Definitions

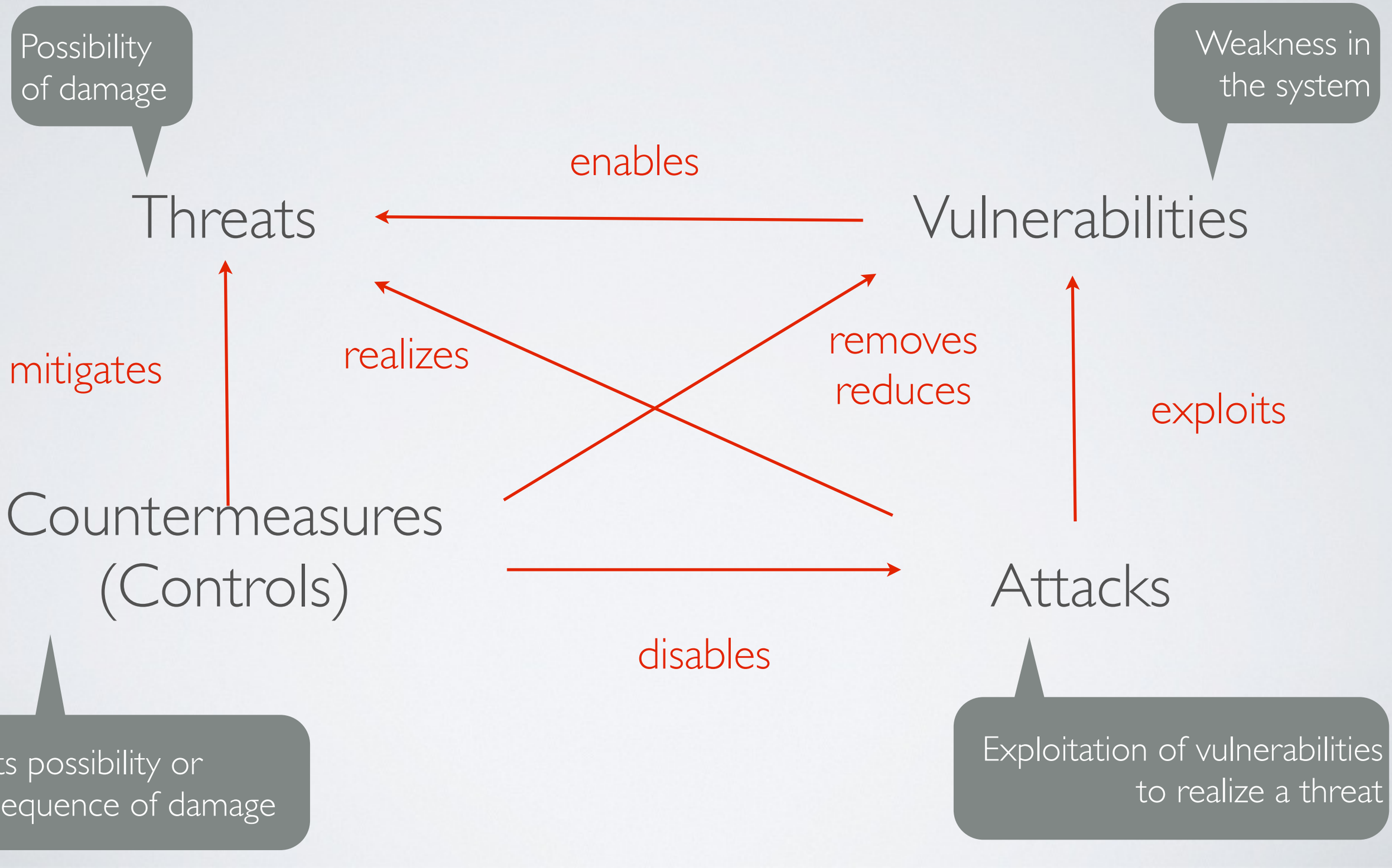
Thierry Sans

Safety (a.k.a correctness) 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

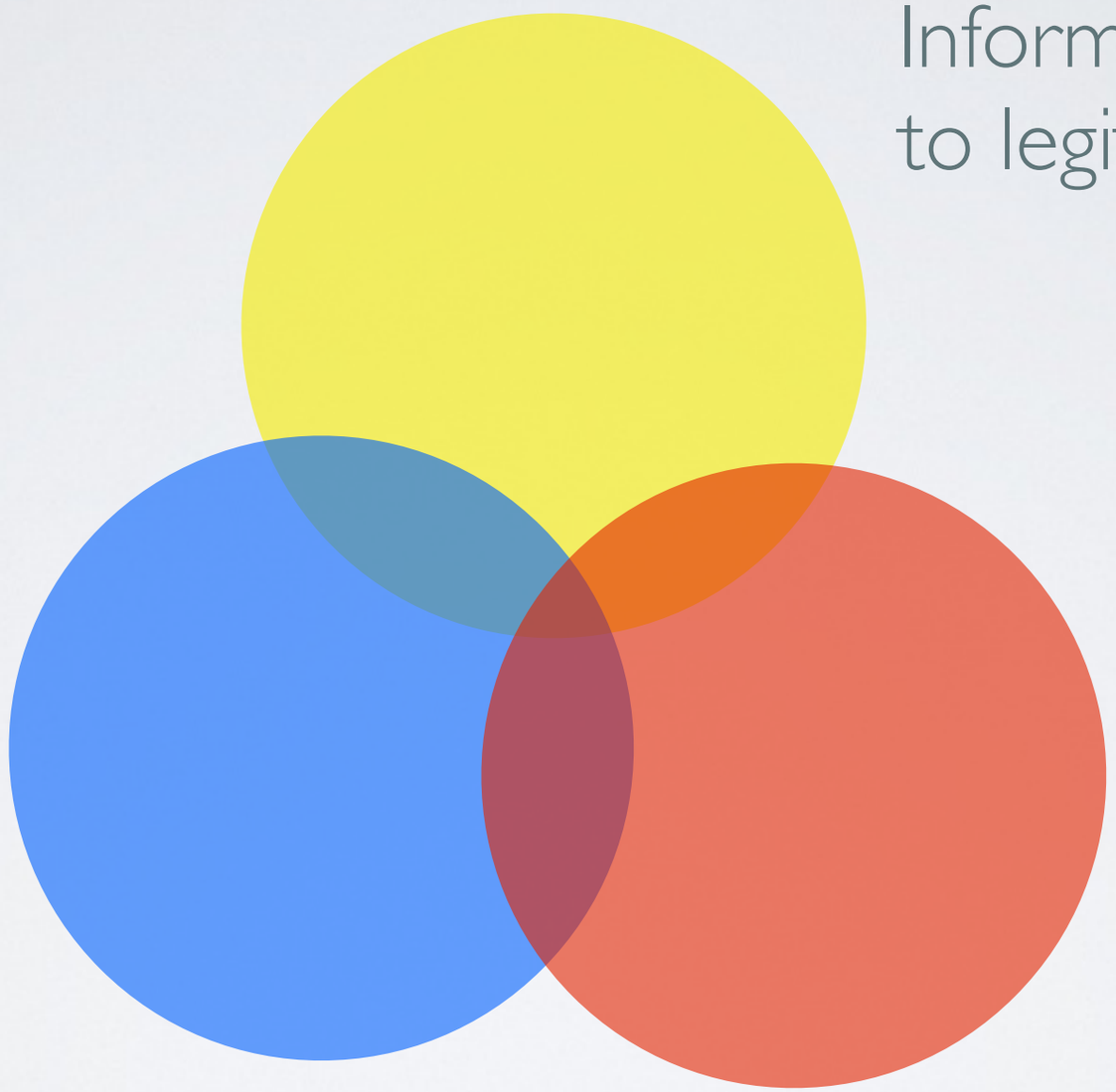
Security Theatre



C I A - Security Properties

Confidentiality

Information is disclosed to legitimate users



Integrity

Information is created or modified by legitimate users

Availability

Information is accessible to legitimate users

Sub Properties

Confidentiality

Secrecy

Anonymity Pseudonymity

Privacy

Authenticity

Non-repudiation

Accountability

and many others ...

Integrity

Availability

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

	System	**Security**
What is it supposed to do?	Specification	Risk Analysis & Security Policy
How does it do it?	Implementation	Mechanisms
Does it really do it?	Validation	Assurance

Risk Analysis & Security Policy

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

Mechanisms

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

Assurance

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