Definitions

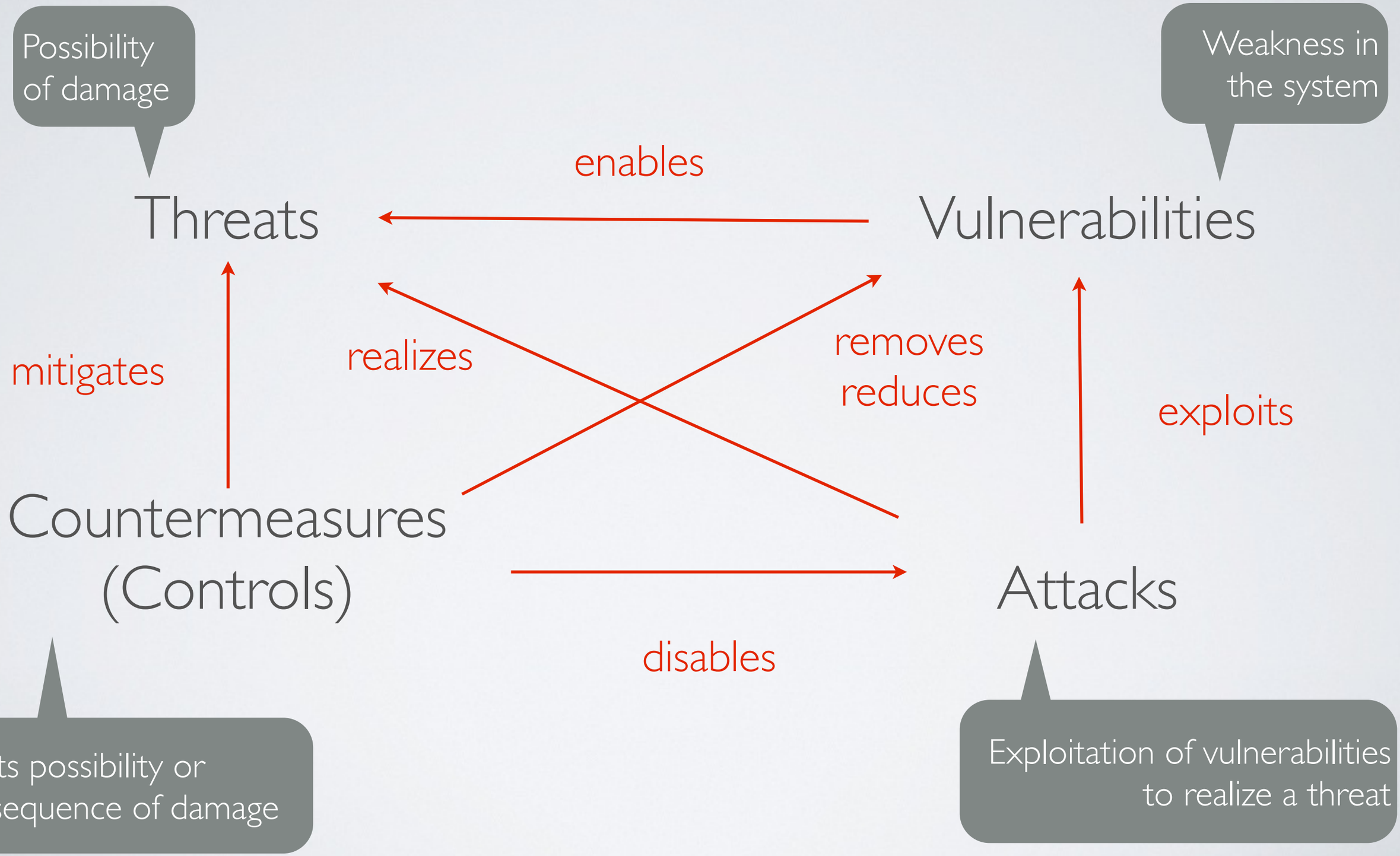
Thierry Sans

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

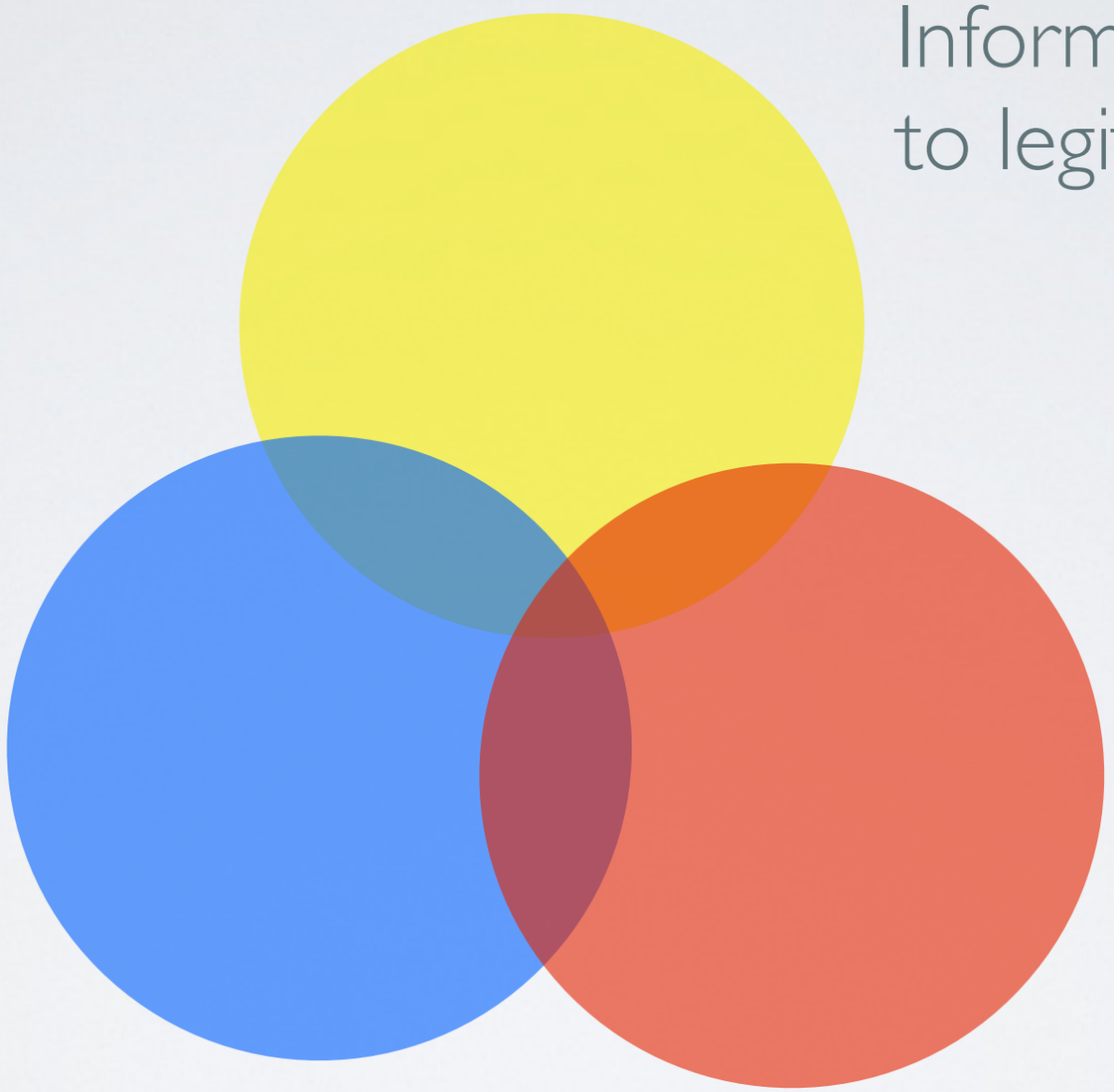
Security Theatre



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)