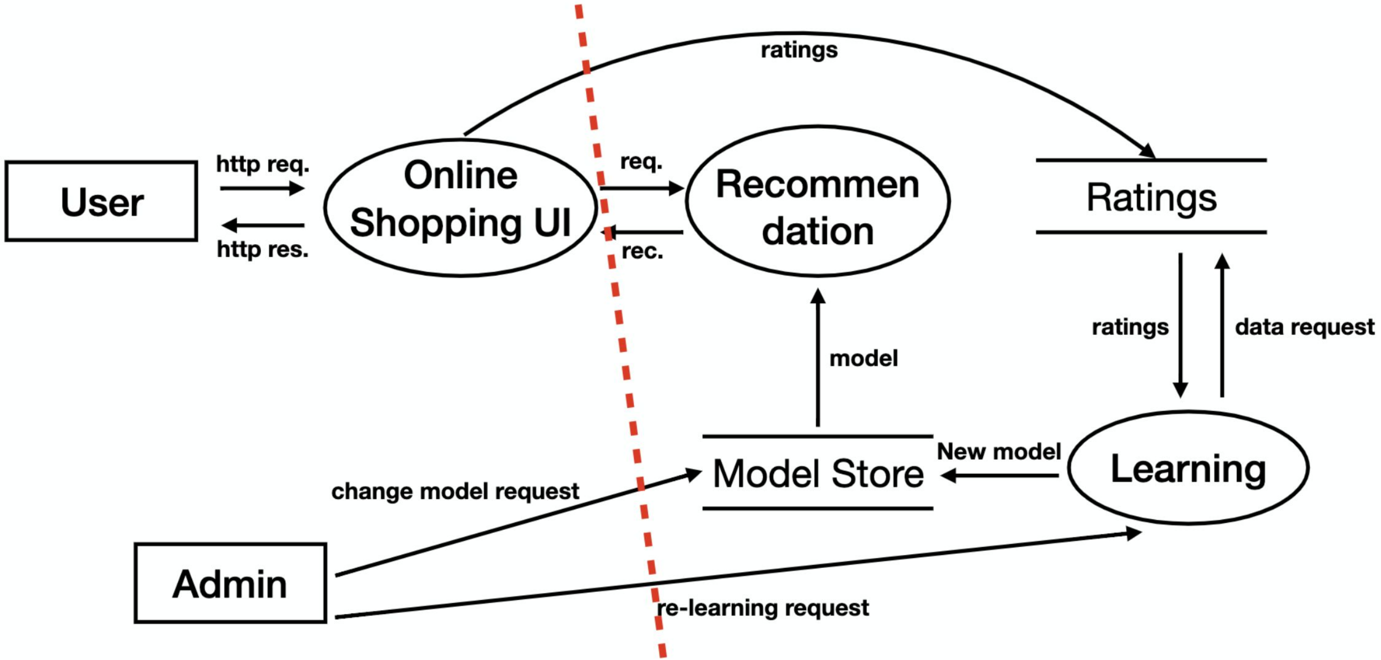
- What are the assets?
- What is our security objective?
- What components are there in our system?
- Where should we draw the trust boundary?
- What data goes in and out via the trust boundary?
    - Includes user interactions via interfaces



Threat Modeling Process

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

Data Flow Diagram



Threats

- **Spoofing**
  - A developer is able to login as an admin by getting access to old cookies - accessed from the same browser
- **Tampering**
  - Modifying the training dataset with incorrect labels (poisoning - data modification)
  - Rate a good product poorly - fed back directly as training data (poisoning - data injection, evasion)
- **Repudiation**
  - User denies giving a bad rating to a product, We're unable to identify who changed the model
- **Information disclosure**
  - Training dataset is accessible to competitors, Model details (algorithm, parameters) are known to outsiders
- **Denial of service**
  - Recommendation system goes down / degrades in latency with X number of concurrent requests
- **Elevation of privilege**
  - A developer is able to change the production model instead of an admin

Thank You!