

# Definitions

Thierry Sans

# Correctness (Safety) vs Security

**Safety**

**Satisfy specifications**

“for reasonable inputs,  
get reasonable outputs”

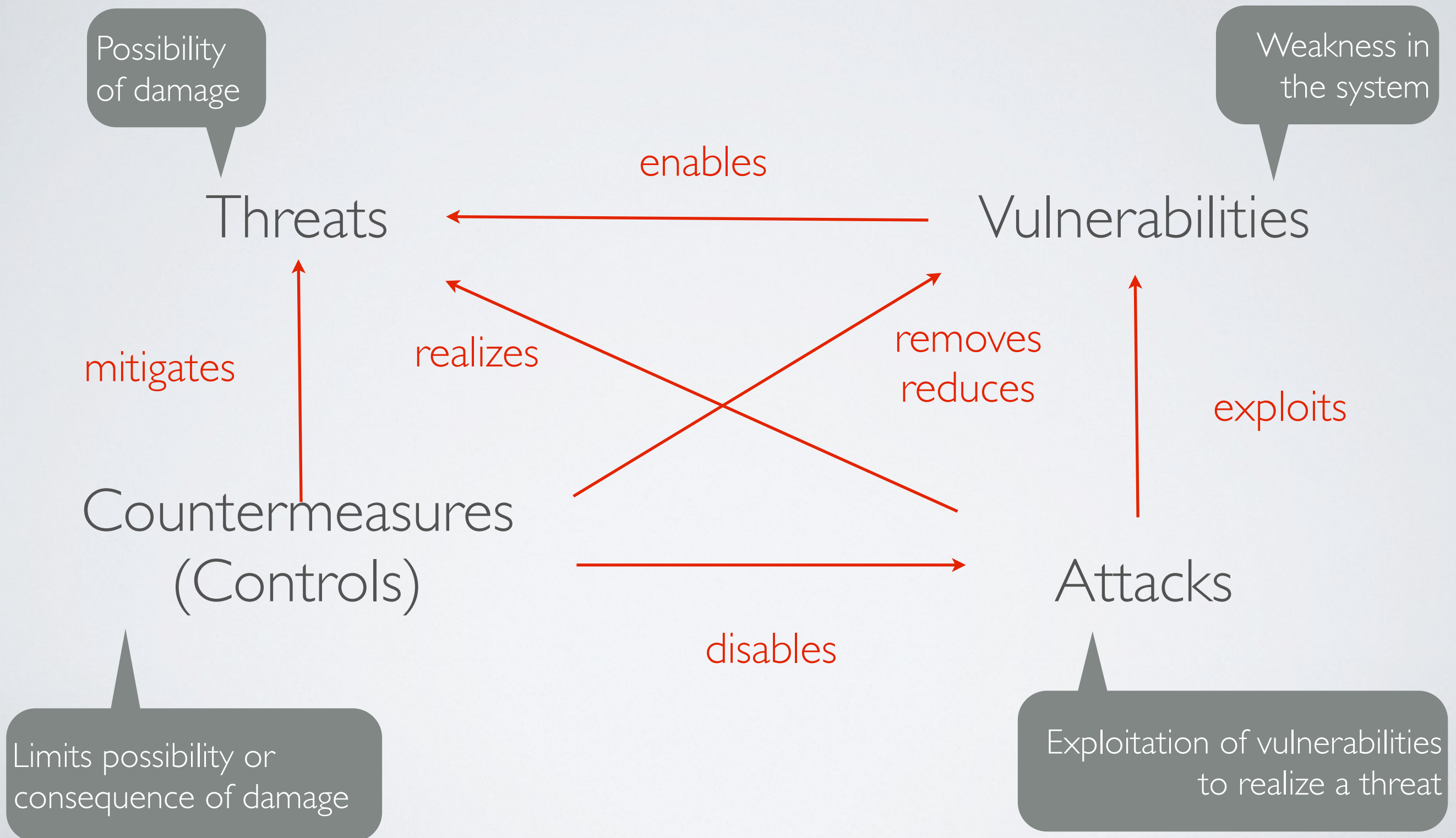
**Security**

**Resist attacks**

“for **un**reasonable inputs,  
get reasonable outputs”

**The attacker is an active entity**

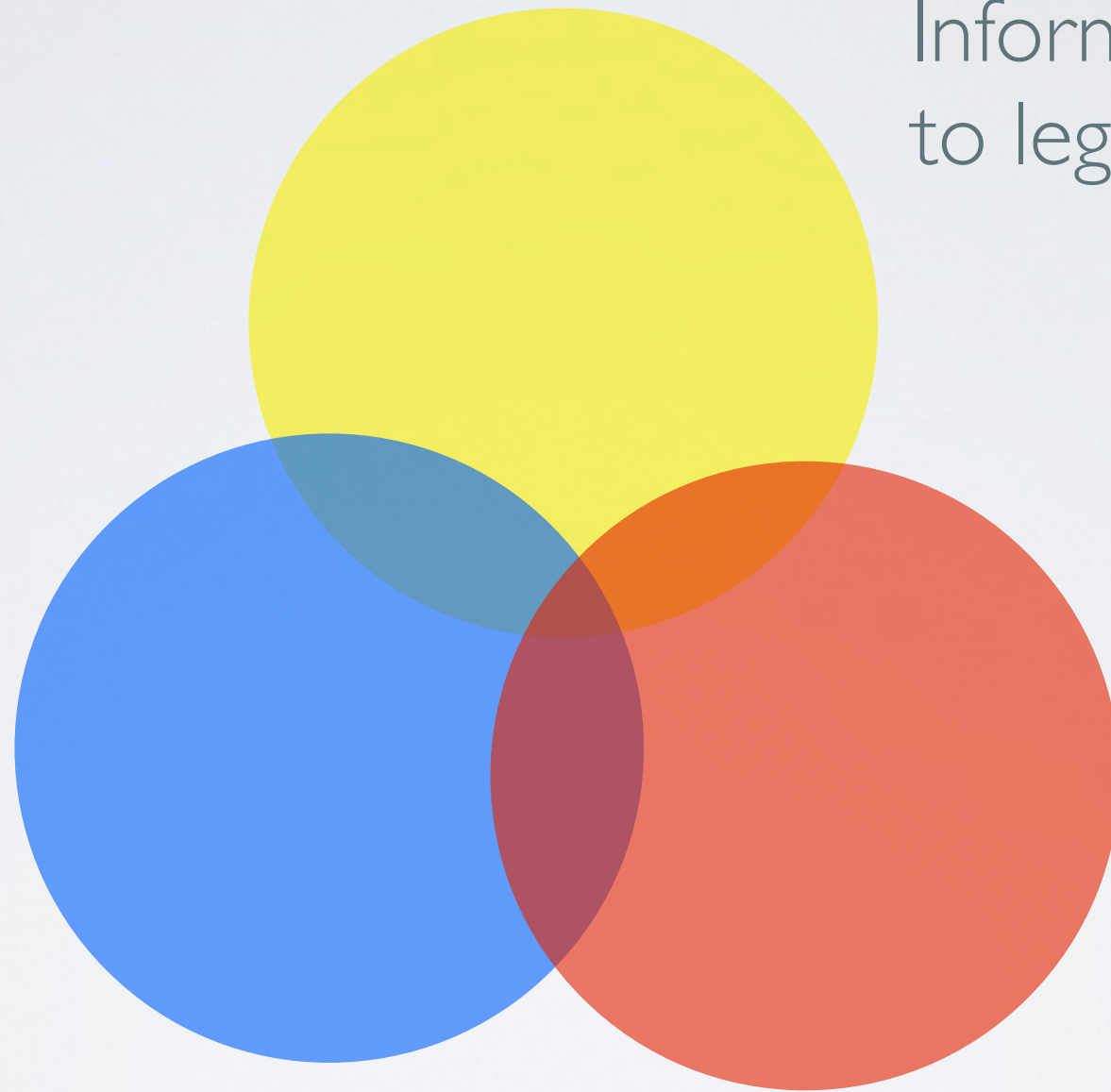
# Security Theatre



# C I A - Security Properties

## **C**onfidentiality

Information is disclosed to legitimate users



## **I**ntegrity

Information is created or modified by legitimate users

## **A**vailability

Information is accessible to legitimate users

# Sub Properties

**C**onfidentiality



Authenticity

Non-repudiation

Accountability

and many others ...

**I**ntegrity

**A**vailability



In some cases, properties can be conflicting

“Do not record the identity of the user that performed an action” (Anonymity)

“Knowing that someone has done an action” (Accountability)



“Someone cannot deny having done an action” (Non-repudiation)

# Dealing with security

- ✓ Security is often a compromise
- ✓ Security is engineered

# Risk Analysis & Policy, Mechanisms and Assurance

	<b>System</b>	<b>Security</b>
<i>What is it supposed to do?</i>	Specification	Risk Analysis & Security Policy
<i>How does it do it?</i>	Implementation	Mechanisms
<i>Does it really do it?</i>	Validation	Assurance



# Risk Analysis & Security Policy

<b>Goal</b>	Inferring what can go wrong with the system
<b>Outcome</b>	Set of security goals
<b>Principles</b>	<p>You never prevent a threat, you lower the risk</p> <p>Performing an attack is more or less difficult the assets to protect versus the attacker's efforts</p>

# Mechanisms

<b>Goal</b>	Define a strategy to realize the security goals
<b>Outcome</b>	Set of security mechanisms
<b>Principle</b>	Deploying security mechanisms has a cost (cost of recovering versus cost of deployment)

# Assurance

<b>Goal</b>	Make sure that the security mechanisms realize the security goals
<b>Outcome</b>	Methodology
<b>Principle</b>	Full assurance cannot be achieved