Impact of the revocation service in PKI prices

Carlos Gañán, Jose L. Muñoz, Oscar Esparza
Jorge Mata-Díaz and Juanjo Alins

Universitat Politècnica de Catalunya (Departament Enginyeria Telemàtica)[**]
{carlos.ganan, jose.munoz, oesparza, jmata,juanjo}@entel.upc.es

Abstract. The ability to communicate securely is needed for many network applications. Public key infrastructure (PKI) is the most extended solution to verify and confirm the identity of each party involved in any secure transaction and transfer trust over the network. One of the hardest tasks of a certification infrastructure is to manage revocation. Research on this topic has focused on the trade-offs that different revocation mechanisms offer. However, less effort has been paid to understand the benefits of improving the revocation policies. In this paper, we analyze the behavior of the oligopoly of certificate providers that issue digital certificates to clients facing identical independent risks. We found the prices in the equilibrium, and we proof that certificate providers that offer better revocation information are able to impose higher prices to their certificates without sacrificing market share in favor of the other oligarchs. In addition, we show that our model is able to explain the actual tendency of the SSL market where providers with worst QoS are suffering loses.

Keywords: PKI pricing, SSL certificates, CRLs.

1 Introduction

Nowadays, there is a wide range of technology, products and solutions for securing electronic infrastructures. As with physical access security, the levels of security implemented should be commensurate with the level of complexity, the applications in use, the data in play, and the measurement of the overall risk at stake. A consensus has emerged among technical experts and information managers in government and industry that Public Key Infrastructure (PKI) offers the best feasible solution to these issues. PKI [1] has been a popular, yet often reviled technology since its adoption in the early nineties.

Currently deployed PKIs rely mostly on Certificate Revocation Lists (CRLs) for handling certificate revocation [2]. Although CRLs are the most widely used way of distributing certificate status information, much research

[**] This work is funded by the Spanish Ministry of Science and Education under the projects CONSOLIDER-ARES (CSD2007-00004), FPU grant AP2010-0244, and TEC2011-26452 "SERVET", and by the Government of Catalonia under grant 2009 SGR 1362.

effort has been put on studying other revocation distribution mechanisms in a variety of scenarios [3, 4]. These studies aim to compare the performance of different revocation mechanisms in different scenarios. However, none of these studies have explicitly modeled the interaction among CAs. In this paper, we model this interaction by using a game-theoretic approach.

With the appearance of novel network environments (e.g VANET or MANET), the quantity of CAs in the SSL certificate market is becoming larger and the market concentration diminishes, but it is not simple to eliminate the oligopoly in the short-term. During the 90s, the certification market, the competition among CAs appears mainly as price competition. In this situation, malignant price competition would be detrimental to the interests of the users and lead to the CA's pay crisis. Facing the situation, the main CAs have begun to change the competitive strategies from basic price competition to price and quality of services (QoS) competition. To provide better QoS, CAs have to improve their revocation service, and specifically the freshness of the CRLs. Users will pay more for a service that issues certificate status information faster. Time-to-revocation metric is visible to costumers by checking the CA's repositories where they publicize the revocation information.

The model of this article deals with an oligopoly of CAs which compete in certificate prices and QoS, and do not know the certificate revocation probability in the next interval for sure. The assumption that the revocation probability is *ex-ante* uncertain is quite logical and intuitive. The number of revoked certificates vary with time and in a manner that cannot predictable with certainty. We show that an uncertain revocation probability introduces a systematic risk that does not decrease by selling more certificates. If CAs are risk averse, this effect relaxes price competition. The equilibrium characteristic of the certification market is found by establishing a price competition model with different QoS. We consider that there are diversities in the certification service quality, and we describe factors that affect the service quality such as the CRL lifetime. By combining the characteristics of the certification market and considering the conveniences of modeling, two key parameters are selected to measure the QoS and a duopoly price competition model with service quality differentiation is established.

2 Related Work

Although PKI has been a widely adopted solution for many years now, very few works have dealt with the impact of the revocation mechanism in the prices CAs offer. Most of the literature [4, 5], intend to optimize the revocation mechanism to minimize the overhead or to improve the reliability. However, the most extended revocation mechanism is still CRL. Authors in [6] analyze the revocation mechanisms based on based on empirical data from a local network. They conclude that the freshness of the revocation data depends on how often the end entities retrieve the revocation information but the bandwidth cost is high if end entities retrieve the revocation lists often.

Ma *et al.* in [7] propose a series of policies that certification authorities should follow when releasing revocation information. According to this study, a CA should take different strategies when providing certificate services for a new type of certificates versus a re-serving type of certificates. Authors give the steps by which a CA can derive optimal CRL releasing strategies and they prove that a CA should release CRLs less frequently in the case that the fixed cost is higher, the variable cost is higher, the liability cost is lower, or the issued age of certificates is shorter. Similarly authors in [8] authors address the CRL release problem through a systematic and rigorous approach which relies on a mix of empirical estimation and analytical modeling. They propose four different models which seek to exploit the variation in certificate specific properties to provide guidance to the CA in determining the optimal CRL release intervals and the associated costs. However, none of these works neither analyze the impact of CRLs releasing policies in the prices that the CA charges nor model the interaction among CAs. In this paper, we address these issues using a game theoretic approach.

3 Modeling the Certificate Provider Competition

To formalize our arguments we describe a model of the certificate market with profit-maximizing certification authorities and a continuum of network users. When a user requests the status of given certificate, the CA does not always provides the most updated information but a pre-signed CRL [4, 5]. In this context, the CA will bear the liability cost due to any damage that may occur between the revocation of a certificate and the release of the CRL.

3.1 Demand for certificates

We consider an oligopoly of A CAs, indexed by $i = 1, \cdots, A-1$, and N users in the economy, where N is large relative to A.Each user has the same strictly concave expected utility function and faces the risk to lose l when using a revoked certificates. The probability π of operating with a revoked certificate is equal for each user in the network, and conditional on π operating with revoked certificates of different users are statistically independent. This probability is out of the user's control so that no moral hazard problem arises. Except for their probabilities of operating with revoked certificates, individuals are assumed to be identical. However, π is not known *ex-ante* with certainty but is a random variable distributed on $[\underline{\pi}; \overline{\pi}]$ with cumulative density function $F(\pi)$. Each user has an initial wealth $w > 0$. When operating with a revoked certificate, users may suffer a loss. We assume that the user's wealth exceeds the potential loss, that is, $l \leq w$.

Users can purchase different certificate types from the CA with different revocation updating service. We characterize this product by the price of the certificate $P_i > 0$ and an indemnity $C_i > 0$ the CA pays to the user if it suffers from an attack and operates with another user whose certificate was revoked. Note that as CRLs are not issued each time a certificate is revoked but periodically, users will be operating with outdated information. Let (P_i, C_i, t_i, s_i) be a certificate contract offered by CA$_i$ which specifies the price P_i to be paid by an user and the level of coverage C_i paid to the user if an attack takes place and she operates with a revoked certificate. Let t_i represent the CRL updating interval, and s_i represent the security level.

Let us assume that the total utility U which users can get after they purchase a certificate consists of two parts. The first part is wealth utility which represented by U_w the other part is QoS utility which the applicant can get after they obtained the CA's services, represented by U_{QoS}. The total utility U is defined as:

$$U(P_i, C_i, t_i, s_i) = \alpha_1 U_w + \alpha_2 U_{QoS}, \forall \alpha_k \in [0,1] \text{ and } \sum \alpha_k = 1;\ k = 1, 2. \tag{1}$$

where α_i represents the significance level of U respectively.

On the one hand, we calculate the wealth utility. If no attack due to misuse of a revoked certificate happens after the user has purchase the service the CA, a user gains $w - P_i$, on the contrary a user gains $w - P_i + C_i$. We assume that all users have same loss with two-point distribution:

$$\mu = (w - P_i)(1 - \pi) + (w - P_i + C_i)\pi \ = w - P_i + \pi C_i, \tag{2}$$

$$\sigma^2 = \pi(1 - \pi)C_i^2. \tag{3}$$

Hence we can characterize the wealth utility by the mean and variance of Eq. (2) and Eq. (3) respectively. Thus, we can define U_w as a mean-variance utility function:

$$U_w(P_i, C_i) = \mu - R\sigma^2, \tag{4}$$

where R represents the Arrow-Pratt index of absolute risk aversion. This means that the larger R is, the more risk averse the user is and the smaller U_w is.

On the other hand, let U_{QoS} be a linear function of the QoS that the CA offers. Thus, we define U_{QoS} as:

$$U_{QoS}(t_i, s_i) = \pi\theta\left(\beta_1 s_i + \beta_2 \frac{1}{t_i}\right), \forall \beta_k \in [0,1], \sum \beta_k = 1 \text{ and } \theta > 0;\ k = 1, 2. \tag{5}$$

where θ represents the quality preference parameter of the user, and β_1 represents the user's preference to security level and β_2 represents the user's preference to CRL issuing interval. Note that the higher the level of security the CA provides, the larger U_{QoS} is; the longer the CRL updating interval is, the smaller U_{QoS} is. It is also worth noting that θ is unknown to the CAs a priori.

In order to calculate the total utility of the user, we must unify the dimension of the security level and the CRL updating interval. Thus, using (1),(4) and (5) the total utility is calculated as:

$$U(P_i, C_i, t_i, s_i) = \alpha_1[w - P_i - \pi C_i - R\pi(1-\pi)C_i^2] + \alpha_2 \left[\pi\theta\left(\beta_1 s_i + \beta_2 \frac{1}{t_i}\right)\right] . \quad (6)$$

Note that according to this expression, users are willing to pay higher prices for those certificates whose issuer provides a better QoS. Note that issuing certificate status information faster, highly increases the QoS of the revocation service. Thus, certificates linked to a better revocation service provide more utility to the user.

3.2 Supply of certificates

We consider an oligopoly of CAs operating in the certification market. CAs compete for users by offering certificates and CRLs. The service qualities of their CA products are also different. The level of service quality is mainly shown by the CRL updating interval and the security level[1].

When choosing a CA, a user takes into account several factors. Our goal is to gauge the impact of the revocation service on the certificate prices. However, it should be noted that, for convenience, many website owners choose the registrar's authority regardless of the price. Before issuing a certificate, the CA verifies that the person making the request is authorized to use the domain. The CA sends an email message to the domain administrator (the administrative or registrant contact, as listed in the Whois database) to validate domain control. If there is no contact information in the Whois database or the information is no longer valid, the customer may instead request a Domain Authorization Letter from his/her registrar and submit the letter to the CA as proof of his/her domain control. If the administrative/registrant contact fails to approve the certificate request, the request is denied. This authentication process ensures that only an individual who has control of the domain in the request can obtain a certificate for that domain. Therefore as CAs compete by quoting a certificate price which has associated a particular quality of service, we have Bertrand competition. The CA that quotes the lowest certificate price with the highest QoS sells to all users.

[1] Note that additional QoS parameters could be introduced in the model. In fact, CAs distinguish themselves by offering additional value-added services (e.g. GoDaddy bundling domain registration with certificate issuance), turn-around time, etc.

4 Equilibrium Certificate Providers

In this section we consider the certification industry with an oligopoly of A certification authorities and analyze the competitive forces that determine equilibrium of certificate selling. Our main goal is to find the prices at which CAs obtain their maximum profit, i.e., when they reach the game equilibrium. Recall that these certificates differ in the QoS so that $\forall i, j; i \neq j, t_i \neq t_j$ and $s_i \neq s_j$. We assume that the certification market is covered in full. Users will intend to maximize their utility, i.e.:

$$\theta^* = \arg\max_{\theta} \quad U(P_i, C_i). \tag{7}$$

On the other hand, CAs will intend to minimize their costs. The CA's costs consists of fixed and variable costs. Each time a new CRL is issued, a CA incurs both fixed and variable costs. The fixed cost depends on two factors. The fix component is due to the release of a new CRL, and does not depend on the number or certificate type. The variable factor depends on the number of certificates contained in the CRL (i.e. depends on the size of the CRL) and on the type of certificate (i.e. certificate with higher security level induce higher costs). Note that in this variable cost it is included the cost of processing each certificate revocation request. We define the service quality cost of CA$_i$ (i.e. $Q(s_i, t_i)$) as a variable that includes both fixed and variable costs associated to the QoS. The first and second derivative of $Q(s_i, t_i)$ with respect to s_i, t_i are positive. Hence, we can calculate the gain function G_i of any CA$_i$:

$$G_i = \theta^* P_i - Q(s_i, t_i), \tag{8}$$

where the gain function captures the overall profits of CA$_i$ for a given certificate product characterized by (P_i, C_i).

We assume that the game between the two CAs is static with incomplete information, they choose the respective certificate price at the same time to maximize their profits. Now we differentiate (8) with respect to P_i and C_i. In order to obtain the certificate price and the coverage in the equilibrium, let each derivative formula equal to zero. Solving the resulting linear system, we will obtain the price of each CA P_i^* and the corresponding coverage C_i^*.

$$P_i^* : \frac{\partial G_i}{\partial P_i} = 0, \quad C_i^* : \frac{\partial G_i}{\partial C_i} = 0. \tag{9}$$

4.1 Duopoly of CAs

To better illustrate the results obtained in the previous section, we particularize the case of the oligopoly to a duopoly where only two CAs are offering certificates. This simplification, we allows us to draw some conclusion that can be easily extrapolated to the real scenario where there are more than a dozen CAs. To show that the level of service quality depends on the CA, we assume that the CA indexed by $i = 1$ offers better quality than the second CA in both QoS parameters, i.e., $t_1 < t_2$ and $s_1 > s_2$.

Following the methodology aforementioned, we have to find the prices in the equilibrium. In this situation, first we find the value of θ^* at which a user has no obvious trend between the certificates offered by different CAs.

$$\alpha_1[w - P_1 - \pi C_1 - R\pi(1-\pi)C_1^2] + \alpha_2 \left[\pi\theta\left(\beta_1 s_1 + \beta_2 \frac{1}{t_1}\right)\right] =$$
$$\alpha_1[w - P_2 - \pi C_2 - R\pi(1-\pi)C_2^2] + \alpha_2 \left[\pi\theta\left(\beta_1 s_2 + \beta_2 \frac{1}{t_2}\right)\right], \quad (10)$$

which results in:

$$\theta^* = \frac{\alpha_1\left(P_1 - P_2 + \pi C_1(1 + RC_1 - R\pi C_1) - \pi C_2(1 - RC_2 + R\pi C_2)\right)}{\pi\alpha_2 K} \quad (11)$$

where $K = \beta_1(s_1 - s_2) + \beta_2\left(\frac{1}{t_1} - \frac{1}{t_2}\right)$. So the market demand of CA$_2$ is θ^*, and the demand of CA_1 is $1 - \theta^*$.

Using (8) we calculate the gain function G_i of CA$_1$ and CA$_2$:

$$G_1 = (1 - \theta^* P_1) - Q(s_1, t_1), \quad (12)$$

$$G_2 = \theta^* P_2 - Q(s_2, t_2). \quad (13)$$

We obtain the certificate price and the coverage in the equilibrium :

$$P_1^* = \frac{2\pi\,\alpha_2 K}{3\alpha_1} \qquad P_2^* = \frac{\pi\,\alpha_2 K}{3\alpha_1}, \qquad C_1^* = C_2^* = \frac{1}{2R\,(-1+\pi)}. \quad (14)$$

From these results we can conclude that:

- In the equilibrium, when both CAs achieve their maximum gain, CA$_1$ obtains a higher price than CA$_2$. This is mainly due to the fact that when both CAs have associated the same probability of an attack, as the QoS of the first CA is better so that CA$_1$ can set a higher price per certificate.
- In the equilibrium, the coverage that each CA should establish is the same and is inversely proportional to the risk-aversion and the probability of operating with a revoked certificate.

5 Analysis and Results

5.1 Impact of the preference ratio $\frac{\alpha_2}{\alpha_1}$

As the ratio between the preference of QoS utility and wealth utility of the user increases (i.e., users are more interested in a high security service and a good revocation mechanism) the prices of both CAs in the equilibrium also increase. This effect is reasonable, as the improvement of the revocation mechanism gives a higher security level which also increases the costs. This cost increment is compensated with a higher price in the equilibrium. Analyzing two CAs operating in the oligopoly such that $t_i < t_j$ and $s_i > s_j$, it is worth noting that the increment speed of CA$_i$'s QoS is faster than that of CA$_j$, so the increment speed of its certificate price is also faster than the other CA.

5.2 Impact of the security level difference

When the level of security that a CA offers is much higher than in the others, the certificate value is also much higher. Thus, CAs that offer certificates with higher level of encryption and larger keys are able to make their certification product differentiable. For instance, SSL security levels vary depending upon the way on SSL certificate is installed on a server and the configuration used. SSL is simple to use but its security can be compromised if basic installation an configurations are not completed to a competent level, hackers are then able to decrypt the security on a badly installed SSL certificate. Once the certificates of a CA are differentiable from the other CAs, CAs do not have to use malignant prices anymore to compete. As the difference of this QoS between CAs becomes bigger, the prices that they can charge also increase. Note that if the preference extent which the user shows to the security level (i.e. β_1) increases, the differences in the certificates as products will be more apparent, thus the increase in the CA's certificate prices will also increase. The same results are expected with the increment of the interest of the users to a better service from the CAs (α_2), that is, not higher security but also a more efficient revocation mechanism.

5.3 Impact of the QoS of the revocation mechanism

CAs that are able to offer revocation mechanisms with fresher information and high availability are able to make their certification product differentiable. Recall that this QoS increase of the revocation mechanism induces higher costs, as revocation information has to be issued more frequently. These costs are compensated with an increase of the price that CAs can charge for the certificates in the equilibrium. The reasons are the same that in the previous case, but now users pay more attention to the revocation mechanism rather than to the level of security. Analytically, that means that β_2 increases, so that the user is more interested in the efficiency of the revocation mechanism. This increase induces a proportional increase in the equilibrium prices of the CAs. Note that in this case, the increase of CA$_i$

which has higher QoS of the revocation mechanism is faster than that of CA$_j$. Again, the CA that has better service (no matter if it is higher security level or a more efficient revocation mechanism) has the advantage in competition.

5.4 Impact of the revocation probability

Logically, with an increase of the probability of operating with a revoked certificate, CAs charge more for their certificates. The reason is obvious as the CAs set they price mainly based on a forecast of this probability. An increase of π will induce an increase of the compensation expenses that a CA will have to pay to any victim of an attack due to the misuse of a revoked certificate. Consequently, this increase will lead to a proportional increase of compensation cost and service cost so that the CAs have to increase their prices to compensate the cost increases. Note that this increase is twice faster in the case of the CA$_i$.

6 Case Study: SSL Providers

Finally, to corroborate the benefits of the presented model, we analyze the case of current SSL providers that issue digital certificates. An SSL certificate can be obtained from amounts as low as $43 to as high as $3000 per year. Whilst the type of encryption can be the same, the cost is determined by the rigour of the certification process as well as the assurance and warranty that the vendor can provide. Table 1 shows the prices and QoS that the leading CAs operating in the SSL Certificate market are offering. The SSL Certificate market was traditionally dominated by a small number of players, namely VeriSign and Thawte. Whilst in a monopolistic position they had the capability of charging inflated prices for a commodity product. However new providers with no necessity to hold prices high were able to offer SSL certificates at far more reasonable prices.

The SSL certificate vendors provide insurance against the misuse of certificates and this differs from one vendor to another. Verisign provides warranties of up to $250,000 while Entrust and GoDaddy offer a $10,000 warranty. The higher the insurance, the more inscription/authentication is provided by the SSL vendors. Analyzing Table 1, it is worth noting that not always a lower price means lower quality. Therefore, it is evident that current CAs operating in this market are competing both in price and quality of service.

To test whether these factors are determinant factors for the certficate prices, we perform a multivariate regression analysis explaining the yearly price of SSL certificates. General regression investigates and models the relationship between a response (Certificate price) and predictors (Warranty, issuing interval and CRL lifetime). Note that the response of this model is

SSL Provider	**Product Name**	**Price/Year($)**	**Warranty($)**	**Assurance**	**Mean Issuing time**	**Mean CRL lifetime**
COMODO	EnterpriseSSL Platinum	311.80	1,000,000	High	Under 1 hour	4 days
COMODO	InstantSSL Pro	169.80	100,000	High	Under 1 hour	4 days
Verisign	Secure Site Pro Cert	826.67	2,500,000	High	2-3 days	15 days
Verisign	Managed PKI for SSL Std	234.00	100,000	High	2-3 days	15 days
GeoTrust	QuickSSL Premium	118.00	100,000	Low	Immediate	10 days
GeoTrust	True BusinessID	159.20	100,000	High	2 days	10 days
Go Daddy	Standard SSL	42.99	10,000	Low	Immediate	1 day
Go Daddy	Standard Wildcard	179.99	10,000	Low	Immediate	1 day
Entrust	Advantage SSL Certificates	167.00	10,000	High	2 days	1 week
Entrust	Standard SSL Certificates	132.00	10,000	High	2 days	1 week
Thawte	SSL 123	129.80	-	Low	Immediate	1 month
Thawte	SGC Super cert	599.80	-	High	2 days	1 month

Table 1. SSL Certificate Types and Services offered by main CAs [9].

continuous, but you we have both continuous and categorical predictors. You can model both linear and polynomial relationships using general regression. With this model we determine how the certficate price changes as a particular predictor variable changes. We use data from a survey of CAs performed in 2010 [9]. The obtained regression model is expressed in the following equations for high and low assurance certificates, respectively:

$$Price/Year(\$) = 98,4353 + 0,000220857\ W - 0,549141\ \overline{I_{time}} + 8,6116\ \frac{1}{\overline{CRL_{Lf}}},$$

$$Price/Year(\$) = 20,0405 + 0,000220857\ W - 0,5491411\ \overline{I_{time}} + 8,6116\ \frac{1}{\overline{CRL_{Lf}}},$$

where W denotes the warranty, $\overline{I_{time}}$ is the mean issuing time, and $\overline{CRL_{Lf}}$ is the mean lifetime of the CRLs issued by the CA.

Note that both regression equations show that the coefficient of the predictor associated to the CRL's mean lifetime is significant. In fact, the p-value associated to this predictor is $0,008$ which indicates that is statistically significantly. Overall, the variables within the model are explaining a large portion of the variation in the certificate price. With a coefficient of determination R^2 above the 81%, we are capturing important drivers of certificate prices. The residuals from the analysis are normally distributed, i.e., no evidence of nonnormality, skewness, or unidentified variables exists.

Using the proposed model, we are able to explain these different prices and the corresponding market share and they potential evolution. First we analyze the number of revoked certificates as it will determine the probability of operating with a revoked certificate. Figure 1 shows the evolution of the daily number of revoked certificates per CA. These data were collected from different SSL CRLs that the CAs make public at their repositories. It is worth

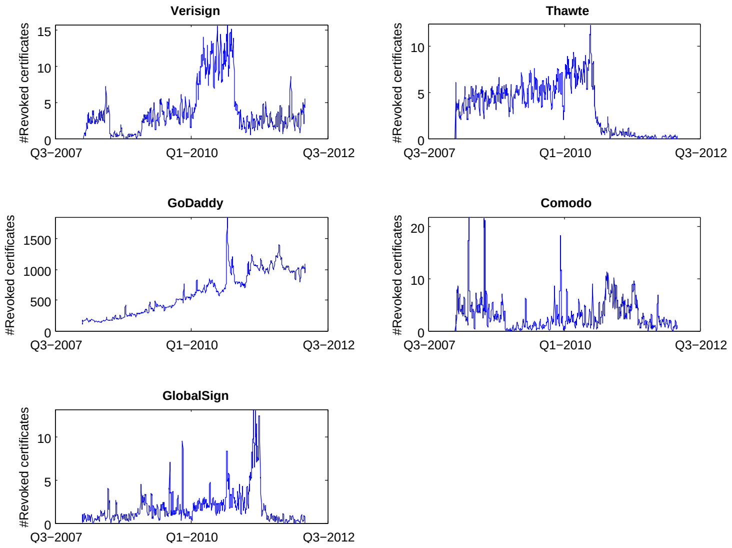

Fig. 1. Evolution of the daily number of revoked certificates per CA.

noting, that the number of revoked certificates highly varies depending on the CA. Thus, GoDaddy revokes more than 500 certificates per day on average while VerSign revokes less than 4 certificates per day on average. Therefore, the probability π of operating with revoked certificates is higher when trusting certificates issued by GoDaddy. As our model shows, using expression (14), the probability π directly affects the price of the certificate. Thus, as GoDaddy has a higher π, we would expect to charge less for its certificates. However, the price is quite similar to its competitors. Thus, GoDaddy is not able to sell as much certificates as the other oligarchs, and its market share is smaller.

Our model would expect GoDaddy to compete not only in prices but also in QoS to gain market share. As our model shows, the reaction of GoDaddy to compete in the oligopoly is to offer better quality of service. From table 1, we can see that GoDaddy is the CA that issues CRLs more often. Using this CRL releasing policy, users increase their utility and, at the same time, the probability of operating with a revoked certificate is also reduced. However, the variable costs increase due to this way of issuing CRLs. Similarly, Comodo intends to gain market share by decreasing the time it takes to issue a certificate and also reducing the CRL lifetime. Note that VeriSign, the leading CA, is the one who is offering the worst QoS, both in terms of CRL lifetime and time to issue a new certificate.

7 Conclusions

The market of certificate providers can be described as an oligopoly where oligarchs compete not only in price but also in quality of service. In this paper we have modeled this oligopoly using a game theoretic approach to find the prices in the equilibrium. We have been able to capture the QoS of the products offered by a CA, by means of the timeliness of the revocation mechanism and the security level. In our model of the certification industry with profit-maximizing CAs and a continuum of individuals we showed that although the undercutting process in certification prices seems similar to the price setting behavior of firms in Bertrand competition there exists a crucial difference depending onf the QoS of the revocation service. The solution of the game for two CAs in the oligopoly that offer certificates with different QoS shows that the revenues of the CA which provides a better revocation mechanism and a higher security level are larger. Therefore, a CA when setting the prices of its certificate and the compensation expenses, it has to take into account not only the probability of operating with a revoked certificate, but also the quality of the revocation mechanism and the security level. Thus, any CA should comprehensively consider the difference in quality of its services compared with other CAs.

References

1. C. Adams and S. Farrell. Internet X.509 Public Key Infrastructure Certificate Management Protocols. RFC 2510, Internet Engineering Task Force, March 1999.
2. R. Housley, W. Polk, W. Ford, and D. Solo. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280, Internet Engineering Task Force, April 2002.
3. T. Perlines Hormann, K. Wrona, and S. Holtmanns. Evaluation of certificate validation mechanisms. *Comput. Commun.*, 29:291–305, February 2006.
4. A. Arnes. Public key certificate revocation schemes. 2000. Queen's University. Ontario, Canada. Master Thesis.
5. D.A. Cooper. A more efficient use of Delta-CRLs. In *2000 IEEE Symposium on Security and Privacy. Computer Security Division of NIST*, pages 190–202, 2000.
6. Mona H. Ofigsbø, Stig Frode Mjølsnes, Poul Heegaard, and Leif Nilsen. Reducing the cost of certificate revocation: a case study. In *Proceedings of the 6th European conference on Public key infrastructures, services and applications*, EuroPKI'09, pages 51–66, Berlin, Heidelberg, 2010. Springer-Verlag.
7. Chengyu Ma, Nan Hu, and Yingjiu Li. On the release of CRLs in public key infrastructure. In *Proceedings of the 15th conference on USENIX Security Symposium - Volume 15*, Berkeley, CA, USA, 2006.
8. Nan Hu, Giri K. Tayi, Chengyu Ma, and Yingjiu Li. Certificate revocation release policies. *J. Comput. Secur.*, 17:127–157, April 2009.
9. WhichSSL. SSL Market Share, 2010. [Online] http://www.whichssl.com/ssl-market-share.html.