



SSE-LAB 3: Security Risk Assessment

Riccardo Scandariato

Institute of Software Security, TUHH, Germany

ric***do . scanda***to @ tuhh.de

Lecturer: Nicolás Díaz Ferreyra

THREAT MODEL

A threat model is a **conceptual representation** of a *system*, and the *threats* that may affect it:

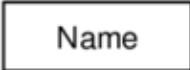


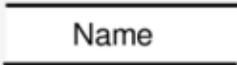
- Assets: Things or entities of **great value** that must be properly secured.
- Threat: Anything that could let someone (or something) *obtain*, *damage*, or *destroy* an asset \Rightarrow potential causes of **unwanted incidents!**

Model A representation or simplified version of a system.

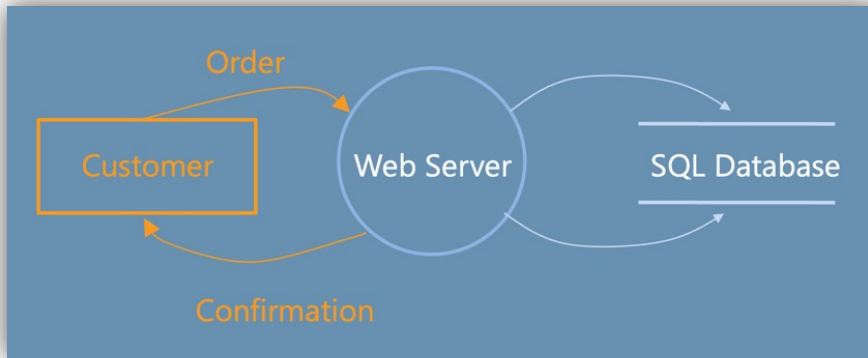
- It abstracts away the details so we can look at the whole picture.
- It contains only those features that are of primary importance.
- Structured diagrams include **DFDs**, swim lanes, and state machines...

It allows to identify and mitigate potential security issues early

DATA FLOW DIAGRAMS (DFDs)

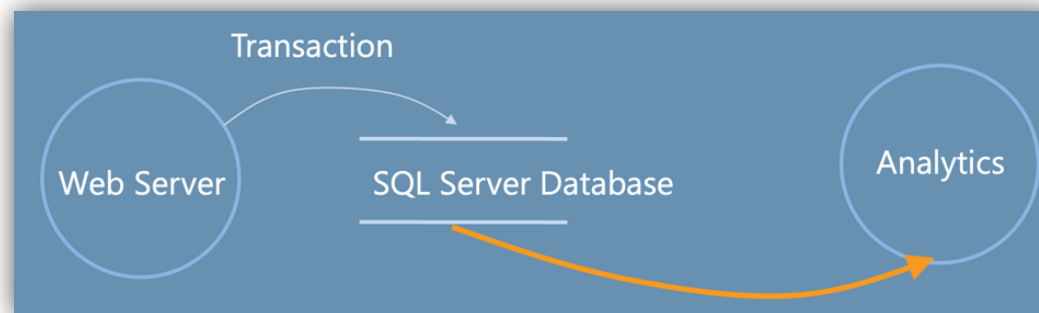
Name	Notation	Meaning
Neighboring System/Actor (also Terminator, Source or Sink)		Depicts persons, organizations of technical systems, equipment, sensors, actuators from the system environment that are source of sink for the information to / from the system
Nodes (Process, Function of the System)		Depicts a desired functionality in the system
Data flow		Depicts moving data (inputs, outputs, intermediate results). Not only data flows can be depicted but also material flows or energy flows.
Data store		Depicts data at rest, i.e., information that is stored for a certain period and that is not directly flowing between functions

DFDs: Heuristics (rules of thumb)



Data comes from external entities or data stores

Data does not flow magically,
it flows through a process



Data stores have a purpose (someone uses the data)

STRIDE

Systematic approach for threat identification:

- It help us to *consider, document, and discuss* security in a structured way.
- Use STRIDE to step through the DFD elements and get specific about security threat manifestations.
- Threats are grouped into **categories**.

Threat	Property we want
S poofing	<i>Authentication</i>
T ampering	<i>Integrity</i>
R epudiation	<i>Nonrepudiation</i>
I nformation Disclosure	<i>Confidentiality</i>
D enial of Service	<i>Availability</i>
E levation of Privilege	<i>Authorization</i>


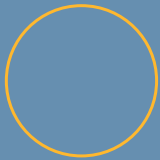




STRIDE: Definitions

Category	Description
Spoofing	Involves illegally accessing and then using another user's authentication information, such as username and password
Tampering	Involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet
Repudiation	Associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non-Repudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package
Information Disclosure	Involves the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers
Denial of Service	Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability
Elevation of Privilege	An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed



Different Threats Affect Each Element Type

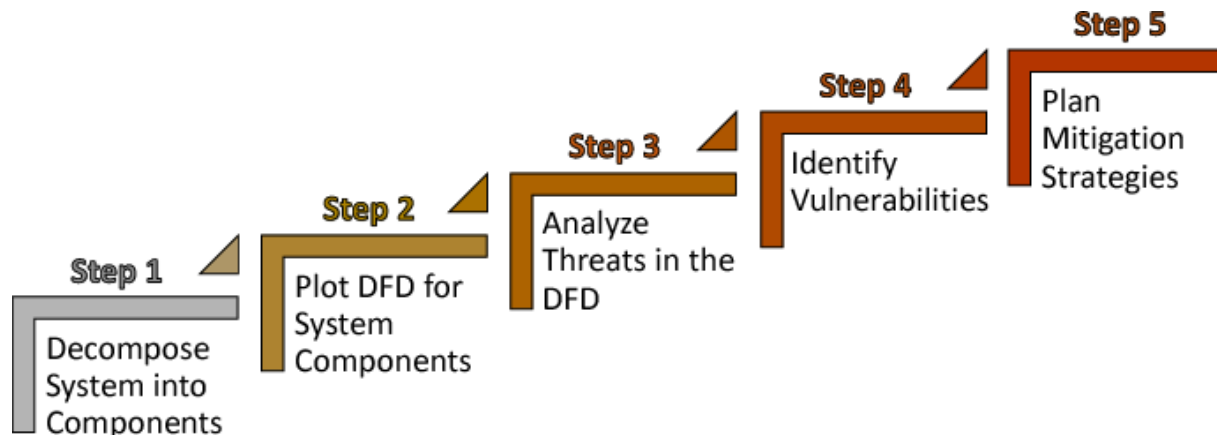
ELEMENT	S	T	R	I	D	E
 External Entity	✓		✓			
 Process	✓	✓	✓	✓	✓	✓
 Data Store		✓	?	✓	✓	
 Data Flow		✓		✓	✓	

STRIDE: Planning mitigation strategies

Step 4: For each item on the DFD, apply the relevant parts of STRIDE.

Step 5: Address each threat. There are our ways to address threats

- i. Redesign to eliminate.
- ii. Apply **standard mitigations** (*“what have similar software packages done and how has that worked out for them?”*).
- iii. Invent **new mitigations** (**riskier**).
- iv. Accept vulnerability in the design (there are some *basic rules* for this).



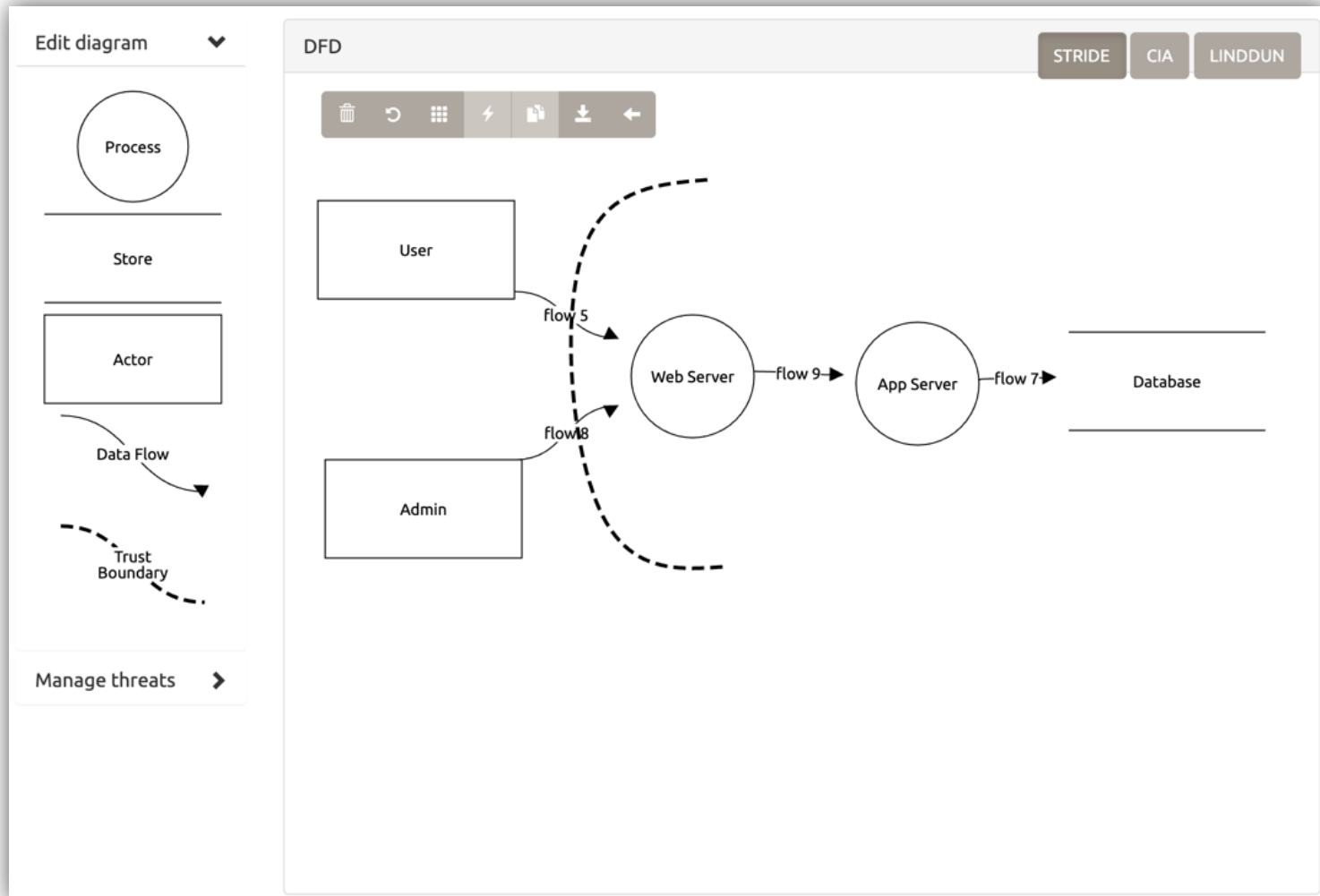


Standard Mitigations

S poofing	<i>Authentication</i>	To authenticate principals: <ul style="list-style-type: none">• Cookie authentication• Kerberos authentication• PKI systems such as SSL/TLS and certificates To authenticate code or data: <ul style="list-style-type: none">• Digital signatures
T ampering	<i>Integrity</i>	<ul style="list-style-type: none">• Windows Vista Mandatory Integrity Controls• ACLs• Digital signatures
R epudiation	<i>Non-Repudiation</i>	<ul style="list-style-type: none">• Secure logging and auditing• Digital Signatures
I nformation Disclosure	<i>Confidentiality</i>	<ul style="list-style-type: none">• Encryption• ACLS
D enial of Service	<i>Availability</i>	<ul style="list-style-type: none">• ACLs• Filtering• Quotas
E levation of Privilege	<i>Authorization</i>	<ul style="list-style-type: none">• ACLs• Group or role membership• Privilege ownership• Input validation



OWASP Threat Dragon





Questions ?

