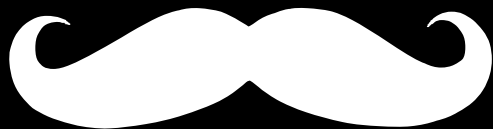




The Bazaar, the Maharaja's Ultimatum, and the Shadow of the Future:

Alfonso De Gregorio

Founder, BeeWise



Extortion and Cooperation in the Zero-day Market

secYOUre

Discuss

/me @secYOUre

#0DayDilemma

#AusCERT2015

secYOUre

Agenda

1. The Zero-day Market

A hairy business

2. Relevance

Should I care?

3. The Zero-day Dilemma

Extortion and Cooperation in the Zero-day Market

4. Recommendations to Zero-day traders

How to maximize the payoff?

The Zero-day Market







iOS 7

The mobile OS from a whole new perspective.











Meet Ty















Meanwhile...







500

FINISH







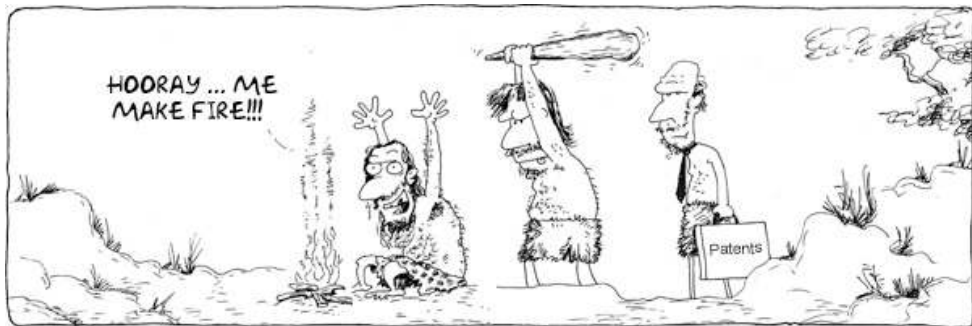


**KEEP
CALM**

because

**WE HAVE
NO RULES**







Inherent obstacles

1. Time-sensitiveness of traded commodities
2. Trust
3. Price fairness
4. Possibility of defection

A hairy business



The Legitimate Vulnerability Market

The Legitimate Vulnerability Market

Inside the Secretive World of 0-day Exploit Sales

Charlie Miller, PhD, CISSP
Independent Security Evaluators
www.securityevaluators.com

May 6, 2007

Time-sensitive commodity



- ❖ Valuable only when they are not widely known
- ❖ Value drops to zero, as soon as the vulnerability is disclosed or a mitigation is released
- ❖ Transactions should complete in short times
- ❖ Discretion required



Every day can be the last day for a 0-day sale

Trust



- ❖ No centralized way to locate its players
- ❖ Finding buyers and sellers is time-consuming
- ❖ Unfamiliar business partners
- ❖ Hard to verify intentions



Oh, grandmother, what a horribly big mouth you have!

Lack of transparency and price fairness



- ❖ Adoption levels of the vulnerable component
- ❖ Presence within a given attack surface
- ❖ Level of authentication required to exploit it
- ❖ Difficulty of independent rediscovery
- ❖ Exploit reliability



Difficult to measure

Tension



- ❖ Disclose and lose?
- ❖ Proving without disclosing
- ❖ Two approaches: reveal or demonstrate
- ❖ Both undesirable

UNDESIRABLE No. 1



HARRY POTTER

CONTACT THE MINISTRY OF MAGIC IMMEDIATELY IF YOU
HAVE ANY INFORMATION CONCERNING HIS WHEREABOUTS.
FAILING TO REPORT WILL RESULT IN IMPRISONMENT.



 **REWARD** 
10,000 GALLEONS ON HIS HEAD



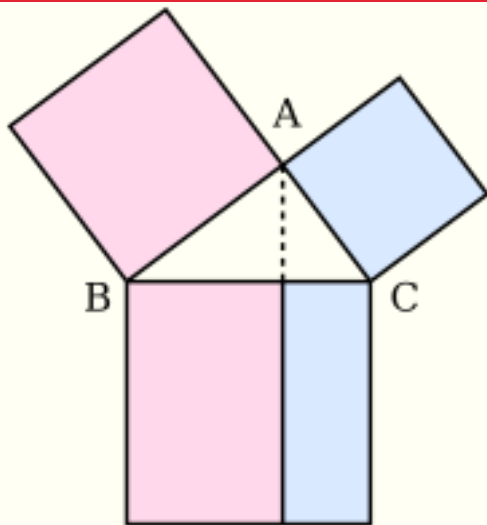
© 2001 Warner Bros. Entertainment Inc. All Rights Reserved. Harry Potter and the Sorcerer's Stone is a trademark of Warner Bros. Entertainment Inc.

Reveal



- ❖ Whoever moves first and lose your asset
- ❖ Buyer steals the vulnerability, if the seller reveals it before the sale
- ❖ Seller runs away with the money, if the buyers pays in advance

Demonstrate



- ❖ Whoever controls the computing environment has an edge
- ❖ Does the seller tamper with the computing environment?
- ❖ Does the buyer record the working of the exploit and steal it?



Any vulnerability claim can't be ensured

Kramer vs. Kramer



Columbia Pictures Presents A Stanley Jaffe Production

Dustin Hoffman
in
Kramer vs. Kramer

Meryl Streep Jane Alexander



Enforce contracts

Exclusive rights to the buyer



- ❖ Grant exclusive rights, to receive the largest payoffs
- ❖ What if the seller defects, selling the same zero-day to multiple parties?
- ❖ This time are the buyers to lack a mean to protect themselves
- ❖ Forcing to return the funds?
- ❖ Difficulty to identify sellers, to attribute multiple transactions to the same supplier, and to enforce contracts helps the seller willing to betray



Proposed solutions

- ❖ Use punishment (i.e., public disclosure of vulnerabilities) to discourage a buyer from defecting;

Proposed solutions

- ❖ Use punishment (i.e., public disclosure of vulnerabilities) to discourage a buyer from defecting;
- ❖ Resort to the use of trusted-third parties (e.g., escrow services), as crucial entities for enabling cooperation of market participants;

Proposed solutions

- ❖ Use punishment (i.e., public disclosure of vulnerabilities) to discourage a buyer from defecting;
- ❖ Resort to the use of trusted-third parties (e.g., escrow services), as crucial entities for enabling cooperation of market participants;
- ❖ Build a reputation system (e.g., reputation score) as an instrument to establish trust relationships between distrustful players.





PHEW!

Motivating questions

1. Can the zero-day market achieve cooperation and efficiency even in absence of trusted-third parties?

Motivating questions

1. Can the zero-day market achieve cooperation and efficiency even in absence of trusted-third parties?
2. Can punishment discourage the buyer from defecting?

Motivating questions

1. Can the zero-day market achieve cooperation and efficiency even in absence of trusted-third parties?
2. Can punishment discourage the buyer from defecting?
3. Under which conditions a player can extort the opponent?

Motivating questions

1. Can the zero-day market achieve cooperation and efficiency even in absence of trusted-third parties?
2. Can punishment discourage the buyer from defecting?
3. Under which conditions a player can extort the opponent?
4. Can cooperation be sustained also in fully anonymous settings?

Motivating questions

1. Can the zero-day market achieve cooperation and efficiency even in absence of trusted-third parties?
2. Can punishment discourage the buyer from defecting?
3. Under which conditions a player can extort the opponent?
4. Can cooperation be sustained also in fully anonymous settings?
5. What about semi-anonymous settings?

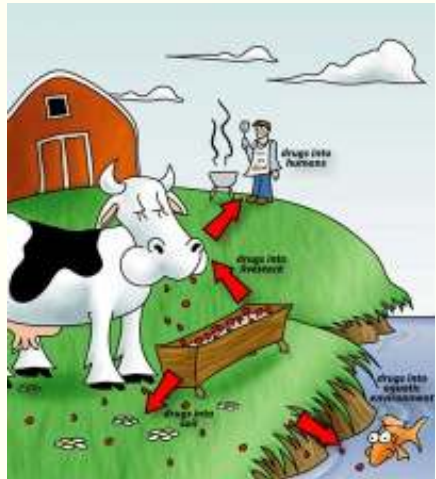


Which trading strategy to employ?

Relevance

At the intersection of software security and security software,
exploring, and trying to contain, the space of unanticipated state.

Market failure



Inability to self-correct



- ❖ Software manufacturers will not forgo market shares
- ❖ Software users will not forgo features
- ❖ Attackers will not forgo attacking tens of millions of vulnerable systems

Information Security Prediction Market



Home | Features | Pricing | About | Contact

Welcome!

BeeWise is the first prediction market for broccasting security events and trends.



At BeeWise we are aimed towards building a financial instrument useful in balancing the information between buyers and sellers in the security market, providing software manufacturers with incentives to build security in, and consumers a way to hedge against security risks.

© 2012

Should I care?

1. More interconnected

Should I care?

1. More interconnected
2. More interdependent

Should I care?

1. More interconnected
2. More interdependent
3. Greater dynamic range of possible failure

Should I care?

1. More interconnected
2. More interdependent
3. Greater dynamic range of possible failure
4. Vulnerability information is key to both offensive and defensive purposes

Should I care?

1. More interconnected
2. More interdependent
3. Greater dynamic range of possible failure
4. Vulnerability information is key to both offensive and defensive purposes
5. Prominent role in modern-day intelligence, national security, and law enforcement operations

Nation-state actors


ממשלת ישראל
Government of Israel
Ministry of Defense

[Redacted]

[Redacted]

Subject: Request for Information – Research and Development (R&D)
Vulnerabilities and Zero-day Exploits

[Redacted]

The Government of Israel - Ministry of Defense ("GID-MOD") invites [Redacted]
[Redacted] to provide information regarding Research and Development (R&D)
Vulnerabilities and Zero-day Exploits. The GID-MOD is at a preliminary stage to the
procurement process and has not made any final decision with respect to whether it will proceed
to issue a Request for Proposal ("RFP") for the capabilities described herein (see attached file).
The information the GID-MOD receives in response to this Request for Information ("RFI") will
assist the GID-MOD in deciding whether it will eventually issue an RFP.

The information you provide should include prices and the anticipated time for delivery
(measured from the effective date of a contract). Because the information to be provided
pursuant to this RFI will be used by the GID-MOD as part of its decision whether to eventually
engage in a procurement that would involve the use of Foreign Military Financing ("FMF")
funds, the GID-MOD requests that you also provide information regarding the percentage of
U.S. and non-U.S. content in your proposal.

All expenses associated with the preparation of your response to this RFI and your
participation in a solicitation (if an RFP is issued to you) are for your account and will not be
reimbursed by the GID-MOD. This letter does not give rise to any commitment by the
GID-MOD to issue an RFP to you.

Please send two copies of your response in a sealed envelope no later than [Redacted]
If you have any questions or comments, please call [Redacted]

Sincerely,



Vendors



Where the results find application?



- Over-the-counter zero-day trading

Where the results find application?

VUPEN
security

000174749002100000
API 07 42032
VAT Reg. No.: FR043802020

Federal Office for Information Security
Chancellery Room 100
53115 Bonn
Germany

Quote	
NUMBER	DATE
000174749002100000	July 7, 2011

DESCRIPTION	PRICE
VUPEN Threat Protection - Comprehensive Level 12 Months / 100 Credits	
Complementary access: VUPEN (N&E) (Policy Analysis & Exploit)	offered

Please sign this quote and return to VUPEN Security

By: 

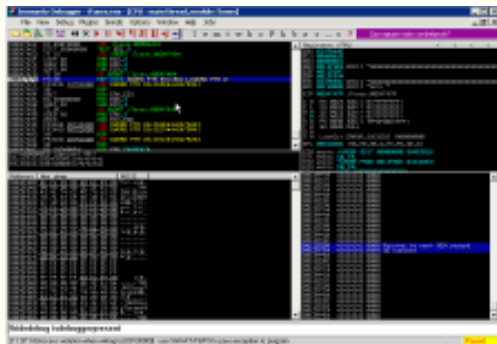
Organization: VUPEN Security
Cap Orange - CS 38021
Rond Point Benjamin Franklin
34080 - Montpellier Cedex 2 (France)

Full Name
VAT No.
Sign Here: _____ Date: _____

VUPEN Security
Cap Orange - CS 38021 - Rond Point Benjamin Franklin - 34080 MONTPELLIER CEDEX 2
SIREN: 484 040 100 - RCS MONTPELLIER 484 040 100
Site web: <http://www.vupen.com> - Email: sales@vupen.com

- Over-the-counter zero-day trading
- Boutique exploit providers offering zero-day vulnerabilities for a subscription fee

Where the results find application?



- ❖ Over-the-counter zero-day trading
- ❖ Boutique exploit providers offering zero-day vulnerabilities for a subscription fee
- ❖ Service models for vulnerability research

The Zero-day Dilemma



The Bazaar

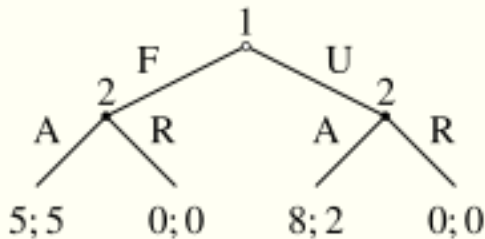


The Maharaja's Ultimatum



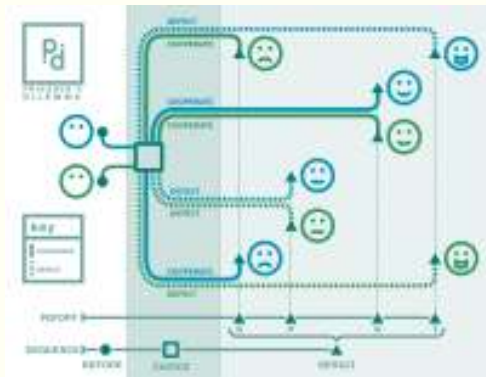
The Shadow of the Future

Ultimatum Game



- ❖ A game in economic experiments
- ❖ Proposer: receives a sum of money and propose how to divide the sum between himself and another player
- ❖ Responder: chooses to either accept or reject the proposal
- ❖ If he accepts, the money is split according to the proposal
- ❖ If he rejects, neither player receives any money

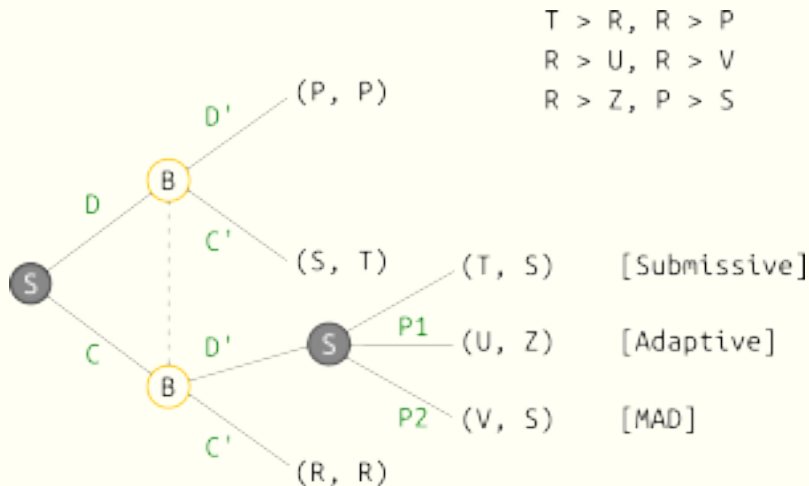
Prisoner's Dilemma



- ❖ Two purely “rational” individuals might not cooperate, even if it appears that it is in their best interest to do so
- ❖ Two prisoners that committed a crime
- ❖ If they both do not confess, they get a low punishment
- ❖ If they both confess, they get a more severe punishment
- ❖ If one confesses and the other does not, then the one that confesses gets a very low punishment and the other gets a very severe punishment

The Iterated Prisoner's Dilemma (IPD) is a repeated game, where the PD is the stage game. Agents play the PD game an indefinite number of times.

The 0-Day Dilemma



Submissive scenario



- ❖ Traders are playing the standard PD
- ❖ $R > P$ implies that mutual cooperation is superior to mutual defection
- ❖ $T > R$ and $P > S$ imply that defection is the dominant strategy for both agents
- ❖ Or, defection is better than cooperation for one player, no matter how that player's opponent may play

Adaptive scenario



- ❖ Neither the buyer nor the seller have a dominant strategy, if we assume $Z > S$ and the $U < R$
- ❖ If the betrayed seller has the ability to close alternative deals for the same exploit (i.e., 1-Day FUD, 1-Day private exploits), then defection would not be a dominant strategy anymore
- ❖ The market nature plays a role
- ❖ Today not a monopsony and weakly regulated. Tomorrow rules and regulations may emerge in this area (e.g., Wassenaar Arrangement) and may impact the market liquidity

MAD scenario



- ❖ A variant of the standard PD, where the seller has the ability to negate the buyer the temptation to defect
- ❖ Just make sure T approaches P
- ❖ Hence, defection is not a dominant strategy for the buyer
- ❖ If factors such as market liquidity, export/trade regulations, mean-time to close a deal prevent the Adaptive retaliation approach from being undertaken, then the seller should consider disclosing publicly the exploit or the vulnerability.

MAD scenario



- ❖ This would not make herself worse off
- ❖ The seller would reduce the buyer incentives to defect in the first place

FD & Brinkmanship

- ❖ To this end, it is important for the 0-Day sellers to have an efficient mean for doing full-disclosure



FD & Brinkmanship



- ❖ To this end, it is important for the 0-Day sellers to have an efficient mean for doing full-disclosure
- ❖ Not for the sake of bragging rights anymore, but for modern-day brinkmanship

FD & Brinkmanship



- ❖ To this end, it is important for the 0-Day sellers to have an efficient mean for doing full-disclosure
- ❖ Not for the sake of bragging rights anymore, but for modern-day brinkmanship
- ❖ As faster the disclosure of the vulnerability, as shorter the window of opportunity to the exploiter and the smaller the Residual payoff (V)

WhistleDay or ZeroLeaks

- ❖ A 0-Day disclosure platform
- ❖ Researchers could use it for full-disclosure
- ❖ Players in the Zero-day market could use to retaliate against buyers who defect
- ❖ Insiders would turn to it to expose the secretive trade in intrusion and surveillance technologies
- ❖ Dub it WhistleDay or ZeroLeaks, if you like

Cooperation is possible

- As long as the seller doesn't play in the Submissive scenario, the buyer is not better off defecting

Cooperation is possible

- As long as the seller doesn't play in the Submissive scenario, the buyer is not better off defecting
- In the one-shot sequential 0-Day Dilemma cooperation is possible

Cooperation is possible

- ❖ As long as the seller doesn't play in the Submissive scenario, the buyer is not better off defecting
- ❖ In the one-shot sequential 0-Day Dilemma cooperation is possible
- ❖ If this is not the case, the rational outcome is the action profile of mutual defection

Cooperation is possible

- ❖ As long as the seller doesn't play in the Submissive scenario, the buyer is not better off defecting
- ❖ In the one-shot sequential 0-Day Dilemma cooperation is possible
- ❖ If this is not the case, the rational outcome is the action profile of mutual defection
- ❖ “We have to distrust each other. It's our only defense against betrayal.” — Tennessee Williams

Cooperation is possible

- ❖ As long as the seller doesn't play in the Submissive scenario, the buyer is not better off defecting
- ❖ In the one-shot sequential 0-Day Dilemma cooperation is possible
- ❖ If this is not the case, the rational outcome is the action profile of mutual defection
- ❖ “We have to distrust each other. It's our only defense against betrayal.” — Tennessee Williams
- ❖ “The dilemma then is that mutual cooperation yields a better outcome than mutual defection but it is not the rational outcome because the choice to cooperate, at the individual level, is not rational from a self-interested point of view.”

Cooperation as an Equilibrium

If no form of punishment can be undertaken by the seller, can the cooperative outcome still be sustained as an equilibrium?

Iterated 0-Day Dilemma

- ✦ The Iterated 0-Day Dilemma (I0DD) is a repeated game, where the 0-Day Dilemma is the stage game. Agents play the 0-Day Dilemma game an indefinite number of times

Iterated 0-Day Dilemma

- ❖ The Iterated 0-Day Dilemma (I0DD) is a repeated game, where the 0-Day Dilemma is the stage game. Agents play the 0-Day Dilemma game an indefinite number of times

Remark: Whenever the Submissive scenario applies, the I0DD reduces to the Iterated Prisoner's Dilemma

Three settings



- ❖ Onymous: The traders know the identity of the party they are dealing with

Three settings



- ❖ Onymous: The traders know the identity of the party they are dealing with
- ❖ Anonymous: Trades takes place among strangers

Three settings



- ❖ Onymous: The traders know the identity of the party they are dealing with
- ❖ Anonymous: Trades takes place among strangers
- ❖ Semi-anonymous: Either the buyer or the seller is anonymous

Cooperation is possible in onymous economies



Aumann, Robert (1959). "Acceptable points in general cooperative n -person games". In Luce, R. D.; Tucker, A. W. Contributions to the Theory 23 of Games IV. Annals of Mathematics Study 40. Princeton NJ: Princeton University Press. pp. 287–324. MR 0104521.

William Press and Freeman Dyson

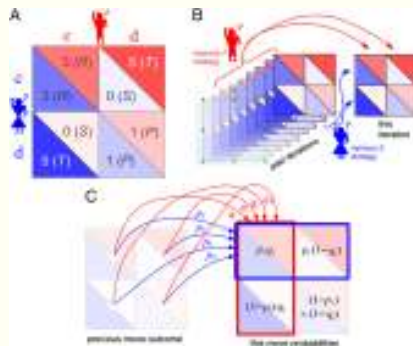


Sentient Player



- ❖ Power granted to a sentient player
- ❖ A player with a *theory of mind*
- ❖ Who realize that her behavior can influence her opponents' strategies

Zero Determinant (ZD) Strategies



$$A \begin{bmatrix} p_1 q_1 & p_1(1-q_1) & (1-p_1)q_1 & (1-p_1)(1-q_1) \\ p_2 q_3 & p_2(1-q_3) & (1-p_2)q_3 & (1-p_2)(1-q_3) \\ p_3 q_2 & p_3(1-q_2) & (1-p_3)q_2 & (1-p_3)(1-q_2) \\ p_4 q_4 & p_4(1-q_4) & (1-p_4)q_4 & (1-p_4)(1-q_4) \end{bmatrix}$$

$$B \quad v \cdot f \equiv D(\mathbf{p}, \mathbf{q}, \mathbf{f})$$

$$= \det \begin{bmatrix} -1 + p_1 q_1 & -1 + p_1 & -1 + q_1 & f_1 \\ p_2 q_3 & -1 + p_2 & q_3 & f_2 \\ p_3 q_2 & p_3 & -1 + q_2 & f_3 \\ p_4 q_4 & p_4 & q_4 & f_4 \end{bmatrix}$$

$$\equiv \bar{\mathbf{p}} \quad \equiv \bar{\mathbf{q}}$$

Extortion



If one trader is aware of ZD strategies, but the opponent is an evolutionary player then the former can choose to *extort* the latter

Evolutionary players



A player is said to be *evolutionary* if she possesses no theory of mind and instead simply seeks to adjust her strategy to maximize her own score in response to whatever the adversary is doing

Extortion strategies

- ❖ Grant a disproportionate number of high payoffs to the extortionist
- ❖ It is the victim's best interest to cooperate with the extortionist, because she is able to increase her score by doing so
- ❖ In so doing, she ends up increasing the extortionist's score even more than her own
- ❖ She will never catch up to the extortionist, and she will accede to her extortionist because it pays her to do so

An extortionist relation

$$S_x - P = 3(S_y - P)$$

Extortionist strategy: Example



- ❖ Let $R = 3, T = 5, P = 1, S = 0$
- ❖ Let the desired payoff relation be $S_x - P = 3(S_y - P)$
- ❖ If we both cooperated last time, then I cooperate with probability $11/13$
- ❖ If I cheated you last time (you cooperated and I defected), then I cooperate with probability $7/26$
- ❖ If you cheated me last time (I cooperated and you defected), then I cooperate with probability $1/2$
- ❖ If we both defected last time, I defect
- ❖ On average over the long run, my score minus one will be thrice your score minus one

Iterated Prisoner's Dilemma contains strategies that dominate any evolutionary opponent

William H. Press^{1,†} and Freeman J. Dyson²

¹Department of Computer Science and School of Biological Sciences, University of Texas at Austin, Austin, TX 78712; and ²School of Natural Sciences, Institute for Advanced Study, Princeton, NJ 08540

Contributed by William H. Press, April 19, 2012 (sent for review March 14, 2012)

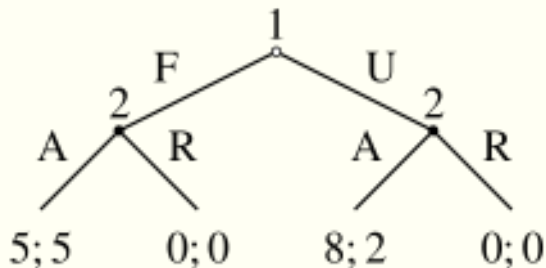
The two-player iterated Prisoner's Dilemma game is a model for both sentient and evolutionary behavior, especially including the emergence of cooperation. It is generally assumed that there exists no simple ultimatum strategy whereby one player can enforce a unilateral claim to an unfair share of rewards. Here, we show that such strategies unexpectedly do exist. In particular, a player X who is writing off these strategies can (i) deterministically set her opponent Y 's score, independently of his strategy or response, or (ii) enforce an extortionate linear relation between her and his scores. Against such a player, an evolutionary player's best response is to accede to the extortion. Only a player with a theory of mind about his opponent can do better, in which case iterated Prisoner's Dilemma is an ultimatum game.

Fig. 1C, then, shows the most general memory-one game. The four outcomes of the previous move are labeled 1, ..., 4 for the respective outcomes $xy \in \{cc, cd, dc, dd\}$, where c and d denote cooperation and defection. X 's strategy is $\mathbf{p} = (p_1, p_2, p_3, p_4)$, her probabilities for cooperating under each of the previous outcomes. Y 's strategy is analogously $\mathbf{q} = (q_1, q_2, q_3, q_4)$ for outcomes seen from his perspective, that is, in the order of $yx \in \{cc, cd, dc, dd\}$. The outcome of this play is determined by a product of probabilities, as shown in Fig. 1.

Methods and Results

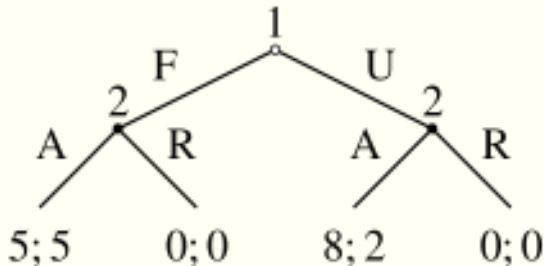
Zero-Determinant Strategies. As is well understood (10), it is not necessary to structure the play of iterated Prisoner's Dilemma to make it

IPD == Ultimatum Game



If both players are sentient, but only one is aware of ZD-Strategies, then the *IPD* reduces to the *Ultimatum Game*

IPD == Ultimatum Game



- ❖ Let's suppose both players are sentient
- ❖ Let's suppose the buyer only knows about ZD-strategies
- ❖ The buyer tries to extort the seller
- ❖ The seller eventually notice
- ❖ The seller decide to sabotage the scores of both
- ❖ This is an Ultimatum Game. The buyer proposes an unfair ultimatum. And the seller respond.

Generous ZD-Strategies



- If both players are sentient and witting of ZD-Strategies, then they can *agree on playing a Generous ZD-Strategy*

Generous ZD-Strategies



- ❖ If both players are sentient and witting of ZD-Strategies, then they can *agree on playing a Generous ZD-Strategy*
- ❖ In fact any tentative to extort the opponent would result in a low payoff for both

Generous ZD-Strategies



- ❖ If both players are sentient and witting of ZD-Strategies, then they can *agree on playing a Generous ZD-Strategy*
- ❖ In fact any tentative to extort the opponent would result in a low payoff for both
- ❖ It is rational to agree on a fair cooperation strategy

Generous ZD-Strategies



- ❖ If both players are sentient and witting of ZD-Strategies, then they can *agree on playing a Generous ZD-Strategy*
- ❖ In fact any tentative to extort the opponent would result in a low payoff for both
- ❖ It is rational to agree on a fair cooperation strategy
- ❖ They agree to *unilaterally set the other's score to an agreed value (presumably the maximum possible)*

Generous ZD-Strategies



- ❖ If both players are sentient and witting of ZD-Strategies, then they can *agree on playing a Generous ZD-Strategy*
- ❖ In fact any tentative to extort the opponent would result in a low payoff for both
- ❖ It is rational to agree on a fair cooperation strategy
- ❖ They agree to unilaterally set the other's score to an agreed value (presumably the maximum possible)
- ❖ Neither player can then improve her score by violating the strategy

Generous ZD-Strategies



- ❖ If both players are sentient and witting of ZD-Strategies, then they can *agree on playing a Generous ZD-Strategy*
- ❖ In fact any tentative to extort the opponent would result in a low payoff for both
- ❖ It is rational to agree on a fair cooperation strategy
- ❖ They agree to unilaterally set the other's score to an agreed value (presumably the maximum possible)
- ❖ Neither player can then improve her score by violating the strategy
- ❖ Each is punished for any purely malicious violation

A generous relation

$$S_x - R = 2(S_y - R)$$

Generous ZD-strategy: Example



- ❖ Let $R = 3, T = 5, P = 1, S = 0$
- ❖ Let the desired payoff relation be $S_x - R = 2(S_y - R)$
- ❖ If we both cooperated last time, then I cooperate
- ❖ If I cheated you last time (you cooperated and I defected), then I cooperate with probability $8/10$
- ❖ If you cheated me last time (I cooperated and you defected), then I cooperate with probability $3/10$
- ❖ If we both defected last time, I cooperate with probability $2/10$
- ❖ On average over the long run, my score minus three will be twice your score minus three

Under the assumption...



- ❖ Ascribe past actions to the same market participants
- ❖ Choose strategies according to the outcome of past interactions

Anonymous Black Market

- Is cooperation possible in anonymous zero-day markets?



Anonymous Black Market

- ❖ Is cooperation possible in anonymous zero-day markets?
- ❖ Do you believe it is?



Anonymous Black Market



- ❖ Is cooperation possible in anonymous zero-day markets?
- ❖ Do you believe it is?
- ❖ If yes, which institutions for monitoring and enforcement promote cooperation in this setting?

Cooperation among Strangers

Cooperation among strangers under the shadow of the future ^{*}

Gabriele Camera
University of Iowa
and
Marco Casari
Purdue University

October 2007

Anonymous Economies: Camera and Casari 1

- ❖ Cooperation is high and increases with experience



Anonymous Economies: Camera and Casari 1



- ❖ Cooperation is high and increases with experience
- ❖ Low degree of cooperation when subject see aggregate outcomes without observing identities (e.g., as might result from discussing trading experiences in *anonymous fora*)

Anonymous Economies: Camera and Casari 1



- ❖ Cooperation is high and increases with experience
- ❖ Low degree of cooperation when subject see aggregate outcomes without observing identities (e.g., as might result from discussing trading experiences in *anonymous fora*)
- ❖ Costly personal punishment significantly promotes cooperation

Anonymous Economies: Camera and Casari 2



- Subject were given the possibility to observe actions and outcomes in their game and to inflict, at a cost, a loss in the earnings of the defecting opponent

Anonymous Economies: Camera and Casari 2



- ❖ Subject were given the possibility to observe actions and outcomes in their game and to inflict, at a cost, a loss in the earnings of the defecting opponent
- ❖ Camera and Casari added a second stage in the one-shot game

Anonymous Economies: Camera and Casari 2



- ❖ Subject were given the possibility to observe actions and outcomes in their game and to inflict, at a cost, a loss in the earnings of the defecting opponent
- ❖ Camera and Casari added a second stage in the one-shot game
- ❖ The retaliation stage resembles in full the Adaptive and MAD scenarios in the 0-Day Dilemma

Anonymous Economies: Camera and Casari 3



- ❖ The player who observed the opponent defect sometimes employed personal punishment (i.e., in-match retaliation), while staying in cooperative mode in the following periods

Anonymous Economies: Camera and Casari 3



- ❖ The player who observed the opponent defect sometimes employed personal punishment (i.e., in-match retaliation), while staying in cooperative mode in the following periods
- ❖ Players show preference for in-match retaliation over the (equilibrium) informal retaliation

Anonymous Economies: Camera and Casari 3



- ❖ The player who observed the opponent defect sometimes employed personal punishment (i.e., in-match retaliation), while staying in cooperative mode in the following periods
- ❖ Players show preference for in-match retaliation over the (equilibrium) informal retaliation
- ❖ Efficiency: defectors who had been punished by a cooperator were more likely to cooperate in the following periods (34.5% vs 24.1%)

Punishment as a Public Good



- ❖ It significantly increases cooperation

Punishment as a Public Good



- ❖ It significantly increases cooperation
- ❖ The subject that benefit the most are cooperators who punish little or not at all

Semi-anonymous Zero-day markets



- ❖ If only one party is anonymous, the anonymous counterpart has not ability to know if she already had any deals with the same participant

Semi-anonymous Zero-day markets



- ❖ If only one party is anonymous, the anonymous counterpart has not ability to know if she already had any deals with the same participant
- ❖ The latter can't benefit from being sentient and is forced to choose her strategies as an evolutionary player would do

Semi-anonymous Zero-day markets



- ❖ If only one party is anonymous, the anonymous counterpart has not ability to know if she already had any deals with the same participant
- ❖ The latter can't benefit from being sentient and is forced to choose her strategies as an evolutionary player would do
- ❖ If the anonymous party knows about the ZD-strategies, she can choose to *extort* the opponent

Semi-anonymous Zero-day markets



- ❖ If only one party is anonymous, the anonymous counterpart has not ability to know if she already had any deals with the same participant
- ❖ The latter can't benefit from being sentient and is forced to choose her strategies as an evolutionary player would do
- ❖ If the anonymous party knows about the ZD-strategies, she can choose to *extort* the opponent
- ❖ Hence, while cooperation can emerge in fully-anonymous markets, extortion can proliferate in the semi-anonymous economies

To sum up

- ❖ Zero-day markets can achieve cooperation even in absence of trusted-third parties

To sum up

- ❖ Zero-day markets can achieve cooperation even in absence of trusted-third parties
- ❖ Cooperation can be sustained even when traders are anonymous

To sum up

- ❖ Zero-day markets can achieve cooperation even in absence of trusted-third parties
- ❖ Cooperation can be sustained even when traders are anonymous
- ❖ Punishment is an effective instrument to discourage traders from defecting

To sum up

- ❖ Zero-day markets can achieve cooperation even in absence of trusted-third parties
- ❖ Cooperation can be sustained even when traders are anonymous
- ❖ Punishment is an effective instrument to discourage traders from defecting
- ❖ It is possible to get extorted, if the adversary knows about ZD-Strategies and we simply seek to adjust our strategy to maximize our own profit

Recommendations

Recommendations

1. Do not deal with anonymous traders, if you cannot ensure your own anonymity

Recommendations

1. Do not deal with anonymous traders, if you cannot ensure your own anonymity
2. Discourage defection by practicing brinkmanship or casting the shadow of the future in every decision of your counterpart

Recommendations

1. Do not deal with anonymous traders, if you cannot ensure your own anonymity
2. Discourage defection by practicing brinkmanship or casting the shadow of the future in every decision of your counterpart
3. Respond: Consider punishing defection to promote cooperation

Recommendations

1. Do not deal with anonymous traders, if you cannot ensure your own anonymity
2. Discourage defection by practicing brinkmanship or casting the shadow of the future in every decision of your counterpart
3. Respond: Consider punishing defection to promote cooperation
4. Let the seller supply the vulnerability first, if interested in a one-time deal

Recommendations

1. Do not deal with anonymous traders, if you cannot ensure your own anonymity
2. Discourage defection by practicing brinkmanship or casting the shadow of the future in every decision of your counterpart
3. Respond: Consider punishing defection to promote cooperation
4. Let the seller supply the vulnerability first, if interested in a one-time deal
5. Learn about Zero Determinant strategies, if playing in an onymous market

Recommendations

1. Do not deal with anonymous traders, if you cannot ensure your own anonymity
2. Discourage defection by practicing brinkmanship or casting the shadow of the future in every decision of your counterpart
3. Respond: Consider punishing defection to promote cooperation
4. Let the seller supply the vulnerability first, if interested in a one-time deal
5. Learn about Zero Determinant strategies, if playing in an onymous market
6. Grim trigger: forever defect, if you see defection while playing in an anonymous market and have no ability to punish the opponent

If interested, please be in touch

Spring 2015: Speaking Dates

- ❖ May 26th, PHDays V, Moscow, Russian Federation
- ❖ May 28th, HITBSecConf 2015, Amsterdam, Netherlands
- ❖ June 4th, AusCERT 2015, Gold Coast, Australia



“

Though I am often in the depths of misery, there is still calmness, pure harmony and music inside me.

”

Vincent van Gogh

“

Though we are often in the depths of insecurity, there is still calmness, pure harmony and music inside us.

”



THANK YOU

QUESTIONS?

Backup



- ❖ BeeWise is the first prediction market for forecasting security events and trends
- ❖ More specifically, it is a security-event futures exchange where participants trade contracts whose payoffs are tied to future events in information security, such as the discovery of a given software vulnerability, a security incident, or the diffusion of new malware



- With a large enough number of people betting on the outcome of selected events, the prices of the contracts will be an approximate measure of the probability of the underlying events at any time. The ability to use market prices as forward-looking indicators of security properties will help in establishing information symmetry between buyers and sellers (ie., build a quality signal), and help security stakeholders to make better and more informed decisions, by telling mediocre security products from good ones