WHITEBOARD HACKING SURVIVAL GUIDE

Dear Whiteboard Hacker,

Whiteboard Hacking or Threat Modeling is the way to avoid risks in your applications upfront. Without Threat Modeling, your protection is a shot in the dark and you will only know your vulnerabilities once they are exploited.

This survival guide is a companion to our whiteboard hacking trainings. The guide provides you with practical guidance and examples that you can rely on when starting your threat modeling workshops.

Our guide will help you, step by step, to go through the minimal stages of threat modeling:

1) Identify what you are building with data flow diagrams;
2) Discover threats with STRIDE;
3) Recommend standard mitigations;
4) Calculate risks of discovered design vulnerabilities.

Also assure that you link any technical vulnerability and recommendations to your business risk. Keep in mind that threat modeling is fun, engaging and will help you raise your team awareness. We hope this guide will help you with your threat modeling.

Cheers,

Sebastien Deleersnyder
CEO Toreon

Table of Contents

We are very happy you've found your way to our Whiteboard Hacking Survival Guide and hope you'll get a lot out of it. Be sure to share any feedback!

Looking for more?
Interested in a full-on Toreon training?
Check our website: **www.toreon com**
or contact us directly at: **training@toreon.com**

Threat Modeling Stages

Step 1	Diagram	What are we building?
Step 2	Identify Threats	What can go wrong?
Step 3	Mitigate	What are we doing to defend against threats?
Step 4	Validate	Validate steps 1 - 3. Report.

Data Flow Diagram Basics

External Entity

Entities outside the application that interact with the application via an entry point.

Process

Tasks that handle data within the application; tasks may process data or perform actions based on the data.

Data Store

Locations where data is stored; data stores do not modify data, they only store it.

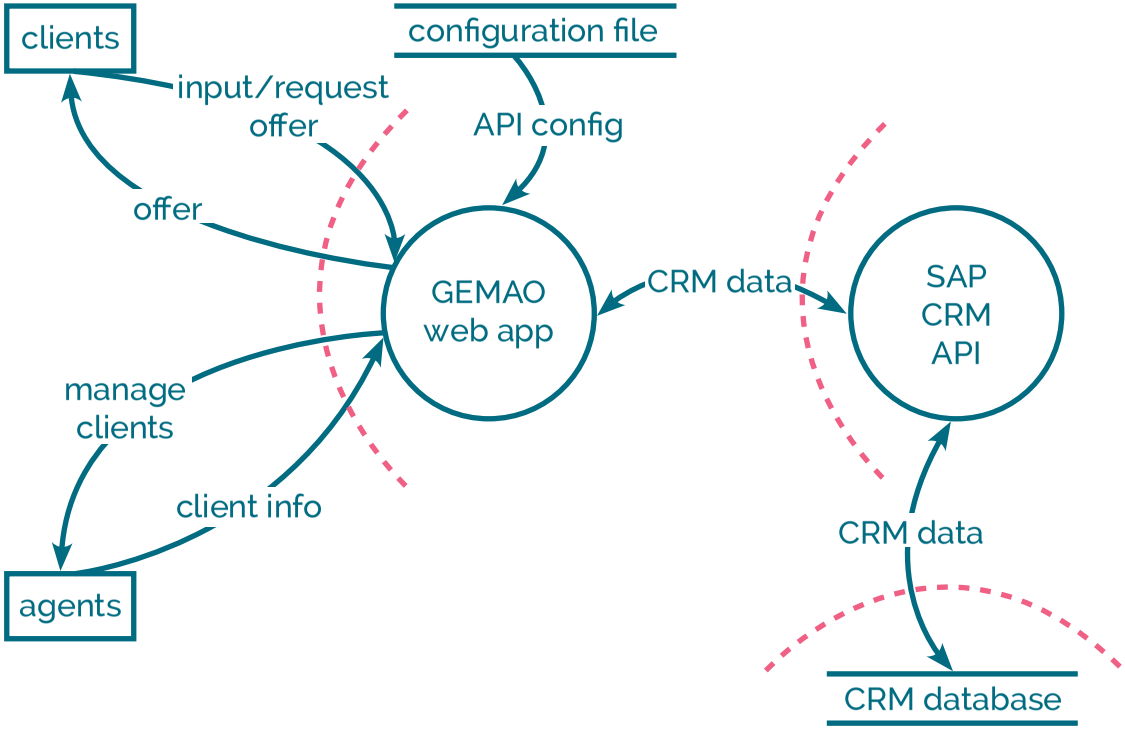
Data Flow

Data movement within applications; the arrow tells the direction of data movement.

Trust Boundary

The change of trust levels as data flows through the application.

Data Flow Diagram Example



STRIDE

Spoofing	Can an attacker gain access using a false identity?
Tampering	Can an attacker modify data as it flows through the application?
Repudiation	If an attacker denies doing something, can we prove he did it?
Information Disclosure	Can an attacker gain access to private or potentially injurious data?
Denial of Service	Can an attacker crash or reduce the availability of the system?
Elevation of Privilege	Can an attacker assume the identity of a privileged user?

Apply STRIDE Threats

Apply the relevant parts of STRIDE to each item on the diagram.

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

** This applies if the data store contains an audit trail.*

STRIDE Table

	Client/Agent (actor)		>>>		GEMAO (process)	
	Mitigations	Vulnerabilities	Mitigations	Vulnerabilities	Mitigations	Vulnerabilities
S	user/PW authentication	no 2FA for agent (V1)			TLS certificate	
T			TLS			no business validation input (V4)
R		no audit trail (V2)				no logging user actions (V5)
I			TLS			clear text API credentials (V6)
D				no fallback ISP (V3)	Load balanced web servers	
E					Access control	

Addressing Each Threat

Mitigation Patterns

Authentication	Mitigates Spoofing
Integrity	Mitigates Tampering
Non-Repudiation	Mitigates Repudation
Confidentiality	Mitigates Information Disclosure
Availability	Mitigates Denial of Service
Authorisation	Mitigates Elevation of Privilege

Risk Rating Example

Threat	Description	Vector	Prevalence	Detectability	Impact	Rating	Risk
V4	No business validation input	2	2	2	3	6.0	High
V1	No 2FA for agent	2	3	3	2	5.3	Medium
V3	No fallback ISP	2	2	1	3	5.0	Medium
V6	Clear text API credentials	2	2	1	3	5.0	Medium
V2	No audit trail	1	2	2	1	1.7	Low
V5	No logging user actions	1	2	2	1	1.7	Low

Low: 1-3, Medium: 4-6, High: 7-9

www.toreon.com