The Bazaar, the Maharaja's Ultimatum, and the Shadow of the Future: Extortion and Cooperation in the Zero-Day Market

Alfonso De Gregorio, 12-16 October 2015, HITB GSEC, Singapore

Abstract

Zero-day vulnerabilities are gaining a prominent role in the modern-day intelligence, national security, and law enforcement operations. At the same time, trading vulnerability information or zero-day exploits is considered a risky ordeal. Players in the secretive zero-day market face some inherent obstacles related to time-sensitiveness of traded commodities, trust, price fairness, and possibility of defection.

To alleviate some of these hurdles, it was suggested to: 1. Use punishment (i.e., public disclosure of vulnerabilities) to discourage a buyer from defecting; 2. Resort to the use of trusted-third parties (e.g., escrow services), as crucial entities for enabling cooperation of market participants; and 3. Build a reputation system (e.g., reputation score) as an instrument to establish trust relationships between distrustful players.

This work presents the first results of an ongoing study on extortion and cooperation in zero-day markets through the lens of game theory.

The questions motivating this research are: a. Can the zero-day market achieve cooperation and efficiency even in absence of trusted-third parties? b. Can punishment discourage the buyer from defecting? c. Under which conditions a player can extort the opponent? d. Can cooperation be sustained also in fully anonymous or semi-anonymous settings? This work addresses these questions and others, and provides an analysis of the zero-day trading strategies applicable to each scenario.

Learn which strategies allows to maximize the profits while trading zero-days in today's marketplaces. Find out how to avoid getting extorted by zero--day traders. Learn how to extort an unwit market participant. Gain a deeper knowledge about the emergence, sustainability, and breakdown of cooperation. Discover under which conditions the zero-day markets can achieve efficiency.

This work find application in a number of markets for vulnerability information and zero-day exploits. They range from over-the-counter zero-day trading, to boutique exploit providers offering zero-day vulnerabilities for a subscription fee, to service models for vulnerability research.

1. The Zero-day Market: A hairy business

Jonathan Stewart has a freelance job, a family, and lives in a Phoenix suburb, featuring stucco houses and manicured lawns. [NPR] Back in 2013, after spending one of his workdays in Redmond, Jonathan was poking around on his own when he stumbled into a vulnerability in iOS7. Jonathan, whose security career is old enough to remember when his colleagues were paid zilch, nothing, or were offered a tiny token for finding these vulnerabilities and writing exploit for them, tells about his discovery to few friends, because he knows that he can make some extra cash from his work --- and he already did so in the past. Meet Ty. Ty is a

vulnerability broker that heard about Jonathan's discovery from another hacker called Geohot and who is touch with some people in China. The plan is to take the Jonathan's vulnerability, let Geohot write an exploit, and sell this as a package deal to the Chinese. Meanwhile, another group of hackers named the Evad3rs also heard about the same vulnerability and cut a $1M deal with a different group of Chinese businessmen. One of Jonathan's friends got in touch with them, in the hope that they all could work together. And you know what? After turning him down, the Evad3rs got to the finish line first, figuring out how to exploit the vulnerability and winning the race. Jonathan "never thought that one of his friends would turn on him, sell him out." When he found out, with "no rules, no watchdogs, no court system to protect [his] discovery", Jonathan "felt used." [NPR]

That is to say that: Trading vulnerability information or zero-day exploits is considered a risky ordeal. Players in the secretive zero-day market face some inherent obstacles related to time-sensitiveness of traded commodities, trust, price fairness, and possibility of defection. Or, to put it succinctly, this is a hairy business!

To begin with, vulnerability information is a time-sensitive commodity, or a wasting asset. Zero-day exploits are valuable only when they are not widely known. Their value drops instantaneously to zero, as soon as the vulnerability is disclosed or a mitigation is released. Therefore transactions should complete in short times and with the required discretion. Or, every day can be the last day for a sale.

Yet, in this market with no centralized way to locate its players, finding buyers and sellers can be time-consuming, and may demand participants to have business deals with individuals they are not familiar with and whose true intentions are hard to verify.

Furthermore, even if buyers and sellers manage to locate each other with ease, negotiating a fair price if often challenging due to a lack of transparency. Adoption degree of the vulnerable component, its presence within a given attack surface, the level of authentication required to exploit it, the level of difficulty of independent rediscovery, exploit reliability, and other factors, all affect the final price. Still, they are difficult to measure.

The position of the security researchers is further impoverished by the tension between the amount of information they are asked to disclose and the risk of losing the intellectual property (IP). As happens for other information goods, proving the validity of the vulnerability information without disclosing the information itself is challenging. The possible approaches are essentially two: reveal or demonstrate; they are both undesirable. If the researcher reveals the information before the sale, the buyer might take it without paying for it, and vice versa. If the buyer pays in advance, the seller might refuse to provide the desired intellectual property. Demonstrating the vulnerability via an exploit is not any better. [CM] Whoever has full control the computing environment has an advantage over the other party. On the one hand, with a seller supplied computing environment, the same would be able to tamper with it, leaving the buyer in the position to be unable to verify its integrity. On the other hand, the buyer would be in the position to record the working of the exploit and steal the intellectual property, if the demonstration has to be carried out on the buyer's devices.

Even worse, any vulnerability claim can't be ensured. Upon learning about the vulnerability information from the seller, the other party might claim the same

information as their own and then sell it or exploit it. As many of these sales may be international and unregulated, it becomes hard to enforce the potential contracts.

Finally, sellers might promise to grant exclusive rights to the buyer, in order to receive the largest payoffs. Yet, the seller might defect and sell the same information to multiple parties. This time are the buyers to lack a mean to protect themselves. Of course, contracts may include language which force the researcher to return the funds, should the same not honor the contractual obligations. But in the zero-day market the difficulty to identify sellers, to attribute multiple transactions of the same good to the same supplier, and to enforce contracts helps the seller willing to betray.

These are obstacles that traditional businesses and services do not have to face.

To alleviate some of these hurdles, it was suggested to:

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

This writeup provides the first results of an ongoing study on extortion and cooperation in zero-day markets through the lens of game theory. The questions motivating this research are:

a) Can the zero-day market achieve cooperation and efficiency even in absence of trusted-third parties?
b) Can punishment discourage the buyer from defecting?
c) Under which conditions a player can extort the opponent?
d) Can cooperation be sustained also in fully anonymous settings?
e) Can it be sustained in semi-anonymous settings?

2. Relevance: Should I care?

The present work addresses these questions and others, by providing an analysis of the zero-day trading strategies applicable to each scenario.

The present author works at the intersection of software security and security software, exploring, and trying to contain, the space of unanticipated state. [LS] The choice of his career was dictated by a dream. He dreams that software manufacturers have the incentives to build security into their products. He dreams that security researchers have efficient means to capitalize on the efforts in security analyzes. He dreams that software users have the instruments to hedge against the information security risks they are exposed to. He dreams that information symmetry is finally established between buyers and sellers in the security market.

The reality is that current economic, regulatory and legal incentives are misaligned, distorted or ineffectual. What we observe today is what economists call a market failure. A market failure is about the inability to self-correct. Software-manufacturers will not forgo markets share. Software buyers will not forgo features, that translates in greater complexity and greater attack surface. Attackers will not forgo attacking tens of millions of vulnerable systems. How to invert this market? How do we change? The same author is on the record for

founding BeeWise, the first information security prediction market. This was his contribution towards establishing the required incentives. Although he didn't succeed so far, there is still hope in him that we can improve our global security posture. And in order to better understand the economic forces behind the zero-day market, and the needs of our community, he turned his attention to the dynamics in this economy.

Understanding the emergence, sustainability, and breakdown of cooperation and extortion in the 0-day market is increasingly important. As our society grows more interconnected, it becomes more interdependent within itself. [DG] And the more interdependence, the greater the dynamic range of possible failures. Hence it comes as no surprise that vulnerability information is key for both offensive and defensive purposes. Zero-day vulnerabilities are gaining a prominent role in the modern-day intelligence, national security, and law enforcement operations. Nation-state actors are buying vulnerabilities. [NP] Security scholars proposed to the intelligence and law-enforcement communities to use zero-days for hacking, as an alternative method for addressing their need to access communications [SB] -- only later to find out that those very communities already mastered the craft and don't really need to be lectured on it. [HT] And the underground community, as well as the surveillance, information security, and defense industries, happily respond!

That is to say that this work find application in a number of markets for vulnerability information and zero-day exploits. They range from over-the-counter zero-day trading, to boutique exploit providers offering zero-day vulnerabilities for a subscription fee, to service models for vulnerability research.

3. Zero-day Dilemma: Extortion and Cooperation in the Zero-day Market

In order to understand cooperation and extortion in the zero-day market, we need to understand the story of the Bazaar, the Maharaja's Ultimatum, and the Shadow of the Future. This is the story of the dilemma faced by zero-day market participants who are each given incentives to exploit each other. Few preliminaries and definitions are due.

"The ultimatum game is a game in economic experiments. The first player (the proposer) receives a sum of money and proposes how to divide the sum between himself and another player. The second player (the responder) chooses to either accept or reject this proposal. If the second player accepts, the money is split according to the proposal. If the second player rejects, neither player receives any money." [UG]

"The prisoner's dilemma is a canonical example of a game analyzed in game theory that shows why two purely "rational" individuals might not cooperate, even if it appears that it is in their best interests to do so." [PD] In the Prisoner's Dilemma there are two prisoners that committed a crime. If they both do not confess (cooperate), they get a low punishment (high payoff). If they both confess (defect), they get a more severe punishment (low payoff). If one confesses and the other does not, then the one that confesses gets a very low punishment (highest payoff) and the other gets a very severe punishment (lowest payoff). [YM]

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 (0DD) is as follows: There are a zero-day seller and a buyer. If the both cooperate, respectively supplying the information good and paying for the

same, they get a reward payoff (R). If the both defect, respectively retaining the intellectual property and the budget, they get a punishment payoff (P). If the buyer pays the seller and the latter does not supply the desired vulnerability information, the buyer gets the sucker payoff (S) and the seller receives the temptation payoff (T). However, if the seller provides the zero-day and the buyer defects, three different options are available to the betrayed participant. The seller might opt to accept the buyer's betrayal (Submissive), or might prefer two forms of in-match retaliation. A first avenue of retaliation is to sell the same IP to other buyers (Adaptive). A second avenue of retaliation, resembling the doctrine of mutually assured destruction, is to publish the IP, negating its value to the exploiter and reducing the window-of-opportunity associated with the discovered vulnerability (MAD). Both in-match retaliation options works as long as the vulnerability information is fresh. The payoffs for each scenario are as follows: for the Submissive outcome, the seller gets the sucker payoff (S) and the buyer the temptation payoff (T); in the Adaptive scenario the seller gets an expired payoff (Z) and the buyer a refurbished payoff (U); for the MAD outcome the seller and buyer get respectively a residual payoff (V) and the sucker payoff (S).

The following conditions holds for the payoffs. The Temptation payoff is strictly greater than the Reward payoff. The Reward payoff is strictly greater than the Punishment payoff. The Reward payoff is also strictly greater than the Refurbished payoff, the Residual payoff, and the Expired payoff. The Punishment payoff is strictly greater than the Sucker payoff.

Few remarks.

In the Submissive scenario 0-day traders are playing the standard Prisoner's Dilemma. The payoff relationship $R > P$ implies that mutual cooperation is superior to mutual defection. The payoff relationships $T > R$ 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.

In the Adaptive scenario, neither the buyer nor the seller have a dominant strategy, if we assume the Expired payoff to be greater than the Sucker payoff and the Refurbished payoff to be smaller than the Reward payoff. In particular, if the betrayed seller has the ability to close alternative deals for the same IP (i.e., 1-Day FUD and 1-Day private exploits), then defection would not be a dominant strategy anymore. Yet the nature of the market plays a role in this capacity. Today the 0-day market is not a monopsony [SM] and it is still weakly regulated. However, starting from the Wassenaar Arrangement, regulations may emerge in this area and may impact the market liquidity.

The MAD scenario is a variant of the standard PD, where the seller has the ability to negate the buyer the temptation to defect. The seller does so by making sure the Temptation payoff approaches the Punishment-payoff. Therefore in the MAD scenario Defection is not a dominant strategy for the buyer. If factors such as the 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. By doing so, the seller will not make herself worse-off --- she was going to get the Sucker payoff anyway. Pretty the other way around. The seller would reduce the incentive of the buyer to defect on the first place. To this end, it is important for the 0-day sellers to have an efficient mechanism 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. Since July 2002 the Full-Disclosure

list experienced a "fair share of legal troubles along the way." [FD] In a market that will likely see an increasing number of regulations in the coming years, posting on a mailing list may translate in an OPSEC failure, if proper steps are not taken to ensure the anonymity of the submitter. That is to say that I would not be surprised to learn about the existence of 0-day disclosure platform. Researchers could use it for doing full disclosure. Players in the black market would use it 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.

It is worth to note that, as long as the seller does not play in the Submissive scenario, the buyer is not better off defecting. Therefore, in the one-shot sequential 0-Day Dilemma game, cooperation is possible if the seller moves first and retains the ability to punish a defecting buyer. If this is not the case, the rational outcome is the action profile of mutual defection. "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." [PD] If no form of punishment can undertaken by the seller, can the cooperative outcome still be sustained as an equilibrium?

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. Whenever the Submissive scenario applies, the I0DD reduces to the Iterated Prisoner's Dilemma (IPD). Therefore it becomes possible to tap into the extensive theoretical and experimental literature devoted to the study of repeated games and draw some predictions on the emergence, sustainability, and breakdown of cooperation in the markets of vulnerability information and zero-day exploits.

I ask you to consider three major settings. In the first economy traders know the identity of the party they are dealing with (i.e., onymous). In a second economy trades take place among strangers (i.e., anonymous agents with random matching [EG]). In the third setup either the buyer or the seller is anonymous (i.e., semi-anonymous economy).

Since the Robert Aumann work published in 1959, it has been well known that in the onymous setting two rational players can sustain the cooperative outcome when they face each other an indefinite number of times.

More recently Press and Dyson [PrDy] have fundamentally changed the viewpoint on this game [SP], illustrating the power granted to a sentient player, or a player with a theory of mind, which is to say a player who realizes that her behavior can influence her opponents' strategies. They describe a special class of strategies called the Zero Determinant (ZD) straetgies, that enforce a linear relationship between the two players' scores. ZD-strategies have far reaching consequences for 0-day traders.

If one trader is aware of ZD strategies, but the opponent is an evolutionary player then the former can choose to extort the latter. A players is said to be evolutionary is she posses 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 to the expenses of the victim. It is the victim's best interest to cooperate with the extortionist player, because she is able to increase her score by doing so. However 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. [SP] An example of such strategy forces the relation S_x - P = 3 (S_y - P) between the two players' score. This strategy guarantees the player X thrice the share of payoffs above the Punishment, compared with those received by her opponent Y. How does it work in practise? Let's assume the Reward, Temptation, Punishment, and Sucker payoffs be respectively equal to 3, 5, 1, and 0. An extortionist player would play as follow: If he and the opponent both cooperated last time, then he cooperates with probability 11/13. If he cheated the opponent last time, then he cooperate with probability 7/26. If he was cheated by the opponent last time, the he cooperate with probability 1/2. If he and the opponent both defected last time, he defects. On average, over the long run, the extortionist score minues one will be thrice the opponent score minus one. I refer you to their paper for the details.

Press and Dyson also showed that if both players are sentient, but only one is aware of ZD-strategies, then the IPD reduces to the Ultimatum Game. Let's suppose the buyer is aware of ZD-strategies and the seller does at least have a theory of mind. The buyer can once again decide to extort the seller. However, the seller will eventually notice that something is amiss: whenever she adjust her strategy to improve her own score, she improves the buyer's score even more. With a theory of mind she may then decide to sabotage both her own score and the buyer's score, by defecting, in the hope of altering the buyer's behavior. The IPD has thus reduced to the Ultimatum Game [UG], with the buyer proposing an unfair ultimatum and the seller responding either by acceding or by sabotaging the payoffs for both players. [SP]

Finally if both players are sentient and witting of ZD-strategies, then they can agree on playing a (Generous) ZD-strategy. They want to consider this option because any tentative to extort the opponent would result in a low payoff for both. Hence the rational thing to do is agree on a fair cooperation strategy. They can do so by agreeing to unilaterally set the other's score to an agreed value (presumably the maximum possible). Neither player can then improve her score by violating this strategy, and each is punished for any purely malicious violation. An example of such strategy forces the relationship S_x - R = 2 (S_y - R) between the players' scores. [SP] This strategy guarantees the player X twice the share of payoffs above the Reward, compared with those received by her opponent Y. In practise, an example generous strategy satisfying this relation would work as follow: If both players cooperated last time, then X cooperates. If X cheated Y last time, then X cooperates with probability 8/10. If Y cheated X last time, then X cooperates with probability 3/10. If both players defected last time, then X cooperates with probability 2/10. On average, over the long run, X score minus three will be twice Y score minues three.

The results cited so far apply if players can recognize the identity of any of their past opponents. Identification is required to ascribe past actions to the same market participants and choose strategies according to the outcome of past interactions.

Nowadays a number of black markets exist where participants are anonymous. Therefore it is natural to ask: 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?

In an experimental study on anonymous economies, Camera and Casari [CC] found out that cooperation is high and increases with experience. They observed a low degree of cooperation when subjects see aggregate outcomes without observing identities (e.g., as might result from discussing experiences in anonymous fora). But they

also noticed how costly personal punishment significantly promotes cooperation. In an experimental treatment, subjects 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 did so adding a second stage in the one-shot game, resembling in full the Adaptive and MAD scenarios in the 0-Day Dilemma. In the same treatment the player who observed the opponent defect sometimes employed personal punishment, which is to say in-match retaliation, while staying in cooperative mode in the following periods. The same authors collected evidences that subjects showed preference for this form of punishment over the (equilibrium) informal retaliation. In-match punishment was found to be also effective, because defectors who had been punished by a cooperator were more likely to cooperate in the following periods (34.5% vs 24.1%). Hence private punishment seems to be a public good. "On the one hand it significantly increases cooperation... On the other hand the subjects who benefit the most are cooperators who punish little or not at all."

For the sake of completeness let's turn now our attention to semi-anonymous zero-day markets. This is a trading scenario documented by the recent Hacking Team leaks. [HT2] According to the leaked correspondence, back in March 2014 the co-founder and CTO of the Milan-based company was contacted through his corporate email address by an anonymous 0-day seller. The seller offered Hacking Team a Windows local privilege escalation vulnerability and research services. Called upon by the CTO for an opinion, the COO recommended against closing business deals with anonymous counterparts, and reaffirmed that accreditation is of the essence. I ask you: Was the COO's intuition correct? Can Hacking Team trust anonymous 0-day sellers? If you were in their place, would you have trusted an anonymous seller with supplying an 0-day? My answer is a corollary to the analysis above: If only one party is anonymous, the onymous counterpart has no ability to know if she already had any deals with the same participant in the past periods. As a result the latter cannot benefit from being sentient and is forced to choose her strategies as an evolutionary player would do. Therefore, if the anonymous party knows about ZD-strategies, she can choose to extort the opponent, granting herself a disproportionate number of high payoffs. Hence, while cooperation can emerge in fully-anonymous markets, extortion can proliferate in the semi-anonymous economies. All of which is to say that the Hacking Team's COO had the correct intuition.

To sum up, I have some good news, a cautionary note, and some recommendations to 0-day traders.

1. Zero-day markets can achieve cooperation even in absence of trusted third parties.
2. Cooperation can be sustained even when traders are anoymous.
3. Punishment is an effective instrument to discourage traders from defecting.
4. 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.

4. Recommendations to Zero-day Traders: How to maximize payoffs?

The recommendations are:

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,

by closing alternate deals for the same vulnerability information or negating its value to the defector.

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.

And that's pretty much it, as far as theory goes. In order to place these recommendations on firmer scientific grounds, an experimental verification needs to be carried out. If interested, please be in touch with the author.

To close, Vincent van Gogh once said:

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

If you, like the present author, believe that insecurity, or the presence of unmitigable surprises [DG2], is the misery of our times. And, if at the same time, you, like the present author, are also sanguine about our ability to attain better security tradeoffs and give our children the chance to reach confidence in the processes to which they will entrust their business, then we can paraphrase Vincent van Gogh and say that:

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

5. References

[CC] Camera, G. and Casari, M. (2009); "Cooperation among Strangers under the Shadow of the Future." American Economic Review, 99(3): 979-1005. http://pubs.aeaweb.org/doi/pdfplus/10.1257/aer.99.3.979

[CM] Miller C. (2007); The Legitimate Vulnerability Market -- Inside the Secretive World of 0-day Exploit Sales, In Sixth Workshop on the Economics of Information Security. http://weis2007.econinfosec.org/papers/29.pdf

[DG] Geer Jr. D. E., (2013); Trends in Cyber Security, NRO, http://geer.tinho.net/geer.nro.6xi13.txt

[DG2] Geer Jr. D. E., (2013); Tradeoffs in Cyber Security, UNCC http://geer.tinho.net/geer.uncc.9x13.txt

[EG] Ellison, G. (1994); Cooperation in the Prisoner's Dilemma with Anonymous Random Matching, Review of Economic Studies, 61: 567-88 http://econweb.ucsd.edu/~jandreoni/Econ264/papers/Ellison%20RES%201994.pdf

[FD] Cartwright J. (2014); Administrivia: The End, Full-Disclosure list, http://seclists.org/fulldisclosure/2014/Mar/332

[HT] Zetter, K. (2015); Hacking Team Shows the World How Not to
Stockpile Exploits
http://www.wired.com/2015/07/hacking-team-shows-world-not-
stockpile-exploits/

[HT2] Russo, G. (2014); Re: vulnerability poc
https://wikileaks.org/hackingteam/emails/emailid/20849

[LS] LangSec: A Workshop on Language Theoretic Security --
Call for Papers, http://spw15.langsec.org/cfp.pdf

[NP] Meister, A. (2014); Vupen „Threat Protection“:
Wir veröffentlichen den Vertrag, mit dem das BSI Sicherheitslücken
und Exploits kauft
https://netzpolitik.org/2014/vupen-threat-protection-wir-
veroeffentlichen-den-vertrag-mit-dem-das-bsi-sicherheitsluecken-
und-exploits-kauft/

[NPR] Henn S. (2015), Episode 596: Johnny Mnemonic's Secret Door,
NPR, Planet Money, http://www.npr.org/blogs/money/2015/01/09/
376164768/episode-596-johnny-mnemonic-s-secret-door

[PD] Wikipedia, Prisoner's Dilemma.
http://en.wikipedia.org/wiki/Prisoner%27s_dilemma

[PDB] Dal Bó, P. (2005); Cooperation under the Shadow of the Future:
Experimental Evidence from Infinitely Repeated Games,
American Economic Review, 95(5): 1591-1604.

[PrD] Press WH, Dyson FJ (2012); Iterated Prisoner’s Dilemma contains
contains strategies that dominate any evolutionary opponent
nent. PNAS. 109:10409—10413.

[SB] Bellovin, S.; Blaze M.; Clark S.; and Landau S. (2013);
Going Bright: Wiretapping without Weaking Communications
Infrastructure, IEEE Security & Privacy 11:1,
http://dx.doi.org/10.1109/MSP.2012.138

[SM] Sulmeyer, M. (2013); The Political Economy of the
Cyber-security and Malware Markets, Breakpoint 2013,
https://soundcloud.com/darren-pauli/michael-sulmeyer-the-political

[SP] Stewart A.J. and Plotkin J.B. (2012);
Extortion and cooperation in the Prisoner's Dilemma, PNAS

[UG] Wikipedia, Ultimatum game,
http://en.wikipedia.org/wiki/Ultimatum_game

[YM] Monsour Y. (2009); Computational Game Theory, Lecture 1,
http://www.tau.ac.il/~mansour/course-games-2009-10/lecture1.pdf