CLIENT SIDE CLOUD COMPUTING SECURITY: A MIXED MARKET ANALYSIS

Yipeng Liu
Northern Illinois University, yliu@niu.edu

Xia Sheng
Northern Illinois University, z1679082@students.niu.edu

Sean R. Marston
Western Kentucky University, sean.marston@wku.edu

Follow this and additional works at: http://aisel.aisnet.org/pacis2014

Recommended Citation
http://aisel.aisnet.org/pacis2014/282

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2014 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
CLIENT SIDE CLOUD COMPUTING SECURITY: A MIXED MARKET ANALYSIS

Yipeng Liu, College of Business, Northern Illinois University, DeKalb, IL, USA, yliu@niu.edu
Xia Sheng, College of Business, Northern Illinois University, DeKalb, IL, USA, z1679082@students.niu.edu
Sean R. Marston, Gordon Ford College of Business, Western Kentucky University, Bowling Green, KY, USA, sean.marston@wku.edu

Abstract

Could computing service providers have to ensure that the service applications, cloud software, and the physical location of the cloud are secure. Furthermore, providers need to ensure that the service is secure on the client’s side of the system. To examine the client side security level we build economic models that consider the tradeoffs between system usability and client side security restrictions. Our mixed market model is based on firms with different objectives (i.e., social welfare maximizing vs. profit maximizing). Under the mixed market model, we show that it is desirable to maintain adequate client side security differentiation. The equilibrium price charged by the welfare maximizing firm for its cloud computing service is always equal to that charged by the profit maximizing firm. The result shows that socially optimal solution is achieved when the welfare maximizing firm is the market leader.

Keywords: Cloud computing security, client side security restriction, mixed market competition, welfare maximizing, profit-maximizing.

1 INTRODUCTION

While the security of cloud computing services is important to the service providers, it is also one of the more expensive and difficult aspects of the service to implement and maintain. Service providers have to ensure that the service applications, cloud software, and the physical location of the cloud are secure. They also need to ensure that the service is secure on the client’s side of the system. The most common security method used by the user to access services is a pair of username and password. Most services indicate that a password needs to have a minimum length with multiple types of characters. Additionally, service providers have other hardware and software options to increase client side security. One example is for the service provider to create a two-step login process, adding a hardware authentication key in addition to the password to increase security. Service providers also have to consider the amount of privileges to give to each user account. The greater the privileges given to the user’s account the greater the security risk the provider takes on if the account is compromised.

One major issue that providers have to deal with on client security is meeting the security needs of all users. Most users want the system to be as secure as possible while wanting the onus of the security to be placed on the service provider, not themselves. Users would like to have all the benefits of high security with none of the potential usability drawbacks. Cloud computing services are only as secure as the weakest security in place and unfortunately one of the weaker areas is the client side of the service. This means cloud service providers want the client side security to be as secure as possible too. One issue that arises with an increase in client side security is the potential decrease in usability by the users. Let’s examine some simple aspects of password security. Many users find password policies requiring a high minimum length, specified number of different characters, and a requirement to regularlychanger their passwords to be frustrating. It can be seen in practice that many users do not
follow the practice of creating strong passwords nor having separate passwords for each account. So the increase in security revolving around users’ passwords can be nullified by the users. Additionally, requiring multiple accounts instead of one with different administrative privileges to run different levels of services reduces the usability of the system and increases the frustration of the users. The more security barriers that are put into place impacting the users access to the services, the greater the chance to decrease usability and frustrate the users. Thus it is important for service providers to balance the tradeoff between usability and security especially when facing competition.

The amount of security that a user is willing to deal with for access to a cloud computing service is also dependent upon the data being used in the service. For example, a user who is storing unimportant files on a cloud storage service will be less willing to put up with more taxing security measures than a user storing sensitive financial documents. This creates difficulties for many service providers since their services are used by a wide variety of users who all have a different valuation on the data being used. Thus service providers have to cater to users who have different levels of security preference. This makes finding the appropriate security level for all users important for the cloud service provider.

Although a majority of the cloud services offered by different providers are similar, the overall objectives of each individual provider can vary. Google for example, make their profits of selling advertisements and use their cloud computing services to increase their overall brand. Facebook provides its social network service via a cloud to its users for free with the aim of making a profit through advertisements as well. Firms with the intent of building their brand often compete with firms whose intent is to maximize profits (called mixed market competition). For example, Microsoft Office 365 and Google Docs are two similar competing services whose providers have different objectives. For users to have access to various common Office suite applications on the Microsoft Office 365 platform, they must purchase one of the premium membership plans. However, similar services are offered on the Google Docs’ platform free of charge. It is clearly seen that Microsoft’s services objective is to turn a profit while Google’s objective is to build up its brand. Firms who are attempting to maximize their overall brand are in essence attempting to maximize the overall social surplus.

The combination of a cloud service provider’s objective and the choice of security level lead to the following research questions:

- For a cloud computing service provider, what would be the appropriate client side security levels facing competition?
- What is the impact of different client side cloud computing security on the firm’s market share?
- How should a firm adjust the price (fee) for its cloud computing service based on the market environment?
- In what conditions, socially optimal outcome is achieved when service providers are competing in a mixed market?

In this work, we examine two service providers facing competition and solve for the equilibrium client side security levels based on each of the service provider’s overall objective. We find, in a mixed market model, the equilibrium security levels are based on the market leader’s objective. If the market leader is a welfare maximizing firm, the total social surplus will be maximized when the welfare maximizing firm selects a client side security restriction level that is sufficiently lower than that of the profit maximizing firm. On the other hand, if the profit-maximizing firm is the market leader, the profit-maximizing firm should choose a client side security restriction level closer to 50%\(^1\) and the welfare maximizing firm should choose an even lower security restriction level. By comparison, when the market leader is a profit maximizing firm, the overall level of security restriction for both firms are lower than when the market leader is a social welfare maximizing firm.

The rest of the paper is presented as follows: A review of literature relevant to information security, cloud computing services and price competition is presented in Section 2. To study different objectives among cloud computing service providers, we present a specific model in Section 3. Our

---

\(^1\) 50% is defined with respect to the maximum client side security level, which is normalized to 1.
model captures the salient features of the decision process facing the service providers within the mixed market environment. This section provides further discussions on the impact of the security level change in react to service provider’s objectives. Useful managerial insights derived from analytical analyses are reported. We conclude the paper and discuss some future research possibilities in Section 4.

2 LITERATURE REVIEW

The research of price competition in a differentiated market is a stream of literature relevant to our study. Most of the prior studies follow the classic model designed by Hotelling (1929) and revised by d’ Aspremont et al. (1979). The model assumes that the transportation costs of consumers are linear and characterizes the horizontal product differentiation as the principle of minimum differentiation. Furthermore, by introducing quality choice into the model of Hotelling (1929) in pure strategies, Economides (1989) demonstrated that the equilibrium exists. The results are characterized by minimum differentiation and maximum differentiation location choices. After Economides’ results (1989), there is a large amount of research using a sequential-move duopoly model for the location choices (Beato et al. 1983; Fraja & Delbono 1990; Matsumura 2003). This stream of research adopted linear transportation costs to examine a market comprised of many asymmetrically positioned firms (Fraja & Delbono 1990). For example, Beato and Mas-Colell (1983) discussed the desirable role of the public firm in a mixed market using quantity-setting duopoly models with homogeneous goods, while Koças (2005) developed a model of price competition in an asymmetric oligopoly to analysis emerging price competition in on-line markets.

Information security is another relevant topic. While a lot of research about information security is currently taking place, many of them choose to focus on how information security investment would increase economic returns (Hoo et al. 2001; Yang & Padmanabhan 2010; Zhao et al. 2008). In addition, most of the studies on the economic returns of information security investment focus on the service provider side IT investment strategies (Agrawal et al. 2000; Chatterjee et al. 2001; Im et al. 2001). Such an approach often requires the estimation of security benefits and cost to perform the security economic analysis (Boehm et al. 2000). Unfortunately, Butler in (2002) has demonstrated that determining the benefit estimation for security investment accurately is very difficult due to the lack of historical data, effective metrics, and the complex and sensitive nature of security.

There is a surprising lack of research addresses the client side information security restrictions despite the apparent need for useful guidelines. Extant literatures (Besnard et al. 2004; Furnell 2005; Johnston et al. 2003; Nodder 2005; Renaud 2005) have identified potential conflicts between desirable levels of information security and security costs. This occurs due to the phenomena that improving security is generally accompanied by increased system complexity. Researchers have found that companies need to strike a balance between security and convenience, while working on a security solution that prevents information breaches on their system. Given the security/convenience tradeoff and the user’s acceptance of the security policies, several studies suggest that new security technologies should be designed based on the convenience principle (Schultz et al. 2001; Smetters & Grinter 2002). Unfortunately, most of these studies only analyze the impact of information security investment from the service provider’s side of the system. There has been very little research conducted on the security level to implement by a service provider on the users and their experience. This paper is intended to help fill this gap. In this work, we focus on the impact of client side security restrictions from the user’s perspective and explore its impact on the security level between firms under competition.

3 THE MODEL

In this section, we examine the client side security issue faced by two cloud computing service providers in a mixed market model. Our study looks to find the appropriate client side security level taking into account the interactions between competing firms.
We consider a model based on Hotelling (1929) and d’Aspremont et al. (1979). In our model, a firm’s choice of client security level lies on the abscissa of a unit line. We assume that users’ heterogeneous preferences about the security level are uniformly distributed with density of one along this interval. Let $z_i \in [0,1]$ denote firm $i$’s client side security level to protect the cloud computing service. A user with security preference $\lambda \in [0,1]$ incurs a fit cost of $t (\lambda - z_i)^2$ when he purchases the cloud computing service from Firm $i$. The quadratic cost function captures the increasing marginal cost associated with meeting a user’s security preference. In addition, each user derives a surplus $s$ from the consumption of the cloud service. We assume that $s$ is so large such that every user would purchase the service. Please see Table 1 for a summary of notation used in our model.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$z_i$</td>
<td>Firm $i$’s client side security restriction level to protect the cloud computing service</td>
</tr>
<tr>
<td>$\lambda$</td>
<td>user’s security preference</td>
</tr>
<tr>
<td>$t$</td>
<td>the unit fit cost</td>
</tr>
<tr>
<td>$s$</td>
<td>the surplus derived by a user from purchasing the cloud computing service</td>
</tr>
<tr>
<td>$v$</td>
<td>the firm’s intrinsic security vulnerability</td>
</tr>
<tr>
<td>$L$</td>
<td>user’s financial loss associated with a security breach</td>
</tr>
<tr>
<td>$S(z_i, v)$</td>
<td>the probability that a firm with vulnerability $v$ will be breached, conditional on that the firm has made a security restriction $z_i$ to protect its service</td>
</tr>
<tr>
<td>$W$</td>
<td>total social surplus</td>
</tr>
<tr>
<td>$p_0$</td>
<td>price of the cloud computing service charged by Firm $i$</td>
</tr>
<tr>
<td>$TC_i$</td>
<td>user’s total cost of ownership incurred by Firm $i$’s product/service</td>
</tr>
<tr>
<td>$D_i$</td>
<td>user’s overall demand of Firm $i$’s cloud computing service</td>
</tr>
</tbody>
</table>

**Table 1. Notation**

Assume there is a single threat to the cloud computing service provided by Firm $i$. The parameter $v$ is used to denote a cloud service’s vulnerability, which is equivalent to the probability that without additional client side security restriction (i.e., $z_i = 0$) a realized security threat (attack) will result in a successful security breach and a loss $L$ will occur. For expositional ease, we refer to $L$ as the loss associated with the security breach. Since $v \in [0,1]$ is a probability, our view of security threats and vulnerabilities is consistent with Gordon and Loeb (2002) and Littlewood et al. (1993) concerning the desirability of a probability-based framework for operational security measurement”. Note that a firm is invulnerable to security threats if $v = 0$. Certainly, this state of invulnerability (and perfect confidentiality) is achieved through having the cloud computing service completely inaccessible. Similarly, if $v = 1$, the cloud computing service is completely vulnerable to security threats.

Firms are able to improve the client side security through additional hardware/software protections (e.g., digital certificate, USB token authentication etc.) or policy regulations (e.g., update password regularly, provide answers to security questions before login etc.) to increase their influence over a cloud service’s vulnerability. The purpose of such security restrictions is to lower the probability that the cloud service is breached. Let $S(z_i, v)$ denote the probability that a firm with vulnerability $v$ will be breached, conditional on the firm choosing a security restriction level $z_i$ to protect its service. We refer to the function $S(z_i, v)$ as the security breach probability function and to its value at a particular level of $z$ and $v$ as the security breach probability. The nature of information vulnerability and cloud computing security leads us to consider the following assumptions concerning $S(z_i, v)$:

- **A1.** $S(z, 0) = 0$ for all $z \in [0,1]$. If the cloud computing service is completely invulnerable, then it will remain perfectly protected for any amount of security restrictions, including zero restriction.
- **A2.** For all $v$, $S(0, v) = v$. If there is no restriction on client side security, the probability of a security breach, conditioned on the realization of a threat, is the firm’s inherent vulnerability, $v$.
- **A3.** For all $v \in [0,1]$, and all $z \in [0,1]$, $S_z(z, v)$, where $S_z$ denotes the partial derivative of $S(z, v)$ with respect to $z$. That is, as the restrictions on security increase, the cloud computing service is
made more secure. Furthermore, we assume that for all \( v \in [0,1] \), \( \lim S(z,v) \to 0 \), as \( z \to 1 \), so that by enforcing in security restriction sufficiently, the probability of a client side security breach, \( S(z,v) \), can be made close to zero.

### 3.1 Mixed Market Competition: welfare maximizing vs. profit maximizing

Although many companies will look to maximize profits when providing a service, some companies use services as a complement to their main source of revenue. For example, Google provides a majority of their cloud services for free to complement its advertising business. Without loss of generality, let Firm 0 denote a welfare-maximizing firm that competes against Firm 1, which is a profit maximizing firm. Firm 0 and Firm 1 provide similar cloud computing services (e.g., Google Docs vs. Microsoft Office 365) and the marginal cost of providing this service is negligible. The two stage sequential move game is as follows: In the first stage, one firm chooses its client side security restriction level and the other firm chooses its level after observing the rival’s restriction level. In the second stage, each firm chooses its price \( p_i \) simultaneously. Without loss of generality, we assume that the two firms have different security restriction choices (i.e., \( z_0 \neq z_1 \)). User of type \( \lambda \), purchasing the cloud computing service from Firm \( i \), would therefore incur a total cost of ownership \( TC_i \) such that:

\[
TC_i = S(z_i,v)L + t(\lambda - z_i)^2 + p_i.
\]

Three key components contribute to the user’s total cost: (i) the financial loss associated with a potential security breach \( S(z_i,v)L \); (ii) the fit cost \( t(\lambda - z_i)^2 \) due to the heterogeneous security preferences among users; and (iii) the price paid to Firm \( i \) for its cloud computing service. In order to gain further insights into the relationship between the vulnerability and the client side security restriction level, we choose to examine a specific security breach probability function such that \( S(z_i,v) = v(1 - z_i) \). It is easy to verify that this probability function satisfies all three conditions (A1 - A3) as we mentioned earlier.

As a result, for a user at

\[
\bar{\lambda} = \frac{z_1 + z_0}{2} + \frac{p_1 - p_0}{2t(z_1 - z_0)} - \frac{vL}{2t},
\]

the total cost of ownership is the same at either of the two firms (i.e., \( TC_0 = TC_1 \)). Figure 1 highlights the type of user who is indifferent between the cloud computing services provided by either Firm 0 or Firm 1. Market share of each firm is therefore divided according to the value of \( \bar{\lambda} \).

**Figure 1.** Marginal customer type \( \bar{\lambda} \) and the division of market

Correspondingly, the demand of Firm 0, denoted by \( D_0 \) and that of Firm 1, \( D_1 \) are given by:

\[
D_1(p_0, p_1, z_0, z_1) = 1 - D_0(p_0, p_1, z_0, z_1)
\]

\[
D_0(p_0, p_1, z_0, z_1) = \begin{cases} 
\bar{\lambda} & \text{if } z_0 < z_1 \\
1 - \bar{\lambda} & \text{otherwise}
\end{cases}
\]

If \( z_0 < z_1 \), the total social surplus of all users \( W \) is given by:
\[ W = s - t \left[ \int_0^\lambda \left( \lambda - z_0 \right)^2 d\lambda + \frac{1}{\Delta} \left( \lambda - z_i \right)^2 d\lambda \right] - \left[ \int_0^\lambda S(z_0, v) Ld\lambda + \frac{1}{\Delta} S(z_i, v) Ld\lambda \right] \]

\[ = s - t \left[ \left( z_i - z_0 \right) D_i^2 + \left( z_i^2 - z_0^2 \right) D_i + \frac{1}{3} \left( z_i + z_0 \right) \right] - \left[ v(1 - z_0) D_0 + (1 - D_0) v(1 - z_i) \right] L \]

If \( z_0 > z_i \), the total social surplus of all users \( W \) is given by:

\[ W = s - t \left[ \int_0^\lambda \left( \lambda - z_0 \right)^2 d\lambda + \frac{1}{\Delta} \left( \lambda - z_i \right)^2 d\lambda \right] - \left[ \int_0^\lambda S(z_0, v) Ld\lambda + \frac{1}{\Delta} S(z_i, v) Ld\lambda \right] \]

\[ = s - t \left[ \left( z_i - z_0 \right) D_i^2 + \left( z_i^2 - z_0^2 \right) D_i + \frac{1}{3} \left( z_i + z_0 \right) \right] - \left[ v(1 - z_0) D_0 + (1 - D_0) v(1 - z_i) \right] L \]

Note that, if \( (z_0, z_i) = (z^*, z^**) \), where \( (z^* < z^**) \) is an equilibrium, then \( (z_0, z_i) = (1 - z^*, 1 - z^**) \) is also an equilibrium. In order to avoid such repetition, we focus on the social surplus function where \( z_0 < z_i \) as shown in Eq. (3).

Consider the problem of maximizing \( W \) with respect to \( z_0, z_i \) and \( D_0 \). From the first-order conditions for optimality we have: \( z_0 = \frac{1}{4} + \frac{v_L}{2t} \), \( z_i = \frac{3}{4} + \frac{v_L}{2t} \), and \( D_0 = \frac{1}{2} \). Substituting \( z_0 \) and \( z_i \) into (2), we have that \( D_0 = \frac{1}{2} \) if and only if \( p_0 = p_i \). Simply put, different prices charged by the firms introduce no distortion to the first best outcome results as long as both firms choose to match the price against each other. The social welfare is maximized when the trade-off between the client side security and the user convenience (measured by the unit fit cost \( t \)) is balanced.

Proposition 1 summarizes the equilibrium market shares \((D_0^*, D_i^*)\), client side security restriction levels \((z_0^*, z_i^*)\) and pricing strategies \((p_0^*, p_i^*)\) for the firms under two different scenarios depending on which firm is the leader in stage 1 of this sequential move game.

**Proposition 1:**

(i) In every equilibrium: \( p_0 = p_i = p^* = vL(z_i - z_0) + t(z_i - z_0)(2 - z_i - z_0) \).

(ii) If Firm 0 is the leader, in equilibrium: \( z_0^* = \frac{1}{4} + \frac{vL}{2t} \), \( z_i^* = \frac{3}{4} + \frac{vL}{2t} \), \( D_0^* = D_i^* = \frac{1}{2} \), and \( p^* = \frac{vL}{2} + \frac{3}{4} - t \).

(iii) If Firm 1 is the leader, in equilibrium: \( z_0^* = \frac{1}{6} + \frac{vL}{2t} \), \( z_i^* = \frac{1}{2} + \frac{vL}{2t} \), \( D_0^* = \frac{1}{3} \), \( D_i^* = \frac{2}{3} \), and \( p^* = \frac{vL}{3} + \frac{5}{9} - t \).

(iv) The social welfare optimum is achieved when Firm 0 is the leader.

First, consider the case in which welfare maximizing firm (Firm 0) is the leader. Proposition 1(i) and (ii) suggest that the total social welfare is maximized when Firm 0 selects a client side security restriction level that is sufficiently lower than that of the profit maximizing firm so as to maintain adequate product differentiation. The appropriate client side security restriction level is always lower than that of the profit maximizing firm (i.e., \( z_i^* - z_0^* = 0.5 \)). Under such a scenario, the market share is divided equally between the two firms such that users who prefer less security restrictions (i.e., \( \lambda < 0.5 \)) choose Firm 0 and those that prefer more security restrictions (i.e., \( \lambda > 0.5 \)) choose Firm
1. In order to obtain such a division of the market, Firm 0 should choose to match the price as offered by Firm 1 (i.e., \( p_o = p_1 \)).

Next, consider the case in which the profit-maximizing firm (Firm 1) is the leader. Proposition 1 (iii) indicates that Firm 1 should choose a client side security restriction level closer to the central point (i.e., \( z = 0.5 \)), meanwhile Firm 0 shall choose an even lower security restriction level to maintain adequate product differentiation. Note that, although the appropriate client side security restriction levels of both firms are changing with the change of the financial loss value \( vL \), and the user’s unit fit cost value \( t \), the difference of the two optimal security restriction levels (i.e., \( z^*_1 - z^*_0 \)) remain the same. Under such a scenario, the profit-maximizing firm enjoys a bigger market share due to first mover advantage. In order to obtain such a division of the market, welfare-maximizing firm (Firm 0) should choose to match the price as offered by the profit-maximizing firm (Firm 1). When the profit-maximizing firm (Firm 1) is the leader, the optimal price of the cloud computing service is lower than the optimal price when the welfare maximizing firm is the leader. Based on Proposition 1(ii) & (iii), equilibrium client side security levels for both firms are positively related to the financial loss, \( vL \), incurred by the security breach, but negatively related to the user’s fit cost \( t \). This means that both firms should increase their client side security restrictions if the anticipated financial loss due to security breach is high, but lower their restriction levels if security restriction is deemed as very expensive by the users (i.e., when \( t \) is large). In contrast, the equilibrium prices for both firms are positively related to the security breach loss and user fit cost simultaneously. The profit-maximizing firm should increase the price of its cloud computing service if the financial loss due to security breach is high or if it is very expensive to make adjustment to the client side security restriction level (i.e., when \( t \) is large). The welfare-maximizing firm should choose to match the price as offered by the profit-maximizing firm regardless whichever firm is the leader.

Finally, Proposition 1 (iv) indicates social welfare is maximized and hence social optimum is achieved when the welfare-maximizing firm is the leader in the two stage sequential move game.

4 CONCLUSION AND FURTHER RESEARCH

In this work, we address issues pertinent to the client side cloud computing security restrictions in a market featuring mixed market competition. In equilibrium, the profit-maximizing firm always selects a higher security restriction level than the social welfare-maximizing firm. Optimal social welfare is achieved when the welfare-maximizing firm is the leader. This allows welfare-maximizing firms to set a security restriction level to ensure the product differentiation while not creating a significant difference in their overall market share. No matter what the firm’s objective is in the mixed market, it is always in the firm’s best interest to be the first mover. In a mixed market, the optimal price of the cloud service is determined by the potential losses for a security breach and the fit cost of the users. It is important to note that the profit-maximizing firm’s price should always equal to that of the social welfare-maximizing firm in all equilibrium.

Our research model is not without limitations. First, the security breach financial loss value \( L \) is assumed to be uniform across all types of breaches. Realistically, it may follow a different distribution. In addition, each user may value the data that is breached differently. Therefore, a specific non-uniform distribution can be adopted when supported by empirical studies. Second, there is a potential correlation between a user’s preference for security \( \lambda \) and the financial loss of his data \( L \), which is not accounted for by our model. Certainly, the model can be modified to include this correlation. However, it is readily seen that users with a higher security preference is likely to favor the service offered by the firm with higher client side security and vice versa. Based on this observation, it is expected that the results from adding the correlation between \( \lambda \) and \( L \) should only reinforce our findings reported in this work.
References

Appendix

Proof of Proposition 1(i):
Without loss of generality, we assume that \( z_0 < z_1 \). Consider the action of Firm 0 in the second stage. From (1), (2) and (3) (Substituting (2) into (3)), we have that
\[
\frac{3(p_0 - p_1)^2 + (z_0 - z_1)(-4t(-3s - t + 3vL) - 3t^2 z_0^3 + 3z_1(2t + vL - tz_1)^2 - 3t^2 z_0^2(-2vL + tz_0) + z_0(3t^2 z_1^2 - 3v^2 L^2))}{12t(z_0 - z_1)}
\]
From the first-order condition, we can easily obtain the best response price of Firm 0 such that \( p_0 = p_1 \). Therefore, in every pure equilibrium, \( p_0 = p_1 \).

We now show the existence of the equilibrium. Using (1) and (2), we see that the profit of Firm 1 is:
\[
p_1 \left( 1 - z_1 + z_0 - \frac{p_1 - p_0}{2t(z_1 - z_0)} + \frac{vL}{2t} \right)
\]
From the first-order condition, we obtain the following best response function of Firm 1 in the second stage;
\[
p_1 = \frac{p_0}{2} + \frac{(z_1 - z_0)}{2} \left[ vL + t \left( 2 - z_1 - z_0 \right) \right]
\]
The second-order condition is satisfied. Let \( p^E \) denote the equilibrium price. Substituting \( p_0 = p_1 \) (best response function of Firm 0) into (A.2), we obtain:
\[
p_1 = p_0 = p^E = (z_1 - z_0) \left[ vL + t \left( 2 - z_1 - z_0 \right) \right]
\]

Proof of Proposition 1(ii):
Suppose that Firm 0 (the leader) chooses \( z_0 = \frac{1}{4} + \frac{vL}{2t} \), substituting \( z_0 = \frac{1}{4} + \frac{vL}{2t} \) and (A.3) into (A.1),
we see that the profit of Firm 1 is:
\[
\pi_1 = -\frac{(t + 2vL - 4tz_1)(7t + 2vL - 4tz_1)^2}{128t^2}
\]
After observing \( z_0 \), Firm 1 chooses \( z_1 \) so as to maximize its profit. The first-order condition yields:
\[
z_1^* = \frac{3}{4} + \frac{vL}{2t}
\]
Since social surplus is maximized when, \( z_0 = \frac{1}{4} + \frac{vL}{2t} \), Firm 0 chooses \( z_0 = \frac{1}{4} + \frac{vL}{2t} \).

Proof of Proposition 1(iii):
Suppose Firm 1 is the leader and chooses \( z_1 \) as its security restriction level. Now consider the decision of Firm 0 over its security restriction level. Given \( z_1 \), Firm 0 chooses \( z_0 \) so as to maximize social surplus. In the proof of Lemma 1(i), we showed that \( p_0 = p_1 \) in all equilibrium regardless
whichever firm is the leader. Thus \( D_0 \mid_{p_0\neq p_1} = \bar{z} = \frac{z_1 + z_0}{2} - \frac{vL}{2t} \), is in equilibrium. Substituting this into (3), we obtain:
\[
W = \frac{1}{12t} \left[ 4t \left( 3s - t - 3vL \right) - 3t^2 z_0^3 + 3z_1 \left( 2t + vL - tz_1 \right)^2 + 3tz_0^2 \left( 2vL - tz_0 \right) + z_0 \left( 3t^2 z_1^2 - 3v^2 L^2 \right) \right]
\] (A.4)
Given $z_1$, Firm 0 chooses $z_0$ so as to maximize (A.4). The first-order condition is

$$z_0 = \frac{vL + tz_1}{3t} \quad (A.5)$$

The second condition is satisfied. Substituting $z_0$ into Firm 1 profit function we have:

$$\pi_1 = -\frac{2(vL - 2tz_1)(3t + vL - 2tz_1)^2}{27t^2}$$

Maximize Firm 1 profit function $\pi_1$ with respect to $z_1$ we have:

$$z_1^* = \frac{1}{2} + \frac{vL}{2t}$$

Substituting $z_1^*$ into

$$z_0^* = \frac{1}{6} + \frac{vL}{2t}$$

**Proof of Proposition 1(iv):**

The first best outcome is achieved when Firm 0 is the leader, while it is not when Firm 0 is the follower. Thus, obviously, *Proposition 1(iv) holds.*

Q.E.D.