Information Security and Economics in Computer Networks: An Interdisciplinary Survey and a Proposal of Integrated Optimization of Investment

Kanta Matsuura*

Institute of Industrial Science, University of Tokyo (Japan)

Abstract

When we take part in economic activities (e.g. e-commerce) over an open computer network, we need information-security technologies. On the other hand, applied cryptography also needs economic approaches; a lot of security breaches occur due to economically insufficient incentive and the resultant mismanagement. Many users may feel uneasy about financial uncertainty of security threats. Information-security management is closely related with financial decision making.

In response to the bi-directional relevance, cryptographers have recently noticed the importance of studying interdisciplinary area between information security and economics. This paper firstly shows a survey on the emerging area, as well as statistics in the two apparently most relevant international conferences. After that, as an example that is highly related to computational economics, an integrated optimization of investment in information security and financial insurance is proposed. The author claims that the area involves good research subjects in computational economics.

Key words: information security, e-commerce, optimum investment, insurance.

1 Introduction

When we take part in economic activities (e.g. e-commerce) over an open computer network, we need information-security technologies. A good example is Secure Electronic Transaction (SET) for on-line use of credit cards; in the SET Specification Books[1]–[3], we can see how significant the role of information-security technologies is.

Correspondence to: Prof. K. Matsuura, Institute of Industrial Science, University of Tokyo, Komaba 4-6-1, Meguro-ku, Tokyo 153-8505, JAPAN. Tel.: +81-3-5452-6284, Fax.: +81-3-5452-6285, E-mail: kanta@iis.u-tokyo.ac.jp

On the other hand, applied cryptography also needs economic approaches; a lot of security breaches occur due to economically insufficient incentive and the resultant mismanagement[4], [5]. Many users may feel uneasy about financial uncertainty of security threats. Information-security management is closely related with financial decision making[6].

In response to the bi-directional relevance, cryptographers have recently noticed the importance of studying interdisciplinary area between information security and economics. For instance, the author started a series of studies on financial risk management in crypto-based networks in early 2001[7]–[12]. And then, in May 2002, the First Workshop on Economics and Information Security was held at University of California, Barkeley [13], [14]. They decided to have the second workshop in a more formal way.

This paper firstly shows a survey on the emerging area, as well as statistics in the two apparently most relevant international conferences, in Section 2. After that, as an example that is highly related to computational economics, an integrated optimization of investment in information security and financial insurance is proposed in Section 3. Finally Section 4 concludes the paper.

2 Information Security and Economics

2.1 Taxonomy

I categorize the interdisciplinary area into the following seven sub-areas. The first three might seem to have no direct relation with economics but I do not omit them here because they are necessary when we see the trends in related conferences.

2.1.1 Primitives

We can find cryptographic primitives whose major applications are economic activities (e.g. e-commerce) over an open computer network. A typical example is blind signature[15], [16]. In lots of digital-cash systems, anonymity is achieved by using blind signature; a bank can generate its digital signature on a digital coin without seeing the recipient information.

Although this category seems a bit far from economics, a famous international conference, Financial Cryptography, accommodates a lot of papers on cryptographic primitives[17].

2.1.2 Protocols

More close to economics are cryptographic protocols for secure digital cash and electronic transactions [16], [18], [19], on-line auction[20]–[23], and digital tickets[24]. Some of them strongly rely on existing financial/transaction infrastructure such as credit-card networks, while others do not.

We have to say that another type of cryptographic protocol is required for achieving economically desirable social systems. For example, an empirical study in network

economics[25] shows that cost sharing through usage-sensitive pricing is effective for managing Internet growth. This charging policy needs a support by cryptographically-secure audit-log protocols [26]–[31]. Without the cryptographic protocols, no one can verify the integrity of log entries in order to solve possible dispute settlement.

2.1.3 Enhancing Circulation

In order to enhance the market of digital objects, we need mechanisms which protect digital rights with respect to digital contents and softwares[32]–[36]; as a total system, Digital Rights Management (DRM) enables an electronic marketplace where previously unimaginable/impossible business models can be designed and implemented.

Social-scientific analysis and optimization of digital-right management systems are important as well[37], [38]. Discussion in this respect brings a lot of open problems mainly due to

- immature study on the mechanism and effects of monopoly related to digital copyright protection

and

- the ongoing fragmentation of intellectual property rights.

2.1.4 Modeling

In information-security management, a difficult task is to find good measures of security, vulnerability, and related properties; (i) the value of the protected information, (ii) the threat to that information, and (iii) the assurance level are extremely important to quantify[39]. Therefore, how to price information-security service is an important and difficult task.

When we tackle those problems, it is worth trying to study modeling based on economic approaches. For example, financial cost required for successful attacks could be used as a good measure of system security[40]. The author's recent framework to price "(information-)security securities" is based on stochastic models similar to those in financial theory[7]–[12]. The intrinsic difference from conventional finance is in the definition of objects in crypto-based networks; that is, uncertain digital objects are modelled as follows.

Definition 2.1 (Setok) *A* **security token** *or* **setok** *is a digital material which* **nominally contains** *the following four attributes:*

- **contents** *which may include MAC (Message Authentication Code), digital signatures, or other security-related control sequences if necessary,*
- *a non-negative* **explicit price** *(denoted by $\bar{S}$) which is paid when the setok is purchased by a customer,*

- *a set of non-negative* **explicit values** *(denoted by* $\bar{V}_1$, $\bar{V}_2$, $\cdots$, $\bar{V}_m$ *where* m *is referred to as the* **dimension** *of the explicit values) which represent some qualities of the contents in a way that larger values of each element imply better qualities regarding the feature represented by the element when the setok is purchased, and*
- *a* **timestamp** *which indicates when the setok is purchased,*

and is associated with

- *a non-negative* **implicit price** *(denoted by* S*) and*
- *a set of non-negative* **implicit values** *(denoted by* V_1, V_2, $\cdots$, V_n *where* n *is referred to as the* **dimension** *of the implicit values)*

in the following way.

- *The explicit price is specified as the occurrence of a* **price-interpretation process** $Y(t)=y(t, S(t))$*;* i.e. *the specific numerical value* $y(t_0, S(t_0))$ *is written as the explicit price of the setok which is purchased at time* $t = t_0$*. Each occurrence of the price-interpretation process is called the* **up-to-date price** *at time* t*. The price-interpretation process is a non-negative process and also called the* **up-to-date price process**. $y(t, s)$ *is called a* **price-interpretation function** *and monotone increasing with respect to* s*. Customers are unable to change the explicit price.*
- *The explicit values are specified as the occurrences of* **value-interpretation processes** $H_1(t)=h_1(t, V_1(t), V_2(t), \cdots, V_n(t))$, $H_2(t)=h_2(t, V_1(t), V_2(t), \cdots, V_n(t))$, $\cdots$, $H_m(t)=h_m(t, V_1(t), V_2(t), \cdots, V_n(t))$*;* i.e. *the specific numerical value* $h_i(t_0, V_1(t_0), V_2(t_0), \cdots, V_n(t_0))$ *is written as the* i*-th explicit value of the setok which is purchased at time* $t = t_0$ *(*$i = 1, 2, \cdots, m$*). Each occurrence* $h_i(t, V_1(t), V_2(t), \cdots, V_n(t))$ *is called the* i*-th* **up-to-date value** *at time* t*. The value-interpretation processes are non-negative processes, and also called the* **up-to-date value processes**. $h_1(t, v_1, v_2, \cdots, v_n)$, $h_2(t, v_1, v_2, \cdots, v_n)$, $\cdots$, $h_m(t, v_1, v_2, \cdots, v_n)$ *are called* **value-interpretation functions**. *Customers are unable to change the explicit values.*

Customers in open networks are distrusted. Depending on the payment scheme, customers may be even **anonymous** when they buy setoks. So each payment must be settled on site in exchange of the corresponding pieces of the setok. This should be done in a secure way; we have to ensure that no customer can exploit a setok without payment, and that no server can exploit a payment without sending the setok. Due to the security requirements, actual protocols would use digital signature. Each digital signature is generated on a particular piece of object. Thus setoks are transmitted to customers **in discrete pieces**; *e.g.* "three pieces" are possible but "two and a half pieces" are impossible. A piece of setok will be referred to as a **share** of the setok.

The price-interpretation function can model the effect of taxes, transaction costs, regulatory issues, and so on. The value-interpretation functions can model the effect of security policies, regulatory issues, editorial policies of financial reports, transmission delay, and so on.

2.1.5 Motivation/Incentive

In the First Workshop on Economics and Information Security, participants discussed a lot on how to provide economic incentives to deploy information-security mechanisms[41]. The discussion included

- cost reduction by standardization in information-security industry[42],
- cost-benefit ratio of privacy-enhancing technologies[43], and
- an optimization of more general cost-benefit ratio by introducing quantified *effort* and *successful outcome*[44].

Apparently opposite but in practice similar approach is the use of *discouragement*; enhancing the cost of attack can discourage malicious entities from attacking [45]– [50]. Liability transfer with respect to information security is related with this approach, too[51].

2.1.6 Information-Security Market

There are at least two approaches for studying information-security market.

The first one is optimization of investment to information security. The existing reports discuss nothing but investment amount at a single time interval [52]–[54]. They are obviously in their infancy; I recommend researchers to take time-series approaches similar to real-option studies[55], [56].

The second approach is a more basic research to discuss market mechanisms in information-security industry. The difficulty of this approach is said to be from relatively strange regulation issues [57].

2.1.7 Economic/Social Infrastructure

Information-security in computer networks requires technological infrastructures such as

- Public-Key Infrastructure (PKI) [58], [59],
- routing infrastructure[60], and
- Domain Name System (DNS)[61].

Protection of those infrastructures themselves is also important[62], [63]. In addition, if users want to feel easier, they need appropriate economic/social infrastructures such as

- information-security insurance [64]–[66],
- security securities[67], or financial derivatives on information-security objects [7]–[12], and
- social mechanisms for promoting information dissemination and collection regarding information security[6].

2.2 Trend in Related Conferences

According to the taxonomy presented in 2.1, let us see the recent trend in two international conferences: the Fifth International Conference of Financial Cryptography in 2001 (FC01) as a representative of conventional studies, and the First Workshop on Economics and Information Security in 2002 (WEIS02) as a representative of emerging (more interdisciplinary) studies. The number of research papers in those conferences were quite similar (27 in the former while 25 in the latter). Table 1 shows the distribution of the papers; the change from FC01 to WEIS02 suggests the emerging importance of relationship between economics and information security.

Table 1: Taxonomy of research papers presented at Financial Cryptography 2001 (FC01) and Workshop on Economics and Information Security 2002 (WEIS02).

Class	FC01	WEIS02
Primitives	33.3%	0.0%
Protocols	33.3%	0.0%
Enhancing Circulation	18.5%	4.0%
Modeling	7.4%	24.0%
Motivation/Incentive	3.7%	32.0%
Information-Security Market	0.0%	32.0%
Economic/Social Infrastructure	3.7%	8.0%

3 Investment in Information Security

Among the interdisciplinary studies reviewed above, optimization problems would interest researchers in computational economics a lot. One of the most clear optimization issues is a theory on information-security investment by Gordon and Loeb[52]. The theory is based on a simple model with a single decision variable. Although the theory provides an important step toward more advanced security management, it fails to incorporate an important variable into the model: that is, information-security insurance. Hence, in this section, after a brief review of the model (Gordon-Loeb model), an extension for simultaneous optimization of insurance will be proposed.

3.1 Gordon-Loeb Model

Gordon and Loeb[52] presented an economic model that determines the optimal amount of a firm's investment for protecting a set of information in a single-period model. An information set is characterized by the following three parameters:

λ : the monetary loss conditioned on a breach occurring.

t : the probability of a threat occurring.

v : the **vulnerability**, defined as the probability that a threat once realized (*i.e.*, an attack) would be successful.

Although the three parameters can change over time in the real world, Gordon-Loeb model assumes them as pre-estimated constants.

Let $S(z, v)$ denote the probability that an information set with vulnerability v will be breached, conditional on the realization of a threat and given that the firm has made an information-security investment of z to protect that information set. The function $S(z, v)$ is referred to as the security-breach probability function. As is common with nearly all economic models, $S(z, v)$ is assumed to be sufficiently smooth and well behaved, continuously twice differentiable in particular.

In addition to a general theory, Gordon and Loeb studied several classes of security-breach probability functions. One of them is given by

$$S(z, v) = v^{\alpha z+1} \tag{1}$$

where the parameter $\alpha(> 0)$ is a measure of the **productivity** of information security. For this class, we can derive a closed-form solution to an optimization problem which maximizes the expected net benefits from an investment in information security (ENBIS) defined as

$$ENBIS = \{v - S(z, v)\}\, t\lambda - z. \tag{2}$$

That is, the optimum investment is given by

$$z = z^*(v) = \frac{\ln\{-1/(\alpha v t \lambda \ln v)\}}{\alpha \ln v}. \tag{3}$$

3.2 A Proposal of Integrated Optimization

In Gordon-Loeb model, there are at least two substantial restrictions.

1. The loss λ is treated as a constant. This suggests that the investment studied in the model is restricted to hardware/software technologies and management services of information security.

2. The investment z is continuous, and hence the investment subjects are treated not as discrete pieces but as a whole.

If we strictly conform to the restrictions above, we would find it difficult to have decision making with respect to information-security insurance. So in the following, I propose an extension for integrating the investment optimization with the insurance decision making.

With respect to the restriction 1, we want to incorporate compensation by insurance. Suppose that investment in insurance reduces the loss. This implies that the loss is not a constant but a variable which can change according to the investment in information-security insurance.

With respect to the restriction 2, we want to incorporate a discrete nature of insurance; we have to choose an insurance contract from a countable and finite set of possible choices.

The two observations above lead us to the following integration.

Suppose that there are m possible choices of insurance contracts. Let the i-th choice costs $z_i(\geq 0)$ $(i = 1, 2, \cdots, m)$. And let $(0 \leq)$ λ_i $(\leq \lambda)$ $(i = 1, 2, \cdots, m)$ be the loss reduction achieved by the insurance[1] . Then we solve the following optimization problem:

$$\max_{i \in \{1,2,\cdots,m\}, z \geq 0} \left\{ [v - S(z, v)]\, t\, (\lambda - \lambda_i) - z - z_i \right\}. \tag{4}$$

Our goal is to find the optimum solution (i^*, z^*) for this problem.

For the class of security-breach probability functions defined by Eq. (1), we can derive the following theorem.

Theorem 3.1 (Solution for the Integrated Optimization Problem) *Assume that the introduction of insurance does not change the productivity of information security. Let the optimum investment including insurance be (i^*, z^*). Then, i^* is determined by the exhaustive search with respect to i for finding the maximum of*

$$vt\,(\lambda - \lambda_i) + \frac{1 - \ln\left\{-1/\left(\alpha v t\,(\lambda - \lambda_i) \ln v\right)\right\}}{\alpha \ln v} - z_i.$$

And then z^* is given by

$$z^* = \frac{\ln\left\{-1/\left(\alpha v t\,(\lambda - \lambda_{i^*}) \ln v\right)\right\}}{\alpha \ln v}.$$

(Proof in Brief) For a given choice of insurance i,

$$z = z_i^*(v) = \frac{\ln\left\{-1/\left(\alpha v t\,(\lambda - \lambda_i) \ln v\right)\right\}}{\alpha \ln v} \tag{5}$$

maximizes the ENBIS. Insert Eq. (5) into the integrated optimization problem (4). □

4 Concluding Remarks

The first part of this paper surveyed the interdisciplinary area between information security and economics. We categorized the area into seven sub-areas: (1) primitives, (2) protocols, (3) enhancing circulation, (4) modeling, (5) motivation/incentive, (6) information-security market, and (7) economic/social infrastructure. The statistics in the two apparently most relevant international conferences suggest the emerging importance of relationship between economics and information security.

After the survey and analysis, an integrated optimization of investment in information security and financial insurance was proposed. Since most users would think of insurance as their final defences, security management integrated with insurance is quite important. When we proceed to more complicated models (e.g. multiple-period models) for such management, there would arise a lot of research topics in the area of computational economics. The author hopes that this paper brings a good starting point.

[1] $z_i = \lambda_i = 0$ indicates that the i-th choice is "no insurance."

References

[1] MasterCard and Visa. "SET Secure Electronic Transaction Specification Book 1: Business Descryption", May 1997. Version 1.0, http://www.setco.org/download.html.

[2] MasterCard and Visa. "SET Secure Electronic transaction Specification Book 2: Programmer's Guide", May 1997. Version 1.0, http://www.setco.org/download.html.

[3] MasterCard and Visa. "SET Secure Electronic transaction Specification Book 3: Formal Protocol Definition", May 1997. Version 1.0, http://www.setco.org/download.html.

[4] R. Anderson. "Why Information Security is Hard —An Economic Perspective—". In *2002 Applied Computer Security Applications Conference (ACSAC)*, Las Vegas, December 2001.

[5] R. Anderson. "Why Information Security is Hard —An Economic Perspective—". In *18th Symposium on Operating System Principles (SOSP2001)*, Chateau Lake Louise, Banff, Canada, October 2001.

[6] L. A. Gordon, M. P. Loeb, and W. Lucyshyn. "An Economic Perspective on the Information Related to Security Breaches: Concepts and Empirical Evidence". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.

[7] K. Matsuura. "Security Tokens and Their Derivatives". Technical Report 29, Centre for Communications Systems Research, University of Cambridge, February 2001.

[8] K. Matsuura. "Digital Security Tokens and Their Derivatives". In *7th International Conference of the Society for Computational Economics (SCE'01)*, New Haven, CT, June 2001.

[9] K. Matsuura. "Security token and its derivative in discrete-time models". In *5th World Multiconference on Systemics, Cybernetics and Informatics*, Orlando, FL, July 2001.

[10] K. Matsuura. "A Derivative of Digital Objects and Estimation of Default Risks in Electronic Commerce". In S. Qing, T. Okamoto, and J. Zhou, editors, *Proceedings of Third International Conference on Information and Communications Security (ICICS'01)*, Lecture Notes in Computer Science 2229, pp. 90–94, November 2001. Springer-Verlag.

[11] K. Matsuura. "Digital Security Tokens in Network Commerce: Modeling and Derivative Application". In *8th International Conference of the Society for Computational Economics: Computing in Economics and Finance (CEF 2002)*, Aix-en-Provence, France, June 2002.

[12] K. Matsuura. "Digital security tokens and their derivatives". *Netnomics* (to appear).

[13] R. Anderson. "Unsettling parallels between security and the environment". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.

[14] B. Schneier. "Computer Security: It's the Economics, Stupid". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.

[15] D. Chaum. "Blind signatures for untraceable payments". In D. Chaum, R. L. Rivest, and A. T. Sherman, editors, *Advances in Cryptology: Proceedings of Crypto 82*, pp. 199–203, 1983. Plenum Press.

[16] D. Chaum and S. Brands. "Minting electronic cash". *IEEE SPECTRUM*, Vol. 34, No. 2, pp. 30–34, February 1997.

[17] D. Naccache, D. Pointcheval, and C. Tymen. "Monotone signatures". In P. F. Syverson, editor, *Financial Cryptography (FC2001)*, Lecture Notes in Computer Science 2339, pp. 305–318, 2001. Springer-Verlag.

[18] T. S. Perry. "Electronic money: toward a virtual wallet". *IEEE SPECTRUM*, Vol. 34, No. 2, pp. 18–19, February 1997.

[19] P. S. Gemmell. "Traceable e-cash". *IEEE SPECTRUM*, Vol. 34, No. 2, pp. 35–37, February 1997.

[20] M. Kudo. "Secure electronic sealed-bid auction protocol with public key cryptography". *IEICE Transactions on Fundamentals*, Vol. E81-A, No. 1, pp. 20–27, 1998.

[21] F. Brandt. "Cryptographic protocols for secure second-price auctions". In M. Klusch and F. Zambonelli, editors, *CIA 2001*, pp. 154–165, 2001. Springer-Verlag. Lecture Notes in Artificial Intelligence 2182.

[22] F. Brandt. "Vicious strategies for Vickrey auctions". In *Proceedings of the 5th International Conference on Autonomous Agents (AGENTS'01)*, pp. 71–72. ACM Press, May 2001.

[23] H. Lipmaa, N. Asokan, and V. Niemi. "Secure Vickrey auctions without threshold trust". In *Proceedings of the 6th Annual Conference on Financial Cryptography, 2002.*

[24] K. Matsuyama and K. Fujimura. "Distributed digital-ticket management for rights trading system". In *1st ACM Conference on Electronic Commerce*, 1999.

[25] N. Brownlee. "Internet pricing in practice". In Lee W. McKnight and Joseph P. Bailey, editors, *Internet Economics*, pp. 77–90, Cambridge, Massachusetts, 1997. MIT Press.

[26] M. K. Franklin and D. Malkhi. "Auditable Metering with Lightweight Security". In *Pre-Proceedings of Financial Cryptography'97*, pp. 1–9, February 1997.

[27] M. Naor and B. Pinkas. "Secure and efficient metering". In *Advances in Cryptology — EUROCRYPT'98*, pp. 576–590, 1998. Springer-Verlag. Lecture Notes in Computer Science 1403.

[28] M. Naor and B. Pinkas. "Secure Accounting and Auditing on the Web". *Computer Networks and ISDN Systems*, pp. 541–550, 1998.

[29] B. Schneier and J. Kelsey. "Cryptographic support for secure logs on untrusted machines". In *Proc. of The Seventh USENIX Security Symposium*, pp. 53–62, Berkeley, January 1998. USENIX Press.

[30] B. Schneier and J. Kelsey. "Secure audit logs to support computer forensics". *ACM Trans. on Information and System Security*, Vol. 2, No. 2, pp. 159–176, May 1999.

[31] J. Kelsey and B. Schneier. "Minimizing bandwidth for remote access to cryptographically protected audit logs". In *Second International Workshop on the Recent Advances in Intrusion Detection (RAID'99)*, September 1999.

[32] S. H. Low, N. F. Maxemchuk, and A. M. Lapone. "Document identification for copyright protection using centroid detection". *IEEE Trans. Commun.*, Vol. 46, No. 3, pp. 372–383, March 1998.

[33] Y. Watanabe, Y. Zheng, and H. Imai. "Software copyright protection in the presence of corrupted providers". In *Proceedings of 2000 International Symposium on Information Theory and Its Applications (ISITA2000)*, pp. 501–504, 2000.

[34] S. Katzenbeisser and F. Petitcolas (eds). *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House Publishers, Boston, London, 2000.

[35] S. Bechtold. "From copyright to information law — implications of digital rights management". In T. Sander, editor, *DRM 2001*, pp. 213–232, 2002. Springer-Verlag. Lecture Notes in Computer Science 2320.

[36] Deok-Gyu Lee, Im-Yeong Lee, Jong-Keun Ahn, and Yong-Hae Kong. "The illegal copy protection using hidden agent". In M. H. Shafazand and A. M. Tjoa, editors, *EurAsia-ICT 2002*, pp. 832–841, 2002. Springer-Verlag. Lecture Notes in Computer Science 2510.

[37] R. A. Gehring. "Software Development, Intellectual Property Rights, and IT Security". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.

[38] M. Stamp. "Risks of Digital Right Management". *Communications of the ACM*, Vol. 45, No. 9, p. 120, September 2002. Inside Risks.

[39] B. Arbaugh. "Security: Technical, Social, and Legal Challenges". *IEEE Computer*, Vol. 35, No. 2, pp. 109–111, February 2002.

[40] S. Schechter. "Quantitatively differentiating system security". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.

[41] A. Acquisti. "Privacy and security of personal information: Economic incentives and technological solutions". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.

[42] B. Fox. "Internet TAO: The Microeconomics of Internet Standards Setting". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.

[43] J. Feigenbaum, M. J. Freedman, T. Sander, and A. Shostack. "Economic Barriers to the Deployment of Existing Privacy Technologies". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.

[44] Hal R. Varian. "System reliability and free riding". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.

[45] K. Matsuura and H. Imai. "Protection of authenticated key-agreement protocol against a denial-of-service attack". *Científica*, Vol. 2, No. 11, pp. 15–19, September 1998.

[46] Y. Yemini, A. Dailianas, D. Florissi, and G. Huberman. "MarketNet: Market-Based Protection of Information Systems". In *Proceedings of First International Conference on Information and Computation Economies (ICE'98)*, Charleston, SC, October 1998.

[47] A. Juels and J. Brainard. "Client Puzzles: A Cryptographic Defense Against Connection Depletion Attacks". In S. Kent, editor, *Proc. of NDSS'99 (Networks and Distributed Security Systems)*, pp. 151–165, 1999.

[48] K. Matsuura and H. Imai. "Modified Aggressive Modes of Internet Key Exchange Resistant against Denial-of-Service Attacks". *IEICE Transactions on Information and Systems*, Vol. E83-D, No. 5, pp. 972–979, May 2000.

[49] C. Dwork and M. Naor. "Pricing via processing or combatting junk mail". In E. F. Brickell, editor, *Advances in Cryptology — CRYPTO'92*, Lecture Notes in Computer Science 740, pp. 139–147, August 1993. Springer-Verlag.

[50] C. Dwork and M. Naor. "Pricing via processing or combatting junk mail". Technical Report CS95-20, Faculty of Mathematical Sciences, The Weizmann Institute of Science, 1995. Technical Reports in Computer Science.

[51] R. Yahalom. "Liability transfers in network exchanges". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.

[52] L. A. Gordon and M. P. Loeb. "The economics of information security investment". *ACM Trans. on Information and System Security*, Vol. 5, No. 4, pp. 438–457, November 2002.

[53] Kin Sing Leung. "Diverging economic incentives caused by innovation for security updates on an information network". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.

[54] Kevin J. Soo Hoo. "How Much Is Enough? A Risk Management Approach to Computer Security". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.

[55] Lenos Trigeorgis. *Real Options: Managerial Flexibility and Strategy in Resource Allocation.* MIT Press, Cambridge, 1996.

[56] Jeannette Capel. "A Real Options Approach to Economic Exposure Management". *Journal of International Financial Management and Accounting*, Vol. 8, No. 2, pp. 87–113, 1997.

[57] C. E. Landwehr. "Improving information flow in the information security market". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.

[58] R. Perlman. "An Overview of PKI Trust Models". *IEEE Network*, Vol. 13, No. 6, pp. 38–43, 1999.

[59] Tom Austin. *PKI: A Wiley Tech Brief.* John Wiley & Sons, Inc., December 2000.

[60] S. Cheung and K. N. Levitt. "Protecting routing infrastructures from denial of service using cooperative intrusion detection". In *Proc. of New Security Paradigms Workshop '97*, pp. 94–106, September 1997.

[61] D. Eastlake. "Domain Name System Security Extensions". rfc2535, March 1999.

[62] S. M. Bellovin. "Cryptography and the internet". In H. Krawczyk, editor, *Advances in Cryptology — CRYPTO'98*, pp. 46–55, August 1998. Springer-Verlag. Lecture Notes in Computer Science 1462.

[63] A. K. Ghosh and T. M. Swaminatha. "Software Security and Privacy Risks in Mobile E-Commerce". *Communications of the ACM*, Vol. 44, No. 2, pp. 51–57, February 2001.

[64] M. K. Reiter and S. G. Stubblebine. "Toward acceptable metrics of authentication". In *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, pp. 10–20, May 1997.

[65] M. K. Reiter and S. G. Stubblebine. "Authentication metric analysis and design". *ACM Transactions on Information and System Security*, Vol. 2, No. 2, pp. 138–158, May 1999.

[66] W. Yurcik and D. Doss. "CyberInsurance: A Market Solution to the Internet Security Market Failure". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.

[67] B. Blakley. "The measure of information security is dollars". In *Workshop on Economics and Information Security*, University of California, Barkeley, May 2002.