A Framework for Conceptualizing Social Engineering Attacks

Jose J. Gonzalez
Agder University College, Grimstad, Norway

Jose M. Sarriegi, Alazne Gurrutxaga
Tecnun (University of Navarra) San Sebastian, Spain

CRITIS'06, Samos

Introduction

- Social engineering consists of acquiring information about computer systems through non-technical means
- While technical security of most critical infrastructure is high…
- …it remains vulnerable to attacks from social engineers, whether outsiders or insiders
- Recent studies conclude that it is relatively cheap and easy to mount a large scale social engineering attack with a high success rate

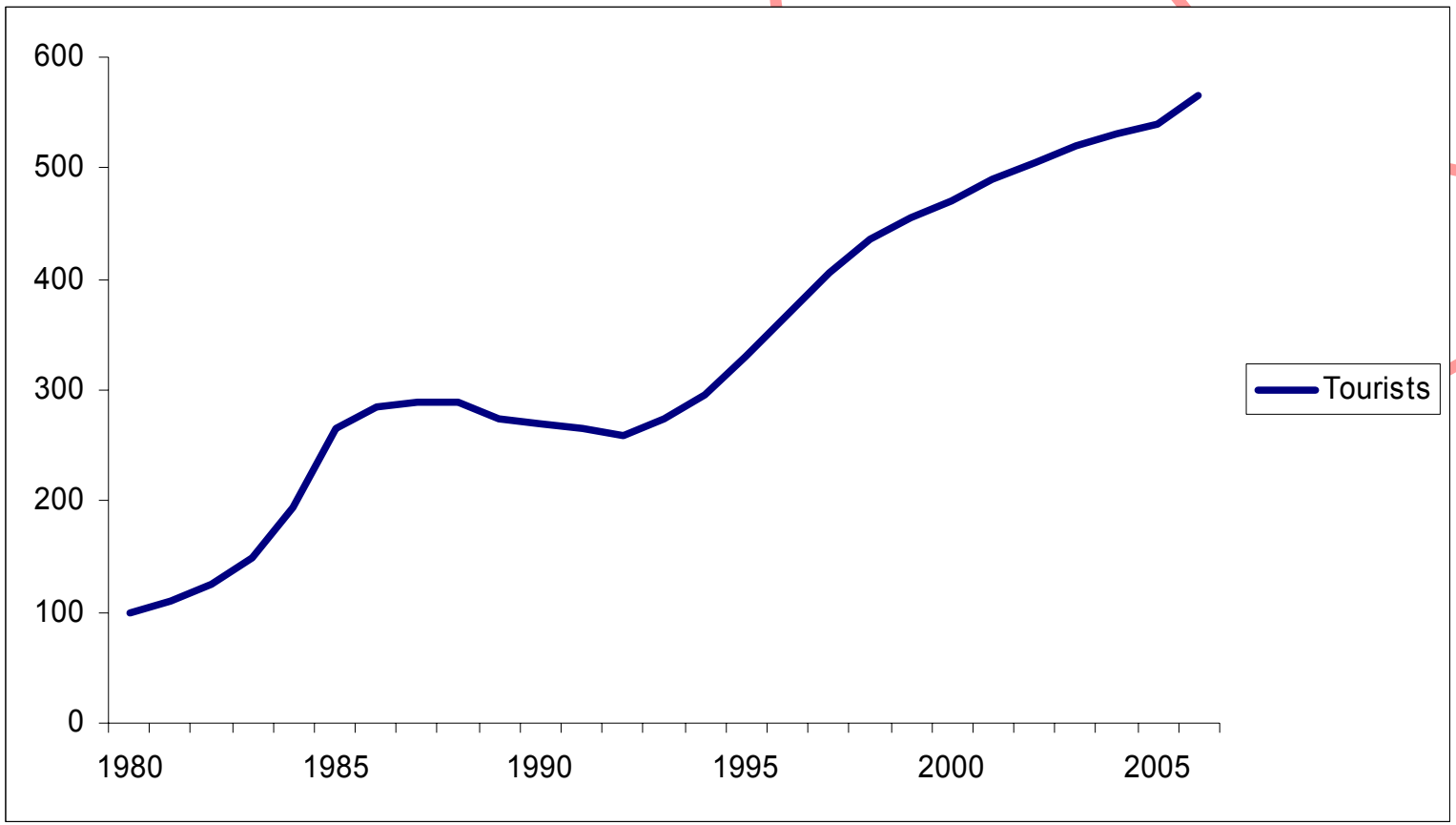
Objective of the paper

- Objective: Classify social engineering attacks according to their dynamic behaviour using system archetypes
- This classification would help designing effective multilayered security procedures

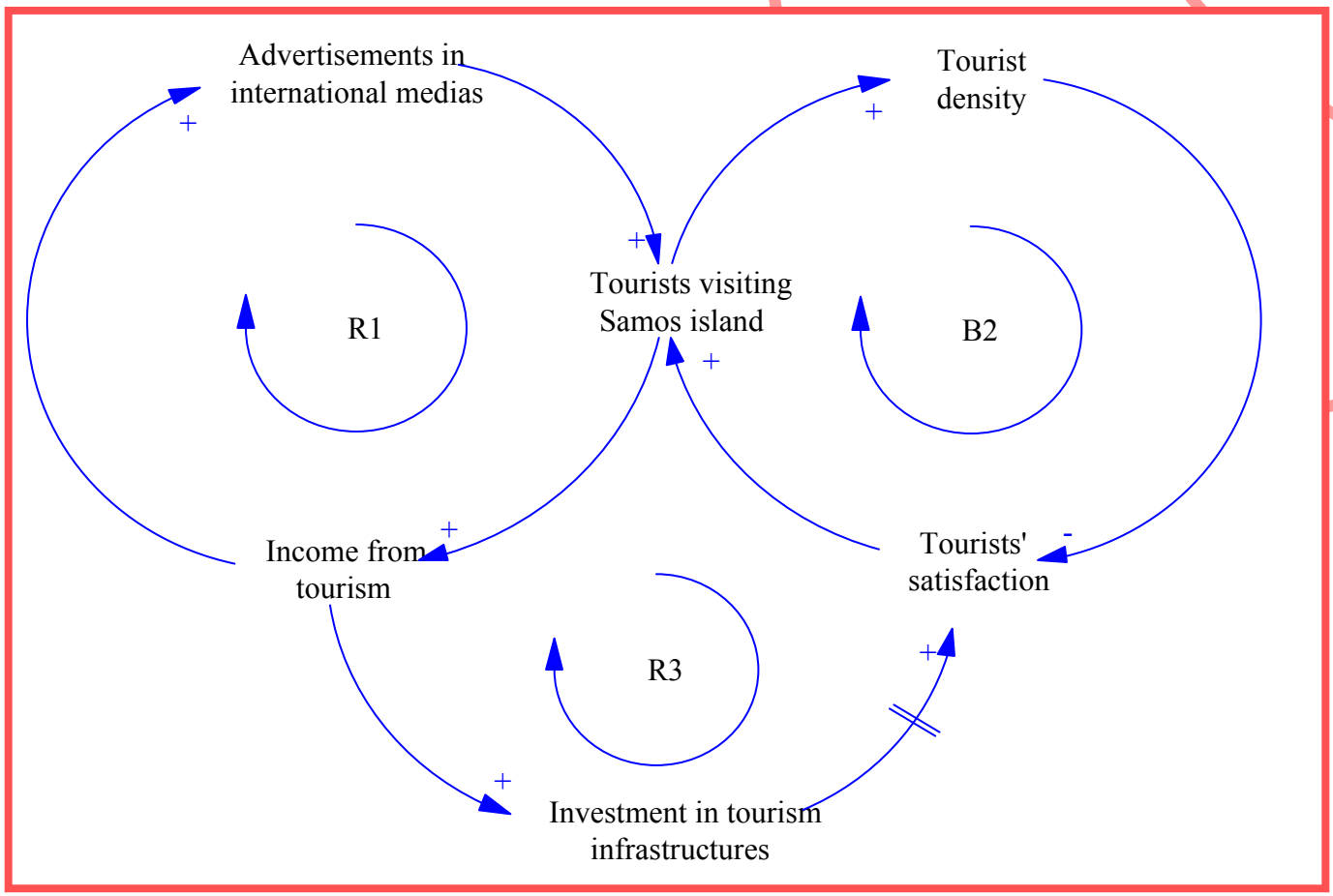
A feedback view of social engineering

- Social engineers often use several small attacks to put them in the position to reach their final goal
- The attack is a dynamic process where the outcome of an action is fed back to execute the next action
- Organizational defences activate security controls that could by anticipated by the attacker.

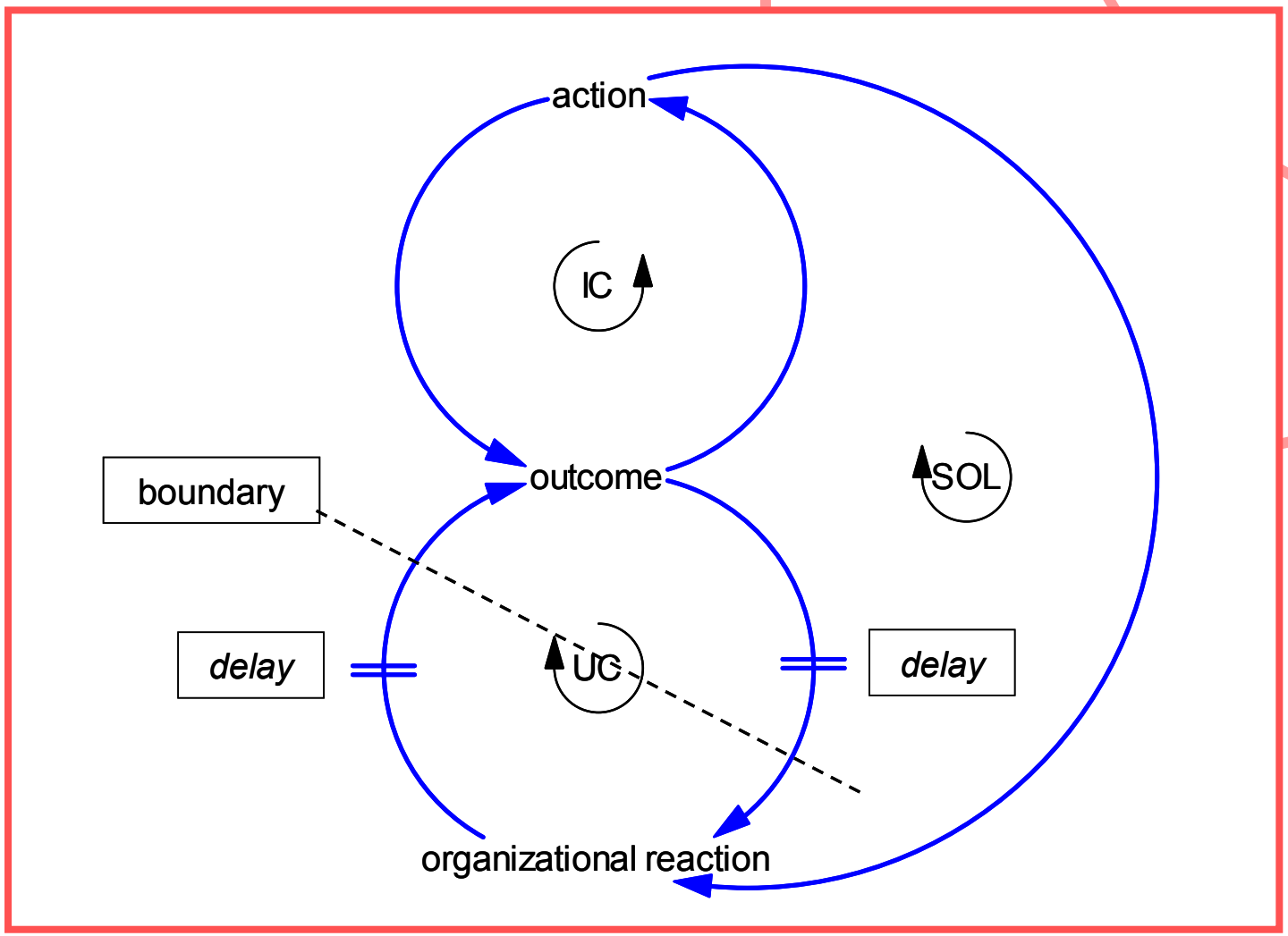
Behaviour of a “Problem”



Causal Loop Diagram



Generic System Archetypes



The four system archetypes

Intended consequence loop	Unintended consequence loop	Archetype
Balancing	Balancing	Relative Control
Reinforcing	Balancing	Underachievement
Reinforcing	Reinforcing	Relative Achievement
Balancing	Reinforcing	Out of control

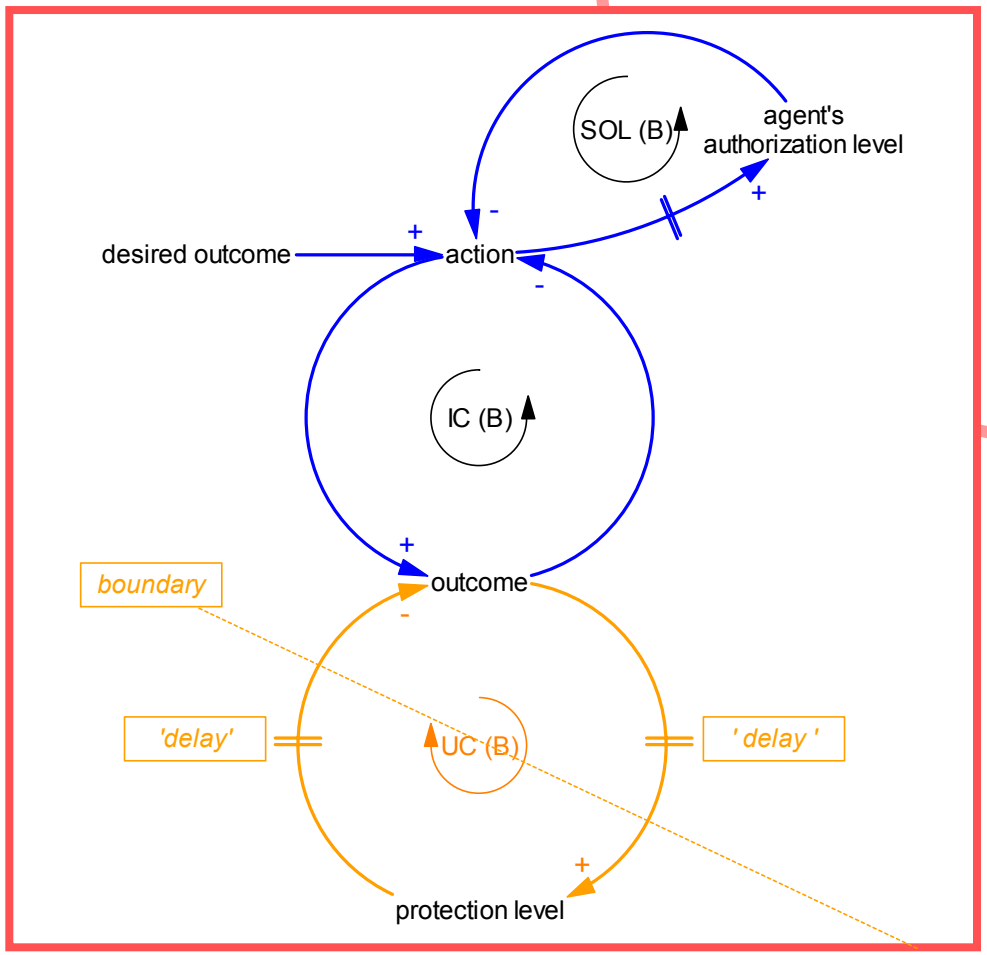
Hypothesis

- Descriptions of social engineering attacks in terms of system archetypes have qualities as strategic patterns. They:
  - Conceptualize crucial aspects of the attack and defense process
  - Are cognitively simple
  - Are fairly easy to recognize and to interpret
  - Are modular and can be combined

External social engineer targeting an explicit goal

- An external agent who is trying to achieve a particular goal
- As he comes closer to the desired outcome, the level of protection is higher and higher
- Hence, the social engineer uses elements from the outcome to gain fake authority

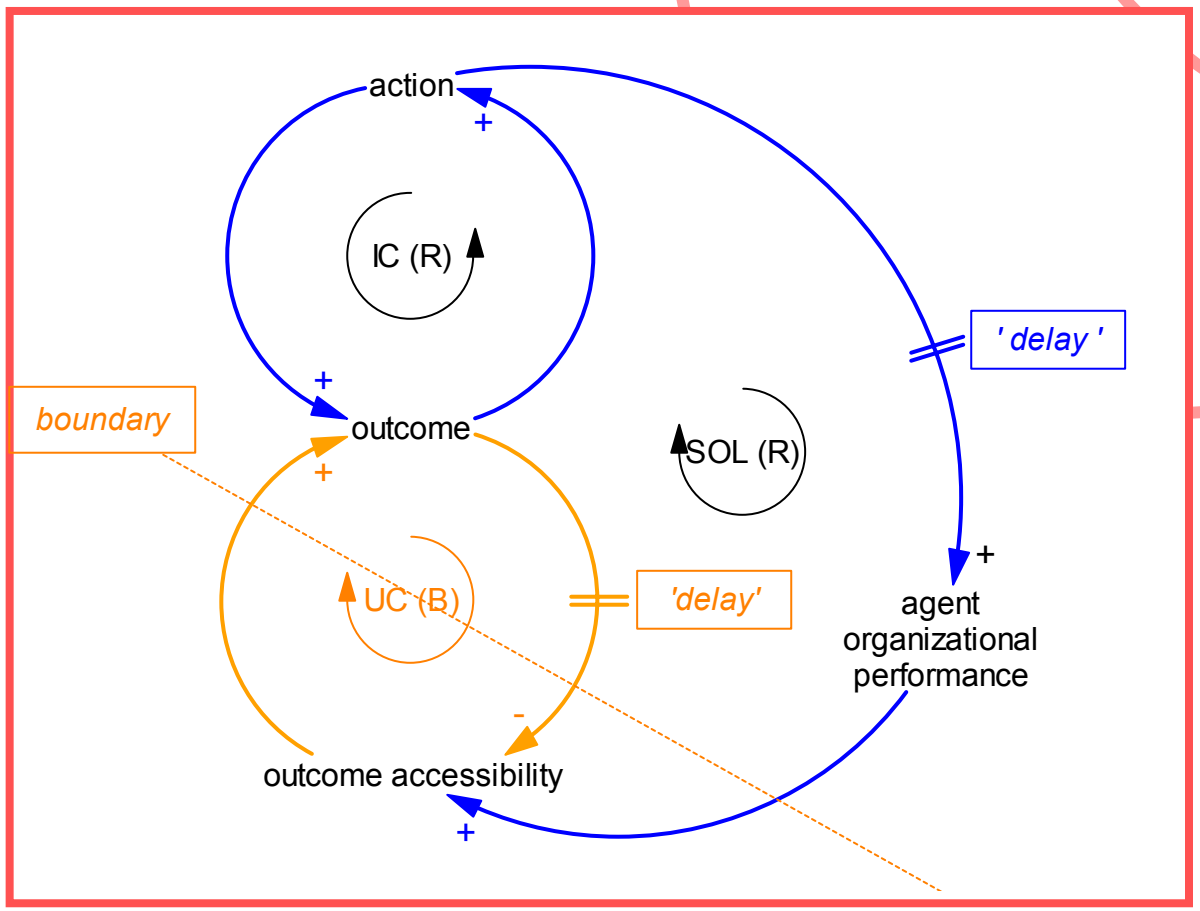
External social engineer targeting an explicit goal



Social engineer targeting a long-term parasitic relationship

- A patient malicious insider provides an external party long term access to more and more valuable assets
- The organization enacts separation of duties
- The social engineer needs to become a star performer to bypass security controls

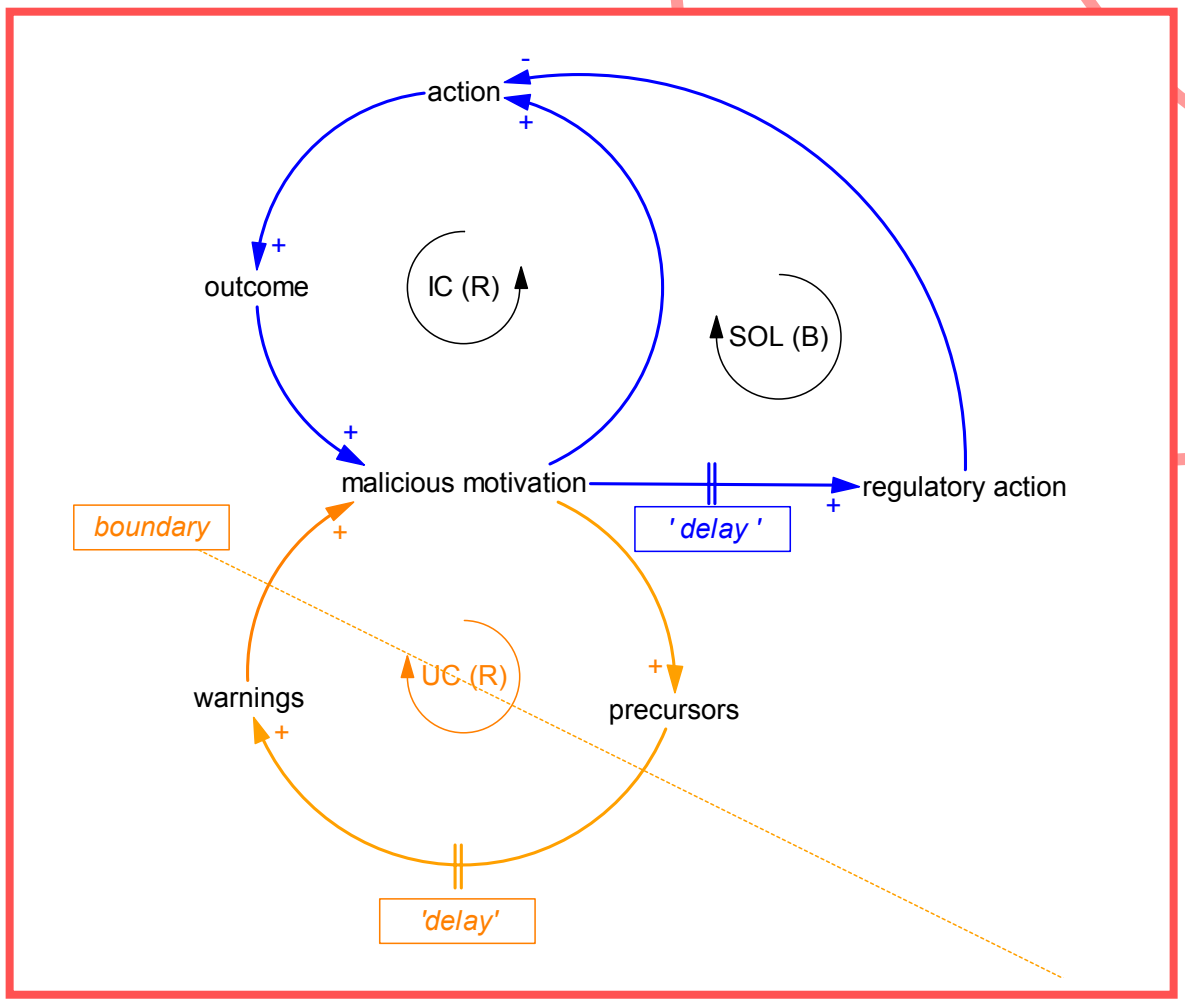
Social engineer targeting a long-term parasitic relationship



Disgruntled insider as social engineer

- An insider acts against his firm, obtaining escalating “outcomes”. As he is successful his motivation to proceed increases
- If precursors are detected the social engineer can be warned or even fired
- He should manage to self-control, targeting major outcomes in a covert way

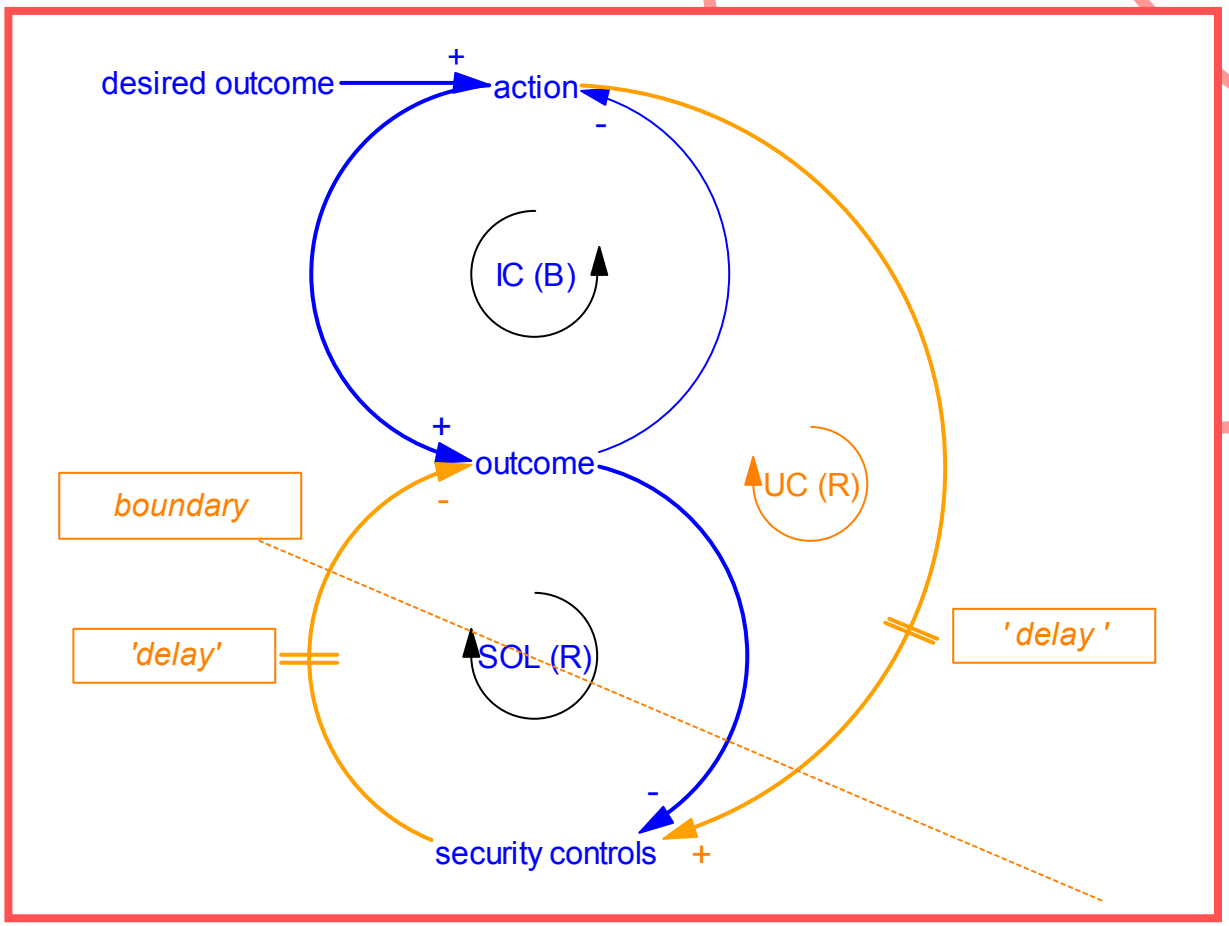
Disgruntled insider as social engineer



A social engineer targeting an ambitious goal

- An insider who is determined to launch a massive strike
- But he also actives security controls that could compromise his desired outcome
- The social engineer should use the obtained outcome not only for generating more actions, but also to weaken security controls

A social engineer targeting an ambitious goal



tecnun

CRITIS'06, Samos

HØGSKOLEN I AGDER

Conclusions

- System archetypes represent at a high level of abstraction and aggregation the main modes of social engineering attacks
- Although they do not do full justice to real cases are a way to conceptualize the most salient aspects of the attack and defence for some time interval
- They are helpful to design security controls that provide multilayered feedback against the social engineer's primary intended consequence and solution loops

A Framework for Conceptualizing Social Engineering Attacks

Jose J. Gonzalez
Agder University College, Grimstad, Norway

Jose M. Sarriegi, Alazne Gurrutxaga
Tecnun (University of Navarra) San Sebastian, Spain

CRITIS'06, Samos