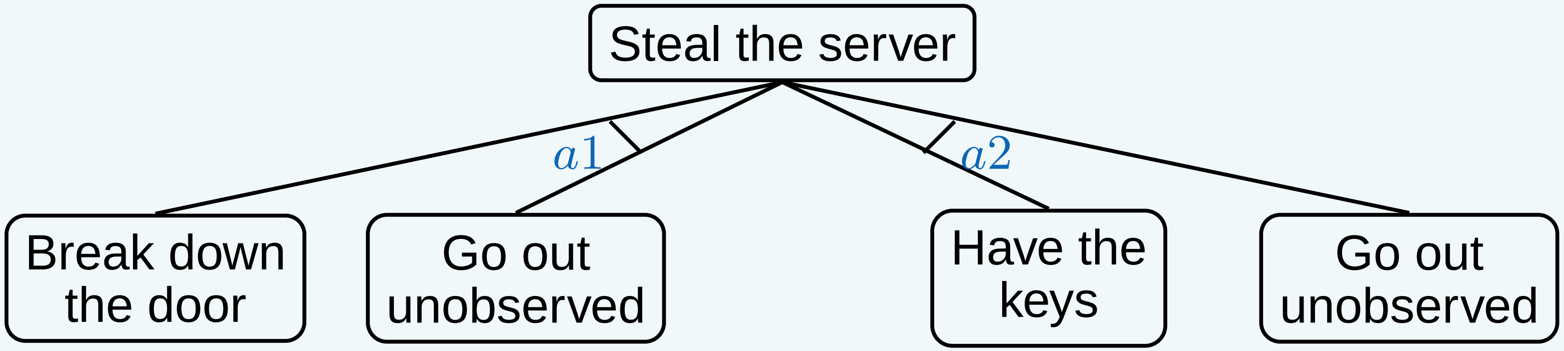
Strategic games on defense trees

(Bistarelli/Dall'Aglio/Peretti) FAST'06

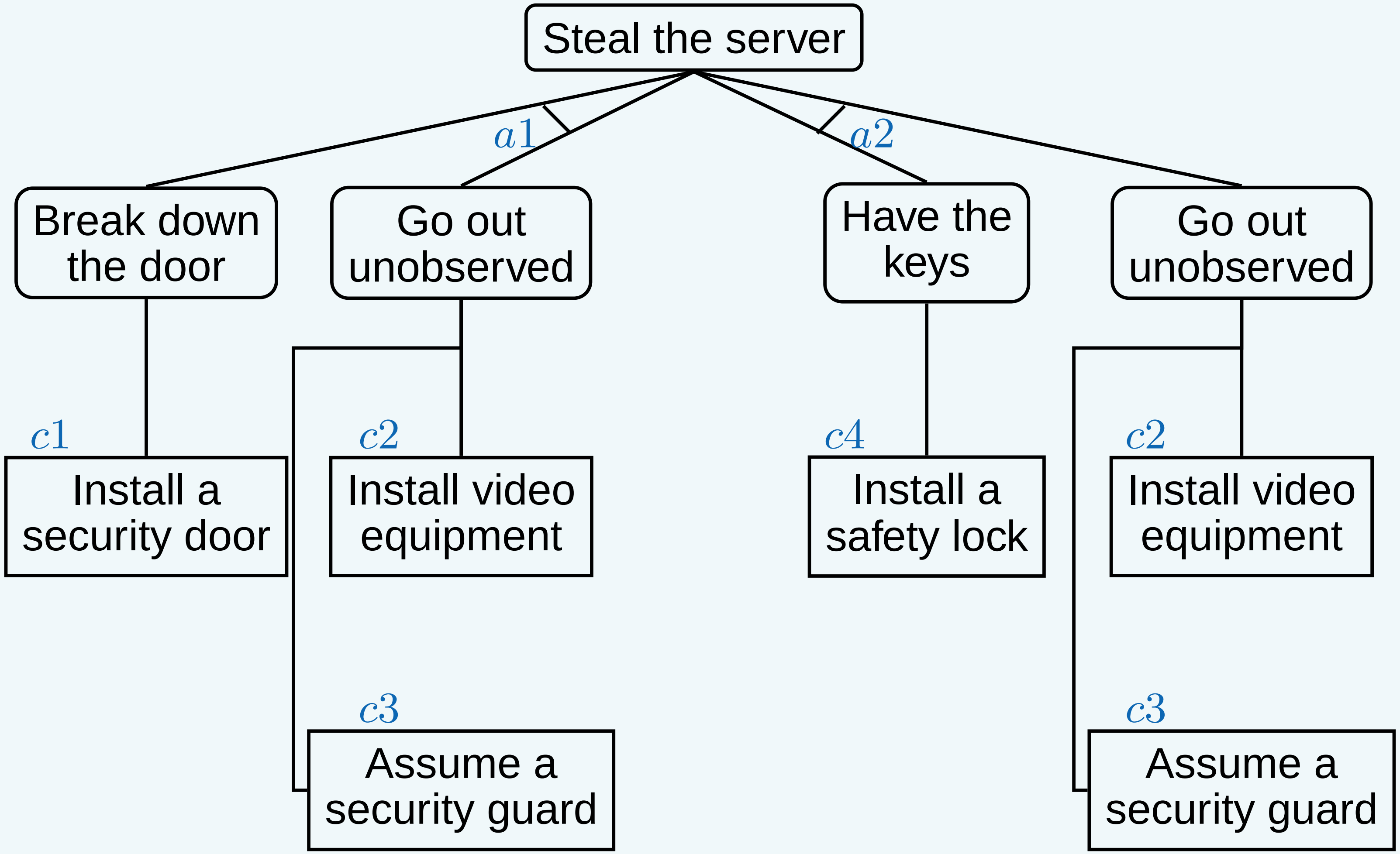
Game theory seminar

Presented by Sjouke Mauw

A simple attack tree



With defences



Attributes

- Return On Investment (ROI) =
  measure of the efficacy of a specific security investment w.r.t. a specific attack.
- Return On Attack (ROA) =
  measure the convenience of an attack by considering the impact of a security solution on the attacker's behaviour.

Return On Investment

$$ROI = \frac{ALE \times RM - CSI}{CSI}$$

Where

- Annualized loss Expectancy
  $ALE = AV \times EF \times ARO$, where
  - Asset Value (AV).
  - Exposure Factor (EF) is fraction of Asset Value measuring the loss due to a threat.
  - Annualized Rate of Occurrence (ARO) is the estimated number of annual occurrences of a threat.
- Risk Mitigated by a countermeasure (RM) is the effectiveness of the countermeasure (a fraction).
- Cost of Security Investment (CSI) is cost of implementing the countermeasure.

ROI computation

Attack	EF	ARO	Countermeasures	RM	CSI	ROI
$a1$ Break down the door and go out unobserved	90%	0.1	$c1$ Install a security door	0.7	1500	3.20
			$c2$ Install video surveillance	0.1	3000	-0.70
			$c3$ Employ security guard	0.5	12000	-0.63
			$c3$ Install security lock	0	300	-1
$a2$ Open door with keys and go out unobserved	93%	0.1	$c1$ Install a security door	0	1500	-1
			$c2$ Install video surveillance	0.1	3000	-0.69
			$c3$ Employ security guard	0.5	12000	-0.61
			$c3$ Install security lock	0.2	300	5.20

AV = 100000 euro.

Return On Attack

$$ROA = \frac{GI \times (1 - RM) - (cost_a + cost_{ac})}{cost_a + cost_{ac}}$$

Where

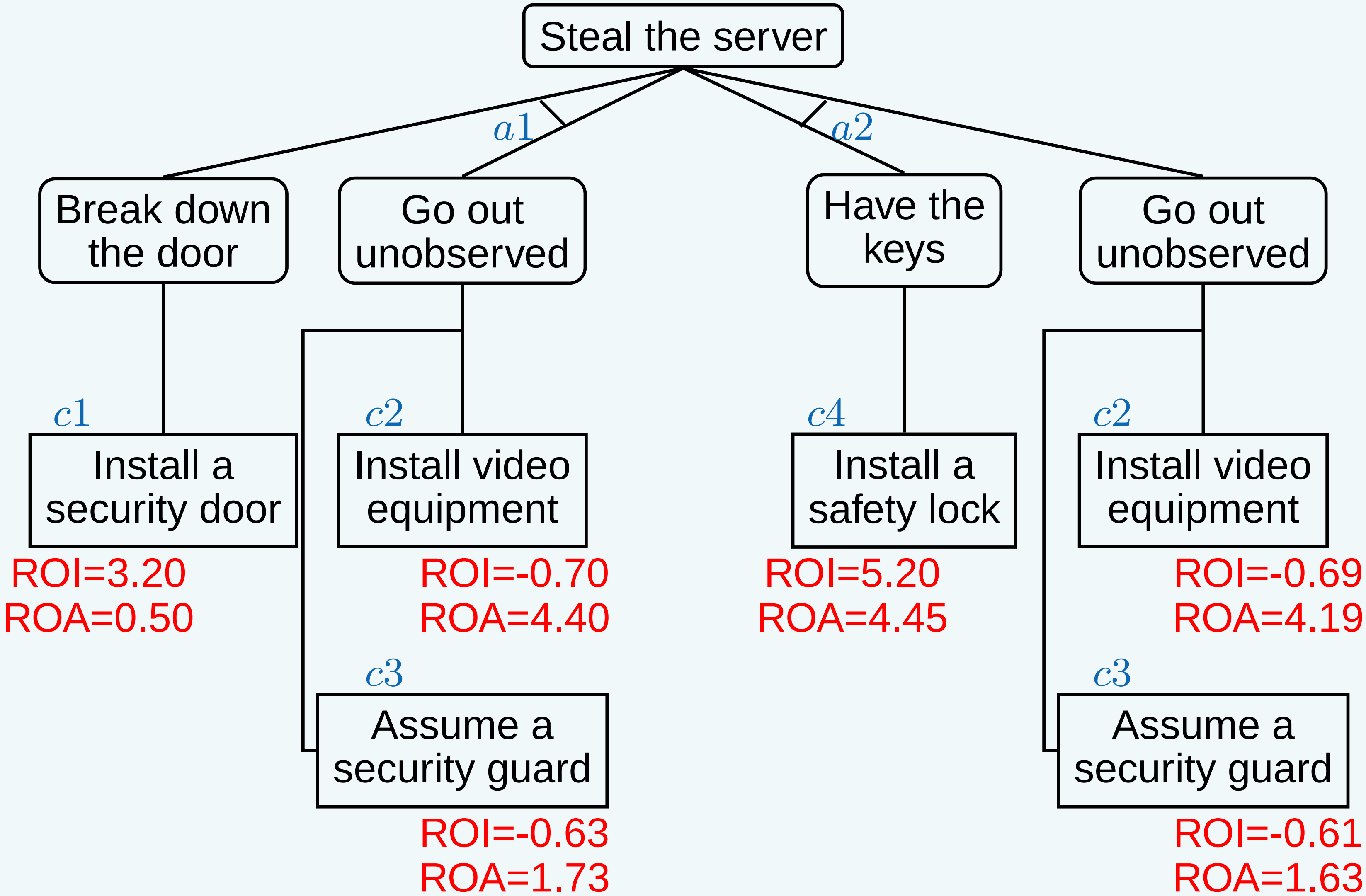
- GI is the expected gain from a successful attack.
- $cost_a$ is the cost sustained by the attacker to succeed.
- $cost_{ac}$ is the additional cost brought by the countermeasure c adopted by the defender to mitigate the attack a.

ROA computation

Attack	$COST_a$	Countermeasures	$Cost_{ac}$	ROA
$a1$ Break down the door and go out unobserved	4000	$c1$ Install a security door	2000	0.50
		$c2$ Install video surveillance	1000	4.40
		$c3$ Employ security guard	1500	1.73
		$c3$ Install security lock	0	6.50
$a2$ Open door with keys and go out unobserved	4200	$c1$ Install a security door	0	5.14
		$c2$ Install video surveillance	1000	4.19
		$c3$ Employ security guard	1500	1.63
		$c3$ Install security lock	200	4.45

Gi = 30000 euro.

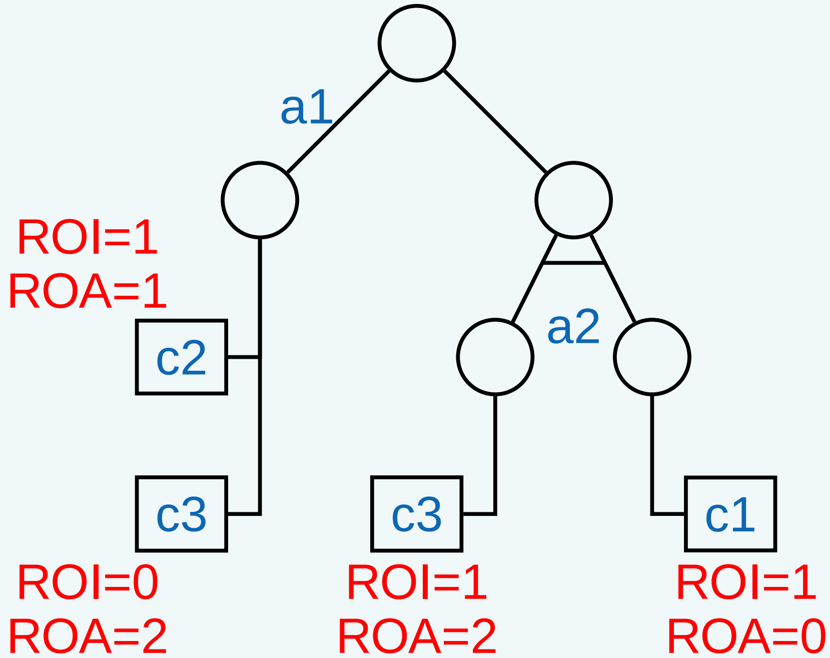
ROI/ROA in the defence tree



Defence trees as strategic games

- Two players: attacker D and defender A.
- Defender's strategies: possible countermeasures $\{c1, c2, c3, c4\}$.
- Attacker's strategies: possible attacks $\{a1, a2\}$.
- Both players want to maximize their payoff functions ROI and ROA.

Simple example



	a1	a2
c1	1,1	1,0
c2	1,1	0,2
c3	0,2	1,2

Nash equilibria: (c1,a1), (c3,a2).

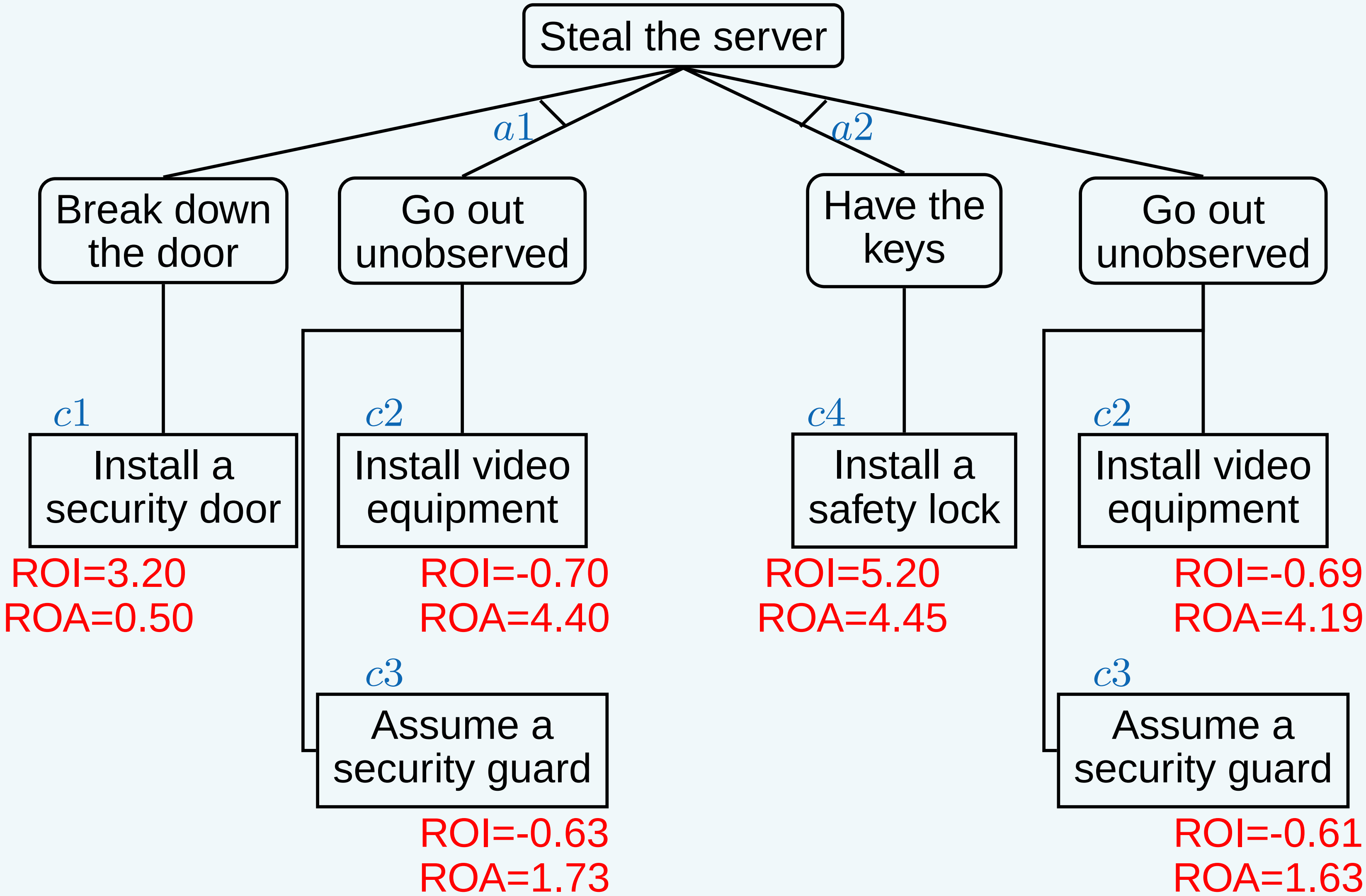
Some quotes

- “The Nash equilibrium represents the best strategies for both the attacker and the defender (with the hypothesis that neither the attacker nor the defender have any knowledge of the other).”
- “The defender will select, if possible, both countermeasure c1 and c3. However if the financial resources available to the system administrator are limited, only countermeasure c3 will be selected (because it will cover both strategy of the attacks).

Mixed strategy

- "Player (especially defender) deals with single attacker drawn from a population of attackers whose actions can be estimated as frequencies from previous attacks."
- Therefore, consider a mixed strategy, consisting of a probability distribution over attacks/defences.

Back to the example



In strategic form

	a1	a2
c1	3.20,0.50	-1.00,6.14
c2	-0.70,4.40	-0.69,4.19
c3	-0.63,1.73	-0.61,1.63
c4	-1.00,6.50	5.20,4.45

No Nash equilibrium.

With mixed strategies

- Use Gambit to compute equilibria.
- Defender plays:
  - c1 with probability $\frac{205}{769}$
  - c4 with probability $\frac{564}{769}$
- Attacker plays:
  - a1 with probability $\frac{31}{52}$
  - a2 with probability $\frac{21}{52}$
- “the best that a system administrator can do is to invest in c1 to avoid the first attack and in c4 to avoid the second attack.”

Consider multiple attacks/countermeasures

- Still no Nash equilibrium with pure strategy.
- Mixed equilibrium:
- Defender plays:
  - c4 with probability $\frac{39}{55}$
  - $\{$c1,c4$\}$ with probability $\frac{16}{55}$
- Attacker plays:
  - a1 with probability $\frac{5}{21}$
  - a2 with probability $\frac{16}{21}$
- Note: strategies $\emptyset$ and $\{a1, a2\}$ are uniformly dominated by simple strategies a1 and a2. So the attacker has no interest in combining the actions together.

Future

- Extend to 1 defender and n attackers.

http://www.sci.unich.it/~bista/papers/papers-download/DG4.pdf