Digital certificate management: Optimal pricing and CRL releasing strategies

Jie Zhang [a, *], Nan Hu [b], M.K. Raja [a]

[a] College of Business Administration, University of Texas, Arlington, Arlington, TX., United States

[b] College of Business, University of Wisconsin at Eau Claire, Eau Claire WI., United States

Published in Decision Support Systems (2014) 58, 74-78. DOI: 10.1016/j.dss.2012.12.043

Abstract: The fast growth of e-commerce and online activities places increasing needs for authentication and secure communication to enable information exchange and online transactions. The public key infrastructure (PKI) provides a promising foundation for meeting such demand, in which certificate authorities (CAs) provide digital certificates. In practice, it is critical to understand consumer purchasing and revocation behaviors so that CAs can better manage the digital certificates and its CRL releasing process. To address this problem, we analytically model a CA's pricing and revocation releasing strategies taking into consideration the users' rational decisions. The model provides solutions two main research questions: (1) How should the CA price the digital certificates? The the price of the digital certificate should be determined by the expected losses of the user's IT system, and the number of certificate revocations per period is expected to decrease over time during the lifecycle of the certificate. This result is supported by the empirical data from VeriSign. (2) How should the CA we further propose a dynamic CRL releasing policy that suggests that the optimal releasing intervals within the lifecycle of a certificate should increase over time.

Keywords: Security management, Key Infrastructure (PKI), Certificate Authority (CA), Certificate Revocation List (CRL), Dynamic programming algorithm

1. Introduction

With the development of information technology, especially the high speed digital electronic communications and electronic commerce, firms of all sizes are storing and sharing a vast amount of information. In addition, both industry reports (CSI Computer Crime and Security Survey 2010/2011 [4], CERT/CC Statistics, Ernst & Young Global Information Security Survey 2011 [5]) and academic literature (Cavusoglu et al. [2]) have revealed increasing level of threats and significant amount of losses due to security breaches. For example, Cavusoglu et al. [2] estimate that this loss in market capitalization reaches $1.65 billion. Therefore, firms are faced with the increasing challenge of securing and managing information against risks. The need for authentication and secure communication to enable timeless and seamless sharing of information has been heightened.

The public key infrastructure (PKI) provides a promising foundation for meeting such demand, especially in the electronic commerce area (Housley et al. [7], Kalvenes and Basu [10]). Developed based on the public-key encryption technique, the PKI creates, stores and manages digital certificates which map public keys to owners. It consists of a certificate authority (CA) that both issues and verifies the digital certificates, a registration authority that verifies the identity of users requesting information from the CA, and a central directory which securely stores keys (refer to textbooks on electronic commerce such as Schneider [11], and Schneier [12] for more technical specifications).

Many security vendors, such as VeriSign, Entrust, Spyrus and Cybertrust, provide digital certificate and public key solutions and services to help protect and secure information storage and communication. Realizing the market potential of websites and users wishing secure communications, they strive to convert PKI schemes into a successful business model. However, they are faced with some operational problems, one of which is to handle certificate revocation and distribute the revocation information to all involved parties to ensure the integrity and authentication of the PKI. A certificate may be revoked before the expiration date for various reasons, including loss of key, suspected or detected key compromise, change of subject name, etc. The standardized and most widely used revocation scheme is to periodically publish a digitally signed data structure called a certificate revocation list (CRL) that contains the certificate serial numbers of all revoked certificates within a CA domain. Administrating the CRL contributes to one of the main running expenses of a PKI.

In practice, various technical solutions dealing with key revocation have been proposed. However, to our best knowledge, no rigorous efforts have been made to understand both user behaviors and the CA strategies related to certificate revocation requests from an economic analysis perspective. In this regards, our paper provides managerial insights to the PKI users, vendors and the industry.

We take a unique approach differing from the literature by examining the issues related to managing the security keys. We analytically examine two main decisions of a CA:

(1) Certificate pricing taking into account the users' purchasing, revoking and replacing behaviors. The theoretical results suggest that the price of the certificates depends on the expected security loss of the users. We also reveal some empirical evidence regarding the PKI digital certificate usage in terms of revocations, which is consistent with the results of the analytical model;

(2) The CA's optimal CRL releasing strategy. We propose a dynamic programming approach of CRL releasing strategy that allows flexibly changing releasing strategies over time according to the size of the revocation requests. This proposed strategy will bring better performance to the CA than either online or fixed-interval offline CRL releasing strategies.

Section 2 reviews related literature. Section 3 models the decisions of the users and the CAs. We derive analytical solutions and empirically support the conclusion that the probability of certificate revocation decreases over a certificate's life cycle. A dynamic optimal CRL releasing strategy of a CA is proposed in Section 4. Section 5 concludes the paper.

2. Literature review

Since its introduction, the public key infrastructure (Housley et al. [7]) has provided a promising foundation for verifying the authenticity of public keys and for transferring trust among users or business partners. Various mechanisms have been designed to achieve efficient, timely, and scalable revocation of certifications (Wohlmacher [13]), such as certificate revocation list (CRL), certificate revocation systems (CRS), certificate revocation tree (CRT), and online certificate status protocol (OCSP).

The CRL mechanism was introduced in 1988 and since then it remains the most common and simplest method for certificate revocation. A CRL is a time-stamped list of certificates which have been revoked before their expiration dates. A CA issues a signed CRL periodically so as to maintain a good synchronization between certificate users and the revocation source. Some extensions of CRL include delta-CRL, partitioned CRL, and indirect-CRL (Arnes et al. [1]).

Researchers have studied various aspects of certificate revocations including the meaning of revocation (Fox and LaMacchia [6]), the model of revocation (Cooper [3]), communication cost of revocation (Naor and Nissim [10]), tradeoffs in certificate revocation schemes (Zheng [14]), and risk management in certificate revocation (Li and Feigenbaum [9]). Though various tradeoffs have been studied for different revocation options, no attempt has been made to understand the distribution of request for certificate revocation. In this paper, we conduct such research for CRL releasing mechanism based on real data and analytical models.

We intend to propose implementable solutions to the problems such as how to price and service the digital certificate, and how to manage the revocation list optimally. This paper differs from that of Hu et al. [8] in that it presents straightforward and intuitive solutions without relying on complicated models and many unnecessary assumptions. We also consider certificate vendor's pricing decision and user behaviors, which are ignored by Hu et al. [8].

3. A model for optimal CRL releasing strategies

We first build an analytical model to study the pricing and CRL revocation strategies of a CA. We consider a scenario in which a single CA provides services for certificates. Suppose the CA offers a key which is valid for a certain time period, defined as T. This valid period is normally 1 year in practice. We describe the decision flows of the CA and the users during the life cycle of a certificate in Fig. 1 where:

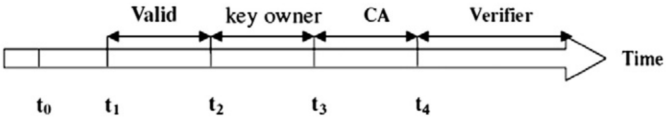

Fig. 1. Life cycle of a certificate.

t_0 CA decides the issuing price, valid period, and the CRL updating rules for the certificate.
t_1 Consumers decide to buy the certificate and CA issues the key.
t_2 An instance that triggers a key revocation (e.g. loss, compromise etc.) occurs and the key owner can either file a revocation request or not.
t_3 CA reissues a replacement key to the owner.
t_4 CA releases a CRL containing the revoked certificate.

We model the certificate issuing, purchasing and usage as a Stackelberg game, where the CA is the leader and the users are the follower. The CA will decide the price p, and the CRL releasing rules before users make purchasing decisions. We derive the equilibrium of the game through backward induction, starting from solving the users' decision. For a detailed notation definition see Table 1.

3.1. Users' purchasing and revoking a certificate

Users can choose to purchase the digital certificates to safeguard their online transactions and services for a price p valid for T periods. Otherwise, all of their online activities including online communication, transactions, and data storage may be at risk. We assume that security breaches occur at an exponential rate ω, thus the probability of a security breach is $\beta(t) = \omega e^{-\omega t}$ [8].

Given the certificate price p, users at time t_1 evaluate the cost of the certificate with the expected loss due to security breaches if running without the PKI certificates. Let C_L be the potential loss (tangible and intangible) of a user when a security breach occurs. They will purchase the digital certificate if

$$p \leq \int_0^T \left(c_L \cdot \omega e^{-\omega t}\right) dt = c_L\left(1 - e^{-\omega T}\right). \tag{1}$$

Therefore the occurring of a security breach, its potential loss, and the valid period of the certificate all increase users' willingness to pay for the certificate.

Regarding the revocation strategies, a user can either file a revocation request or not if the trigger event (key loss, key compromise or new information) occurs at time t_2. If the user revokes, the key becomes invalid and is replaced with a new key. Otherwise, the user has to be faced with the risk of security vulnerabilities with the associated losses. Since revocation and replacement of certificates have no additional charges according to business practices,[1] a user will choose the dominant strategy of revoking and replacing the digital certificate at time t_2.

3.2. CA's pricing decision and the expected certificate replacements

Next we consider the CA decision on the price of the certificate p and demand. In the monopoly setting, CA will consider users' purchasing evaluation into account to choose the optimal price: that is, the highest price that makes users buy, $p = c_L(1 - e^{-\omega T})$ by Eq. (1). Thus we have the following Lemma regarding CA's pricing decision.

[1] http://www.verisign.com/ssl/current-ssl-customers/revoke-replace-ssl.

Table 1
Notations.

Parameters	Meaning of parameters
$\alpha(t)$	Probability of key being lost or other reasons for key revocation at time t, assume it follows an exponential distribution with rate λ, therefore $\alpha(t)=\lambda e^{-\lambda t}$.
$\beta(t)$	Probability of a security breach to an unprotected system occurs at time t, assume it follows an exponential distribution with rate ω, therefore $\beta(t)=\omega e^{-\omega t}$.
p	Price of a digital certificate valid for T periods.
c_L	The total losses of a user due to a security breach.
c_p	CA's marginal cost of processing a revocation request included in the CRL.
F_p	CA's fixed cost of publishing a CRL.
c	CA's marginal cost of generating a new key.
N	Total number of users in the market. Assume the market size is stable.
T	The valid time of a digital certificate.
d	The releasing intervals of a CRL under dynamic offline CRL releasing strategy. There are n releasing intervals in the life cycle of a certificate: $d=\{d_1,d_2,\ldots d_n\}$ where d_i $(i=1\ldots n)$ represents the ith releasing interval.

Lemma 1. *The optimal price of a digital certificate with valid period T is* $c_L(1-e^{-\omega T})$.

Taking a period as a discrete level, say, a day or a week, we derive the demand for new certificates at each period as follows. At the initial time period $t=0$, the N users in the market purchase the digital certificate at the unit price p. At each following period before the expiration day, a key revocation trigger (e.g. loss, compromise, information updates) occurs following an exponential distribution at rate λ. The key owner will replace the digital certificate with a new one immediately after the incident occurs and the new key will have the same expiration date as the original certificate. Thus the expected amount of certificate revocation in a given period includes both the original certificates issued at period 0 and the replacements issued in any of the previous T periods. At period 1, there are $\alpha(1)N$ expected revocation requests and replacements from generation 0. At period 2, there are $\alpha(2)(1-\alpha(1))N$ expected revocation requests from the remaining generation 0 and $\alpha(1)^2N$ from generation 1. At period 3, there are $\alpha(3)(1-\alpha(2))(1-\alpha(1))N$ expected revocation requests from generation 0, $\alpha(2)\alpha(1)(1-\alpha(1))N$ from generation 1 and $\alpha(1)(\alpha(2)(1-\alpha(1))+\alpha(1)^2)N$ from generation 2. The computation will go on at the following periods until period T-1. The process will start over again at period T when all the certificates expire and have to be renewed. We illustrate the expected quantities of the digital certificates issued, revoked, and replaced for the first 3 periods in Table 2.

If we use $Rev(t)$ to represent the number of revocations at period t $(t=1,2,\ldots T)$ and let $Rev(0)=N$, the expected number of revocation at period t $(t>0)$ can be expressed as

$$Rev(1)=\alpha(1)N \tag{2}$$

$$Rev(t)=\alpha(1)Rev(t-1) + \sum_{k=2}^{t}\left[\prod\nolimits_{l=1}^{k-1}(1-\alpha(l))*\alpha(k)*Rev(t-k)\right] \quad (t=2,3,\ldots T). \tag{3}$$

We theoretically propose that the number of revocations decreases over time during the life cycle of a digital certificate.

Proposition 1. *The expected number of certificate revocations per period is decreasing over time during its valid period.*

Proof. Given the discrete time considered in this problem, we prove this proposition by mathematical induction.

When $t=2$, $Rev(2)=\alpha(1)Rev(1)+\alpha(2)(1-\alpha(1))N$ by Eq. (3). Therefore $Rev(1)-Rev(2)=(1-\alpha(1))Rev(1)-\alpha(2)(1-\alpha(1))N=(1-\alpha(1))(\alpha(1)-\alpha(2))N>0$ since $\alpha(t)$ is a decreasing function of t.

Suppose $Rev(t-1)-Rev(t)>0$, then we have

$$Rev(t)-Rev(t+1)$$

$$=(1-\alpha(1))Rev(t)-\sum_{k=2}^{t+1}\left[\prod_{l=1}^{k-1}(1-\alpha(l))*\alpha(k)*Rev(t+1-k)\right]$$

$$=(1-\alpha(1))\left\{Rev(t)-\sum_{k=2}^{t+1}\left[\prod_{l=2}^{k-1}(1-\alpha(l))*\alpha(k)*Rev(t+1-k)\right]\right\}$$

$$=(1-\alpha(1))\left\{\alpha(1)Rev(t-1)+\sum_{k=2}^{t}\left[\prod_{l=1}^{k-1}(1-\alpha(l))*\alpha(k)*Rev(t-k)\right]\right.$$
$$\left.-\sum_{k=2}^{t+1}\left[\prod_{l=2}^{k-1}(1-\alpha(l))*\alpha(k)*Rev(t+1-k)\right]\right\}$$

$$=(1-\alpha(1))(\alpha(1)-\alpha(2))Rev(t-1)+\sum_{k=2}^{t}\left[\prod_{l=2}^{k-1}(1-\alpha(l))\right.$$
$$*((1-\alpha(1))\alpha(k)-(1-\alpha(k))\alpha(k+1))*Rev(t-k)]\}.$$

Given $(1+\lambda)e^{-\lambda}<1$, $((1-\alpha(1))\alpha(k)-(1-\alpha(k))\alpha(k+1)=\alpha(k)(1-(1+\lambda)e^{-\lambda}+\lambda e^{-\lambda(k+1)})>0$. Therefore we have $Rev(t)-Rev(t+1)>0$. *Q.E.D.*

We simulate the above certificate revocation process with the parameter values $N=1000$, $\lambda=0.1$, and $T=62$. The expected number of revocations is plotted as a decreasing curve over time in Fig. 2. We define existence age as the number of periods (say, days) between the revocation date and the issue date. Fig. 2 supports our analytical result in Proposition 1.

3.3. Empirical evidence for revocation requests at each period

To study the properties of certificate revocation, we collected four series of CRLs from VeriSign (http://crl.verisign.com) between November 1st and November 7th, 2005. As one of the largest CAs in the world, VeriSign provides services for different types of digital certificates.

The four CRL files form a hierarchical chain of CAs (see Fig. 3), where a CA at a higher level may issue a certificate for the CA at a lower level but not vice versa. For example, an individual user can be certified by an enterprise or administrative CA, and the latter can be certified by an organizational CA, which is in turn certified by a root CA at the end of the chain.

The data of CRL files collected from VeriSign support our analysis. The data contain 52,826 revocation records in total. Among the four types of CRL files, individual subscription belongs to level 1 in the

Table 2
A partial illustration of the certificate generation, revocation (negative) and replacements.

Period (gen.)	0	1	2	3
0	N			
1	$-\alpha(1)N$	$\alpha(1)N$		
2	$-\alpha(2)(1-\alpha(1))N$	$-\alpha(1)^2Ns$	$(\alpha(2)(1-\alpha(1))+\alpha(1)^2)N$	
3	$-\alpha(3)(1-\alpha(2))(1-\alpha(1))N$	$-\alpha(2)\alpha(1)(1-\alpha(1))N$	$-\alpha(1)(\alpha(2)(1-\alpha(1))+\alpha(1)^2)N$	$(\alpha(3)(1-\alpha(2))(1-\alpha(1))+2\ \alpha(2)\alpha(1)(1-\alpha(1))+\alpha(1)^3)N$

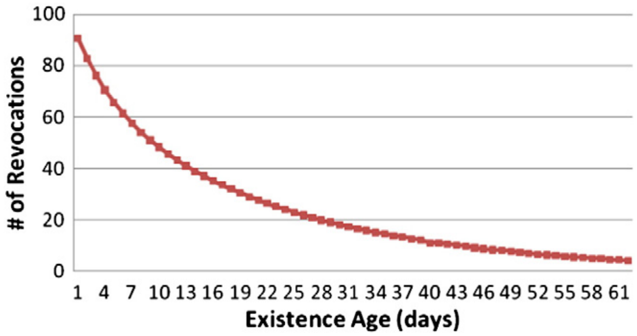

Fig. 2. Simulated number of revocations during a life cycle of a digital certificate.

hierarchical chain, CodeSigning and SVRIntl belong to level 3, and RSASecureServer belongs to level 4.

The number and the percentage of revocation requests are shown in Fig. 4 and Fig. 5, respectively. The distributions of revocation requests for these four types of certificates over time all demonstrate a similar pattern: the majority of the certificate revocations occur on the first few days after issuing, and the revocation requests decrease with elapsed time. This distribution pattern is robust, insensitive to the type of CRLs or the research year selected.

Both the numerical example and the above empirical observations support our analytical results (Proposition 1).

4. CA's CRL optimal releasing strategy

Other than selling and replacing certificates, a CA also maintains a publicly accessible CRL, which contains the certificate numbers of all revoked certificates within the CA domain. We discuss two most commonly used CRL releasing strategies: (1) online releasing, that is, the CA releases the revoked digital certificates immediately after a revocation request is made at each period of the life cycle; and (2) offline releasing, that is, the CA periodically releases a batch of certificates revoked since the last release.

The CA incurs a fixed cost F_p in publishing a CRL plus a marginal cost of processing a revocation request and including it in the CRL c_p. In the online releasing scenario, a CRL is published daily including the revocation requests filed on that day. The CA's expected payoff within the life cycle of the digital certificates is

$$\begin{aligned}\max E\left(\Pi_{\text{on}}|T\right) &= N(p-c)-\sum_{t=1}^{T-1} Rev(t)\left(c+c_p\right)-F_pT \\ &= N\left(c_{\text{L}}\left(1-e^{-\omega T}\right)-c\right)-\textstyle\sum_{t=1}^{T-1} Rev(t)\left(c+c_p\right)-F_pT,\end{aligned} \tag{4}$$

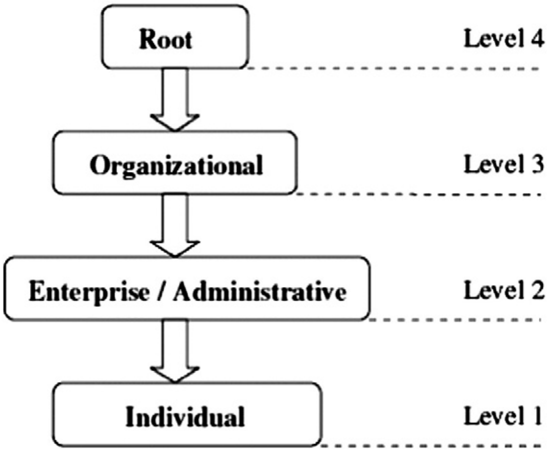

Fig. 3. Hierarchical chain of CAs.

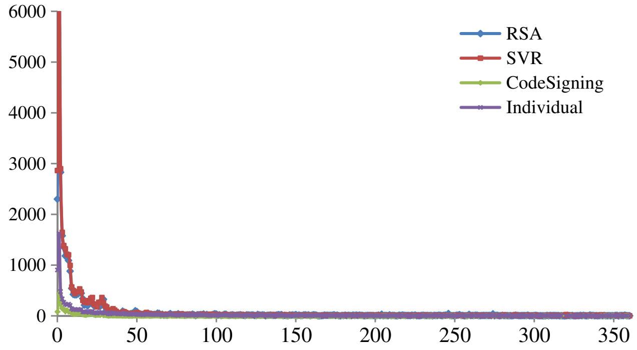

Fig. 4. Number of revocation requests.

where $N(p-c)$ is the profit from selling N certificates for the life cycle of the certificates. $\sum_{t=1}^{T-1} Rev(t)(c+c_p)$ is the total cost in processing and replacing the revoked certificates at the life cycle. And F_pT is the fixed cost for releasing the CRL at every period.

In the offline releasing scenario, the CA accumulates the revocation requests to a certain threshold and then releases a CRL to include them all. Offline releasing can reduce the fixed costs in releasing multiple CRLs, however, it increases the chance of authenticating a revoked certificate. If that happens, the CA will have to bear the liability cost incurred by the user of the revoked certificate. Suppose the liability cost occurs over time following an exponential distribution $\gamma(t)=ve^{-vt}$. Let $d=\{d_1, d_2, \ldots d_n\}$ represent the releasing intervals of a CRL in a life cycle of a certificate, where n is the number of releasing intervals in the life cycle of a certificate and d_i $(i=1\ldots n)$ is the ith releasing interval. The CA's expected payoff is similar to $\text{E}(\Pi_{\text{on}}|T)$ but with lower fixed costs in releasing CRLs and additional expected liability costs during those periods with no CRL releases.

$$\begin{aligned}\text{E}(\Pi_{\text{off}}|T) &= N(p-c)-\textstyle\sum_{t=1}^{T-1} Rev(t)\left(c+c_p\right) \\ &\quad -F_pn-\textstyle\sum_{i=1}^{n}\sum_{t=2}^{d_i-1}\gamma(t-1)Rev\left(\sum_{j=1}^{i-1} d_j+t\right)\end{aligned} \tag{5}$$

where $\sum_{i=1}^{n}\sum_{t=2}^{d_i-1}\gamma(t-1)Rev\left(\sum_{j=1}^{i-1} d_j+t\right)$ is the expected liability cost due to delayed releasing of revoked certificates.

Comparing the two payoff functions (2) and (5), we propose the following dynamic programming algorithm to solve the optimal offline CRL releasing intervals.

(1) Starting from $t=1$, the CA receives $Rev(1)$ revocation requests. The cost of not releasing the CRL at this period is expected to be $Rev(1)$ $\gamma(1)$ and the benefit of offline releasing is the cost saving of F_p. Comparing this cost and benefit, the CA should not adopt the online releasing strategy for this period if $Rev(1)\gamma(1)<F_p$. Otherwise, the CA should release the CRL at this period.

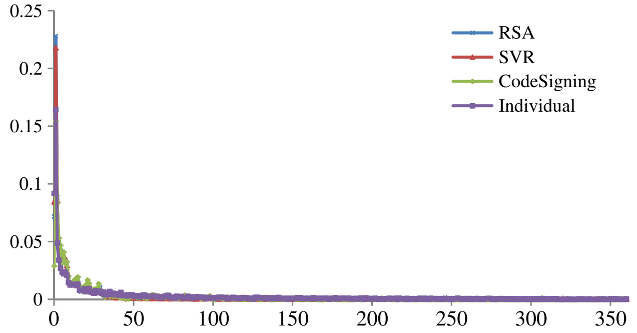

Fig. 5. Percentage of revocation requests.

(2) At period 2, if CA releases the CRL at the last period, then the expected cost for offline releasing is $Rev(2)\ \gamma(1)$, otherwise, the expected cost for offline releasing is $Rev(1)\gamma(2)+Rev(2)\ \gamma(1)$. Compare this cost with F_p, adopt the online releasing strategy for this period if the expected cost is less then F_p; otherwise, release the CRL at this period.

(3) Following similar decision making process, the releasing decision is made dynamically at each period of the life cycle of the certificate by comparing the expected cost of not releasing and the cost saving.

This dynamic CRL releasing strategy allows flexible releasing intervals and varying strategies over time. Since we have shown in Section 3 that the expected amount of certificate revocation requests drops over time, this dynamic CRL releasing strategy can overcome the restrictions of the online releasing or the fixed-interval releasing strategies and will provide the optimal payoff for the CA.

5. Conclusions

Research on security has mainly focused on technical problems. This paper studies the PKI certificate strategies using an economic game model. We solve the optimal price of the certificate and the expected number of revocation requests at each period of the life cycle. Both analytically and empirically, we show that the amount of certificate revocation is not stationary but decreasing over time during a certificate's life cycle. Given this result, the commonly adopted online CRL releasing and fixed-interval offline CRL releasing strategies, which are both stationary over time, do not offer the CAs the best solution for CRL releasing policy. We propose a dynamic solution that allows varying releasing intervals and makes the releasing decision at the beginning of each period by comparing the expected liability loss and the cost saving due to delayed release.

The above results provide important business insights to PKI vendors. First of all, in the absence of competition, the game theory model suggests that the optimal pricing depends on the users' expected loss from security breaches. Second, the CA is better off following a dynamic CRL releasing strategy rather than the traditional fixed-interval offline releasing strategy or the online releasing strategy.

There are several limitations to this study. First, we assume that CA offers certificates with a fixed issued age. To further minimize the total operational cost, CA may optimize its payoff by changing not only the releasing time interval but also the issued age simultaneously. Second, we consider only a monopoly CA and ignore the competition among multiple CAs. Under those assumptions, we are able to derive some useful and meaningful results. In future work, we would like to relax those assumptions to derive more results.

References

[1] A. Arnes, M. Just, S. Knapskog, S. Lloyd, H. Meijer, Selecting revocation solutions for PKI, Proceedings of NORDSEC 2000 Fifth Nordic Workshop on Secure IT Systems, Reykjavik, 2000.

[2] H. Cavusoglu, B. Mishra, S. Raghunathan, The effect of Internet security breach announcements on shareholder wealth: capital market reactions for breached firms and Internet security developers, International Journal of Electronic Commerce 9 (1) (2004) 69–105.

[3] D.A. Cooper, A model of certificate revocation, ACSAC '99: Proceedings of the 15th Annual Computer Security Applications Conference, IEEE Computer Society, Washington, DC, USA, 1999, p. 256.

[4] CSI (Computer Security Institute), Computer Crime and Security Survey, 2010/2011.

[5] Ernst & Young, Into the cloud, out of the fog, Global Information Security Survey, 2011.

[6] Fox and LaMacchia, Certificate revocation: mechanics and meaning, FC: International Conference on Financial Cryptography, LNCS, Springer-Verlag, 1998.

[7] R. Housley, W. Ford, W. Polk, D. Solo, RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL, Profile, 1999.

[8] N. Hu, G.K. Tayi, C. Ma, Y. Li, Certificate revocation release policies, Journal of Computer Security 17 (2009) 127–157.

[9] N. Li, J. Feigenbaum, Nonmonotonicity, user interfaces, and risk assessment in certificate revocation (position paper), Proceedings of the 5th International Conference on Financial Cryptography (FC'01), 2002, pp. 166–177, (number 2339 in LNCS).

[10] M. Naor, K. Nissim, Certificate revocation and certificate update, Proceedings 7th USENIX Security Symposium (San Antonio, Texas), 1998.

[11] G.P. Schneider, Electronic Commerce, 4th ed. Course Technology, Boston, MA, 2003.

[12] B. Schneier, Applied Cryptography, John Wiley, New York, 1996.

[13] P. Wohlmacher, Digital certificates: a survey of revocation methods, MULTIMEDIA '00: Proceedings of the 2000 ACM Workshops on Multimedia, ACM Press, New York, NY, USA, 2000, pp. 111–114.

[14] P. Zheng, Tradeoffs in certificate revocation schemes, Computer Communication Review 33 (2) (2003) 103–112.