Economic Evaluation of Interactive Audio Media for Securing Internet Services

Theodosios Tsiakis[1], Panagiotis Katsaros[2], and Dimitris Gritzalis[3]

[1] Dept. of Marketing, Technological Educational Institute of Thessaloniki, Greece
[2] Dept. of Informatics, Aristotle University of Thessaloniki, Greece
[3] Dept. of Informatics, Athens University of Economics and Business, Greece
tsiakis@mkt.teithe.gr, katsaros@csd.auth.gr, dgrit@aueb.gr

Abstract. Internet Telephony (Voice over Internet Protocol or VoIP) has recently become increasingly popular mainly due to its cost advantages and range of advance services. On the same time, SPam over Internet Telephony (SPIT) referred as unsolicited bulk calls sent via VoIP networks by botnets, is expected to become a serious threat in the near future. Audio CAPTCHA (Completely Automated Public Turing test to tell Computers and Human Apart) mechanism were introduced and employed as a security measure to distinguish automated software agents from human beings. The scope of this paper is to present the security economics frame and to have an in-depth review of the related economic models of SPAM and its analogies with SPIT.

1 Introduction

The evolution of technological innovations for robust Internet Services must not only be efficient enough to solve current security problems at the technical level, but should also incorporate what in [1] is referred as economic implications of a solution's technical design. Today's Internet does not only comprise a series of fast-growing technologies, but it is an entire ecosystem of economic agents with monetary incentives and interdependence [2].

One big challenge is protecting services and resources that are provided through the web from waste or abuse due to the prevalence of malicious software running automated tasks, which is well-known as bot. Bots perform simple tasks that are repeated at a much higher rate than would be possible for a human alone. They usually infect as many vulnerable computers as needed for launching massive attacks against the targeted service or resource. The infected computers is said to form a botnet. In CSI's 2008 Computer Crime and Security Survey, computer security incidents that involved bots were ranked as the second most expensive with an average annual loss of $300,000 for each of the 522 surveyed companies.

The technology used for protecting Internet services and resources is the "Completely Automated Public Turing test to tell Computers and Humans Apart", widely known with the acronym CAPTCHA. A CAPTCHA is a type of challenge-response test trying to ensure that the response to a given challenge is not generated by a computer. It usually involves a server asking the service user to complete a test that is

H. Jahankhani et al. (Eds.): ICGS3/e-Democracy 2011, LNICST 99, pp. 46–53, 2012.

automatically generated and graded, but other computers are supposedly unable to solve. In effect, any user entering a correct solution is presumed to be human. A number of CAPTCHA generation mechanisms have been successfully broken by bots. Also, in [3] it is shown that if someone can employ workers for solving CAPTCHAs with wages no more than 50 cents of dollar for 1000 solved CAPTCHA it is possible to economically break this protection mechanism. The authors claim that this is feasible, since it is a work with no particular skill requirements and therefore is not too difficult to find many willing to do it.

SPHINX is a research project that aims to investigate the use of Interactive Audio Media as a means to lower the costs for provisioning adequate protection for Internet services and resources. SPHINX develops a service that will integrate the use of audio CAPTCHA with appropriate security policies that will allow adjusting the frequency of the resource demanding audio CAPTCHAs to the anticipated needs of a given security problem.

The economic perspective of the technology being developed is a fundamental research component and this article focuses on this particular aspect. In section 2, we place the security economics frame that we consider suitable for evaluating the economic implications of the developed service. In section 3, we provide an in-depth review of the related economic models. The paper concludes with a summary on the current findings and the future research prospects.

2 Economic View

Economics is the social science that studies how people and society decide and choose to allocate their scarce resources among alternative uses and get out the most. It is common to distinguish positive economics that attempts with scientific and objective epexegesis to attribute how economy functions (e.g. imposition of taxes will cause increase in product price), from normative economics that address subjective evaluation methods (deontological – ethical) to admeasure the efficiency of economic plans (e.g. a tax should be enforced in order to ban smoking in public places).

The economic aspect of information considers that dissimilar economic actors have access to different information and so information defines and determines differently economic choices. Economic organizations (especially those of technological sector) develop attitudes that set them in risks and those risks are carried over economy. This diffusion of risk from economic organization to economic organization and from economic sector to economic sector, deregulate economics caused by problems concerned with externalities. Externalities are side effects (external) that arise when actions of a person have effect on the well being of another person. In economics, we are concerned with actions that inhere value. Those in the process of a transaction are translated into expenses associated with an action that do not charge diametrically the relative one with the action people, but some other outside this. Decisions (of production or consumption) that a person will take have direct affect on production or consumption of other persons. Positive externality consist the benefit that people derive from market operation that they do not participate, whereas negative externality is the damage obtained and not recompensed in people that they do not participate in the production or consumption process of a market. Consider creating a college campus in a city. The value of the certain area will increase as it is upgraded and that causes a positive externality. On the contrary, if a city dump is created, then the value of the area will decrease due to the fact that the operation will cause damnification not able to be claimed [4, 5].

Network externalities can cause encirclement by creating a technological pattern that is difficult to replace. They comprise the consequences that a user of a product or service receives from other users that use analogous or compatible products or services. Positive externality is experienced when benefits consist of an ascending function of the number of other users and vice versa negative externality when benefits consist of a descending function of the number of other users. Security is characterized by positive externality. If I take measures at a personal level, I support/invigorate security for others as well as for myself. This discernment broach the subject of free rider problem as one of the classical cases of market imperfection or failure (here the security market). In the frame of this problem, users or private individuals (as individual entities) are not willing to apply security measures or policies, expecting from others to act or relying on others to assure their social welfare. Users partially invest in security as they do not run the real social cost of their actions, which cause negative externality [6, 7]. This application reveals the market failure and necessitates public intervention through regulations [8]. [9] describes the security process in transportation. Security consist positive externality for non users since it is offered to anyone and leaves them with no motive to act collectively, which is the cause of the free rider problem mentioned above. Namely, security is described in terms of marginal social benefits (MSB), payments for services are described as marginal social costs (MSC), while the marginal private benefits (MPB) are also taken into account. The societal optimum occurs where MSB = MSC (for simplicity it has been assumed that marginal social costs are equal to marginal private costs). The equilibrium is established at point F (social optimum) given a quantity Q* and price P*. Point F requires government expenditure to supply the needed quantity of security (Q*- Q), while private sector supplies Q units (Figure 1).

But why there is such a plethora of vulnerabilities? The answer is economic terms is given as follows. Software companies in case are not (economically) motivated to develop secure software and customers are primarily concerned for the price and the special benefits/characteristics. Hereupon, if a software developer is concerned with designing secure software, will have higher production cost and will need a longer period of time to circulate, effectively giving the chance to another developer that might be established and win the market by circulating sooner and faster rich in characteristics products.

Losses from security incidents emerge from inefficient security measures, human errors, frauds, system failures, exogenous factors (economical, technical) etc. Information losses can cause direct economic losses (quantitative determinable) and indirect economic losses (reputation, trust). Economic losses can be classified in several categories such as damage in operational function, computer resources, and human hypostasis.

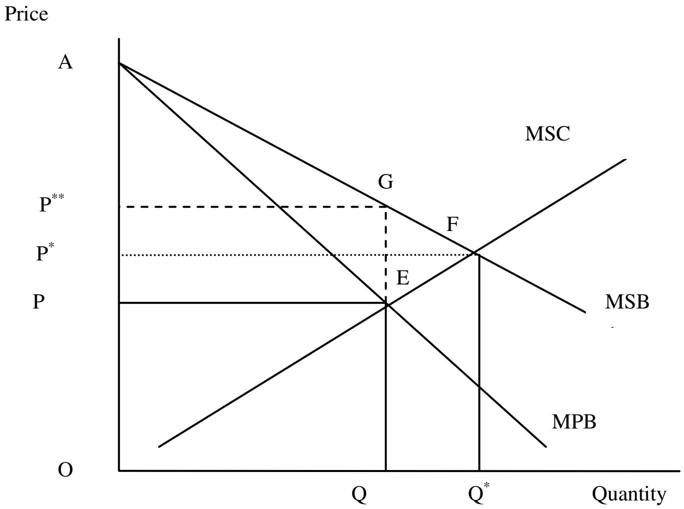

Fig. 1. Economic model of social benefits and costs

Economic analysis is the base of budgeting expenses (investments) in information security. Economic evaluation of security methods is necessary for the rationalization of budgeting/financing security actions. A first group of researchers aim to develop more practical methods to analyze, determine and quantify the optimal level of security investments in terms “what should I implement, what will it cost me and what will I earn”? Economic security metrics are concerned with how efficient a security measure is. Those methods include, Annual Loss Expectancy (ALE), Return On Security Investment (ROSI), Net Present Value, (NPV), Internal Rate of Return (IRR), risk management and focus on economic/managerial evaluation of security investments [10, 11].

The second group is based on classic economic theory, with methods such as efficient market hypothesis. In this theory every stakeholder should try to maximize utility and have orthological expectations in order for optimal investments to emerge, which should be escalated when new information arise.

Investments are divided into two key categories. Firstly in ex ante that aims in determine what firm intends to invest (total expenditure per investment plan). Secondly in ex post that analyze and measure the actual past performance (return achieved) of an investment. The first one consists in deciding whether or not to invest in one security measure or not, as to choose the best alternative solution from the available one. The second one can lead to precise observation and comparison of target. On the other side of security there is insecurity as a formal and not quantitative form of risk. There are several sources of such risk and in economy too. Insecurity causes cost to people and to investors that are risk averse. Economic theory reveals that economic agents who abominate risk prefer economic environment less insecure and are willing to pay insurance to limit risk [12].

3 Economic Modeling

One field for applying SPHINX with economic extensions is fighting Spam over IP Telephony (SPIT). Spamming activity comes from spammers (who create and send spam), but its effects expand far more, concerning Internet Service Providers (ISP), companies and users (receivers of spam), since all of them are stakeholders of this phenomenon [13].

Every economic actor, major companies, tries to achieve the maximum profit by maximizing sells and minimizing costs. Practically, this means raising the price of product – service and lowering expenses such as marketing that should be relatively low. From the moment that spamming has been used as a marketing method it creates benefits rather than cost. Consequently, spam will rise since as we mentioned before forms rational economic choice – behaviour [14]. The spam-based marketing method is also a little bit of paradox, because we all receive disturbing marketing calls/messages but few are those who admit to have taken into consideration those marketing calls and stepped forward to a buying procedure.

At the same time, we observe the enrichment of the content of spam and coinstantaneously maturation of anti-spam/spit tools-methods [15]. The basic problem is indicated in the limited perception we have in three parameters of value proposition of spam: the cost of spam, counterbalance of conversion rate, namely converting visitors/guests into customer and marginal utility (profit) per selling. Furthermore, as [16] suggests according to the subjective Theory of Value “reasonable people are likely to disagree about what constitutes desirable and undesirable content”.

[17] mentions that spam makes economic essence, though the negligible percentages of responses that achieves, because it can happen, almost at no cost and that is the reason to be included in internet side effects (Net parasites). The parasitic economics of spam means that cost of sending a message is less for sender than for the other parties implicated in the process, meaning transferring to others the cost than to the sender [18]. While spam has no effect on spammers, for all other postulates a loss of time, disturbance, lost resources (e.g. bandwidth) [19]. How much does spam cost is difficult to quantify in terms of bandwidth, time and nuisance [20].

[21] refers that in order to understand the economics of spam we have to examine two models:

1. There only exists one spammer who has many recipients of his spam
2. A user (of email in his paper of VoIP Services for us) receives spam from many spammers and some other calls for us (emails in the paper)

Spam harmfulness is shown by [22] in three major ways by:

1. degrading user experience
2. containing malicious software that, when is executed, could destroy the computing system
3. transferring and discovering waste a significant amount of network and computing resources

[23] from user side, shows that internet users consider spam "objectionable" due to fact that it induce direct cost (security infrastructure) and indirect cost (information overload). The real financial profit of spam is aiming for the cost of sending spam against anti-spam techniques to be less than the return from the negligible response from recipients [24]. Comparably to e-mail spam SPIT network resources might be ten times more loaded and more obtrusive since the phone will ring with every spam call/message, anytime, disrupting users activity [25]. Companies are also unwilling to outsource their security to outside security providers fearing that they might not execute their services in order to shrink costs and increase their profit. In economics this called as moral hazard problem and depicts the disposition of companies to lower efforts as one part will go to capital [26].

[27] clarifies that many organizations evaluate and predict the economic harm of spam but the numerical data are difficult to compare because they include "different types of spam harm, computation methods and make different assumptions about economic data". He furthermore categories cost as "direct" if it is produced by just occurring and "indirect" if the harm is happening from operations or disoperation that result from spam. [28] also indicates that the existence of Spam directly and indirectly damages the economy. Spam damages production function, decreases labour productivity and the level of the GDP (Gross Domestic Product) [29].

4 Conclusion

Economic measures for solving spam mails are solutions that could be suggested and applied for securing VoIP services, which find application in voice CAPTCHA. Aim should be to find a solution that demands the minimum efforts for changing the way we use Internet services. The basic semblance of solving spam or spit comes from comparing the cost of sending mails with the cost of a telephone call [30]. Since a solution (countermeasure) is defined, the hardest part is to analyze whether benefits overcome costs. If the suggested solution is more likely to cause bigger harm than benefits, then in the possibility of market failure or of choosing not to do anything, this might be the wisest choice. Consequently, Cost Benefit Analysis demands considering the effect of economic motives at the same time with possible no intended results.

Economic literature often formulates concerns of regulating accidents as problems of minimizing cost. Accidents end in harm, economical or physical. Prevention and deterrence of accidents also involves cost. In order to solve the problem we need to minimize the sum of accident cost, prevention cost and also management cost (ex. by applying normative or law). For a CAPTCHA solution the problem is similar. Normative border/matrix and institutional framework/structure must minimize the sum of harm cost that caused from security incidents, costs of preventing incidents and costs of management.

Acknowledgements. This work was performed in the framework of the SPHINX (09SYN-72-419) Project, which is partly funded by the Hellenic General Secretariat for Research and technology.

References

1. Anderson, R.: Why information security is hard: An economic perspective. In Proc. of the 17th Annual Computer Security Applications Conference (ACSAC 2001), USA, pp. 358-365 (2001)
2. Zhao, X., Fang, F., Whinston, A.: An economic mechanism for better Internet security. Decision Support Systems 45(4), 811–821 (2008)
3. Motoyama, M., Levchenko, K., Kanich, C., McCoy, D., Voelker, G., Savage, S.: Re: CAPTCHAs - Understanding CAPTCHA-Solving from an Economic Context. In: Proc. of the USENIX Security Symposium, USA (2010)
4. Lai, F., Wang, J., Hsieh, C., Chen, J.: On network externalities, e-business adoption and information asymmetry. Industrial Management & Data Systems 107(5), 728–746 (2007)
5. Bauer, J., van Eeten, M.: Cybersecurity: Stakeholder incentives, externalities, and policy options. Telecommunications Policy 33, 706–719 (2009)
6. Shetty, N., Schwartz, G., Walrand, J.: Can Competitive Insurers Improve Network Security? In: Acquisti, A., Smith, S.W., Sadeghi, A.-R. (eds.) TRUST 2010. LNCS, vol. 6101, pp. 308–322. Springer, Heidelberg (2010)
7. van Eeten, M., Bauer, J.: The economics of malware: security decisions, incentives and externalities, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, DSTI/ICCP/REG, 27, Paris, OECD (2007), http://www.oecd.org/dataoecd/53/17/40722462.pdf
8. Vaknin, S.: The Economics of Spam, http://www.Buzzle.com
9. Prentice, B.: Tangible and intangible benefits of transportation security measures. Journal of Transportation Security 1(1), 3–14 (2008)
10. Ravi, B., Derrick, H., Qing, H.: A System Dynamics Model of Information Security Investments. In: Proc. of the ECIS (2007)
11. Böhme, R., Nowey, T.: Economic Security Metrics. In: Eusgeld, I., Freiling, F.C., Reussner, R. (eds.) Dependability Metrics. LNCS, vol. 4909, pp. 176–187. Springer, Heidelberg (2008)
12. Lelarge, M.: Economics of Malware: Epidemic Risks Model, Network Externalities and Incentives. In: Proc. of the 5th Bi-annual Conference on the Economics of the Software and Internet Industries, France, pp. 1353–1360 (2009)
13. Ridzuan, F., Potdar, V., Talevski, A.: Factors Involved in Estimating Cost of Email Spam. In: Taniar, D., Gervasi, O., Murgante, B., Pardede, E., Apduhan, B.O. (eds.) ICCSA 2010. LNCS, vol. 6017, pp. 383–399. Springer, Heidelberg (2010)
14. Allman, E.: The Economics of Spam. Queue-Distributed Development 1(9), 203–212 (2003)
15. Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G., Paxson, V., Savage, S.: Spamalytics: An Empirical Analysis of Spam Marketing Conversion. In: Proc. of the 15th ACM Conference on Computer and Communications Security (CCS), USA, pp. 27–31 (2008)
16. Kimakova, A., Rajabiun, R.: The Dangerous Economics of Spam Control. In: Proc. of the MIT Spam Conference, USA (2008)

17. Leyden, J.: The economics of spam, the register (2003), http://www.theregister.co.uk/2003/11/18/the_economics_of_spam/
18. Cobb, S.: The Economics of Spam. Technical Report (2003)
19. Petur, J.: The economics of spam and the context and aftermath of the CAN-SPAM Act of 2003. International Journal of Liability and Scientific Enquiry 2(1), 40–52 (2008)
20. Minto, R.: The economics of spam, Financial Times Tech Blog: Industry analysis (2008), http://blogs.ft.com/techblog/2008/11/the-economics-of-spam
21. Khong, D.: An economic analysis of SPAM law. Erasmus Law and Economics Review 1(1), 23–45 (2004)
22. Jia, D.: Cost-Effective Spam Detection in P2P File-Sharing Systems. In: Proc. of the 2008 ACM Workshop on Large-Scale Distributed Systems for Information Retrieval (LSDS-IR 2008), USA, pp. 19–26 (2008)
23. Plice, R., Pavlov, O., Melville, N.: Spam and Beyond: An Information-Economic Analysis of Unwanted Commercial Messages. Journal of Organizational Computing and Electronic Commerce 18(4), 278–306 (2008)
24. Chim, H.: To Build a Blocklist Based on the Cost of Spam. In: Deng, X., Ye, Y. (eds.) WINE 2005. LNCS, vol. 3828, pp. 510–519. Springer, Heidelberg (2005)
25. Quinten, V.M., van de Meent, R., Pras, A.: Analysis of Techniques for Protection Against Spam over Internet Telephony. In: Pras, A., van Sinderen, M. (eds.) EUNICE 2007. LNCS, vol. 4606, pp. 70–77. Springer, Heidelberg (2007)
26. Ding, W., Yurcik, W., Yin, X.: Outsourcing Internet Security: Economic Analysis of Incentives for Managed Security Service Providers. In: Deng, X., Ye, Y. (eds.) WINE 2005. LNCS, vol. 3828, pp. 947–958. Springer, Heidelberg (2005)
27. Schryen, G.: Spam and its economic significance. In: Anti-Spam Measures Analysis and Design, pp. 7–27 (2007)
28. Takemura, T., Ebara, H.: Spam Mail Reduces Economic Effects. In: Berntzen, L. (ed.) Proc. of the 2nd International Conference on Digital Society (ICDS), France, pp. 20–24 (2008)
29. Ukai, Y., Takemura, T.: Spam Mails Impede Economic Growth. Rev. Socionetwork Strat. 1, 14–22 (2007)
30. Nakulas, A., Ekonomou, L., Kourtesi, S., Fotis, G., Zoulias, E.: A Review of Techniques to Counter Spam and Spit. In: Mastorakis, N., et al. (eds.) Proc. of the European Computing Conference. LNEE, vol. 27, pp. 501–510. Springer science+Business media, LLC (2009)