Cybersecurity and Game Theory

COMS6998 sec:12 | The Economics of Cybersecurity

March 26, 2024

What is a “Game”?

What is a “Game”?

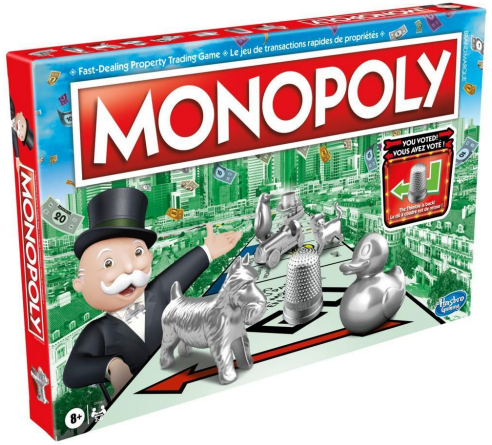
Everyday usage:

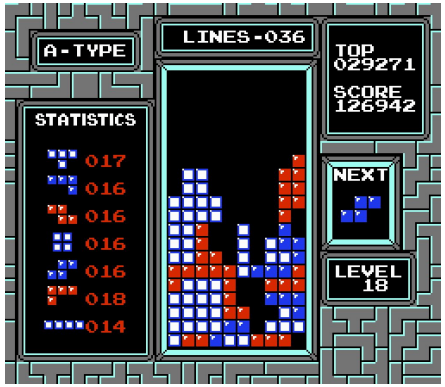
- Typically some kind of competition
- Usually more than one player
- Can involve luck
- Can involve strategy
- Can involve skill
- Usually for fun

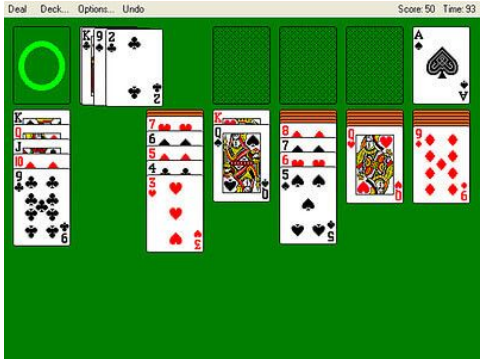
What is a “Game”?

Everyday usage:

- Typically some kind of competition
- Usually more than one player
- Can involve luck
- Can involve strategy
- Can involve skill
- Usually for fun







What is a “Game”?

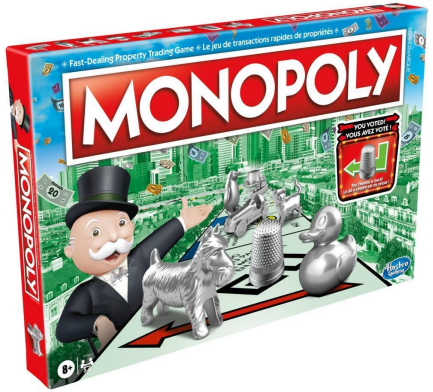
Everyday usage:

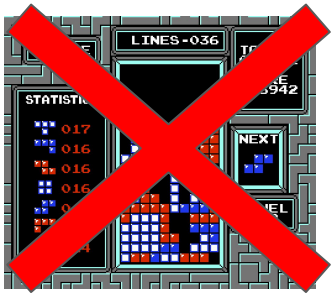
- Typically some kind of competition
- Usually more than one player
- Can involve luck
- Can involve strategy
- Can involve skill
- Usually for fun

In Game Theory:

- A mathematical description of a competition
- 2+ players (1-player games = decision theory)
- Can involve “luck” (i.e. nondeterminism)
- Strategy is the central focus of game theory
- Not really about skill (unless skill = choosing best strategy!)
- Always fun (for us, not always the players)

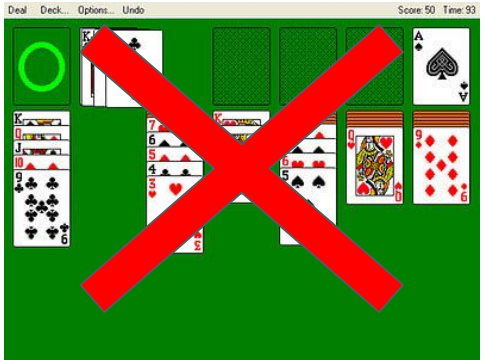
What is a “Game”?





In Game Theory:

- A mathematical description of a competition
- 2+ players (1-player games = decision theory)
- Can involve “luck” (i.e. nondeterminism)
- Strategy is the central focus of game theory
- Not really about skill (unless skill = choosing best strategy!)
- Always fun (for us, not always the players)

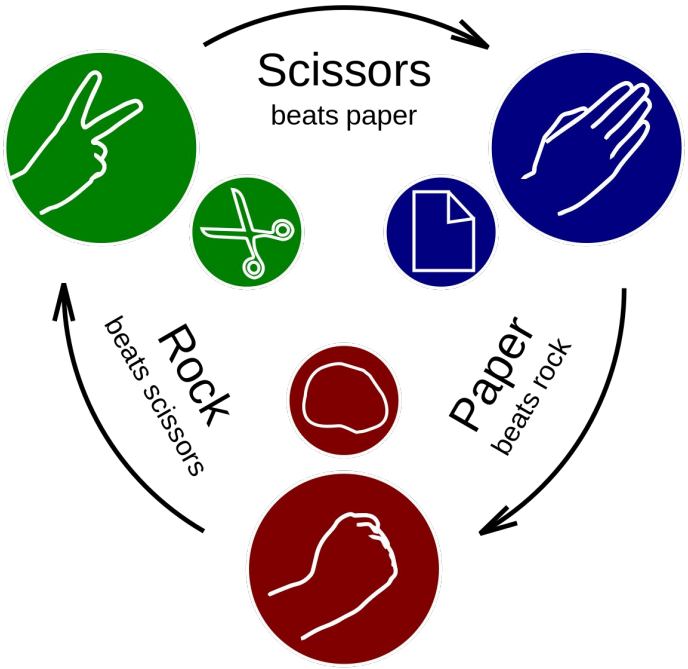


Types of Games

Two-player

Multi-player

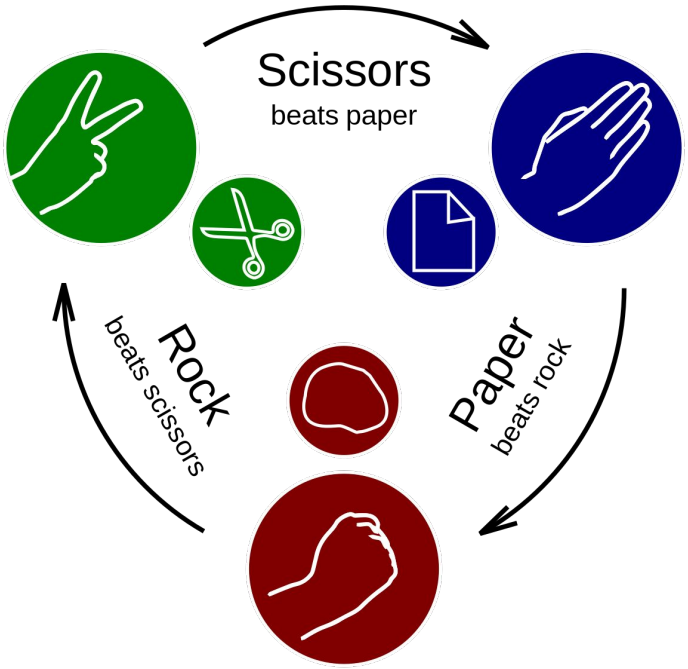
Types of Games



Simultaneous

Sequential

Types of Games



One shot

Iterated

Types of Games

Perfect information

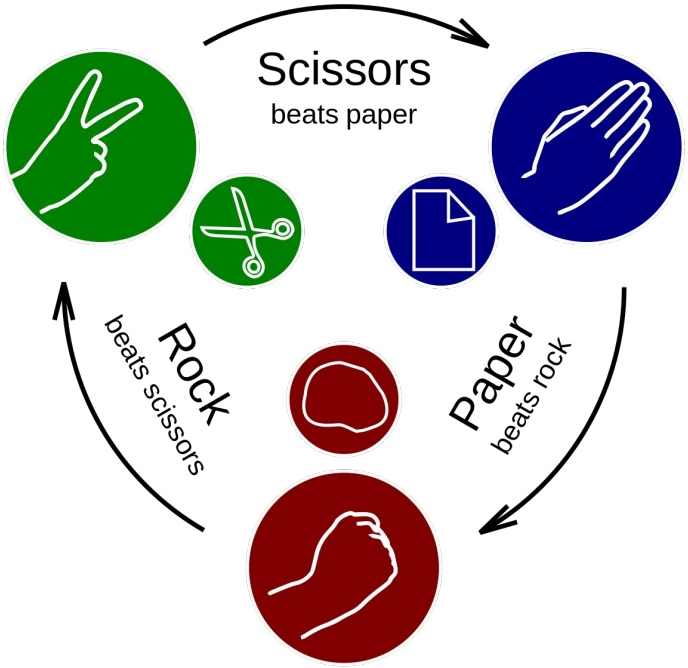
Imperfect information

Types of Games

Deterministic

Non-deterministic

Types of Games



Finite strategies

Infinite strategies*

*if $ ∈ ℝ

How are games expressed mathematically?

Definition of a “Normal-form” game:

- A set of players **P** = {1, 2, … , n}
- Each player p_i has a set of available actions a_i = {1,2, … , k}
  - We can represent the actions of all n players as **A** = (a_1, a_2, … a_n)
- For group of actions, each player has a utility or payoff function $u_i(\mathbf{A}) \rightarrow \mathbb{R}$
  - We can represent the payoff functions of all n players an **U** = (u_1, u_2, … u_n)
- A normal-form game is defined as the tuple (**P**, **A**, **U**)

Other assumptions

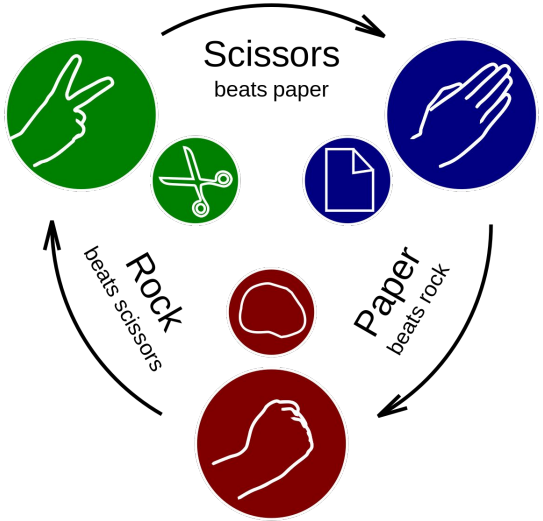
- Games are *inherited* (players do not choose the rules)

- Players are generally assumed to be “perfect players” (i.e. perfectly rational)
  - “Perfectly rational” = “Always pick the strategy that maximizes utility”
  - In combinatorics games, we often assume that players have infinite compute powers

Example: Rock Paper Scissors

- **P** = {player1, player2}
- $a_1 = a_2$ = {rock, paper, scissors}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

	Player2			
Player1		Rock	Paper	Scissors
	Rock	Player1 ← 0 Player2 ← 0	Player1 ← -1 Player2 ← 1	Player1 ← 1 Player2 ← -1
	Paper	Player1 ← 1 Player2 ← -1	Player1 ← 0 Player2 ← 0	Player1 ← -1 Player2 ← 1
	Scissors	Player1 ← -1 Player2 ← 1	Player1 ← 1 Player2 ← -1	Player1 ← 0 Player2 ← 0



The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

What type of game is this?

One shot or Iterated?

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

What type of game is this?

One shot or Iterated?

Simultaneous or Sequential?

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

What type of game is this?

One shot	or	Iterated?
Simultaneous	or	Sequential?
Deterministic	or	Non-Deterministic?

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

What type of game is this?

One shot	or	Iterated?
Simultaneous	or	Sequential?
Deterministic	or	Non-Deterministic?
Perfect information	or	Imperfect information?

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

What type of game is this?

One shot	or	Iterated?
Simultaneous	or	Sequential?
Deterministic	or	Non-Deterministic?
Perfect information	or	Imperfect information?
Finite	or	Infinite?

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

What type of game is this?

One shot	or	Iterated?
Simultaneous	or	Sequential?
Deterministic	or	Non-Deterministic?
Perfect information	or	Imperfect information?
Finite	or	Infinite?
2 player	or	Multiplayer?

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

What type of game is this?

One shot	or	Iterated?
Simultaneous	or	Sequential?
Deterministic	or	Non-Deterministic?
Perfect information	or	Imperfect information?
Finite	or	Infinite?
2 player	or	Multiplayer?

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

What will be each player's strategy?

- Choose the action a_i that maximizes $u_i(A)$
- If such a strategy exists, we call this a *best response*

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

What will be each player's strategy?

- Choose the action a_i that maximizes $u_i(A)$
- If such a strategy exists, we call this a *best response*

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

What will be each player's strategy?

- Choose the action a_i that maximizes $u_i(A)$
- If such a strategy exists, we call this a *best response*

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

What will be each player's strategy?

- Choose the action a_i that maximizes $u_i(A)$
- If such a strategy exists, we call this a *best response*

If Prisoner 2 cooperates, Prisoner 1 should defect

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

What will be each player's strategy?

- Choose the action a_i that maximizes $u_i(A)$
- If such a strategy exists, we call this a *best response*

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

What will be each player's strategy?

- Choose the action a_i that maximizes $u_i(A)$
- If such a strategy exists, we call this a *best response*

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

What will be each player's strategy?

- Choose the action a_i that maximizes $u_i(A)$
- If such a strategy exists, we call this a *best response*

If Prisoner 2 defects, Prisoner 1 should defect

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

What will be each player's strategy?

- Choose the action a_i that maximizes $u_i(A)$
- If such a strategy exists, we call this a *best response*

Regardless of Prisoner 2's strategy, Prisoner 1 should defect

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

What will be each player's strategy?

- Choose the action a_i that maximizes $u_i(A)$
- If such a strategy exists, we call this a *best response*

Regardless of Prisoner 2's strategy, Prisoner 1 should defect

Regardless of Prisoner 1's strategy, Prisoner 2 should defect

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

Dominant strategy is to defect

What will be each player's strategy?

- Choose the action a_i that maximizes $u_i(A)$
- If such a strategy exists, we call this a *best response*

Regardless of Prisoner 2's strategy, Prisoner 1 should defect

Regardless of Prisoner 1's strategy, Prisoner 2 should defect

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** → (ℝ, ℝ)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

Dominant strategy is to defect

Is this welfare-optimizing?

What will be each player's strategy?

- Choose the action a_i that maximizes $u_i(A)$
- If such a strategy exists, we call this a *best response*

Regardless of Prisoner 2's strategy, Prisoner 1 should defect

Regardless of Prisoner 1's strategy, Prisoner 2 should defect

The Prisoner's Dilemma

- **P** = {prisoner1, prisoner2}
- $a_1 = a_2$ = {cooperate, defect}, **A** = $a_1 \times a_2$
- Payoff matrix **U**: **A** $\rightarrow$ ($\mathbb{R}$, $\mathbb{R}$)

		Prisoner 2	
		Cooperate	Defect
Prisoner 1	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

Dominant strategy is to defect

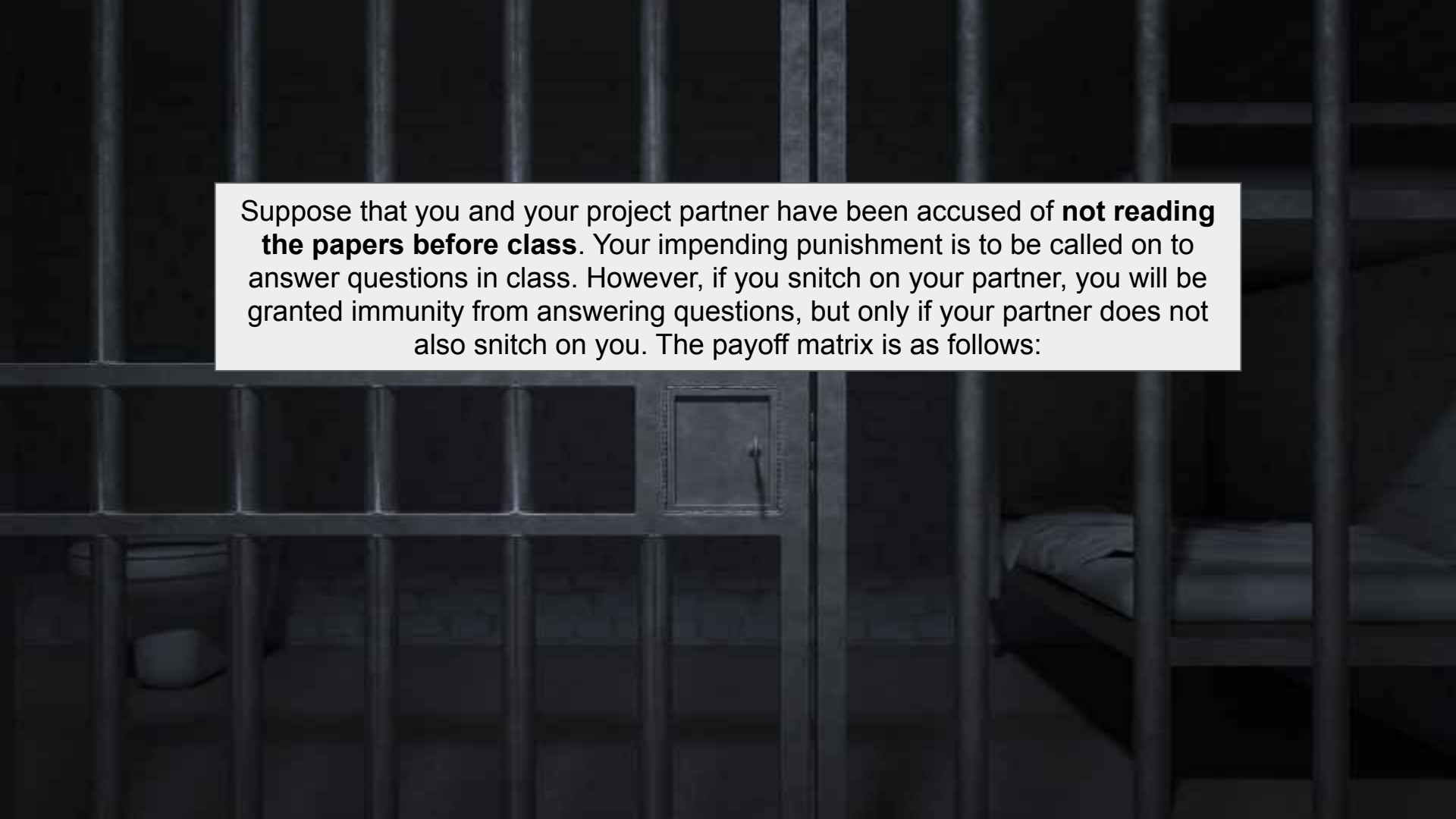
Is this welfare-optimizing? No!!

What will be each player's strategy?

- Choose the action a_i that maximizes $u_i(A)$
- If such a strategy exists, we call this a *best response*

Regardless of Prisoner 2's strategy, Prisoner 1 should defect

Regardless of Prisoner 1's strategy, Prisoner 2 should defect



Suppose that you and your project partner have been accused of **not reading the papers before class**. Your impending punishment is to be called on to answer questions in class. However, if you snitch on your partner, you will be granted immunity from answering questions, but only if your partner does not also snitch on you. The payoff matrix is as follows:

Suppose that you and your project partner have been accused of **not reading the papers before class**. Your impending punishment is to be called on to answer questions in class. However, if you snitch on your partner, you will be granted immunity from answering questions, but only if your partner does not also snitch on you. The payoff matrix is as follows:

		Student 2	
		Cooperate	Defect
Student 1	Cooperate	Student 1 ← answer 1 question Student 2 ← answer 1 question	Student 1 ← answer 3 questions Student 2 ← answer 0 questions
	Defect	Student 1 ← answer 0 questions Student 2 ← answer 3 questions	Student 1 ← answer 2 questions Student 2 ← answer 2 questions

Does this mean people never cooperate?

- Simplified game's payoff function does not include:
  - Trust
  - Fear of retribution
  - Reputation

- Real-world games are often iterated
  - Axelrod's Tournament: "tit-for-tat" strategy won

Where do we see prisoner’s dilemmas in security?

Where do we see prisoner’s dilemmas in security?

After an insured cyber incident:

- If a policyholder is open honest with their insurer about what led to a breach, they might not recover all losses (due to exclusions), but the insurer can better learn what types of defenses to recommend to policyholders.
  - This is the **cooperate-cooperate** strategy.
  - We can give this a payoff (-1, -1)

Where do we see prisoner’s dilemmas in security?

After an insured cyber incident:

- If a policyholder is evasive with their insurer about what caused the breach, they may not trigger any exclusions. If all the other policyholders were honest with the insurer, the insurer will still have good advice for how to defend against future attacks.
  - This is the **defect-cooperate** strategy
  - We can give this a payoff (0,-3)

Where do we see prisoner's dilemmas in security?

After an insured cyber incident:

- If a policyholder is honest with their insurer, they may suffer exclusions. If none of the other policyholders were honest with the insurer, the insurer has no good advice for how to defend against future attacks.
  - This is the **cooperate-defect** strategy
  - We can give this a payoff (-3,0)

Where do we see prisoner’s dilemmas in security?

After an insured cyber incident:

- If all policyholders are evasive with their insurer, the insurer does not learn which defenses are cost effective. The cost of premiums goes up.
  - This is the **defect-defect** strategy
  - We can give this a payoff (-2,-2)

Where do we see prisoner's dilemmas in security?

After an insured cyber incident:

- If all policyholders are evasive with their insurer, the insurer does not learn which defenses are cost effective. The cost of premiums goes up.
  - This is the **defect-defect** strategy
  - We can give this a payoff (-2,-2)

The payoff matrix is identical to the prisoner's dilemma

Dominant strategy is to defect i.e. be evasive with insurer

Overall utility is not pareto efficient!

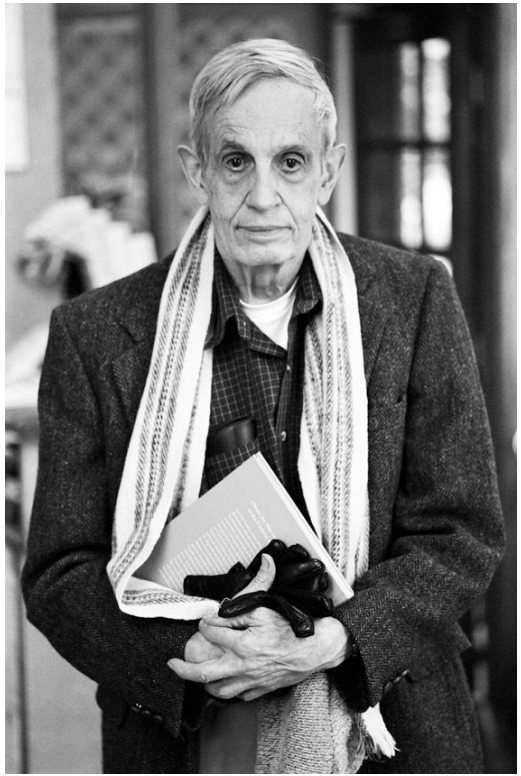
Some additional terminology

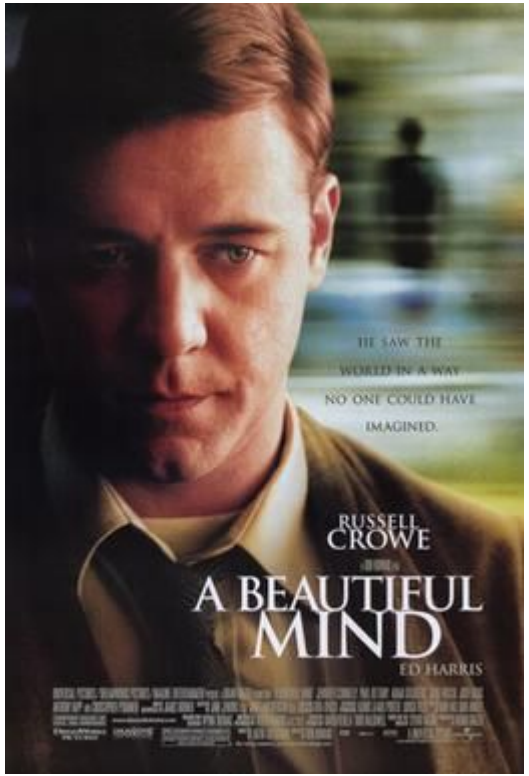
- **Dominant strategy:** A strategy that produces the highest possible outcome for every possible competitor action such that
  - $u_i(a_i \mid a_{\sim i}) \geq u_i(a'_i \mid a_{\sim i}) \quad \forall\, a'_i, \quad \forall\, a_{\sim i}$
  - E.g. in the prisoner's dilemma, it's always rational to defect, regardless of the other player's action

- **Best reply/best response:** Player i's strategy that produces the highest possible outcome for a given profile of opponent strategies $a_{\sim i}$ such that
  - $u_i(a_i \mid a_{\sim i}) \geq u_i(a'_i \mid a_{\sim i}) \quad \forall\, a'_i$

- **Nash equilibrium:** A profile of strategies $a \in \mathbf{A}$ if a_i is a best response to $a_{\sim i}$ for each player i
  - $u_i(a_i \mid a_{\sim i}) \geq u_i(a'_i \mid a_{\sim i}) \quad \forall\, i, \quad \forall\, a_{\sim i}$
  - How is this different from a dominant strategy?
    - All it requires is that there is a optimal strategy for each player i for each of the other players' actions (not necessarily that this strategy is the same regardless of the other players' actions)

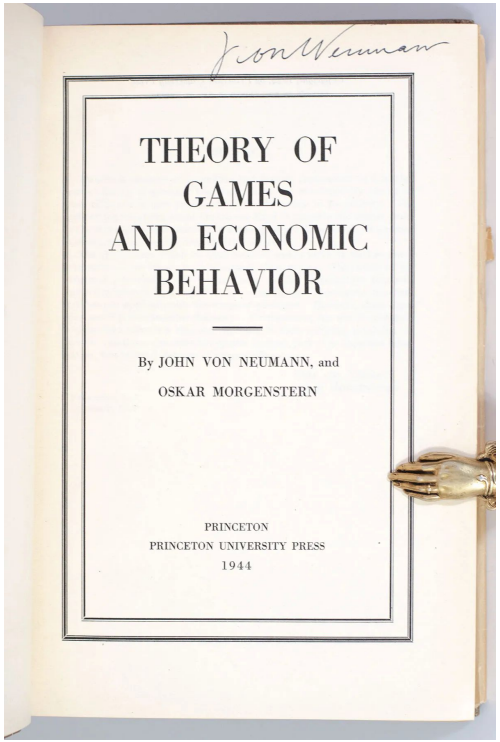
Why a “Nash” equilibrium?

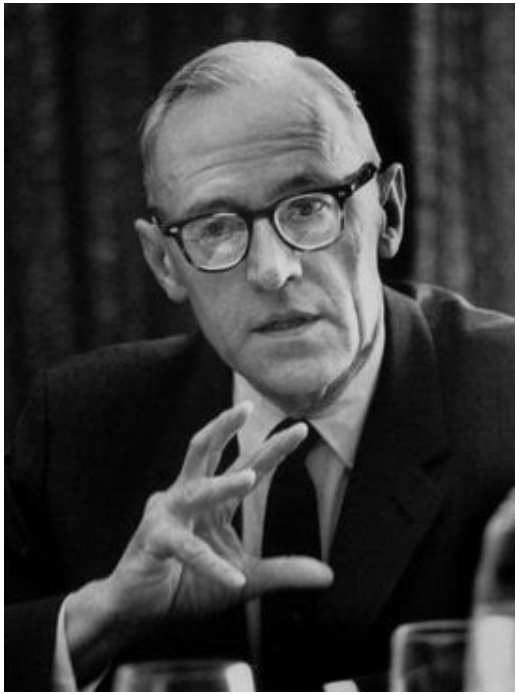




(These guys were important too)

John von Neumann

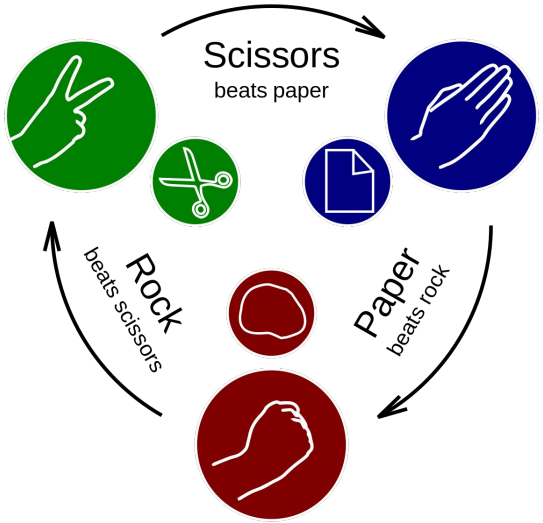




Oskar Morganstern

Zero sum games

		Player2		
		Rock	Paper	Scissors
Player1	Rock	Player1 ← 0 Player2 ← 0	Player1 ← -1 Player2 ← 1	Player1 ← 1 Player2 ← -1
	Paper	Player1 ← 1 Player2 ← -1	Player1 ← 0 Player2 ← 0	Player1 ← -1 Player2 ← 1
	Scissors	Player1 ← -1 Player2 ← 1	Player1 ← 1 Player2 ← -1	Player1 ← 0 Player2 ← 0

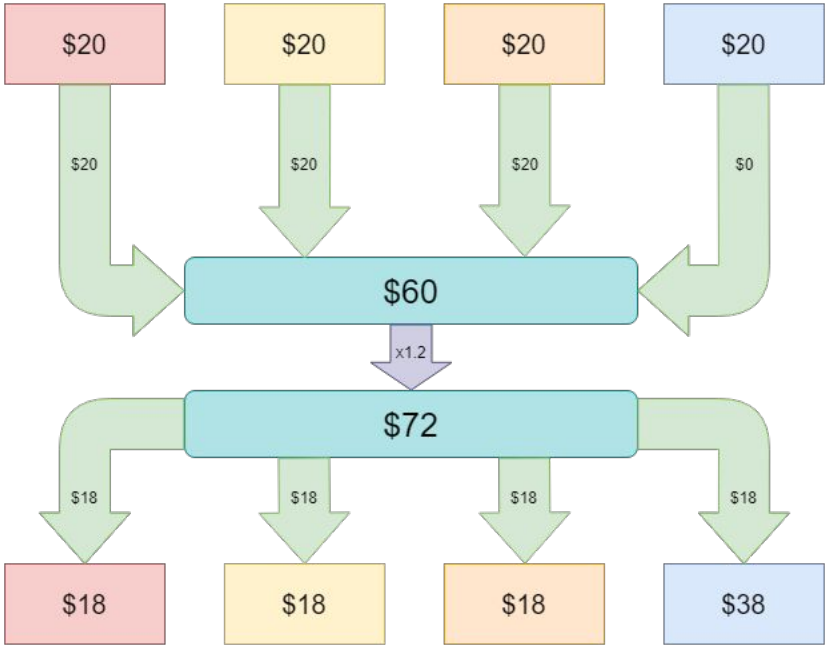


Negative sum games

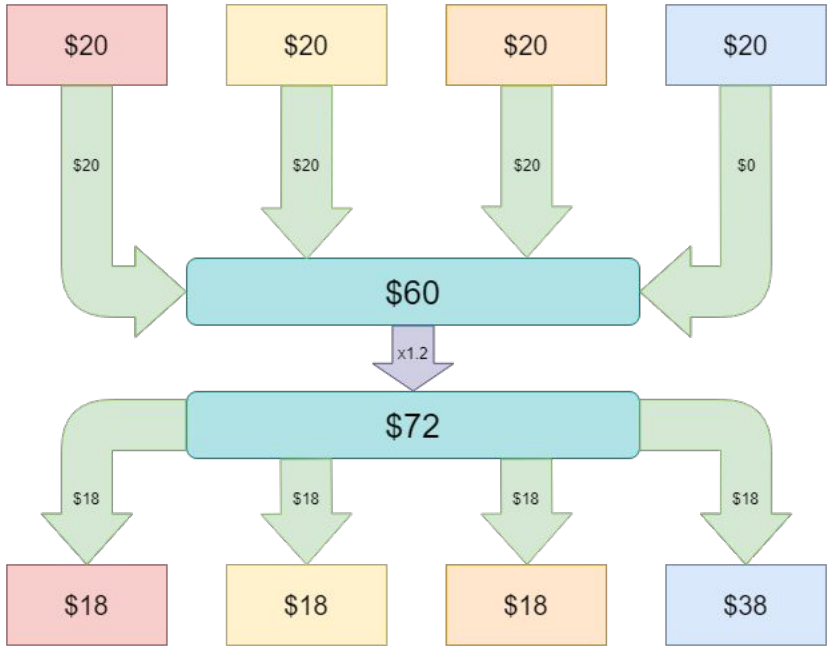
	Prisoner 2		
Prisoner 1		Cooperate	Defect
	Cooperate	Player1 ← -1 Player2 ← -1	Player1 ← -3 Player2 ← 0
	Defect	Player1 ← 0 Player2 ← -3	Player1 ← -2 Player2 ← -2

Positive sum games?

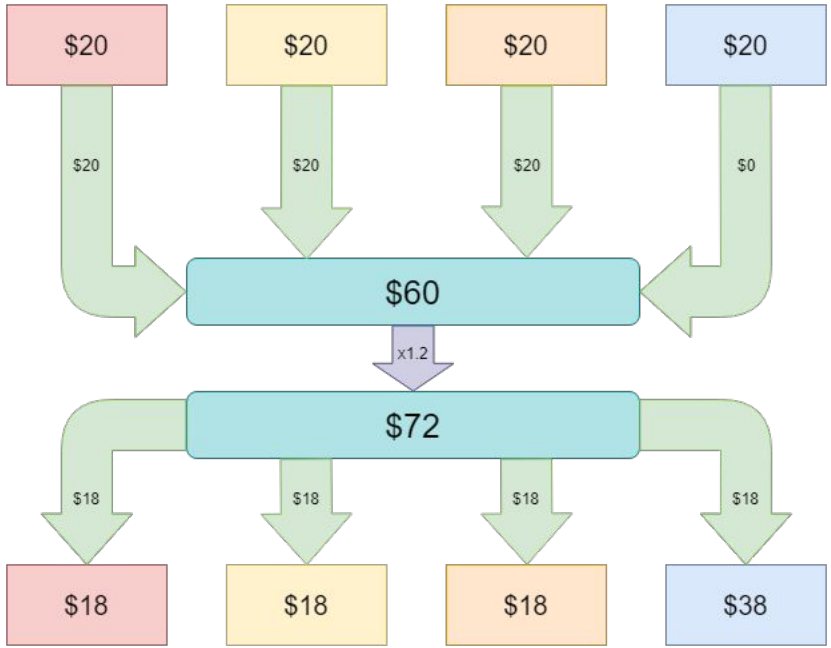
The Public Goods game (a positive sum game)



The Public Goods game (a positive sum game)



The Public Goods game (a positive sum game)



$\sum$ = +$12

Chapter 1

SYSTEM RELIABILITY AND FREE RIDING

Hal Varian
*School of Information Management and Systems, UC Berkeley**
hal@sims.berkeley.edu

In the total effort case, the agents with the least cost of effort to avoid systems failure should bear all the liability.

System reliability often depends on the effort of many individuals, making reliability a public good. It is well-known that purely voluntary provision of public goods may result in a free rider problem: individuals may tend to shirk, resulting in an inefficient level of the public good.

How much effort each individual exerts will depend on his own benefits and costs, the efforts exerted by the other individuals, and the technology that relates individual effort to outcomes. In the context of system reliability, we can distinguish three prototypical cases.

Total effort. Reliability depends on the sum of the efforts exerted by the individuals.

Weakest link. Reliability depends on the minimum effort.

Best shot. Reliability depends on the maximum effort.

Each of these is a reasonable technology in different circumstances. Suppose that there is one wall defending a city and the probability of successful defense depends on the strength of the wall, which in turn depends on the sum of the efforts of the builders. Alternatively, think of the wall as having varying height, with the probability of success depending on the height at its lowest point. Or, finally, think of a there being several walls, where only the highest one matters. Of course, many systems involve a mixture of these cases.

*First published in *ICEC2003: Fifth International Conference on Electronic Commerce,* N. Sadeh, ed., ACM Press, 2003, pp. 355–366.

But first: a (non-game theory) game

- I want to know how easy or difficult these readings were for you
- However, if I ask each of you directly, you might not answer truthfully
  - There might be an incentive to overstate your comprehension
- What can we do?
  - Write down your answer on a sheet of paper?
    - Handwriting is easily de-anonymized
  - Anonymous online survey?
    - Maybe, but have to trust the survey host not to collect IPs or de-anonymize another way
  - Secret ballot voting?
    - Requires physical ballots, ballot box, secret room
    - We are a virtual class today

An incentive compatible mechanism for eliciting truthful responses

- I will send one of you a secret number via chat
- If you thought the readings were easy, add 1 to the number
- If you thought the readings were hard, subtract 1 from the number
- Pass the new number to the next person in the chain.

Adam → Gabe → Ina → Madhura → Nashita → Noam → Neha → Adam

- Advantages:
  - If the final number is greater than the starting number, I know the class overall found the readings to be easy
  - If the final number is less than the starting number, I know the class overall found the readings to be hard
  - No one is able to infer the responses of anyone else

Total effort. Reliability depends on the sum of the efforts exerted by the individuals.

Weakest link. Reliability depends on the minimum effort.

Best shot. Reliability depends on the maximum effort.

Total effort. ~~Reliability~~ security depends on the sum of the efforts exerted by the individuals.

Weakest link. ~~Reliability~~ security depends on the minimum effort.

Best shot. ~~Reliability~~ security depends on the maximum effort.

Let x_i be the effort exerted by agent $i = 1, 2$, and let $P(F(x_1, x_2))$ be the probability of successful operation of the system. Agent i receives value v_i from the successful operation of the system and effort x_i costs the agent $c_i x_i$.

The expected payoff to agent i is taken to be

$$P(F(x_1, x_2))v_i - c_i x_i$$

and the social payoff is

$$P(F(x_1, x_2))[v_1 + v_2] - c_1 x_1 - c_2 x_2.$$

We assume that the function $P(F)$ is differentiable, increasing in F, and is concave, at least in the relevant region.

We examine three specifications for F, motivated by the taxonomy given earlier.

Total effort. $F(x_1, x_2) = x_1 + x_2$.

Weakest link. $F(x_1, x_2) = \min(x_1, x_2)$.

Best shot. $F(x_1, x_2) = \max(x_1, x_2)$.

Let x_i be the effort exerted by agent $i = 1, 2$, and let $P(F(x_1, x_2))$ be the probability of successful operation of the system. Agent i receives value v_i from the successful operation of the system and effort x_i costs the agent $c_i x_i$.

The expected payoff to agent i is taken to be

$$P(F(x_1, x_2))v_i - c_i x_i$$

and the social payoff is

$$P(F(x_1, x_2))[v_1 + v_2] - c_1 x_1 - c_2 x_2.$$

?

We assume that the function $P(F)$ is differentiable, increasing in F, and is concave, at least in the relevant region.

We examine three specifications for F, motivated by the taxonomy given earlier.

Total effort. $F(x_1, x_2) = x_1 + x_2$.

Weakest link. $F(x_1, x_2) = \min(x_1, x_2)$.

Best shot. $F(x_1, x_2) = \max(x_1, x_2)$.

Let x_i be the effort exerted by agent $i = 1, 2$, and let $P(F(x_1, x_2))$ be the probability of successful operation of the system. Agent i receives value v_i from the successful operation of the system and effort x_i costs the agent $c_i x_i$.

The expected payoff to agent i is taken to be

$$P(F(x_1, x_2))v_i - c_i x_i$$

and the social payoff is

$$P(F(x_1, x_2))[v_1 + v_2] - c_1 x_1 - c_2 x_2.$$

We assume that the function $P(F)$ is differentiable, increasing in F, and is concave, at least in the relevant region.

We examine three specifications for F, motivated by the taxonomy given earlier.

Total effort. $F(x_1, x_2) = x_1 + x_2$.

Weakest link. $F(x_1, x_2) = \min(x_1, x_2)$.

Best shot. $F(x_1, x_2) = \max(x_1, x_2)$.

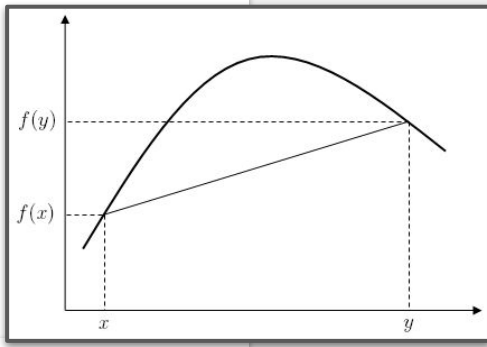
Let x_i be the effort exerted by agent $i = 1, 2$, and let $P(F(x_1, x_2))$ be the probability of successful operation of the system. Agent i receives value v_i from the successful operation of the system and effort x_i costs the agent $c_i x_i$.

The expected payoff to agent i is taken to be

$$P(F(x_1, x_2))v_i - c_i x_i$$

and the social payoff is

$$P(F(x_1, x_2))[v_1 + v_2] - c_1 x_1 - c_2 x_2.$$



We assume that the function $P(F)$ is differentiable, increasing in F, and is concave, at least in the relevant region.

?

We examine three specifications for F, motivated by the taxonomy given earlier.

Total effort. $F(x_1, x_2) = x_1 + x_2$.

Weakest link. $F(x_1, x_2) = \min(x_1, x_2)$.

Best shot. $F(x_1, x_2) = \max(x_1, x_2)$.

Total effort

Agent 1 chooses x_1 to solve

$$\max_{x_1} v_1 P(x_1 + x_2) - c_1 x_1,$$

which has first-order conditions

$$v_1 P'(x_1 + x_2) = c_1.$$

Letting G be the inverse of the derivative of P', we have

$$x_1 + x_2 = G(c_1/v_1).$$

Defining $\bar{x}_1 = G(c_1/v_1)$ we have the reaction function of agent 1 to agent 2's choice

$$f_1(x_2) = \bar{x}_1 - x_2.$$

Similarly

$$f_2(x_1) = \bar{x}_2 - x_1.$$

Total effort

Agent 1 chooses x_1 to solve

$$\max_{x_1} v_1 P(x_1 + x_2) - c_1 x_1,$$

?

which has first-order conditions

$$v_1 P'(x_1 + x_2) = c_1.$$

Letting G be the inverse of the derivative of P', we have

$$x_1 + x_2 = G(c_1/v_1).$$

Defining $\bar{x}_1 = G(c_1/v_1)$ we have the reaction function of agent 1 to agent 2's choice

$$f_1(x_2) = \bar{x}_1 - x_2.$$

Similarly

$$f_2(x_1) = \bar{x}_2 - x_1.$$

Total effort

Agent 1 chooses x_1 to solve

$$\max_{x_1} v_1 P(x_1 + x_2) - c_1 x_1,$$

which has first-order conditions

$$v_1 P'(x_1 + x_2) = c_1.$$

Letting G be the inverse of the derivative of P', we have

$$x_1 + x_2 = G(c_1/v_1).$$

Defining $\bar{x}_1 = G(c_1/v_1)$ we have the reaction function of agent 1 to agent 2's choice

$$f_1(x_2) = \bar{x}_1 - x_2.$$

Similarly

$$f_2(x_1) = \bar{x}_2 - x_1.$$

The expected payoff to agent i is taken to be

$$P(F(x_1, x_2))v_i - c_i x_i$$

?

Total effort. $F(x_1, x_2) = x_1 + x_2.$

Total effort

Agent 1 chooses x_1 to solve

$$\max_{x_1} v_1 P(x_1 + x_2) - c_1 x_1,$$

which has first-order conditions

?

$$v_1 P'(x_1 + x_2) = c_1.$$

Letting G be the inverse of the derivative of P', we have

$$x_1 + x_2 = G(c_1/v_1).$$

Defining $\bar{x}_1 = G(c_1/v_1)$ we have the reaction function of agent 1 to agent 2's choice

$$f_1(x_2) = \bar{x}_1 - x_2.$$

Similarly

$$f_2(x_1) = \bar{x}_2 - x_1.$$

Total effort

Agent 1 chooses x_1 to solve

$$\max_{x_1} v_1 P(x_1 + x_2) - c_1 x_1,$$

which has first-order conditions

$$v_1 P'(x_1 + x_2) = c_1.$$

Letting G be the inverse of the derivative of P', we have

$$x_1 + x_2 = G(c_1/v_1).$$

Defining $\bar{x}_1 = G(c_1/v_1)$ we have the reaction function of agent 1 to agent 2's choice

$$f_1(x_2) = \bar{x}_1 - x_2.$$

Similarly

$$f_2(x_1) = \bar{x}_2 - x_1.$$

?

Find where d/dx = 0

Because P(F) is concave, we know this is a maximum

Total effort

Agent 1 chooses x_1 to solve

$$\max_{x_1} v_1 P(x_1 + x_2) - c_1 x_1,$$

which has first-order conditions

$$v_1 P'(x_1 + x_2) = c_1.$$

Letting G be the inverse of the derivative of P', we have

$$x_1 + x_2 = G(c_1/v_1).$$

Defining $\bar{x}_1 = G(c_1/v_1)$ we have the reaction function of agent 1 to agent 2's choice

$$f_1(x_2) = \bar{x}_1 - x_2.$$

Similarly

$$f_2(x_1) = \bar{x}_2 - x_1.$$

Total effort

Agent 1 chooses x_1 to solve

$$\max_{x_1} v_1 P(x_1 + x_2) - c_1 x_1,$$

which has first-order conditions

$$v_1 P'(x_1 + x_2) = c_1.$$

Letting G be the inverse of the derivative of P', we have

$$x_1 + x_2 = G(c_1/v_1).$$

Defining $\bar{x}_1 = G(c_1/v_1)$ we have the reaction function of agent 1 to agent 2's choice

$$f_1(x_2) = \bar{x}_1 - x_2.$$

?

Similarly

$$f_2(x_1) = \bar{x}_2 - x_1.$$

Total effort

Agent 1 chooses x_1 to solve

$$\max_{x_1} v_1 P(x_1 + x_2) - c_1 x_1,$$

which has first-order conditions

$$v_1 P'(x_1 + x_2) = c_1.$$

Letting G be the inverse of the derivative of P', we have

$$x_1 + x_2 = G(c_1/v_1).$$

Defining $\bar{x}_1 = G(c_1/v_1)$ we have the reaction function of agent 1 to agent 2's choice

$$f_1(x_2) = \bar{x}_1 - x_2.$$

Similarly

$$f_2(x_1) = \bar{x}_2 - x_1.$$

If Agent 2 spends x_2, then Agent 1's personal welfare is maximized when Agent1 spends \bar{x}_1 - x_2

Total effort

Agent 1 chooses x_1 to solve

$$\max_{x_1} v_1 P(x_1 + x_2) - c_1 x_1,$$

which has first-order conditions

$$v_1 P'(x_1 + x_2) = c_1.$$

Letting G be the inverse of the derivative of P', we have

$$x_1 + x_2 = G(c_1/v_1).$$

Defining $\bar{x}_1 = G(c_1/v_1)$ we have the reaction function of agent 1 to agent 2's choice

$$f_1(x_2) = \bar{x}_1 - x_2.$$

Similarly

$$f_2(x_1) = \bar{x}_2 - x_1.$$

If Agent 1 spends x_1, then Agent 2's personal welfare is maximized when Agent 2 spends \bar{x}_2 - x_1

Total effort

Agent 1 chooses x_1 to solve

$$\max_{x_1} v_1 P(x_1 + x_2) - c_1 x_1,$$

which has first-order conditions

$$v_1 P'(x_1 + x_2) = c_1.$$

Letting G be the inverse of the derivative of P', we have

$$x_1 + x_2 = G(c_1/v_1).$$

Defining $\bar{x}_1 = G(c_1/v_1)$ we have the reaction function of agent 1 to agent 2's choice

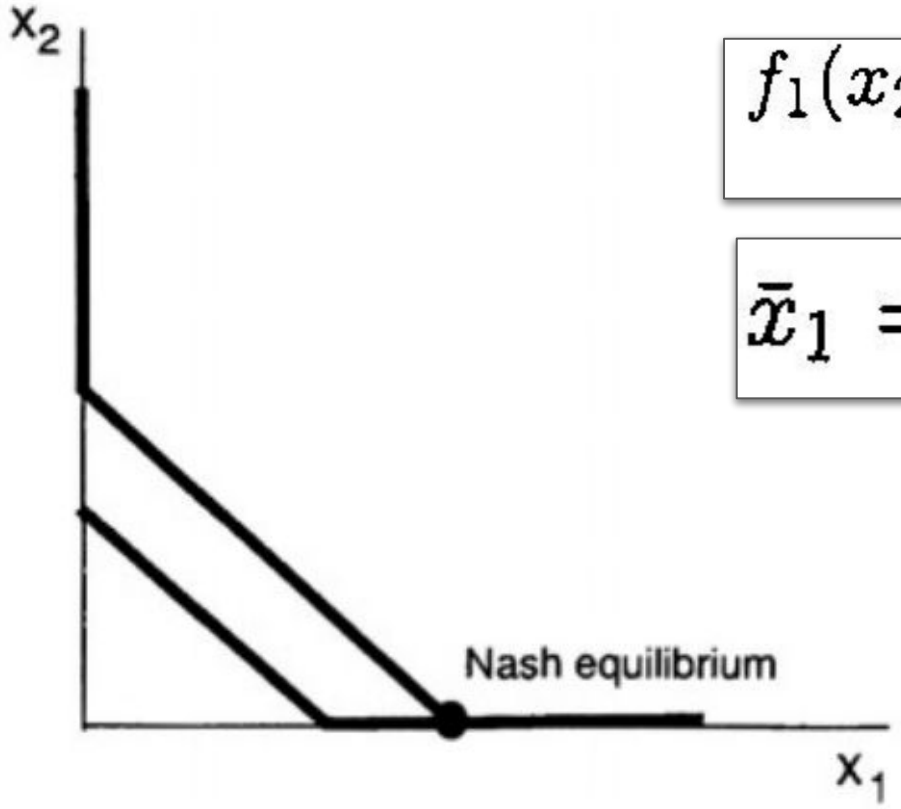
$$f_1(x_2) = \bar{x}_1 - x_2.$$

Similarly

$$f_2(x_1) = \bar{x}_2 - x_1.$$

If Agent 1 spends x_1, then Agent 2's personal welfare is maximized when Agent 2 spends \bar{x}_2 - x_1

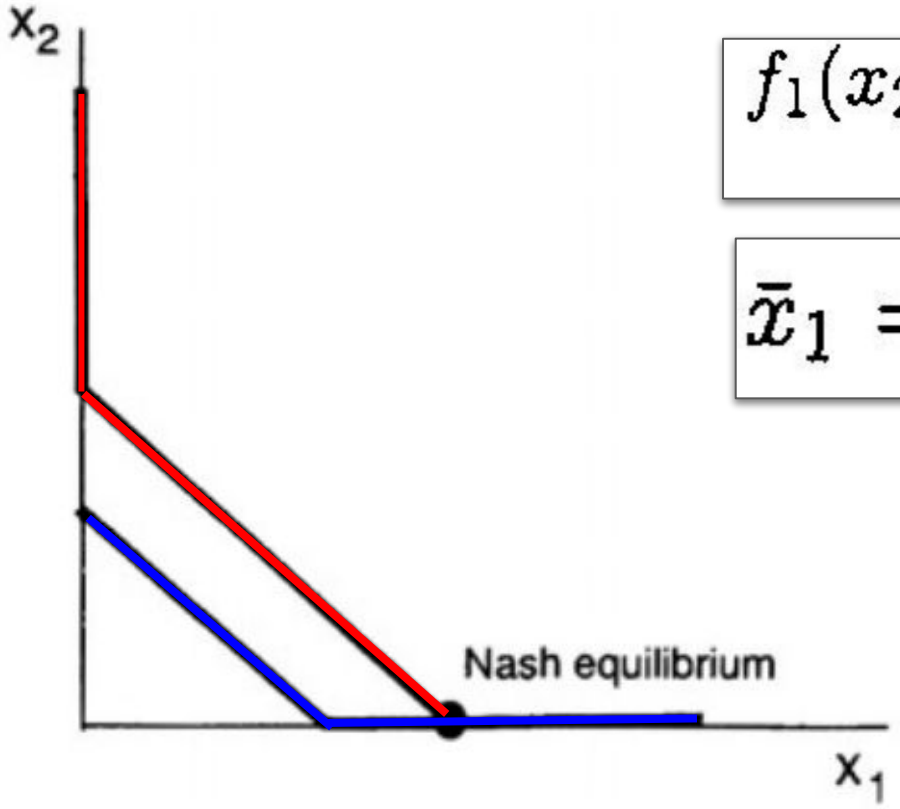
Aka "Best response"



$$f_1(x_2) = \bar{x}_1 - x_2.$$

$$\bar{x}_1 = G(c_1/v_1)$$

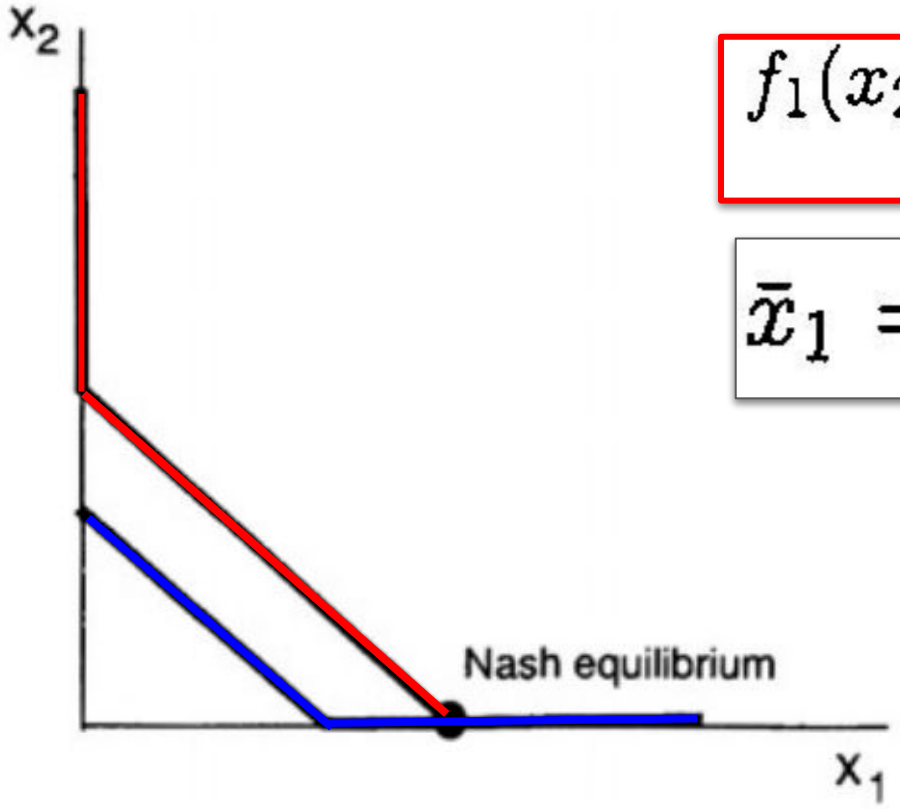
Figure 1.1. Nash equilibrium in total effort case.



$$f_1(x_2) = \bar{x}_1 - x_2.$$

$$\bar{x}_1 = G(c_1/v_1)$$

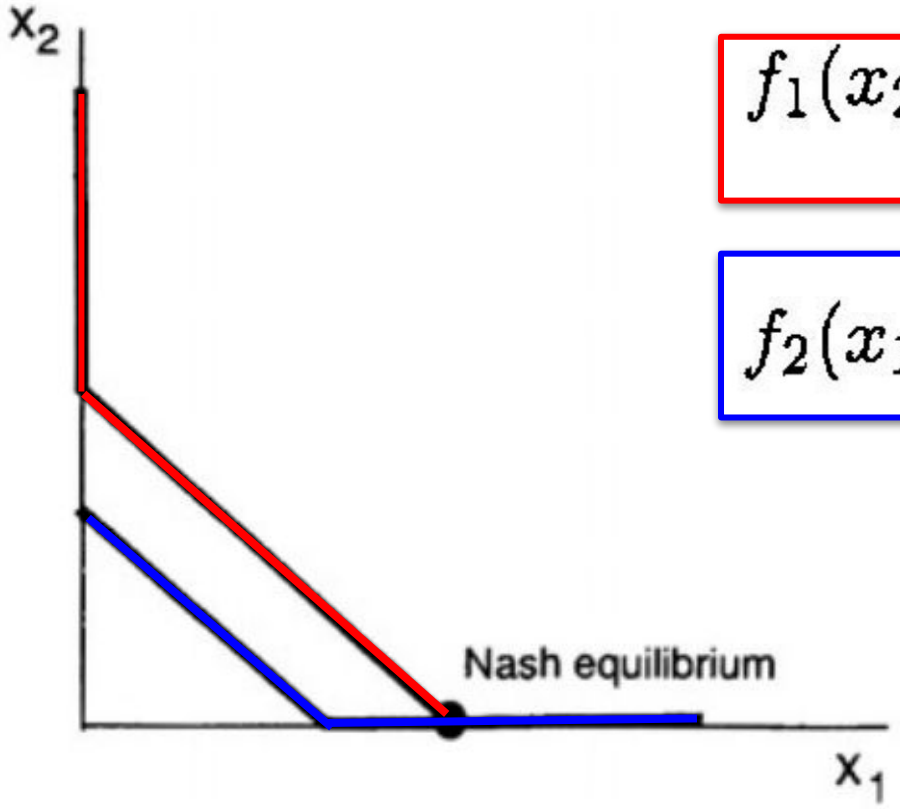
Figure 1.1. Nash equilibrium in total effort case.



$$f_1(x_2) = \bar{x}_1 - x_2.$$

$$\bar{x}_1 = G(c_1/v_1)$$

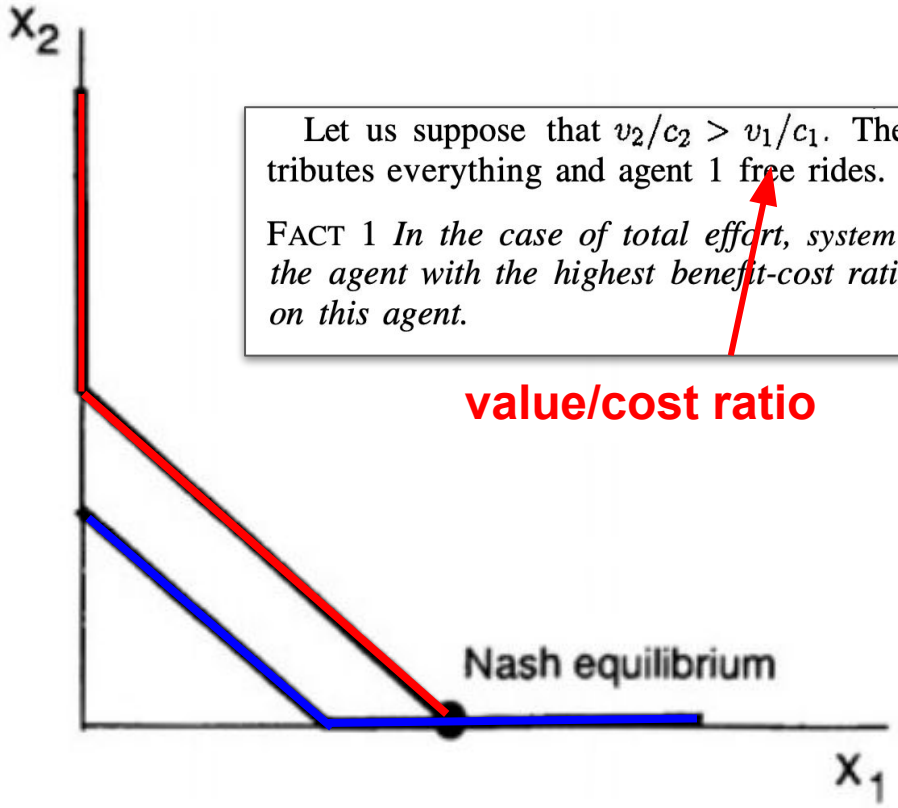
Figure 1.1. Nash equilibrium in total effort case.



$$f_1(x_2) = \bar{x}_1 - x_2.$$

$$f_2(x_1) = \bar{x}_2 - x_1.$$

Figure 1.1. Nash equilibrium in total effort case.

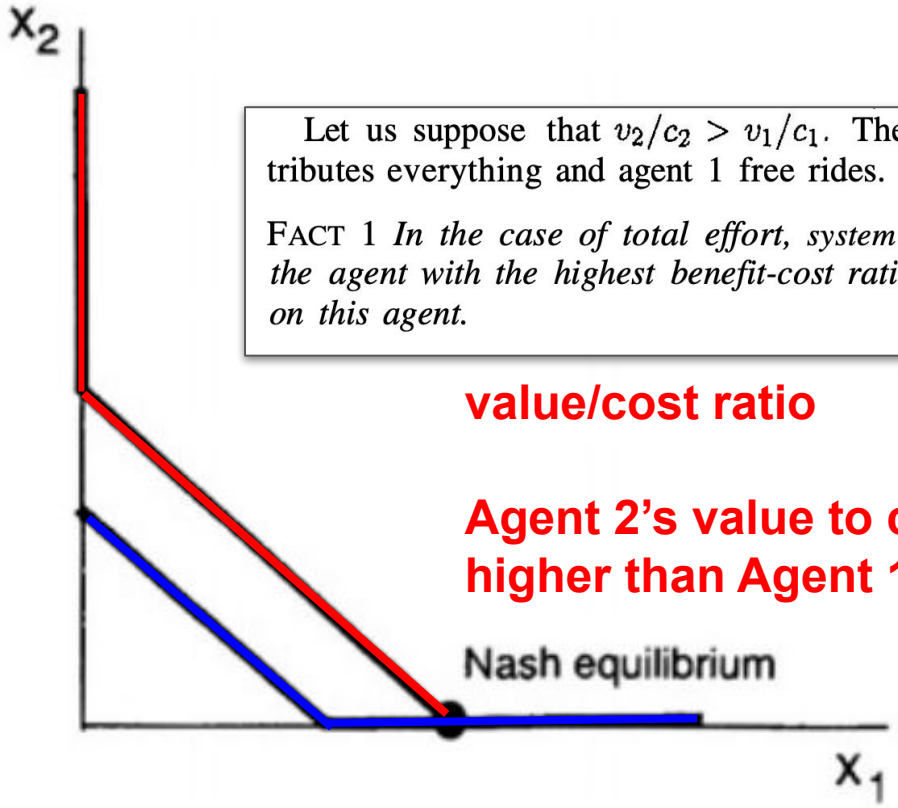


Let us suppose that $v_2/c_2 > v_1/c_1$. Then, $\bar{x}_2 > \bar{x}_1$, so agent 2 contributes everything and agent 1 free rides.

FACT 1 *In the case of total effort, system reliability is determined by the agent with the highest benefit-cost ratio. All other agents free ride on this agent.*

value/cost ratio

Figure 1.1. Nash equilibrium in total effort case.



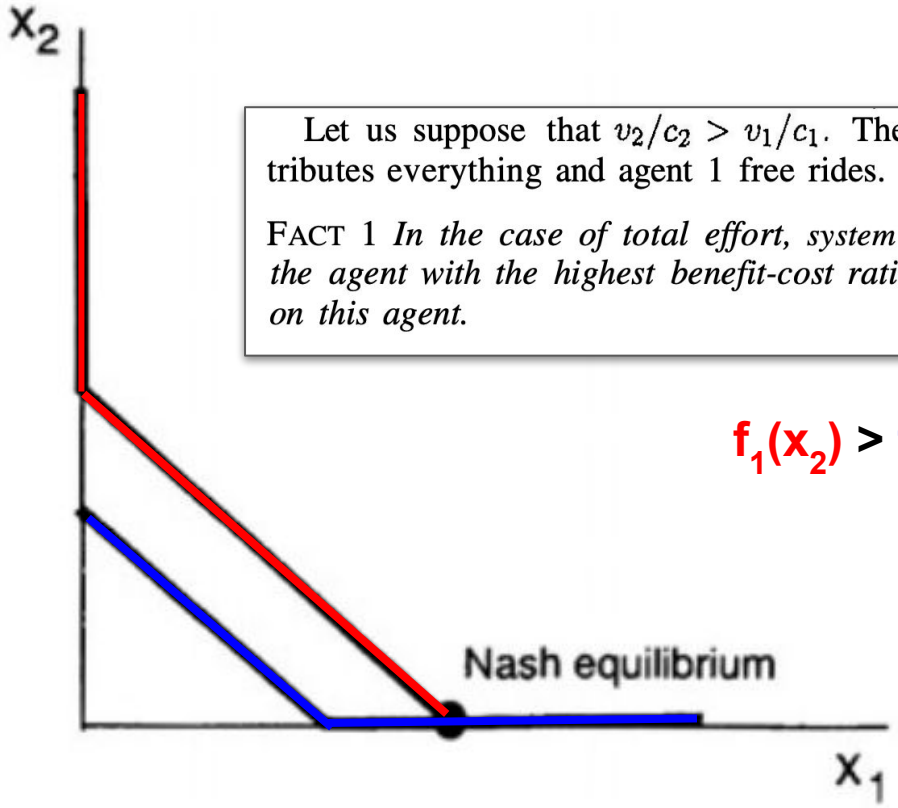
Let us suppose that $v_2/c_2 > v_1/c_1$. Then, $\bar{x}_2 > \bar{x}_1$, so agent 2 contributes everything and agent 1 free rides.

FACT 1 *In the case of total effort, system reliability is determined by the agent with the highest benefit-cost ratio. All other agents free ride on this agent.*

value/cost ratio

Agent 2's value to cost ratio is higher than Agent 1's

Figure 1.1. Nash equilibrium in total effort case.



Let us suppose that $v_2/c_2 > v_1/c_1$. Then, $\bar{x}_2 > \bar{x}_1$, so agent 2 contributes everything and agent 1 free rides.

FACT 1 *In the case of total effort, system reliability is determined by the agent with the highest benefit-cost ratio. All other agents free ride on this agent.*

$f_1(x_2) > f_2(x_1)$

Figure 1.1. Nash equilibrium in total effort case.

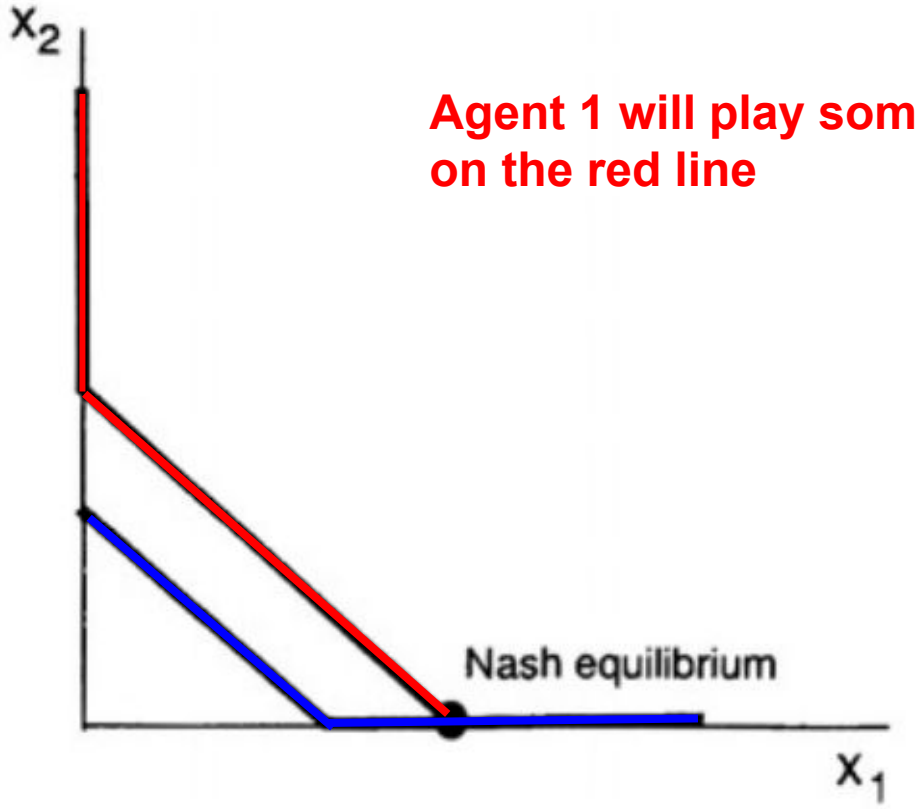
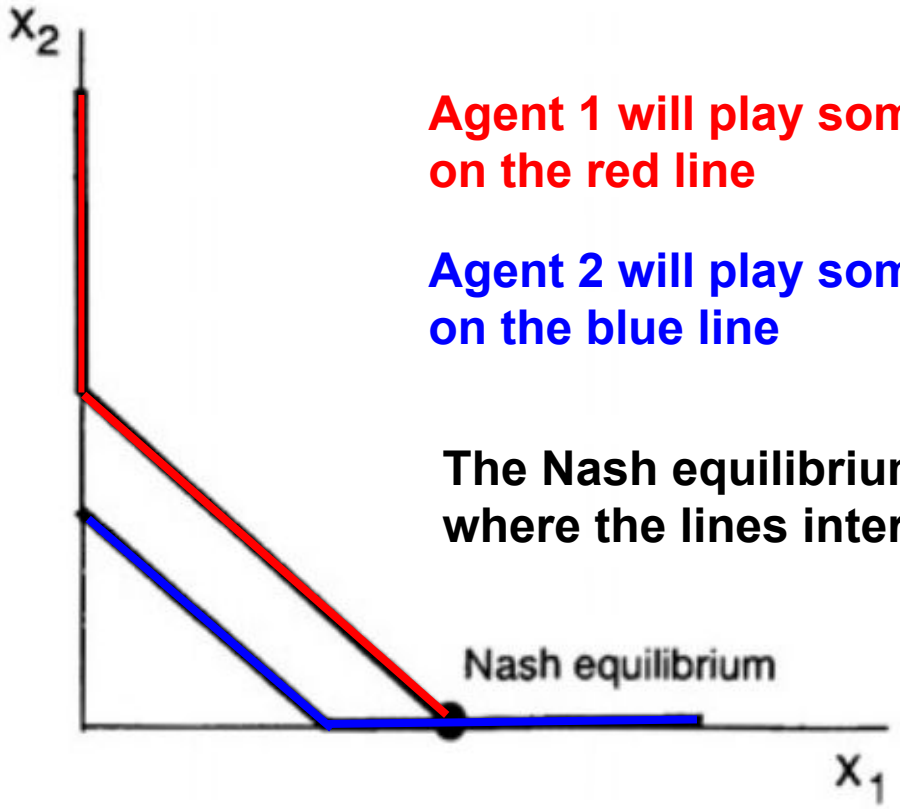


Figure 1.1. Nash equilibrium in total effort case.

Figure 1.1. Nash equilibrium in total effort case.



Agent 1 will play somewhere on the red line

Agent 2 will play somewhere on the blue line

The Nash equilibrium is where the lines intersect

Figure 1.1. Nash equilibrium in total effort case.

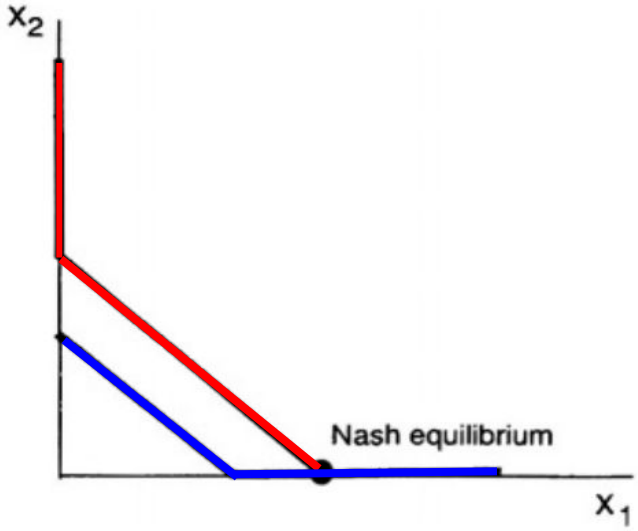


Figure 1.1. Nash equilibrium in total effort case.

FACT 1 *In the case of total effort, system reliability is determined by the agent with the highest benefit-cost ratio. All other agents free ride on this agent.*

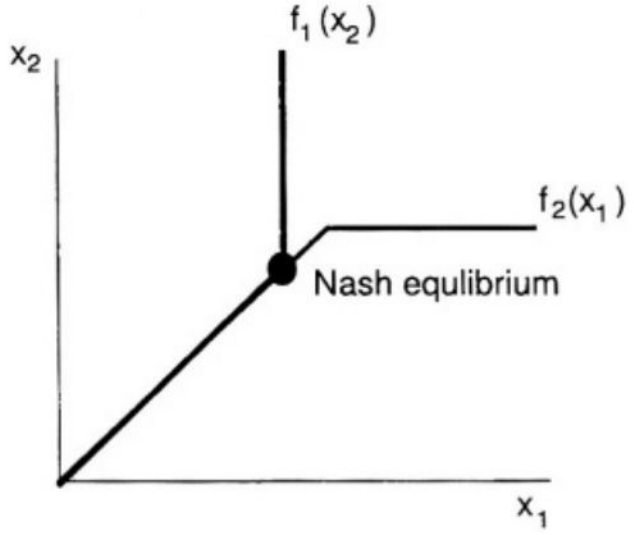


Figure 1.2. Nash equilibrium in weakest link case.

FACT 2 *In the weakest-link case, system reliability is determined by the agent with the lowest benefit-cost ratio.*

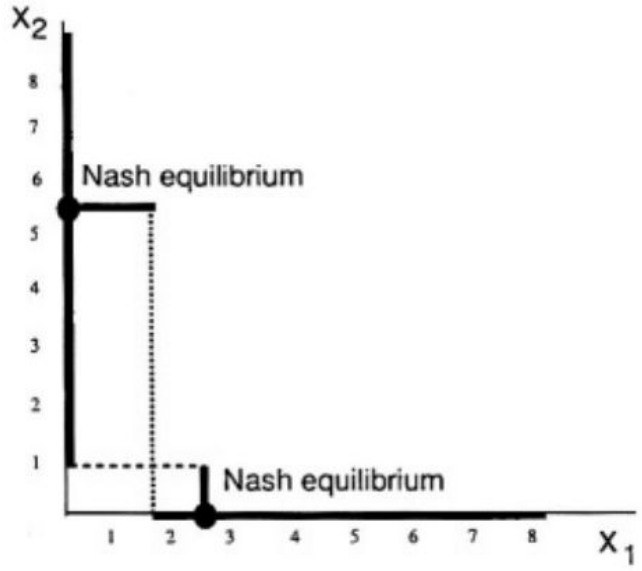


Figure 1.3. Nash equilibria in best-shot case.

Total effort

The social problem solves

$$\max_{x_1,x_2} P(x_1 + x_2)[v_1 + v_2] - c_1 x_1 - c_2 x_2.$$

The first-order conditions

$$P'(x_1 + x_2)[v_1 + v_2] \leq c_1 \tag{1.3}$$
$$P'(x_1 + x_2)[v_1 + v_2] \leq c_2. \tag{1.4}$$

At the optimum, the agent with the lowest cost exerts all the effort. Let $c_{min} = \min\{c_1, c_2\}$, so that the optimum is determined by

$$x_1^* + x_2^* = G(c_{min}/(v_1 + v_2)). \tag{1.5}$$

Summarizing, we have:

FACT 3 *In the total effort case, there is always too little effort exerted in the Nash equilibrium as compared with the optimum. Furthermore, when* $v_2/c_2 > v_1/c_1$ *but* $c_1 < c_2$, *the "wrong" agent exerts the effort.*

Best shot

The social and private outcomes in this case are the same as in the total effort case.

Weakest link

The social objective is now

$$\max_{x_1,x_2} \; P(\min(x_1, x_2))[v_1 + v_2] - c_1 x_1 - c_2 x_2.$$

At the social optimum, it is obvious that $x_1 = x_2$ so we can write this problem as

$$\max_{x} \; P(x)[v_1 + v_2] - [c_1 + c_2]x,$$

which has first-order conditions

$$P'(x)[v_1 + v_2] = c_1 + c_2,$$

or

$$x_1 = x_2 = x = G((c_1 + c_2)/(v_1 + v_2)). \tag{1.6}$$

FACT 4 *The probability of success in the socially optimal solution is always lower in the case of weakest link that in the case of total effort.*

Other situations explored in the paper:

- What happens when you add more agents to the game?
  - Systems become more reliable in total effort game
  - Systems become less reliable in weakest link game
- Can we improve social welfare by imposing fines?
  - FACT 8 A fine equal to the costs imposed on the other agents should be imposed on the agent who has the lowest cost of reducing the probability of failure.
  - FACT 9 In the case of weakest link, strict liability is not adequate in general to achieve the socially optimal level of effort, and one must use a negligence rule to induce the optimal effort.
- What happens if this a sequential game instead of a simultaneous one?
  - FACT 10 The equilibrium in the sequential-move, the total-effort game always involves the same or less reliability than the simultaneous-move game.
  - FACT 11 If you want to ensure the highest level of security in the sequential move game, then you should make sure that the agent with the lower benefit-cost ratio moves first.
- What happens if adversaries are introduced?

Secure or Insure? A Game-Theoretic Analysis of Information Security Games

Jens Grossklags
UC Berkeley
School of Information
Berkeley, CA 94720
jensg@ischool.berkeley.edu

Nicolas Christin
Carnegie Mellon University
INI/CyLab Japan
Kobe, 650-0044 Japan
nicolasc@cmu.edu

John Chuang
UC Berkeley
School of Information
Berkeley, CA 94720
chuang@ischool.berkeley.edu

ABSTRACT

Despite general awareness of the importance of keeping one's system secure, and widespread availability of consumer security technologies, actual investment in security remains highly variable across the Internet population, allowing attacks such as distributed denial-of-service (DDoS) and spam distribution to continue unabated. By modeling security investment decision-making in established (e.g., weakest-link, best-shot) and novel games (e.g., weakest-target), and allowing expenditures in self-protection versus self-insurance technologies, we can examine how incentives may shift between investment in a public good (protection) and a private good (insurance), subject to factors such as network size, type of attack, loss probability, loss magnitude, and cost of technology. We can also characterize Nash equilibria and social optima for different classes of attacks and defenses. In the weakest-target game, an interesting result is that, for almost all parameter settings, more effort is exerted at Nash equilibrium than at the social optimum. We may attribute this to the "strategic uncertainty" of players seeking to self-protect at just slightly above the lowest protection level.

Categories and Subject Descriptors

C.2 [**Computer Systems Organization**]: Computer-Communication Networks; J.4 [**Computer Applications**]: Social and Behavioral Sciences—*Economics*; K.4.4 [**Computers and Society**]: Electronic Commerce—*Security*

General Terms

Economics, Reliability, Security

Keywords

Economics of the Internet, Game Theory, Public Goods, Incentive-Centered Design and Engineering, Security, Protection, Self-Insurance

1. INTRODUCTION

The Internet has opened new and attractive channels to publicize and market products, to communicate with friends and colleagues, and to access information from spatially distributed resources. Though it has grown significantly, the network's architecture still reflects the cooperative spirit of its original designers [32]. Unfortunately, today's network users are no longer held together by that same sense of camaraderie and common purpose. For instance, concrete evidence of the tragedy of the commons [21] occurring in peer-to-peer filesharing networks has been documented for a long time [2]. Accordingly, studies of networking protocols and user interaction have been assuming users to be selfish and to act strategically [37].

Selfish users are one thing, but the expansion of the Internet has also attracted individuals and groups with often destructive motivations; these "attackers" intend to improve on their perceived utility by exploiting or creating security weaknesses and harming or inconveniencing other network users. Some malicious entities are motivated by peer recognition, or curiosity, and are often undecided regarding the ethical legitimacy of their behavior [19, 20]. Others have clearly demonstrated financial goals [17]. Problematic behaviors and threats include attacks on the network as a whole, attacks on selected end-points, undesirable forms of interactions such as spam e-mail, and annoyances such as Web pages that are unavailable or defaced. As a result, users cannot rely and trust other network participants [13].

When asked in surveys, network users say they are interested in preventing attacks and mitigating the damages from computer and information security breaches [1, 40]. Researchers and industry have responded by developing numerous security technologies to alleviate many of the aforementioned problems [4], thereby expecting to help improving individual security practices.

Nevertheless, security breaches are common, widespread and highly damaging. The "I Love You" virus [27], Code Red [29] and Slammer worms [28], to cite the most famous cases, have infected hundreds of thousands of machines and caused, all together, billions of dollars in damages. Underground markets for processor time on compromised end-systems are developing [17] thanks to large population of home computers that can be easily commandeered by third-parties. The high financial impact of security failures is explained by user surveys [6, 10], which show strong evidence that comprehensive security precautions, be they patching, spyware-removal tools, or even sound backup strategies, are missing from a vast majority of systems surveyed.

In other words, despite a self-professed interest in security, most individuals do not implement effective security on their systems, even though necessary technologies and methods are (by and large) readily available. We propose to investigate the root causes of the disconnect between users' actions and their intentions.

In practice, there is a large variety of situations in which users face security threats, and an equally large number of possible responses to threats. However, we postulate in this paper that one can model most security interactions through a handful of "security games," and with a small number of decision parameters upon which each user can act.

More precisely, building upon public goods literature [23, 43], we consider the classical best shot, total effort, and weakest-link

WWW 2008, April 21–25, 2008, Beijing, China.
ACM 978-1-60558-085-2/08/04.

What types of games are these?

- **Game structure:** total effort, weakest link, best shot, *weakest target*
- Simultaneous or sequential?
- 2-player or multiplayer?
- Perfect Information or imperfect information?
- Deterministic or non-deterministic?
- Finite actions or infinite actions?
- One-shot or iterated?

Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$

Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$

Utility of player i

Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$

Utility of player i

Initial endowment

Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$

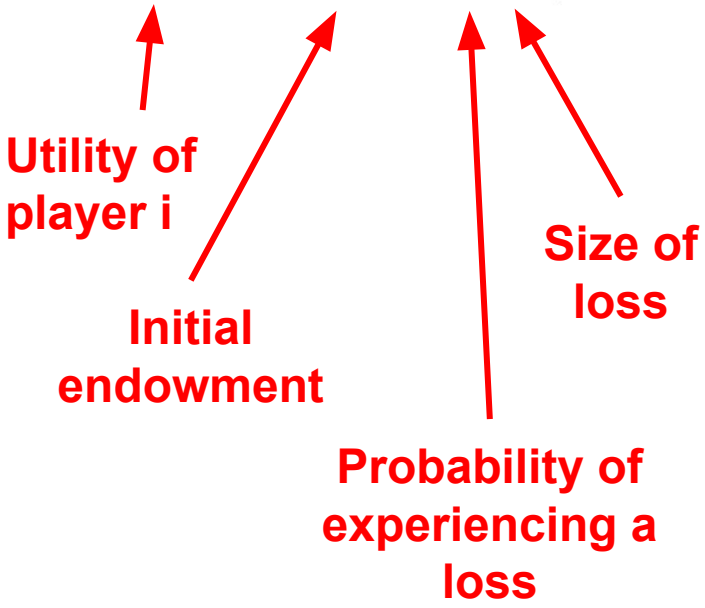
Utility of player i

Initial endowment

Probability of experiencing a loss

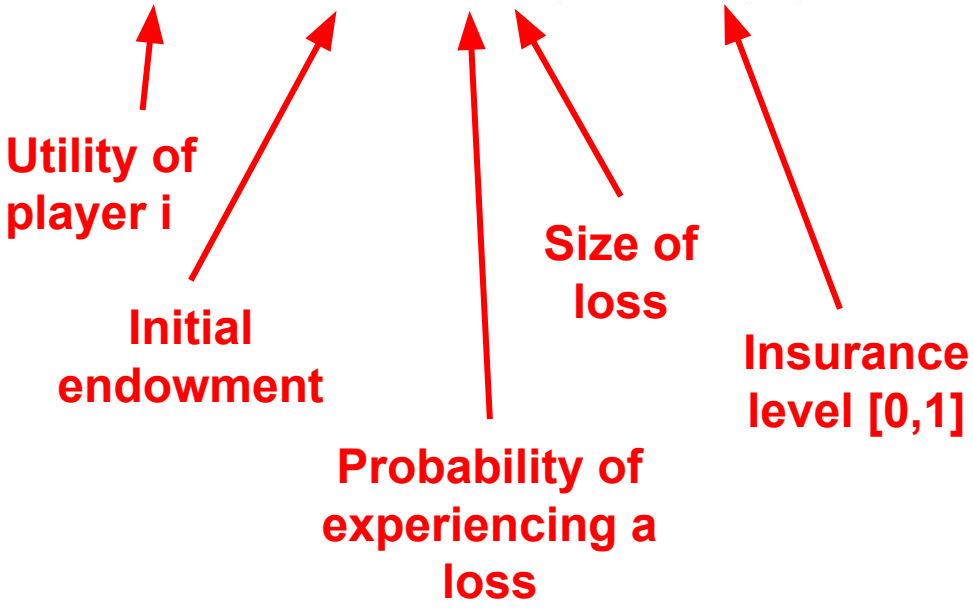
Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$



Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$



Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$

Utility of player i

Initial endowment

Probability of experiencing a loss

Size of loss

Insurance level [0,1]

"Contribution"function

Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$

Utility of player i

Initial endowment

Probability of experiencing a loss

Size of loss

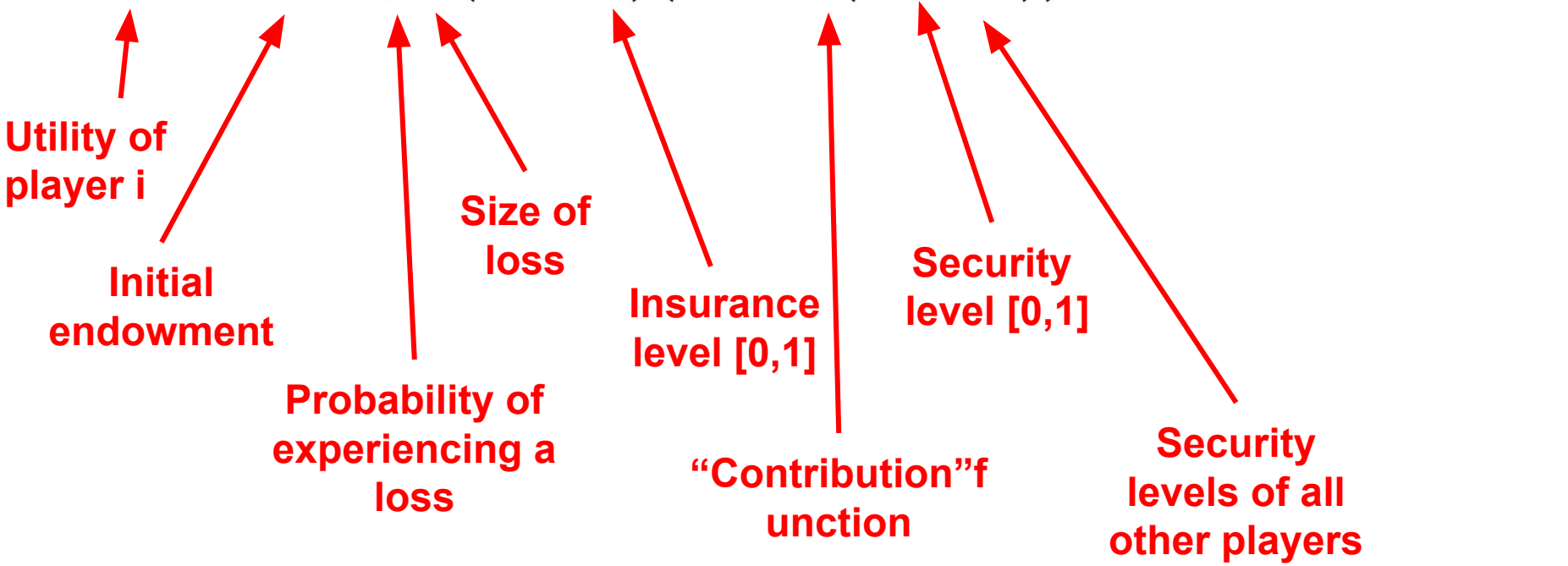
Insurance level [0,1]

"Contribution"function

Security level [0,1]

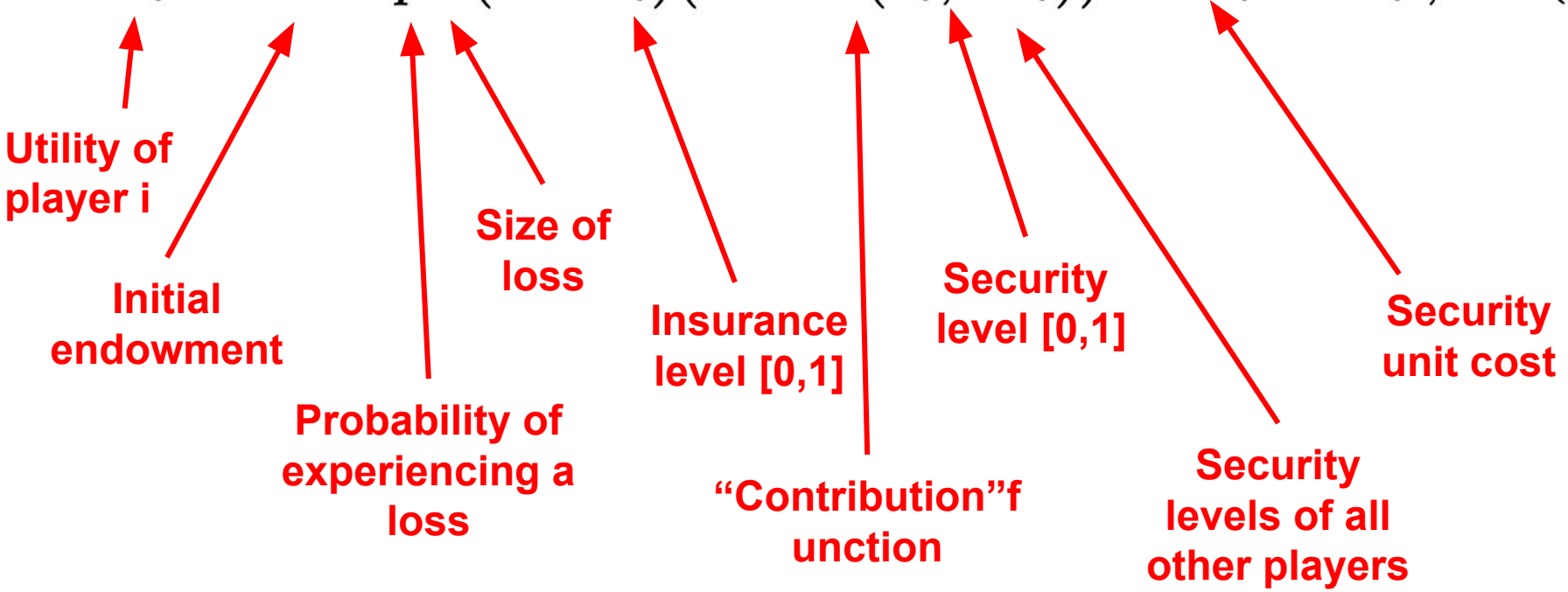
Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$



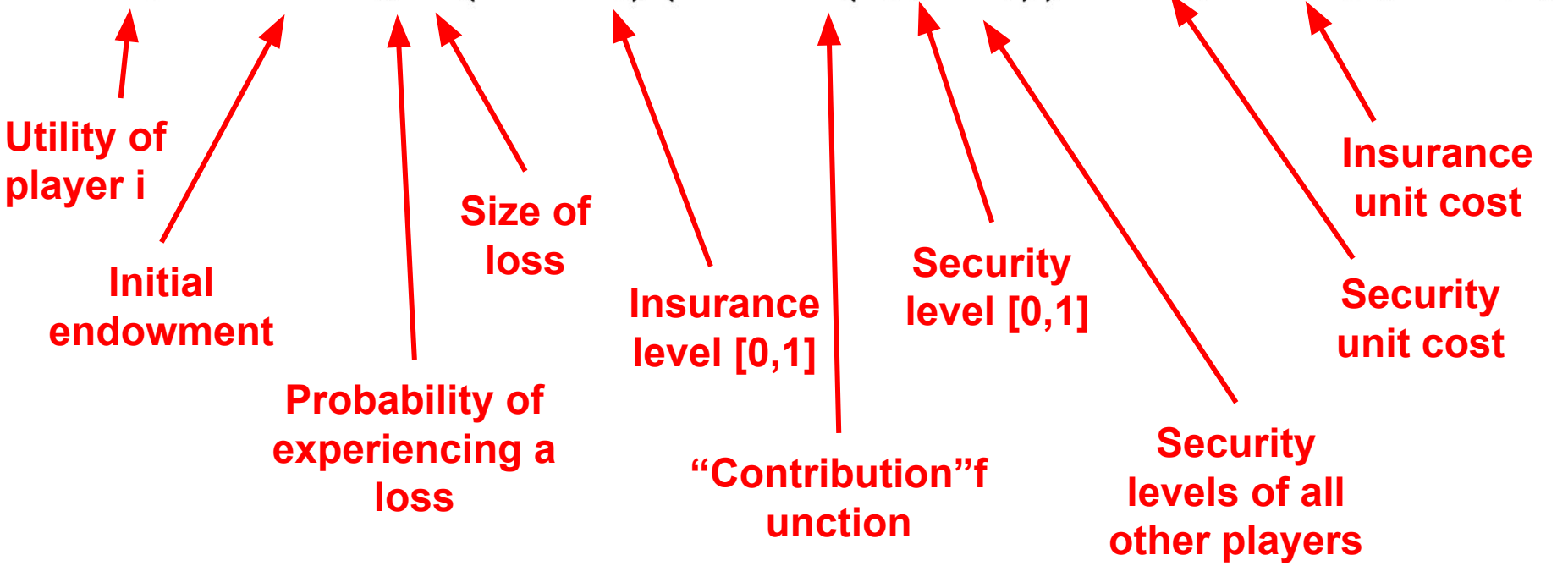
Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$



Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$



Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$

Total effort, weakest link, best shot, or weakest target?

$$H(e_i, e_{-i}) = \max(e_i, e_{-i})$$

Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$

Total effort, weakest link, best shot, or weakest target?

$$H(e_i, e_{-i}) = \frac{1}{N} \sum_i e_i,$$

Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$

Total effort, weakest link, best shot, or weakest target?

$$H(e_i, e_{-i}) = \min(e_i, e_{-i})$$

Generic utility function:

$$U_i = M - pL(1 - s_i)(1 - H(e_i, e_{-i})) - be_i - cs_i \ , \qquad (1)$$

Total effort, weakest link, best shot, or weakest target?

$$H(e_i, e_{-i}) = \begin{cases} 0 & \text{if } e_i = \min(e_i, e_{-i}), \\ 1 & \text{otherwise,} \end{cases}$$

Nash equilibrium analysis: Total Effort

Result 1: *After investigating Eqs. (9–11) we can identify three Nash equilibrium strategies.*

- *Full protection eq.:* If $pL > bN$ and $c > b + pL\frac{N-1}{N}$, meaning that protection is cheap, potential losses are high, and insurance is extremely overpriced, then the (only) Nash equilibrium is defined by everybody protecting but not insuring, that is, $(e_i, s_i) = (1, 0)$.
- *Full self-insurance eq.:* In the other cases where $pL > bN$, $(e_i, s_i) = (0, 1)$ is a Nash equilibrium. Also, if $c < pL < bN$ (expected losses above insurance costs), then $(e_i, s_i) = (0, 1)$, is a Nash equilibrium.
- *Passivity eq.:* If $pL < bN$ and $pL < c$, then the expected losses are small enough so that complete passivity, defined by $(e_i, s_i) = (0, 0)$ for all players, is a Nash equilibrium.

Nash equilibrium analysis: Weakest Link

Result 2: *In the weakest link security game, we can identify three types of Nash equilibrium strategies. However, there exist multiple pure protection equilibria.*

Denote by $\hat{e}_0$ the minimum of the protection levels initially chosen by all players. We have

- *Multiple protection equilibria:* If $pL > b$ and $\{(\hat{e}_0 > (pL - c)/(pL - b) \text{ for } c < pL) \cup (pL \geq c)\}$, then $(e_i, s_i) = (\hat{e}_0, 0)$ for all i is a Nash equilibrium: everybody picks the same minimal security level, but no one has any incentive to lower it further down. This equilibrium can only exist for $b \leq c$, and may be inefficient, as it could be in the best interest of all parties to converge to $e_i = 1$, as we discuss later in Section 5.
- *Full self-insurance eq.:* If $pL > c$ and $\{\hat{e}_0 < (pL-c)/(pL-b) \cup b > pL\}$, then $(e_i, s_i) = (0, 1)$ for all i is a Nash equilibrium: essentially, if the system is not initially secured well enough (by having all parties above a fixed level), players prefer to self-insure.
- *Passivity eq.:* If $pL < b$ and $pL < c$, then $(e_i, s_i) = (0, 0)$ is the only Nash equilibrium – both insurance and protection are too expensive.

Nash equilibrium analysis: Best Shot

Result 3: *From the above relationships, we can identify the following pure Nash equilibrium strategies.*

- *Full self-insurance eq.:* If $b > c$ we find that the self-insurance equilibrium ($\forall i, (e_i, s_i) = (0, 1)$) is the only possible Nash equilibrium.

- *Passivity eq.:* If $pL < b$ and $pL < c$ agents prefer to abstain from security actions ($\forall i, (e_i, s_i) = (0, 0)$).

Nash equilibrium analysis: Weakest Target

Result 4: *In the weakest-target game with an attacker of infinite strength we find that pure Nash equilibria for non trivial values of b, p, L and c do not exist.*

Nash equilibrium analysis: Weakest Target (with mitigation)

Let us assume that there exists a Nash equilibrium where $0 < K < N$ players who satisfy $e_i = e_0 = \min(e_i, e_{-i})$, while $(N - K > 0)$ players satisfy $e_i > e_0$. We can show that such an equilibrium does not exist and that players rather congregate at the highest protection level if certain conditions are met. Due to space constraints, we will only sketch the analysis of this equilibrium. By computing the partial derivatives $\partial U_i/\partial s_i$ and $\partial U_i/\partial e_i$, and discriminating among values for e_i and s_i, we get the following results.

Result 6: In contrast to the infinite strength weakest-target game we find that a pure Nash equilibrium may exist.

- *Full protection eq.:* If $b \leq c$ we find that the full protection equilibrium $(\forall i, (e_i, s_i) = (1, 0))$ is the only possible pure Nash equilibrium.
- *For $b > c$ we can show that no pure Nash equilibrium exists.*
- *There are no pure self-insurance equilibria.*

Social optima analysis: Total Effort

Result 8: *In the total effort security game we observe that in the Nash equilibrium there is almost always too little protection effort exerted compared to the social optimum. In fact, for a wide range of parameter settings no protection equilibria exist while the social optimum prescribes protection at a very low threshold.*

Social optima analysis: Weakest Link

Result 9: *The availability of self-insurance lowers the risk of below-optimal security in the Nash equilibrium since agents have an alternative to the unstable Pareto-optimal protection equilibrium. From the analysis of the weakest link game with many agents we know that deviation from the Pareto-optimal highest protection level is very likely. A social planner can overcome these coordination problems.*

Social optima analysis: Best Shot

Result 10: *In the best shot security Nash outcome there is almost always too little effort exerted compared to the social optimum. Exceptions are few points in which full self-insurance remains desirable for the social planner and all agents remain passive.*

Social optima analysis: Weakest Target

Result 11: *A social planner can easily devise a strategy to overcome the coordination problems observed in the Nash analysis for the weakest-target game with mitigation. We found that no pure Nash strategy exists and, therefore, had to rely on the increased rationality requirement for entities to play a mixed strategy.*[4] *The average payoff for each player in the social optimum is considerably higher compared to the mixed Nash equilibrium.*

Social optima analysis: Weakest Target (with mitigation)

Result 12: *Compared to the weakest-target game without mitigation the social planner is better off if protection is cheap. Otherwise the planner has to sacrifice a node with or without self-insurance. Interestingly, while compared to the pure Nash equilibrium outcome the social planner can increase the overall utility in the network we find that security expenditures are lowered. In the Nash equilibrium agents were willing to fully protect against threats as long as* $(b \leq c)$.

The last observation also holds for the mixed strategy case in both weakest-target games (with or without mitigation). That is, agents exert ***more*** *effort in the Nash equilibrium (except when* $Nb < c$ *for the game with mitigation).*

What is the value of analyzing security games this way?

- Does this actually help anyone? Why or why not?

- I don’t think I’ve ever heard or seen this type of game theory ever discussed among real-world security practitioners. Why?

What is the value of analyzing security games this way?

- Does this actually help anyone? Why or why not?

- I don’t think I’ve ever heard or seen this type of game theory ever discussed among real-world security practitioners. Why?
  - Are the models too simple? (e.g. linear costs of protection)
  - Do we not know how to estimate variables (like “unit cost of insurance”)
  - Other strong assumptions?
  - Is game theory beyond the abilities of most security practitioners?
  - Remember Gordon-Loeb model?

Cybersecurity and Game Theory

COMS6998 sec:12 | The Economics of Cybersecurity

March 26, 2024

120