Economic assessment of externalities for interactive audio media anti-SPIT protection of internet services

Theodosios Tsiakis*

Department of Marketing,
Technological Educational Institute of Thessaloniki,
P.O. 141, 57400, Sindos, Thessaloniki, Greece
E-mail: tsiakis@mkt.teithe.gr
*Corresponding author

Panagiotis Katsaros

Department of Informatics,
Aristotle University of Thessaloniki,
Aristotle University Campus,
54124 Thessaloniki, Greece
E-mail: katsaros@csd.auth.gr

Dimitris Gritzalis

Department of Informatics,
Athens University of Economics and Business,
6 Papaflessa St., Dasos-Haidari,
GR-12462, Athens, Greece
E-mail: dgrit@aueb.gr

Abstract: Spam over internet telephony (SPIT) refers to all unsolicited and massive scale attempts to establish voice communication with oblivious users of voice over internet protocol (VoIP) services. SPIT exhibits a significant increase over the last years, thus developing into a serious threat with adverse impact and costs for the business economy. An audio completely automated public Turing test to tell computers and human apart (CAPTCHA) has been introduced as a means to distinguish automated software agents (bots) from human. CAPTCHA has been proposed as a security measure against SPIT. In this paper, we lay the principles for an adequate understanding of the SPAM-related economic models, as well as their analogies to the SPIT phenomenon, so as to weigh the benefits of audio CAPTCHA protection against the incurred costs. Our approach is based on the economic assessment of externalities, i.e., the economic impact associated with the SPIT side effects on the everyday life.

Keywords: security economics; spam over internet telephony; SPIT; CAPTCHA; voice over internet protocol; VoIP; externalities.

Reference to this paper should be made as follows: Tsiakis, T., Katsaros, P. and Gritzalis, D. (2012) 'Economic assessment of externalities for interactive audio media anti-SPIT protection of internet services', *Int. J. Electronic Security and Digital Forensics*, Vol. 4, Nos. 2/3, pp.164–177.

Biographical notes: Theodosios Tsiakis is a Lecturer of Management of Information Systems in the Department of Marketing at the School of Management and Economy of the Alexandrian Technological Educational Institute of Thessaloniki. He holds a PhD in Information Security Economics from the Department of Applied Informatics of the University of Macedonia, in Thessaloniki, Greece. His research interests include information security economics, risk, trust and human factors. He has published numerous articles in international journals and conference proceedings in the aforementioned areas and in the broader area of management of information systems.

Panagiotis Katsaros is an Assistant Professor of Computer Science in the Department of Informatics of the Aristotle University of Thessaloniki (AUTh) in Greece. He holds a Diploma in Mathematics and PhD in Computer Science from AUTh, as well as a Master of Science in Software Engineering from the University of Aston in Birmingham, UK. He has published one book and more than 50 research articles in international journals and conference proceedings, in the areas of dependability and security, formal methods and software engineering.

Dimitris Gritzalis is a Professor of ICT Security and the Director of the Information Security and Critical Infrastructure Protection Research Group (http://www.cis.aueb.gr) with the Department of Informatics of the Athens University of Economics and Business. He has served as Associate Commissioner of the Greek Data Protection Commission and as the President of the Greek Computer Society. He is the Representative of Greece to IFIP TC-11. His technical publications include nine books and more than 150 papers. His current research interests focus on security in ambient intelligence, new security paradigms, critical infrastructure protection, and strategies for security-critical infrastructures.

This paper is a revised and expanded version of a paper entitled ‘Economic evaluation of interactive audio media for securing internet services’ 7th International Conference in Global Security, Safety and Sustainability (ICGS3) and 4th International Conference on e-Democracy, Thessaloniki, Greece, 24–26 August 2011.

1 Introduction

We view the internet as an ecosystem of economic agents characterised by monetary incentives with complex interdependencies (Zhao et al., 2008). From this perspective, technology developments to confront security threats for providing robust internet Services should take into account the economic implications of their design at the technical level (Anderson, 2001).

According to CSI’s 2010 Computer Crime and Security Survey, the second most expensive type of security incidents involved some bot, i.e., a malicious software repeating tasks at a much higher rate than would be possible for a human alone. Bots are used to infect as many vulnerable computers as needed for launching massive-scale attacks against internet services and resources, thus developing the so-called botnets.

A widely deployed countermeasure for protecting internet services and resources is a completely automated public Turing test to tell computers and humans apart

(CAPTCHA) test. CAPTCHA is a reverse-Turing test, or else a challenge-response test, aiming at ensuring that the response to a given challenge is not generated by a computer. CAPTCHA involve a server generating requests to the users to complete tests that are automatically selected and graded, while they are supposed not to be able to be solved by non-human agents. However, a number of CAPTCHA generation mechanisms have been successfully broken by bots.

Audio CAPTCHAs for countering spam over internet telephony (SPIT) are considered more robust from their ordinary counterparts that are mainly used for the protection of other internet services. Audio CAPTCHAs is a relatively new technology and any new technology according to Newell (2004) evolves through the following stages:

a invention, i.e., conception of a new idea

b innovations, i.e., new products are brought to the market

c diffusion, i.e., new products are gradually adopted.

In this cycle, the economic perspective of the technology being developed plays a fundamental role towards its adoption. With respect to this paper's technology focus, it is worth to note the claim of Motoyama et al. (2010), saying that if someone can employ workers for solving CAPTCHA with wages no more than 0.5$ for 1,000 solved tests, it is then possible to economically solve the CAPTCHA.

We elaborate the economic aspects of the spam phenomenon and their analogies to the SPIT threat based on the assessment of the externalities impact, which includes all side effects on the business economy and the everyday life. Our approach sets the foundation towards the development of appropriate economic models for the cost effectiveness of an audio CAPTCHA protection as a means for countering SPIT.

The rest of this paper is organised as follows: In Section 2, we introduce the security economics framework that we consider suitable for evaluating the economic implications of SPIT and the effects of the CAPTCHA countermeasure. In Section 3, we build on the aforementioned framework so as to review the related economic models and to subsequently introduce an externalities assessment approach for evaluating the cost-effectiveness of the audio CAPTCHA anti-SPIT approach. This 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 (individuals) and the society decide to allocate their scarce resources among alternative uses, in order to produce goods and services and maximise the gains. Goods are the produced consumable items that increase the well-being of an individual and services are the non-material equivalent. Both are referred to as products, due to their availability for consumption within the frame of some market process. A good can be public, meaning that it can be consumed by more than one consumer or, alternatively, private, where consumption by one person prevents consumption by another. All goods can be categorised as shown in Table 1.

Table 1 Categories of goods produced in economic systems

	Non-rivalrous	*Rivalrous*
Non-excludable	(Pure) public goods	Common-pool resources
Excludable	Club goods	Private goods

Public goods are characterised as non-rival and non-exclusive. The former means that goods consumption by an increasing number of persons does not reduce anyone else's enjoyment of the good. The latter means that, once the good is available, non-payers cannot be prevented from using and benefiting from it. A public good does not necessarily mean that the good is provided by the government. Electricity is a public good, which is not always provided by a government. Private goods are characterised as rival and excludable. When consumption is non-rivalrous but excludable, we refer to club goods. An example is a road with tolls. Rivalrous consumption but non-excludable is a characteristic of the so-called common-pool resources.

Systems security is a non-rival and non-excludable good, as it is a good that everyone may enjoy, while at the same time is hardly possible to exclude one from benefiting from it. Therefore, systems security is classified as a public good.

Economic analyses are mainly based on market incentives. According to this perspective, the market allocates resources without the government interfering to the business process itself, apart from setting the legal framework that regulates the market. There are three basic governmental instruments:

a social norms and common values

b control and commands

c market incentives and rules (also known as economic incentives).

Economic incentives refer to the external factors determining production or consumption individual decisions, whatever the economic unit consists of. In van Eeten and Bauer (2009), it is argued that security can be better understood in terms of the outcomes of incentive structures, rather than in terms of the technological problem itself.

Security failures – and specifically internet security incidents – are caused by economic incentives that stem from private costs and benefits as they are comprehended by the actors involved in security-related decisions (Segura and Lahuerta, 2010). We distinguish the positive economics from the normative economics. Positive economics attempt, with scientific and objective epexegesis, to attribute how the economy works (e.g., imposition of taxes causes an increase in product prices). Normative economics 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).

Economic organisations (including those in the technological sector) develop attitudes that set them in risks carried over economy. This diffusion of risk from economic organisation to economic organisation, and from economic sector to economic sector, deregulate economics related to externalities. Externalities are side-effects that arise when actions of a person affect the well-being of another person. In economics, we are interested in actions that in here a value. In a transaction process such actions are translated into expenses that do not charge diametrically only the people related to the actions, but they also charge people that are not directly related to them. Decisions of

production or consumption that a person takes have an impact on the production or consumption of other persons. Positive externality refers to the benefit that people derive from a market operation in which they do not participate. Negative externality is the damage obtained and not recompensed for the people that do not participate in the production or consumption process.

Let us consider that a college campus is to be created in a city. The value of the area of the college neighbourhood will increase, as it is upgraded. As a result, this causes a positive externality. On the contrary, if a city dump is created, then the value of that area will decrease, due to the fact that it causes damnification that cannot be claimed (Bauer and van Eeten, 2009; Lai et al., 2007).

Direct network externalities exist in certain goods and services, like telephone and computing systems that become more valuable to a user, as the number of users increases. Indirect network externalities exist when the utility of a product/service increases with an increasing availability of compatible complementary products.

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 are represented by an ascending function of the number of other users and vice versa negative externality when the benefits are a descending function of the number of other users. Network externalities are a kind of chicken-and-egg problem, because in the contemporary broadband environment the service demand is dependent on the infrastructure, and vice-versa (Woodside, 2007).

Security is characterised by positive externality. If I take measures at a personal level, I also support and invigorate security for others, while protecting myself. This discernment broaches the subject of a free rider problem as one of the classical cases of market imperfection or failure. Users and individuals are not willing to apply security measures and policies, expecting from others to act or relying on others to assure their social welfare. Users are only partially involved in security investments, as they do not carry the real social cost of their actions, which cause negative externality (Shetty et al., 2010; van Eeten and Bauer, 2009). This finding reveals the market failure cause and necessitates public intervention through regulations (Vaknin, 2011). The types of externalities for a security system are not known a priori. Therefore, they cannot be designated before the deployment of security (Abbas et al., 2010). Furthermore, negative externalities of security measures can take different forms such as:

a disrupting availability of security services

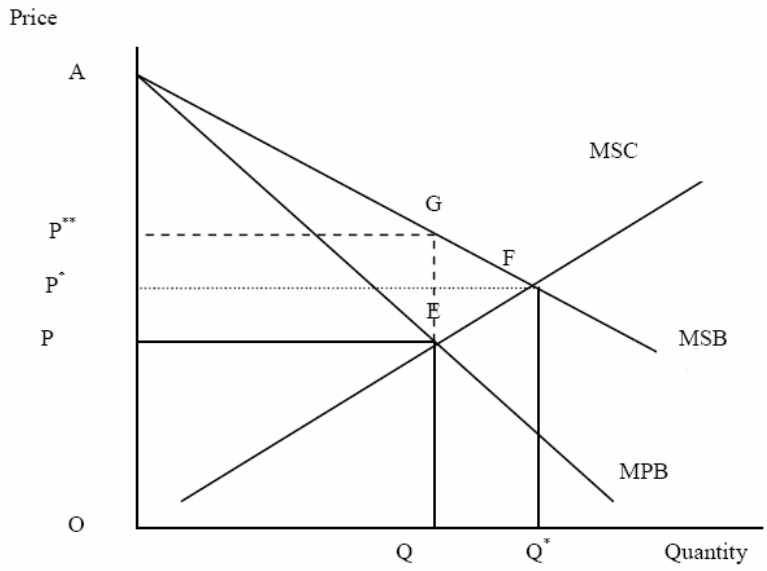
b security mechanisms that can malfunction

c security measures violating other concerns, such as privacy.

In Prentice (2008), the author describes the security process in transportation. They refer to the positive externality for non-users of transportation services, as well as to the aforementioned free rider problem. As shown in Figure 1, security is described in terms of marginal social benefits (MSB), payments for services are described as marginal social costs (MSC), while marginal private benefits (MPB) are also taken into account. The societal optimum occurs where MSB = MSC (we 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 a price P*. Point F requires government expenditure

to supply the needed quantity (level) of security (Q* – Q), while private sector supplies only Q units.

Figure 1 Economic model of social benefits and costs



But what is the economic reason for such a plethora of security threats? In general, software companies are not economically motivated for adequate investments in software security. From their side, the customers are primarily concerned for the price and the special benefits/characteristics. Hereupon, if a developer invests resources in software security, his work is characterised by an increased production cost and the result will need a longer time period to circulate. Thus, it is possible for another developer to win the market by circulating, sooner and faster, products that may be rich in characteristics but not secure enough. Losses from security incidents emerge from inefficient security measures, human errors, frauds, system failures, exogenous factors (economical, technical), etc. They 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, human hypostasis, etc.

Economic analysis is the base for budgeting expenses (investments) in security measures. Economic evaluation of security methods is necessary for the rationalisation of budgeting and the financing of security actions. An important direction of research aims to develop practical methods for analysing, determining and quantifying the optimal level of security investments, in terms of "what should be implemented, how much it would cost and what would be the gain"?

Metrics for security economics refer to how efficient a security measure is. The most well-known metrics are used in risk management and in economic/managerial evaluation of security investments (Bohme and Nowey, 2008; Ravi et al., 2007). They include the annual loss expectancy (ALE), the return on security investment (ROSI), the net present value (NPV), and the internal rate of return (IRR).

A second line of research in security economics builds on established methods of the classic economic theory, such as the method of efficient market hypothesis. According to this theory, every stakeholder should try to maximise utility and have orthological expectations, in order to emerge optimal investments that will be possible to escalate when new information arises. Investments are classified into two key categories. Ex ante approaches aim to determine what a firm intends to invest (total expenditure per investment plan). They involve a decision for whether to invest in a security measure or not, in which case the investor should choose the best alternative solution from the available ones. Ex post approaches are based on analysing and measuring the past performance of investments (return achieved).

On the other side, insecurity is perceived as a formal non-quantitative form of risk. There are several sources of such a risk, with many of them lying with the economy. Insecurity causes cost to the people and to investors who are risk averse. The economic theory reveals that agents who abominate the risk prefer a less insecure economic environment and are willing to pay insurance, in order to limit the risk (Lelarge, 2009). Security measures/policies and security financing are characterised by the economic trade-offs shown in Table 2 (Brück, 2005).

Table 2 Economic tradeoffs for security investments

Security spending versus other spending	Expenditures concerning security-related versus other goods and services by both the public (government) and private sector.
Security versus efficiency	Economic efficiency is achieved if the highest possible level of production and therefore satisfaction is obtained from a given set of resources and technologies. Technological (security) efficiency relates quantities of inputs to the quantity of outputs, while economic efficiency relates the monetary value of inputs to the monetary value of output.
Security versus technological change	The structural change of open economies due to technological change (e.g., openness of internet) sets new rules – regulations (following technical standards as ISO).
Security versus equity	It is not clear in on hand who should pay more for security and on the other hand which group of people gain or lose most from higher security (e.g., IT security products/services are provided by highly skilled, while on opposite simple security solutions are provided by the low skilled).
Security versus freedom and privacy	Maintain the stability of freedom, rights, privacy against the need to grand more security. IT infrastructures (internet, computers, and mobiles) are vulnerable to security attacks and in parallel these infrastructures can be used to control individuals or goods.

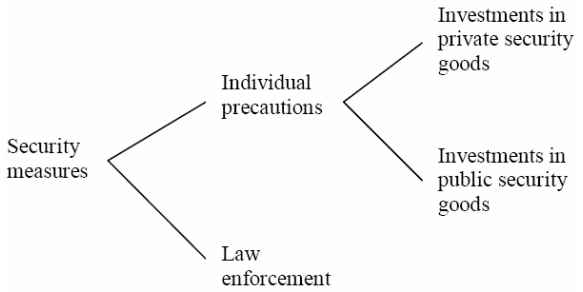
Security measures in the form of precautions can be categorised in two main forms (Majuca, 2006):

a investments in private security goods (e.g., purchase of firewalls, anti-virus, etc.)

b investments in public security goods (e.g., creating state-of-the-art mechanisms for security incidents, etc.).

The model shown in Figure 2 suggests that there must be a combination of individual-private investments by end-users and ISP taking measures with both private and public security goods, as well as the public enforcement of law.

Figure 2 Security measures and investments in private and public goods



3 Spam economics

Spamming activities affect internet service providers (ISP), companies and end-users (receivers of spam) (Ridzuan et al., 2010). Every economic actor tries to achieve the maximum profit by optimising sells and minimising costs. Practically, this can be achieved by raising the price of a product-service and lowering expenses. From the moment that spamming has been used as a marketing method, it creates benefits rather than cost. Therefore, spam is expected to rise, as it forms a rational economic choice and behaviour (Allman, 2003). The spam-based marketing method is a kind of paradox, because we all receive disturbing marketing calls/messages but few are those who admit having taken them into consideration and having stepped forward to a buying procedure. At the same time, we observe the enrichment of the spam content and co-instantaneously a maturation of anti-spam/spit tools and methods (Kanich et al., 2008). The basic problem lies with the limited perception that we have for three parameters of the value proposition of spam, namely:

a the cost of spam

b the counterbalance of conversion rate focused on how to convert visitors/guests into customer

c the marginal utility (profit) per selling.

Furthermore, as suggested in Kimakova and Rajabiun (2008) and according to the subjective theory of value, "reasonable people are likely to disagree about what constitutes desirable and undesirable content".

In Leyden (2003), the authors argue that spam has an economic essence despite the negligible percentages of responses that achieves, because it can happen at almost no cost and this is why it has been included in the internet side effects (net parasites). The parasitic economics of spam means that the cost of sending a message is less for the sender than for the other parties implicated in the process. Spam has no visible effect on spammers, whereas for all other postulates a loss of time, disturbance, and waste of resources (Petur, 2008) thus transferring to the others the cost rather than to the sender (Cobb, 2003). However, it is not easy to quantify how much the spam costs, in terms of bandwidth, time, and nuisance (Minto, 2008). In Khong (2004), the authors suggest that in order to understand the economics of spam, we have to examine two different models:

a The one where there is only one spammer with many recipients

b the one where a user receives spam from many spammers.

Spam causes harm (Jia, 2008) by:

a degrading user experience

b containing malicious software

c wasting a significant amount of network and computing resources.

In Plice et al. (2008), it is showed that internet users consider spam 'objectionable', due to the fact that it induces direct cost (security infrastructure) and indirect cost (information overload). Spam is mainly fought by two parties (van Eeten and Bauer, 2009). The first refers to all end-users and includes:

1 large businesses with 250 or more employees

2 small and medium enterprise – SMEs with fewer than 250 employees

3 individual end-users.

The second party refers to the ISPs and includes all kinds of providers that offer access to the internet for individuals and organisations.

Due to the fact that improving the end-user security beyond a certain level is exceptionally difficult and costly, the focus is shifted to the other part of the ecosystem, i.e., the ISP. ISP efforts focus on:

1 costs for customer support and abuse management

2 costs of blacklisting

3 costs of brand damage and reputation effects

4 costs of infrastructure expansion

5 benefits of maintaining reciprocity

6 costs of security measures

7 legal risks and constraints

8 cost of customer acquisition

9 an overall assessment.

The first five are incentives that support the benefits of security. The following four are disincentives in the form of costs of additional security measures.

The real financial profit from spamming comes when the cost of sending spam despite existing anti-spam protection is less than the return from the negligible response from the recipients (Hung, 2005). Comparably to e-mail spam, SPIT network resources might be ten times more loaded and more obtrusive, as the phone will ring with every spam call/message, anytime, disrupting user's activity (Quinten et al., 2007). Companies are also unwilling to outsource their security to security providers, fearing that they might not execute their services so as to limit costs and increase their profit. In economics, this is called a moral hazard problem and depicts the disposition of companies to lower efforts as one part will go to capital (Ding et al., 2005).

In Schryen (2007), it is reported that many organisations evaluate and predict the economic harm of spam. However, the numerical data are difficult to compare because they include "different types of spam harm, computation methods, and make different assumptions about economic data". Moreover, the cost is categorised as 'direct', if it is produced by just occurring, and 'indirect', if the harm is happening from operations or disoperation that result from spam. In Takemura and Ebara (2008), it is reported that spamming causes damages to the economy, as it affects the production function and decreases labour productivity and the level of the gross domestic product (GDP) (Ukai and Takemura, 2007).

4 Economic defence modelling

Voice over internet protocol (VoIP) consists a technology that is being rapidly deployed, servicing as an economically viable alternative\substitute to traditional PSTN telephony services. This lays out that supporting and securing VoIP system is both vital and challenging.

Everyone is familiar with the idea that there's no such thing as 'perfect' security. Large amounts of time and resources capacitate hacker to eliminate most of security measures. An economic framework allows focusing on the incentives of the security game actors as economic incentives shape decisions of security players. But even if show prejudice in and good faith in a certain security mechanism, it is very difficult to measure the effectiveness of a defensive measure. The key point is that CAPTCHA as a technical countermeasure might not be adequate for securing spam, as cheap\low-cost human labour can solve 1,000 CAPTCHAs for $0.5, but CAPTCHA raise a certain economic barrier to entry and create economic disincentives for any online prospective deceiver wiling to abuse online services that are protected by CAPTCHA. A solution for spam must address the problem that spam is information pollution (externality). This insight gives us ascendancy as there are already market-based or incentive-based instruments\mechanisms (including technological, regulatory and market-based standards and approaches).

So what we need is to find and establish a pragmatic approach for the systematic identification, quantification, measurement and reporting of the actual costs of SPIT. Towards this aim, we adopt from environmental economics the impact pathway method-analysis and adapt it in the frame of security economics. Developed by the ExternE community for accounting all externalities in a consistent way when making decisions (Friedrich and Bickel, 2001), this method:

a identifies specific impact pathways

b quantifies impacts by taking into consideration the sensitivity of receptors

c monetises them.

The method (Figure 3) maps the pathway running from an emission to the damage of people or ecosystems (Mensink et al., 2007).

The first stage of the method refers to the assessment procedure of the calculation of emissions (spam volume) resulting from a transport (call) activity. The second stage refers to the dispersion of chemical reactions – transportation of emission – from

pollutants (meaning the false negative for our model). Then concentrations are translated into impacts through dose-response relationships and the final stage concerns the economic valuation of the damages in terms of money or estimated values that have been previously quantified. Each stage requires an intense analysis for valuing. The cost is calculated by multiplying the four stages:

a the emission factor

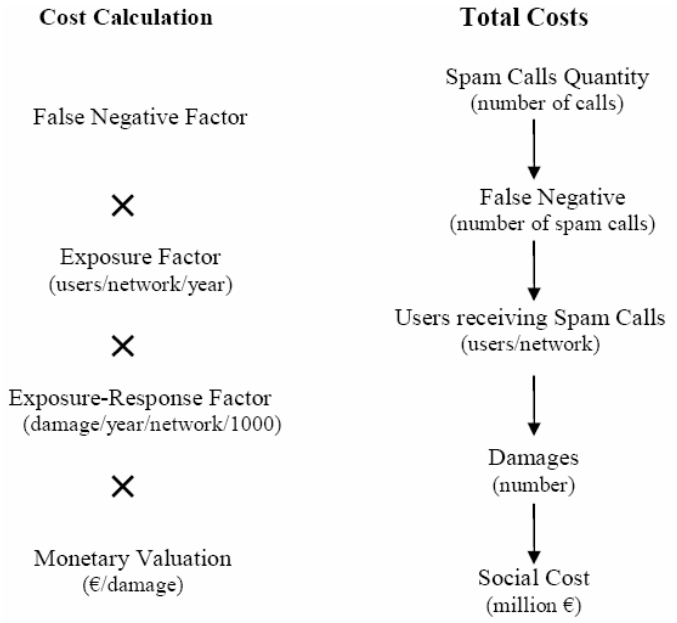
b the exposure factor

c the exposure-response factor

d the monetary valuation of the damage (the response).

Partially, exposure factor and exposure-response factor can be included in one factor (the dose-response factor). In Figure 3, the left part shows how the cost per spam call is calculated in terms of the four mentioned factors and the right part indicates the operationalised chain (system scope).

Figure 3 Impact pathway method for quantifying SPIT activity costs



5 Conclusions

Economic measures for fighting SPIT should not change the way we use internet services. The basic semblance of fighting SPIT comes from comparing the cost of sending mails with the cost of a telephone call (Nakulas et al., 2009). After a solution (countermeasure) is defined, the real (and often the hardest) part is to analyse whether benefits overcome costs. If the suggested solution is likely to cause bigger harm than benefits, then in the possibility of market failure, or of choosing not to do anything, this

might be a wise choice. Consequently, cost benefit analysis should consider the effect of economic motives at the same time with possible no intended results.

Accidents end in harm, economical or physical. Prevention and deterrence of accidents also involves cost. In order to solve the problem, we need to minimise the sum of accident cost, prevention cost, and management cost (e.g., by applying normative or legal measures). Externalities are social costs that are not carried by the private costs and prices of market goods/services. It is element to establish a policy to consider and reduce the social costs that system generates either by regulating such operations, or by imposing high economic penalties, or both.

The main challenge is to associate economic valuation with SPIT data in a proper way. We propose the impact pathway approach as a pragmatic method in the area of information security economics. For a CAPTCHA solution, the problem is similar. Normative border/matrix and institutional framework/structure must minimise 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

Abbas, H., Magnusson, C., Yngström, L. and Hemani, A. (2010) 'A structured approach for internalizing externalities caused by IT security mechanisms', in *Proc. of the 2nd International Workshop on Education Technology and Computer Science*, pp.149–153.

Allman, E. (2003) 'The economics of spam', *Queue-Distributed Development*, Vol. 1, No. 9, pp.203–212.

Anderson, R. (2001) 'Why information security is hard: an economic perspective', in *Proc. of the 17th Annual Computer Security Applications Conference (ACSAC 2001)*, USA, pp.358–365.

Bauer, J. and van Eeten, M. (2009) 'Cybersecurity: stakeholder incentives, externalities, and policy options', *Telecommunications Policy*, Vol. 33, Nos. 10–11, pp.706–719.

Bohme, R. and Nowey, T. (2008) 'Economic security metrics', in *Proc. of the Dependability Metrics, LNCS*, Vol. 4909, LNCS 4909, pp.176–187.

Brück, T. (2005) 'An economic analysis of security policies', *Defence and Peace Economics*, Vol. 16, No. 5, pp.375–389.

Cobb, S. (2003) 'The economics of spam', Technical report.

Ding, W., Yurcik, W. and Yin, X. (2005) 'Outsourcing internet security: economic analysis of incentives for managed security service providers', in *Proc. of the 1st Workshop on Internet and Network Economics (WINE)*, China, pp.947–958.

Friedrich, R. and Bickel, P. (2001) *Environmental External Costs of Transport*, Springer-Verlag, Berlin.

Hung, C. (2005) 'To build a blocklist based on the cost of spam', in *Proc. of the 1st Workshop on Internet and Network Economics (WINE)*, China, pp.510–519.

Jia, D. (2008) 'Cost-effective spam detection in P2P file-sharing systems', in *Proc. of the ACM Workshop on Large-Scale Distributed Systems for Information Retrieval (LSDS-IR)*, USA, pp.19–26.

Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G., Paxson, V. and Savage, S. (2008) '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.

Khong, D. (2004) 'An economic analysis of SPAM law', *Erasmus Law and Economics Review*, Vol. 1, No. 1, pp.23–45.

Kimakova, A. and Rajabiun, R. (2008) 'The dangerous economics of spam control', in *Proc. of the MIT Spam Conference*, USA.

Lai, F., Wang, J., Hsieh, C. and Chen, J. (2007) 'On network externalities, e-business adoption and information asymmetry', *Industrial Management & Data Systems*, Vol. 107, No. 5, pp.728–746.

Lelarge, M. (2009) '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.

Leyden, J. (2003) 'The economics of spam', available at http://www.theregister.co.uk/2003/11/18/the_economics_of_spam/ (accessed on 11 June 2011).

Majuca, R. (2006) 'Public goods and externalities aspects of internet security: modelling the spill-over effects of interrelated risks and solutions', in *Proc. of the TPRC Conference.*

Mensink, C., De Nocker, L. and De Ridder, K. (2007) 'Integrated assessment modelling: Applications of the impact pathway methodology', in Ebel, A. et al. (Eds.): *Air, Water and Soil Quality Modelling for Risk and Impact Assessment*, NATO Security through Science Series, Springer, Netherlands, pp.67–82.

Minto, R. (2008) 'The economics of spam', *Financial Times Tech Blog Industry Analysis*, available at http://blogs.ft.com/techblog/2008/11/the-economics-of-spam (accessed on 7 May 2011)

Motoyama, M., Levchenko, K., Kanich, C., McCoy, D., Voelker, G. and Savage, S. (2010) 'Re: CAPTCHAs – understanding CAPTCHA-solving from an economic context', in *Proc. of the USENIX Security Symposium*, USA.

Nakulas, A., Ekonomou, L., Kourtesi, S., Fotis, G. and Zoulias, E. (2009) 'A review of techniques to counter spam and spit', in *Proc. of the European Computing Conference, Lecture Notes in Electrical Engineering*, Vol. 27, No. 6, pp.501–510.

Newell, R. (2004) 'Energy efficiency challenges and policies', *in Proc. of the 10-50 Solution: Technologies and Policies for a Low-Carbon Future*.

Petur, J. (2008) 'The economics of spam and the context and aftermath of the CAN-SPAM Act of 2003', *International Journal of Liability and Scientific Enquiry*, Vol. 2, No. 1, pp.40–52.

Plice, R., Pavlov, O. and Melville, N. (2008) 'Spam and beyond: an information-economic analysis of unwanted commercial messages', *Journal of Organizational Computing and Electronic Commerce*, Vol. 18, No. 4, pp.278–306.

Prentice, B. (2008) 'Tangible and intangible benefits of transportation security measures', *Journal of Transportation Security*, Vol. 1, No. 1, pp.3–14.

Quinten, V., van de Meent, R. and Pras, A. (2007) 'Analysis of techniques for protection against spam over internet telephony', in *Proc. of the 13th Open European Summer School and IFIP TC6.6 Workshop (EUNICE)*, Netherlands, pp.70–77.

Ravi, B., Derrick, H. and Qing, H. (2007) 'A system dynamics model of information security investments', in *Proc. of the ECIS.*

Ridzuan, F., Potdar, V. and Talevski, A. (2010) 'Factors involved in estimating cost of email spam', in *Proc. of the International Conference on Computational Science and its Applications (ICCSA)*, Japan, pp.383–399.

Schryen, G. (2007) *Anti-Spam Measures Analysis and Design*, Springer, USA.

Segura, V. and Lahuerta, J. (2010) 'Modelling the economic incentives of DDoS attacks: Femtocell case study', in Moore, T. et al. (Eds.): *Economics of Information Security and Privacy*, pp.107–119, Springer, UK.

Shetty, N., Schwartz, G. and Walrand, J. (2010) 'Can competitive insurers improve network security', in *Proc. of the 3rd International Conference on Trust and Trustworthy Computing (TRUST)*.

Takemura, T. and Ebara, H. (2008) 'Spam mail reduces economic effects', in in Berntzen, L. (Ed.): *Proc. of the 2nd International Conference on Digital Society (ICDS)*, pp.20–24, France.

Ukai, Y. and Takemura, T. (2007) 'Spam mails impede economic growth', *The Review of Socionetwork Strategies*, Vol. 1, No, 1, pp.14–22.

Vaknin, S. (2011) 'The economics of spam', available at http://www.Buzzle.com (accessed on 23 May 2011).

van Eeten, M. and Bauer, J. (2008) '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(2007)27, Paris, OECD, available at http://www.oecd.org/dataoecd/53/17/40722462.pdf (accessed on 16 May 2011).

van Eeten, M. and Bauer, J. (2009) 'Emerging threats to internet security incentives, externalities and policy implication', *Journal of Contingencies and Crisis Management*, Vol. 17, No. 4, pp.221–232.

Woodside, J. (2007) 'Economic externalities of health information technology, a game theoretic model for electronic health record adoption', *Journal of Healthcare Information Management*, Vol. 21, No. 4, pp.25–31.

Zhao, X., Fang, F. and Whinston, A. (2008) 'An economic mechanism for better internet security', *Decision Support Systems*, Vol. 45, No. 4, pp.811–821.