Introduction to Game Theory

Tyler Moore

Computer Science & Engineering Department, SMU, Dallas, TX
Slides are modified from version written by Benjamin Johnson, UC Berkeley

Lecture 15–16

Notes

Topics

We now discuss the final big idea in the course

1. Introduction
2. Security metrics and investment
3. Measuring cybercrime
4. **Security games**

- We now consider strategic interaction between players

Notes

Recall how we model rationality

- Economics attempts to model the *decisions* we make, when faced with multiple choices and when interacting with other strategic agents
- Rational choice theory (RCT): model for decision-making
- Game theory (GT): extends RCT to model strategic interactions

Notes

Model of preferences

- An agent is faced with a range of possible outcomes $o_1, o_2 \in \mathcal{O}$, the set of all possible outcomes
- Notation
  - $o_1 \succ o_2$: the agent is strictly prefers o_1 to o_2.
  - $o_1 \succeq o_2$: the agent weakly prefers o_1 to o_2;
  - $o_1 \sim o_2$: the agent is indifferent between o_1 and o_2;
- Outcomes can be also viewed as tuples of different properties $\hat{x}, \hat{y} \in \mathcal{O}$, where $\hat{x} = (x_1, x_2, \ldots, x_n)$ and $\hat{y} = (y_1, y_2, \ldots, y_n)$

Notes

Rational choice axioms

Rational choice theory assumes consistency in how outcomes are preferred.

Axiom

Completeness. For each pair of outcomes o_1 and o_2, exactly one of the following holds: $o_1 \succ o_2$, $o_1 \sim o_2$, or $o_2 \succ o_1$.

⇒ Outcomes can always be compared

Axiom

Transitivity. For each triple of outcomes o_1, o_2, and o_3, if $o_1 \succ o_2$ and $o_2 \succ o_3$, then $o_1 \succ o_3$.

⇒ People make choices among many different outcomes in a consistent manner

Notes

Utility

Rational choice theory defines utility as a way of quantifying consumer preferences

Definition

(Utility function) A utility function U maps a set of outcomes onto real-valued numbers, that is, $U\colon \mathcal{O} \to \mathbb{R}$. U is defined such that $U(o_1) > U(o_2) \iff o_1 \succ o_2$.

Agents make a rational decision by picking the outcome with highest utility:

$$o^* = \arg\max_{o \in \mathcal{O}} U(o) \quad (1)$$

Notes

Why isn't utility theory enough?

- Only rarely do actions people take directly determine outcomes
- Instead there is uncertainty about which outcome will come to pass
- More realistic model: agent selects action a from set of all possible actions $\mathcal{A}$, and then outcomes $\mathcal{O}$ are associated with probability distribution

Notes

Expected utility

Definition

(Expected utility (discrete)) The *expected utility* of an action $a \in \mathcal{A}$ is defined by adding up the utility for all outcomes weighed by their probability of occurrence:

$$E[U(a)] = \sum_{o \in \mathcal{O}} U(o) \cdot P(o|a) \quad (2)$$

Agents make a rational decision by maximizing expected utility:

$$a^* = \arg\max_{a \in \mathcal{A}} E[U(a)] \quad (3)$$

Notes

Example: process control system security

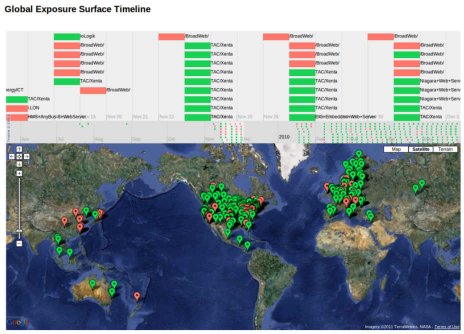


Figure 2.1: Example exposure time-map with red marking systems with known exploits

Source: `http://www.cl.cam.ac.uk/~fms27/papers/2011-Leverett-industrial.pdf`

Notes

Example: process control system security

- Actions available: $\mathcal{A} = \{\text{disconnect}, \text{connect}\}$
- Outcomes available: $\mathcal{O} = \{\text{successful attack}, \text{no successful attack}\}$
- Probability of successful attack is 0.01 ($P(\text{attack}|\text{connect}) = 0.01$)
- If systems are disconnected, then $P(\text{attack}|\text{disconnect}) = 0$

Notes

Example: process control system security

	successful attack		no succ. attack		
Action	U	$P(\text{attack}|\text{action})$	U	$P(\text{no attack}|\text{action})$	$E[U(\text{action})]$
connect	-50	0.01	10	0.99	9.4
disconnect	-10	0	-10	1	-10

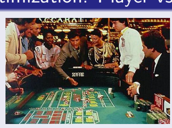
$\Rightarrow$ risk-neutral IT security manager chooses to connect since $E[U(\text{connect})] > E[U(\text{disconnect})]$.

This model assumes fixed probabilities for attack. Is this assumption realistic?

Notes

Games vs. Optimization

Optimization: Player vs Nature



Games: Player vs Player



Notes

Strategy

Book of Qi

- War
- Business
- Policy

36 Stratagems (Examples)

- Befriend a distant state while attacking a neighbor
- Sacrifice the plum tree to preserve the peach tree
- Feign madness but keep your balance
- See http://en.wikipedia.org/wiki/Thirty-Six_Stratagems

Notes

Representing a game with a payoff matrix

- Suppose we have two players A and B.
  - A's actions $\mathcal{A}_A = \{u, d\}$
  - B's actions $\mathcal{A}_B = \{l, r\}$
  - Possible outcomes $\mathcal{O} = \{(u,l),(u,r),(d,l),(d,r)\}$
  - We represent 2-player, 2-strategy games with a *payoff matrix*

	Player B chooses l	Player B chooses r
Player A chooses u	$(U_A(u,l), U_B(u,l))$	$(U_A(u,r), U_B(u,r))$
Player A chooses d	$(U_A(d,l), U_B(d,l))$	$(U_A(d,r), U_B(d,r))$

Notes

Returning to the process control system example

- Suppose we have two players: plant security manager and a terrorist
  - Manager's actions $\mathcal{A}_{\text{mgr}} = \{\text{disconnect}, \text{connect}\}$
  - Terrorist's actions $\mathcal{A}_{\text{terr}} = \{\text{attack}, \text{don't attack}\}$
  - Possible outcomes $\mathcal{O} = \{(a_1,a_3),(a_1,a_4),(a_2,a_3),(a_2,a_4)\}$
  - We represent 2-player, 2-strategy games with a *payoff matrix*

		Terrorist	
		attack	don't attack
Manager	connect	$(-50, 50)$	$(10, 0)$
	disconnect	$(-10, -10)$	$(-10, 0)$

Notes

Important Notions

Zero-Sum

In a zero-sum game, the sum of player utilities is zero.

zero-sum

	heads	tails
heads	$(1, -1)$	$(-1, 1)$
tails	$(-1, 1)$	$(1, -1)$

not zero-sum

	invest	defer
invest	$(1, 1)$	$(1, 2)$
defer	$(2, 1)$	$(0, 0)$

Notes

How can we determine which outcome will happen?

- We look for particular *solution concepts*
  1. Dominant strategy equilibrium
  2. Nash equilibrium
- Pareto optimal outcomes

Notes

Dominant strategy equilibrium

- A player has a *dominant strategy* if that strategy achieves the highest payoff regardless of what other players do.
- A *dominant strategy equilibrium* is one in which each player has and plays her dominant strategy.

Example 1: Dominant Strategy Equilibria?

		Bob left	Bob right
Alice	top	(1, 2)	(0, 1)
	bottom	(2, 1)	(1, 0)

Notes

Nash equilibrium

Nash equilibrium

A Nash equilibrium is an assignment of strategies to players such that no player can improve her utility by changing strategies.

- A Nash equilibrium is called *strong* if every player strictly prefers their strategy given the current configuration.
- It is called *weak* if at least one player is indifferent about changing strategies.

Nash equilibrium for 2-player game

For a 2-person game between players A and B, a pair of strategies (a_i, a_j) is a Nash equilibrium if $U_A(a_i, a_j) \geq Utility_A(a_{i'}, a_j)$ for every $i' \in \mathcal{A}_A$ where $i' \neq i$ and $U_B(a_i, a_j) \geq U_B(a_i, a_{j'})$ for every $j \in \mathcal{A}_B$ where $j' \neq j$.

Notes

Finding Nash equilibria

Nash equilibrium for 2-player game

For a 2-person game between players A and B, a pair of strategies (a_i, a_j) is a Nash equilibrium if $U_A(a_i, a_j) \geq U_A(a_{i'}, a_j)$ for every $i' \in \mathcal{A}_A$ where $i' \neq i$ and $U_B(a_i, a_j) \geq U_B(a_i, a_{j'})$ for every $j \in \mathcal{A}_B$ where $j' \neq j$.

Example 1: Nash equilibria? (top,left) and (bottom, right)

		Bob left	Bob right
Alice	top	(2, 1)	(0, 0)
	bottom	(0, 0)	(1, 2)

(top,left)?: $U_A(\text{top}, \text{left}) > U_A(\text{bottom}, \text{left})$?
$2 > 0$? yes!
$U_B(\text{top}, \text{left}) > U_B(\text{top}, \text{right})$?
$1 > 0$? yes!

(top,right)?: $U_A(\text{top}, \text{right}) > U_A(\text{bottom}, \text{right})$?
$0 > 1$? no!
$U_B(\text{top}, \text{right}) > U_B(\text{top}, \text{left})$?
$0 > 1$? no!

Notes

Exercise: is there a dominant strategy or Nash equilibrium for these games?

	left	right
top	$(1, 1)$	$(1, 2)$
bottom	$(2, 1)$	$(0, 0)$

	left	right
top	$(1, -1)$	$(-1, 1)$
bottom	$(-1, 1)$	$(1, -1)$

Notes

Pareto Optimality

Definition

An outcome of a game is Pareto optimal if no other outcome makes at least one player strictly better off, while leaving every player at least as well off.

Example: Pareto-optimal outcome? everything except defect/defect

	cooperate	defect
cooperate	$(-1, -1)$	$(-5, 0)$
defect	$(0, -5)$	$(-2, -2)$

Notes

Prisoners' dilemma

	deny	confess
deny	$(-1, -1)$	$(-5, 0)$
confess	$(0, -5)$	$(-2, -2)$

Notes

Thoughts on the Prisoners' Dilemma

- Can you see why the equilibrium strategy is not always Pareto efficient?
- Exemplifies the difficulty of cooperation when players can't commit to a actions in advance
- In a *repeated game*, cooperation can emerge because anticipated future benefits shift rewards
- But we are studying *one-shot* games, where there is no anticipated future benefit
- Here's one way to use psychology to commit to a strategy: `http://www.tutor2u.net/blog/index.php/economics/comments/game-show-game-theory`

Notes

Split or Steal

		Nick	
		split	steal
Ibrahim	split	$(6\,800, 6\,800)$	$(0, 13\,600)$
	steal	$(13\,600, 0)$	$(0, 0)$

Notes

Prisoners' dilemma in infosec: sharing security data


www.bankinfosecurity.com/alert-attacks-target-bank-employees-a-5128/op-1

Home > Articles

Alert: Banks at High Risk of Attack

Agencies Warn of New Threats to Institutions, Employees

By Tracy Kitten, September 20, 2012. Credit Eligible Email Tweet Like Share

U.S. financial institutions are now at high risk of cyberattack, according to the Financial Services Information Sharing and Analysis Center, which alerted member institutions on Sept. 19.

Citing "credible intelligence" about the potential for distributed denial of service and other attacks against institutions, the FS-ISAC raised its cyberthreat level from "elevated" to "high."

"Members should maintain a heightened level of awareness, apply all appropriate updates and update AV and IDS/IPS signatures, and ensure constant diligence in monitoring and quick response to any malicious events," the alert says.

	share	don't share
share	$(-1, -1)$	$(-5, 0)$
don't share	$(0, -5)$	$(-2, -2)$

Note, this only applies when both parties are of the same type, and can benefit each other from sharing. Doesn't apply in the case of take-down companies due to the outsourcing of security

Notes

Assurance games: Cold war arms race

		USSR	
		refrain	build
USA	refrain	(4,4)	(1,3)
	build	(3,1)	(2,2)

Exercise: compute the equilibrium outcome (Nash or dominant strategy)

Notes

Assurance games in infosec: Cyber arms race

		Russia	
		refrain	build
USA	refrain	(4,4)	(1,3)
	build	(3,1)	(2,2)

Notes

Assurance games in infosec: Upgrading protocols

Many security protocols (e.g., DNSSEC, BGPSEC) require widespread adoption to be useful

	upgrade	don't upgrade
upgrade	(4,4)	(1,3)
don't upgrade	(3,1)	(2,2)

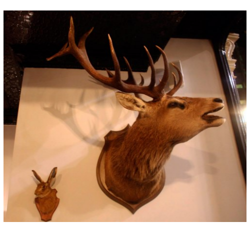
Notes

Battle of the sexes

	party	home
party	$(10, 5)$	$(0, 0)$
home	$(0, 0)$	$(5, 10)$

Notes

Stag-hunt games and infosec: joint cybercrime defense



Stag hunt

	stag	hare
stag	$(10, 10)$	$(0, 7)$
hare	$(7, 0)$	$(7, 7)$

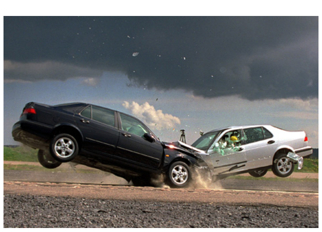
CONFICKER WORKING GROUP

Coordinating malware response

	join WG	protect firm
join WG	$(10, 10)$	$(0, 7)$
protect firm	$(7, 0)$	$(7, 7)$

Notes

Chicken



	dare	chicken
dare	$(0, 0)$	$(7, 2)$
chicken	$(2, 7)$	$(5, 5)$

Notes

Chicken in infosec: who pays for malware cleanup?


fcw.com/articles/2010/06/29/web-aussie-isp-code.aspx

FCW THE BUSINESS OF FEDERAL TECHNOLOGY

TRENDING: Cybersecurity Second Term Skills & Training Mobility

POLICY MANAGEMENT EXEC TECH WHO & WHERE

Australia taps ISPs to fight 'zombies'

Internet Industry Association releases code of conduct for Internet

THE H SECURITY

Security

You are a guest

In association

Last 7 days News Archive Features Forums Newsletter RSS Downloads

08 December 2009, 15:32

« previous | next »

Germany to set up centre to coordinate fight against botnets

In 2010 the German government is planning to pick up the fight against infected home computers. In the first half of next year it plans to set up an advisory centre which will help users purge their computers of viruses and bots. The idea, jointly developed by the Federal Office for Information Security (BSI) and the Association of the German Internet Industry (eco), is based on the premise that internet service providers (ISPs) have long had the technical capability to identify infected computers by analysing network traffic. The project was officially announced by BSI and eco at today's fourth national IT summit in Stuttgart.

		ISPs	
		Pay up	Don't pay
Gov	Pay up	$(0, 0)$	$(-1, 1)$
	Don't pay	$(1, -1)$	$(-2, -2)$

Notes

How to coordinate (Varian, Intermediate Microeconomics)

- Goals of coordination game: force the other player to cooperate
  - **Assurance game**: "coordinate at an equilibrium that you both like"
  - **Stag-hunt game**: "coordinate at an equilibrium that you both like"
  - **Battle of the sexes**: "coordinate at an equilibrium that one of you likes"
  - **Prisoner's dilemma**: "play something other than an equilibrium strategy"
  - **Chicken**: "make a choice leading to your preferred outcome"

Notes

How to coordinate (Varian, Intermediate Microeconomics)

- In assurance, stag-hunt, battle-of-the-sexes, and chicken, coordination can be achieved by one player moving first
- In prisoner's dilemma, that doesn't work? Why not?
- Instead, for prisoner's dilemma games one must use repetition or contracts.
- Robert Axelrod ran repeated game tournaments where he invited economists to submit strategies for prisoner's dilemma in repeated games
- Winning strategy? Tit-for-tat

Notes

Assurance games: Cyber arms race

		Russia	
		refrain	build
USA	refrain	(4,4)	(1,3)
	build	(3,1)	(2,2)

Notes

Russia proposed a cyberwar peace treaty

www.reuters.com/article/2012/04/25/germany-cyber-idUSL6E8FP40M20120425

REUTERS

Russia says many states arming for cyber warfare

Wed Apr 25, 2012 2:13pm EDT

* Russian-sponsored gathering rallies support for UN treaty

* U.S. opposes attempts to restrict use of web

* Russia says cyber attacks are new level of confrontation

By Adrian Croft

GARMISCH-PARTENKIRCHEN, Germany, April 25 (Reuters) - Russia has stepped up its campaign for a globally binding treaty on cyber security, warning that many states are acquiring cyber warfare capabilities that, if unleashed, could subvert economies and bring down critical infrastructure.

Hosting a gathering of experts in the German Alps to try to rally support for its controversial proposals for a U.N. convention to crack down on Internet crime and terrorism, Russia said 120 countries now conducted online war games to try to understand the Internet's military potential.

"We won't use nuclear weapons - it is a Doomsday weapon. But when we have a situation where we have millions of hacker attacks on our money,

Related News

Suspected cyber attack hits Iran oil industry
Mon, Apr 23 2012

Pentagon sees progress, challenges in cyber warfare
Tue, Apr 17 2012

Accused LulzSec hacker pleads guilty

Notes

Review: rational choice model
Game theory
Introduction and notation
Finding equilibrium outcomes

US Department of Homeland Security signals support for DNSSEC

« Photos from ICANN DNSSEC workshop in Dakar now online — Comcast signs 90% of its domain names; urges commerce, banking domain owners to deploy DNSSEC »

DHS wins national cybersecurity award for DNSSEC work

The SANS Institute, which operates the Internet Storm Center, has awarded the 2011 U.S. National Cybersecurity Innovation award to the U.S. Department of Homeland Security's Cyber Security Research & Development Center. The center is part of the agency's Science and Technology Directorate's Cyber Security Division, which sponsors the DNSSEC Deployment Coordination Initiative, which works to encourage all sectors to voluntarily adopt security measures that will improve security of the Internet's naming infrastructure as part of a global, cooperative effort that involves many nations and organizations in the public and private sectors.

The institute announced that the award recognizes the creation of "a federal cybersecurity research and development program that ensures that the research funded by federal agencies has a practical effect in reducing cyber risk....This has required the R&D community to think beyond the theoretical and to consider a more practical horizon." It noted that "In particular, DHS S&T's long-term support of DNSSEC ensures that public users of online government services are confident the website they visit and over which they transmit information is an authentic government website and is secure."

"It's gratifying to see our six years of support for DNSSEC recognized in this way," said Douglas Maughan, Ph.D., who directs the DHS division for cyber security R&D. "DNSSEC is a great example of how research can pay off, through a process that continually calls upon researchers to focus on work that can result in real products and real risk reductions. DNSSEC today is providing increased security for the Internet infrastructure and is impacting Internet operations organizations, private industry, and the U.S. Government."

Edward Rhyne, the division's program manager, accepted the award from White House Cyber Coordinator Howard Schmidt at the National Cybersecurity Innovation Conference in Washington, DC, on October 11.

Source:

https://www.dnssec-deployment.org/index.php/2011/11/dhs-wins-national-cybersecurity-award-for-dnssec-work/

Notes

Notes

Notes