An Examination of Private Intermediaries’ roles in Software Vulnerabilities Disclosure

Jessica Pu Li
Department of Management Science & Systems
School of Management
State University of New York at Buffalo
325 Jacobs Management Center
Buffalo, NY 14260-4000, USA
+1(716) 645-3285
puli@buffalo.edu

H. Raghav Rao¹
Department of Management Science & Systems
School of Management
State University of New York at Buffalo
325C Jacobs Management Center
Buffalo, NY 14260-4000, USA
+1(716) 645-3425
mgmtrao@buffalo.edu

Submitted to WEIS 2006 Conference

¹ Corresponding author
Abstract
Software vulnerability disclosure has generated much interest and debate. Recently some private intermediaries have entered this market. This paper examines the effects of such private intermediaries on optimal timing of disclosure policy made by public intermediaries and vendors’ reactions. Our analysis of private intermediaries’ role suggests that public intermediary’s optimal disclosure time does not change with private intermediary’s participation. However, a vendor’s patching time becomes less responsive to the disclosure policy. As more customers subscribe to private intermediaries’ service, the less responsive will the vendor’s patching time be. In other words, private intermediaries’ service decreases a vendor’s willingness to deliver the quick patch.

Key words: software vulnerability, disclosure, private intermediary
1. INTRODUCTION

According to the Symantec Internet Security Threat report (2003), on an average, firms experience about 30 attacks per day. Most of such attacks exploit software defects or vulnerabilities. We anticipate that vulnerabilities will continue to be discovered and disclosed in future. When a vulnerability is discovered by a malicious hacker, vulnerable computer systems are most likely to be attacked, with loss of data, sensitive information being stolen, or even worse, the whole computer system being controlled. On the other hand, when a vulnerability is discovered by a benign user, the situation is more complicated. He may just simply inform the vendor about the discovered vulnerability and give time to the vendor to fix it. This is known as the “friendly disclosure” method. Alternately, some users directly make the information about the vulnerability available public through some open forums.

A challenging issue in internet security is how to manage the disclosure of vulnerability information. In the early days of the Internet, Computer Emergency Response Team (CERT) played an extremely important role as an intermediary where the friendly disclosure of vulnerability could be carried out. After learning about the discovery of vulnerability, CERT informs the software vendor and provides them a time window to produce the patch. The typical events that CERT will do after the discovery of vulnerability are as follows. First CERT determines the severity level of the vulnerability. For severe vulnerabilities, CERT informs the related software vendor, and provides them with a certain time window (normally 45 days) as the patch development time. After that time window, CERT publicly discloses that vulnerability to all users. A vulnerability note will be created: the note includes links to patches available and also enough technical knowledge and information about that vulnerability, enabling users to take actions. Regarding the several disclosure policies that are possible, for example, immediate or non-disclosure or middle-of-the-road, there are many intensive debates about which policy should be adopted by coordinating agencies such as CERT (Symantec, 2003).

In the recent past, the marketplace of vulnerability has a new player. Some private firms such as iDefense have now started acting as private intermediaries. They pay the persons who report the vulnerabilities, provide the discovery information to users who have subscribed to the service, and also sometime report to software vendors. For instance, iDefense has been a comprehensive provider of security intelligence to government and Fortune 500 organizations (iDefense, 2005). They assist customers in avoiding or mitigating threats to their information assets, computers, networks Internet functions and proprietary information before a crisis occurs. Thereby they help to minimize potential disruption to network and business operations. Their reports are timely and offered 365 days per year (iDefense, 2005).

There is still considerable debate about when and how the vulnerabilities should be disclosed. With the new private intermediaries in the market, the proper timing to inform vulnerability disclosures becomes more complicated and unclear. Generally speaking, the disclosure policy affects three major participants. The first one is the software vendor. After the vulnerability discovery, he needs to invest in developing and testing patches, and in the meantime, suffers from loss of reputation, market share and also customer goodwill. He needs to decide when to release the patch, sooner or
later, with what quality, high or low. The second main participant is the user of the vulnerable system. He may suffer from loss of data, security breaches, and incur the cost of installing and implementing patches. The third participant is the malicious hacker. The question regarding “What is the effect of private intermediaries who provide information to their subscribed users on optimal disclosure policies?” is an open research question and is still under investigation.

The major goal of this paper is to develop a framework to examine the private intermediaries’ role in software vulnerability disclosure and focus on their effect on design of optimal policy for vulnerability disclosure. In this model, we consider vendor’s decision on when to patch, and in turn the policy makers’ action to maximize social welfare.

The rest of the paper is organized as follows. The next section discusses some existing research related to the issue of our interest. In section 3, we propose our model. Finally, we present the concluding remarks in section 4.

2. PRIOR LITERATURE

There are many papers addressing problems in information security field. One direction is to analyze security investment that software users could use to protect themselves from potential vulnerability exploits. For example, Gordon and Loeb (2002) introduce a model to achieve optimal information security investment decisions. They show that firms should make investment in information security far less than the expected loss from a security breach. Schechter and Smith (2003) discuss how to take the cost from intruder site for breaking-in, into account for security investment. Similarly, Choi et. al. (2005) model the firm’s choice of an upfront investment in the quality of the software to reduce potential vulnerabilities and how to price the software. Some other papers focus on issues of ROI on security investment. Cavusoglu et al (2004b) study security breach issues from the perspective of market value of the firm. They show that the announcement of a security breach negatively impacts the Cumulative Abnormal Return of a firm whose information systems have been breached. Campbell et al (2003) comment that only the impact of confidentiality related security breaches is negative and significant. And the impact of those non-confidentiality related security breaches is not significantly different from zero. Telang and Wattal (2005) examine the role that financial markets play in determining the impact of vulnerability disclosures on software vendors. They confirm that vulnerability disclosure adversely and significantly affects the stock performance of a software vendor.

Another direction is to study the optimal policy with regard to vulnerability disclosure. Arbaugh et al (2000) initialize a life cycle model to conduct vulnerability analysis and also show how frequently the vulnerability could be exploited since the time it is disclosed to the public. Arora et al (2003) introduce an economic model to study vendor’s decision: when to introduce the product and how much to invest on patching computers after software launch. They show that a profit-maximizing vendor will deliver a software product with less vulnerability than a socially optimal one. However, he is less willing to patch than is socially efficient. Arora (2004) examines the optimal policy for software vulnerability disclosure. That paper demonstrates how
through optimal timing of disclosure policy, policy makers can influence the behavior of vendors and also reduce the social cost. They show that, in general, neither instant disclosure nor non-disclosure is optimal. And vendors always choose to issue patches later than is socially optimal. They also imply that although early disclosure is not necessarily socially optimal, it would result in the vendor releasing a patch more quickly. However, in their paper, they made one critical assumption that vulnerability can be exploited by hackers only after a benign user discovers it. This assumption ignores the possibility that vulnerability can be exploited by hackers before a benign user discovers it. We will release this assumption in our model. In addition, in most research, there are only three main actors - vendors, users and policy makers such as CERT. The role of the private intermediaries, such as iDefense, is not considered. In this paper we consider the aspect of private intermediaries. Table 1 lists some of the key literature in the area.

<table>
<thead>
<tr>
<th>TOPIC</th>
<th>DESCRIPTION</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Investment</td>
<td>Discussion of taking cost from intruder site to security investment</td>
<td>[Schechter and Smith 2003]</td>
</tr>
<tr>
<td>Security Investment</td>
<td>Models of firm’s choice on an upfront investment in the quality of the software to reduce potential vulnerability</td>
<td>[Choi, Fershtman et al. 2005]</td>
</tr>
<tr>
<td>Market impact of security breach</td>
<td>The announcement of a security breach is negatively impact some market return of the firm</td>
<td>[Cavusoglu and Mishra et al. 2004]</td>
</tr>
<tr>
<td>Market impact of security breach</td>
<td>Comments that only the impact of confidentiality related security breaches is negative and significant</td>
<td>[Campbell and Gordon et al. 2003]</td>
</tr>
<tr>
<td>Market impact of security breach</td>
<td>The examination of the role that financial markets play in determining the impact of vulnerability disclosure on software vendors</td>
<td>[Telang and Wattal 2005]</td>
</tr>
<tr>
<td>Policy of vulnerability disclosure</td>
<td>Initialization of a life cycle model to conduct vulnerability analysis</td>
<td>[Arbaugh, Fithen et al. 2000]</td>
</tr>
<tr>
<td>Policy of vulnerability disclosure</td>
<td>Examination of vendor’s decision on when to introduce product and how much to invest on patch</td>
<td>[Arora, Caulkins et al. 2003]</td>
</tr>
<tr>
<td>Policy of vulnerability disclosure</td>
<td>Examination of the optimal timing of the disclosure policy of software vulnerability</td>
<td>[Arora 2004]</td>
</tr>
<tr>
<td>Policy of vulnerability disclosure</td>
<td>Comparisons of all available disclosure policies</td>
<td>[Cavusoglu, Huseyn Cavusoglu et al. 2004]</td>
</tr>
<tr>
<td>Policy of vulnerability disclosure</td>
<td>Analysis of the impact of vulnerability disclosure mechanisms on the decision of stakeholders</td>
<td>[Cavusoglu, Mishra et al. 2004]</td>
</tr>
<tr>
<td>Policy of vulnerability</td>
<td>Study on the optimal policy under the scenario that vulnerability affects</td>
<td>[Cavusoglu, Cavusoglu, 2005]</td>
</tr>
</tbody>
</table>
Policy of vulnerability disclosure

Empirical study on the results of the instantaneous disclosure policy with those of the responsible disclosure policy

[Arora, Krishnan et al. 2004]

Policy of vulnerability disclosure

Re-examination on vendor’s response to disclosure policy using the data set from CERT/CC

[Arora, Krishnan et al. 2005]

Market Mechanism for disclosure policy

Examination on whether a market based mechanism is better than a public agency (CERT) acting as the policy intermediaries

[Kannan and Telang 2004; Ozment 2004; Schechter 2004; Nizovtsev and Thursby 2005]

Table 1 List of recent relevant literature

While the above research provides insights into the behavior of various parties involved in the vulnerability issues, none of them examines the private intermediaries’ role in timing of software vulnerability disclosure under the situation of coexistence of public and private intermediaries. The goal of our paper is to fill this void. A contribution of this research is that this is one of the first studies, to our knowledge, to measure the influence of private intermediary on public intermediary’s decision of optimal disclosure timing and also vendor’s reaction.

3. MODEL

3.1 Software Life Cycle

Compared with previous models of vulnerability disclosure, our model has a new player, the private intermediaries. After the disclosure of software vulnerability, a vendor invests on developing and testing patches, and in the meantime, tries to minimize the cost from the loss of reputation, market share and also customer goodwill. A main assumption about a vendor is that the vendor will not disclose vulnerabilities themselves publicly unless they release the patch. Customers therefore, suffer from loss when a vulnerable system is exploited by attackers. Some of them do nothing to protect themselves until patches are available. However some others subscribe to those private intermediaries who provide them the discovery information as the return. Those private intermediaries promise to protect customers’ systems to some degree. However, we should also note that customers’ own effects are limited, in terms of fully vulnerability protection. Only after a vendor’s release of patches, the specific vulnerability problem can be solved.

We model a situation that when the vulnerability is discovered by a benign user, he reports it to the private intermediary. The motivation for him to do it is that he can get paid by the intermediary because of his discovery. In the mean time, he has the alternative either to report it to public planners (e.g. CERT) or not. It all depends on his personal preference, since CERT doesn’t pay anything to benign users for their discovery of vulnerability. We also assume that private intermediaries disclose the vulnerability information to the vendor after they get the information. That is the real practice most of the time (iDefense, 2005). For simplicity, we treat the disclosure
policy as binary, which means either full or no information is disclosed. No partial disclosure of information is involved. In our model, CERT’s goal remains the same as it appears in previous literature. Its job is to choose time T, during which vendors could develop patches before the vulnerability information is released to the public. Our main goal is to examine the change in time T with the participation of private intermediary.

Following Arbaugh et al (2000)’s software life cycle, we set the timeline for the vulnerability discovery disclosure process and patch development as follows: as shown in figure 1 and figure 2.

Figure 1. Software Life Cycle (1)

Regarding figure 1, point “0” depicts the release of the software. $T_0$ is the point of time the benign user finds the vulnerability. One assumption in (Arora A, 2004) is that they ignore the possibility that vulnerability can be exploited by hackers before a benign user discovers it. This implies that the hacker can only discover the vulnerability after a benign user discovers it. This is a strong assumption. We release this assumption here, and the hacker can discover the vulnerability either before or after a benign user finds it, as shown as case 1 and case 2 in figure 1. In other words, a malicious attacker can discover the vulnerability at $T_h$ and immediately exploit it, if he doesn’t find the vulnerability before public disclosure. The reason to assume instant exploit is because based the report from (Symantec, 2003), approximately 60% of the documented vulnerabilities can be exploited almost instantly because either no exploit tool is needed or exploit codes can be found easily via Internet free downloads.

Figure 2. Software Life Cycle (2)
We also assume that vendor releases the patches at timeslot $\tau + T_0$. It can be either before or after the public disclosure of vulnerability. In order to effectively examine the impact of private intermediary’s role on vulnerably disclosure policy, we keep all the other assumptions of the model developed by (Arora A, 2004) the same. Based on their initial model, we have added into it another new player, which is the private intermediary. This is the main difference between the two models. We have two assumptions in our model. The first is that a vendor will not disclose vulnerability publicly unless it releases the corresponding patch. The second is that when a benign user finds the vulnerability, he or she informs both the public and private intermediaries. Table 2 shows the notations used in the model.

<table>
<thead>
<tr>
<th>Notations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_0$</td>
<td>The calendar time that benign user identifies the vulnerability</td>
</tr>
<tr>
<td>$T_h$</td>
<td>The calendar time that the hacker identifies the vulnerability</td>
</tr>
<tr>
<td>$C(\tau)$</td>
<td>Vendor’s patch development cost</td>
</tr>
<tr>
<td>$T$</td>
<td>The time window of vulnerability disclosure by public intermediary</td>
</tr>
<tr>
<td>$\tau$</td>
<td>The time window of patch development by vendor</td>
</tr>
</tbody>
</table>

**Scenario 1:** There is no participation of private intermediary

- $T^*$: The optimal time window of vulnerability disclosure by public intermediary
- $\tau^*$: The optimal time window of patch development by vendor
- $V$: Vendor’s total cost
- $\theta(\tau, T)$: Total customers’ cost
- $S$: Total social cost

**Scenario 2:** There is participation of private intermediary

- $T_i^*$: The optimal time window of vulnerability disclosure by public intermediary
- $\tau_i^*$: The optimal time window of patch development by vendor
- $V_i$: Vendor’s total cost
- $\theta_i(\tau, T)$: Total customers’ cost
- $S_i$: Total social cost

Table 2. Notations

3.2 Cost Functions

Vendor’s cost can be characterized in two parts. The first part is its investment on patch development and testing, which can be represented as $C(\tau)$. Based on common sense, the faster the patch is released, the higher the development cost is, which means $\frac{\partial C(\tau)}{\partial \tau} < 0$. The second part comes from the loss of reputation and customer goodwill. Similar to the model of (Arora A, 2004), a vendor takes responsibility for a proportion of customer’s loss, which can be represented as $\lambda$. Originally in their model (Arora A, 2004), customer’s loss function is $\theta(\tau, T)$, a function of the time window of disclosure of the policy and patching, which are $T$ and $\tau$. However, in our model, some customers subscribe to private intermediary’s vulnerability-disclosure service. And they can initiate some self-protection instead of just waiting for vendor’s release of patches. We believe that those customers would suffer a lower loss. We
assume that a proportion of $\alpha$ customers subscribe to this service, where $0<\alpha<1$. Because of their self-awareness and self-protection, their losses can be reduced to a proportion of $\beta$, where $0<\beta<1$. Since the subscription fee is always very low compared to the potential vulnerability cost incurred by customers, we assume the cost of subscription is zero. So the total customer loss function can be viewed as follows:

$$\theta(\tau, T) = (1 - \alpha)\theta(\tau, T) + \alpha \beta \theta(\tau, T)$$

$$= (1 - \alpha + \alpha \beta)\theta(\tau, T)$$

$$= \delta \theta(\tau, T),$$

where $\delta = 1 - \alpha + \alpha \beta$, where $0<\delta<1$.

So the vendor’s cost can also be expressed as follows:

$$V_i = C(\tau) + \lambda \delta \theta(\tau, T)$$

(2)

Here the social cost simply comes from two sources, the vendor and the customers. So the social cost function can be expressed as follows:

$$S_i = C(\tau) + \delta \theta(\tau, T)$$

(3)

The comparison of cost functions with (Arora A, 2004)’s model is as follows:

<table>
<thead>
<tr>
<th></th>
<th>Arora A 2004 Model</th>
<th>Our Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Cost</td>
<td>$V = C(\tau) + \lambda \theta(\tau, T)$</td>
<td>$V_i = C(\tau) + \lambda \delta \theta(\tau, T)$</td>
</tr>
<tr>
<td>Customer Cost</td>
<td>$\theta(\tau, T) = \theta(\tau, T)$</td>
<td>$\theta_i(\tau, T) = \delta \theta(\tau, T)$</td>
</tr>
<tr>
<td>Social Cost</td>
<td>$S = C(\tau) + \theta(\tau, T)$</td>
<td>$S_i = C(\tau) + \delta \theta(\tau, T)$</td>
</tr>
</tbody>
</table>

3.3 Propositions

**Proposition 1:**
Public intermediary’s optimal disclosure time $T^*$ doesn’t change with private intermediary’s participation

Recall that from equation (3), the first order condition (FOC) for public intermediary’s new optimal disclosure policy $T_i^*$ is

$$\frac{dS_i}{dT} = \frac{\partial C}{\partial \tau} \frac{d\tau}{dT} + \frac{\partial \theta}{\partial \tau} \frac{d\tau}{dT} + \frac{\partial \delta \theta}{\partial \tau}$$

(4)

Regarding the vendor, the first order condition (FOC) for vendor’s new optimal release policy $\tau^*$ is

$$\frac{\partial C}{\partial \tau} + \lambda \delta \frac{\partial \theta}{\partial \tau} = 0$$

(5)

Insert equation (5) into equation (4), we can get as follows:
\[
\frac{dS'}{dT} = -\lambda \theta \frac{\partial \theta}{\partial \tau} + \lambda \theta \frac{\partial ^2 \theta}{\partial \tau \partial T} + \lambda \theta \frac{\partial \theta}{\partial T}
\]
\[
= (1 - \lambda) \frac{\partial \theta}{\partial \tau} + \lambda \theta \frac{\partial \theta}{\partial T}
\]
\[
= (1 - \lambda) \frac{\partial \theta}{\partial \tau} + \frac{\partial \theta}{\partial T} = 0
\]

Compared to original optimal \(T^*\), which is the solution of equation (Arora, 2004)
\[
(1 - \lambda) \frac{\partial \theta}{\partial \tau} + \frac{\partial \theta}{\partial T} = 0
\]

Arora (2004) has proved that \(S\) is locally convex in \(T\) and there exists a point that makes \(\frac{dS}{dT} = 0\). From equation (6) and (7) which are exactly the same, we know that the two optimal \(T^*\) are the same, which is \(T^* = T_{i^*}\). This means that the public intermediary’s optimal disclosure time \(T^*\) doesn’t change with private intermediary’s participation. On an aside, we also notice that the coexistence of a profit-based private intermediary and a non-profit-based public intermediary could yield a higher social welfare than the only existence of non-profit-based public intermediary.

**Proposition 2:**

Vendor’s optimal patch release time window \(\tau\) is increased with the private intermediary’s participation.

Vendor’s original cost function is
\[
V = C(\tau) + \lambda \theta(\tau, T) \tag{8}
\]
Vendor’s new cost function has been changed to
\[
V_i = C(\tau) + \lambda \delta \theta(\tau, T) \quad \text{where } 0 < \delta < 1 \tag{9}
\]

Regarding function (8), the original optimal \(\tau^*\) can be calculated with FOC (first order condition), which satisfies
\[
\frac{\partial C}{\partial \tau} + \lambda \frac{\partial \theta}{\partial \tau} = 0 \tag{10}
\]

Regarding function (9), new optimal \(\tau_i^*\) satisfies
\[
\frac{\partial C}{\partial \tau} + \lambda \delta \frac{\partial \theta}{\partial \tau} = 0 \quad \text{where } 0 < \delta < 1 \tag{11}
\]

And the longer the time is taken for the patch to be released, the lower the investment cost will be; however, the longer the time for the patch to be released, the higher the loss of customer will be.

This means: \(\frac{\partial C}{\partial \tau} < 0, \text{and } \frac{\partial \theta}{\partial \tau} > 0\)

It is easy to see here, \(\tau^*\) which satisfies equation (10), makes the left site of equation (11) less than zero, which means,
\[
\frac{\partial C}{\partial \tau^*} + \lambda \delta \frac{\partial \theta}{\partial \tau^*} < 0 \tag{12}
\]

As the release time window \(\tau\) increases, the increase rate of the investment cost \(C\) will become lower. Since the investment cost \(C\) will become less sensitive to time
window \( \tau \) as \( \tau \) becomes larger and larger. Regarding customer loss, it is the reverse. As the release time window \( \tau \) increases, the increase rate of the customer loss will become higher, due to propagation effects and network effects, which are prevalent in the computer software industry. This implies
\[
\frac{\partial^2 C(\tau)}{\partial \tau^2} < 0 \quad \text{and} \quad \frac{\partial^2 \theta(\tau)}{\partial \tau^2} > 0
\]

So here, as \( \tau \) increases, \( \frac{\partial C}{\partial \tau} \) is less negative, \( \lambda \delta \frac{\partial \theta}{\partial \tau} \) is more positive, together makes (12) tend to 0.
So we can see that \( \tau^* < \tau_i^* \)

The intuition behind this phenomena is the following: With the participation of private intermediary, some customers who have subscribed to the service of the intermediary could protect their computer systems to some extent and their losses are reduced. The total loss from all customers is also reduced. So the vendor is liable to face a smaller loss to customers. The vendor will face less pressure to release the patch earlier. This also suggests that vendor’s patching time becomes less responsive to public intermediary’s disclosure policy.

**Proposition 3:**
As more customers subscribe to the awareness service offered by private intermediary, the longer the optimal patch release time window \( \tau \) tends to be.

Here the assumption is that each customer, who subscribes to the service, offered by private intermediary, will carry out self-protection of own computer systems after they are aware of the software vulnerability notified by the private intermediary. The more the customers subscribe, the lower is the total customers’ loss, which leads to a smaller \( \delta \).

We can compare the two functions with different \( \delta \), where \( \delta_1 > \delta_2 \)
Vendor’s cost function with \( \delta_1 \) is
\[
V_1 = C(\tau) + \lambda \delta_1 \theta(\tau, T)
\]
Vendor’s cost function with \( \delta_2 \) is
\[
V_2 = C(\tau) + \lambda \delta_2 \theta(\tau, T)
\]

Regarding function (13), the optimal \( \tau_1^* \) can be calculated with FOC (first order condition), which satisfies
\[
\frac{\partial C}{\partial \tau} + \lambda \delta_1 \frac{\partial \theta}{\partial \tau} = 0
\]
(15)

Regarding function (14), optimal \( \tau_2^* \) satisfies
\[
\frac{\partial C}{\partial \tau} + \lambda \delta_2 \frac{\partial \theta}{\partial \tau} = 0
\]
(16)

As explained in proposition 2, here we know:
\[
\frac{\partial C}{\partial \tau} < 0, \text{ and } \frac{\partial \theta}{\partial \tau} > 0
\]

It is easy to see here, \( \tau_1^* \) which satisfies equation (15), makes the left site of equation (16) less than zero, which means,
\[
\frac{\partial C}{\partial \tau_1^*} + \lambda \delta \frac{\partial \theta}{\partial \tau_1^*} < 0 \quad (17)
\]

Using the same logic as in proposition 2, as \( \tau \) increases, \( \frac{\partial C}{\partial \tau} \) is less negative, \( \lambda \delta \frac{\partial \theta}{\partial \tau} \) is more positive, together makes (17) goes to 0. So, we can conclude that \( \tau_1^* < \tau_2^* \).

It is straightforward to see that as more customers get vulnerability notices from the private intermediary, more customers will do self-protection. Then the total liability that vendor is responsible to customers becomes lower. This has similar effects as in proposition 2, which suggests that vendor’s patching time becomes less responsive to public intermediary’s disclosure policy.

4. CONCLUSIONS

Recently, some private security organizations (e.g. iDefense, ISS Inc.) are actively involved in discovering vulnerabilities. In fact, some organizations such as iDefense, have vulnerability contributor programs to encourage users to submit vulnerability information to them to get paid in return. Then those firms pass the vulnerability knowledge to their customers who have subscribed to their services. In the meantime, both iDefense and ISS Inc. inform the affected vendor about the reported vulnerability at the same time or before releasing the vulnerability knowledge to their subscribers.

In this paper, we propose an approach to analyze private intermediary’s impact on disclosure issues of software vulnerabilities. We find that from the social welfare standpoint, public intermediary’s optimal disclosure time doesn’t change with private intermediary’s participation. In the meantime, their service could allow some individual customers who have subscribed to their services to reduce their expected loss from attacks. From public intermediary’s perspective, it improves social welfare. From the vendor’s perspective, they are liable to less loss from customers. Then its optimal patching time becomes less responsive to the public intermediary’s disclosure policy. More customers who subscribe to private intermediary’s service are, less responsive will vendor’s patching time be. In other words, private intermediaries’ service decreases vendor’s willingness to deliver the quicker patch.

There are several research extensions that can be addressed in future research. The profit-seeking organization always pays the users who discover the vulnerability. The impact of monetary incentives may even raise competition between benign users and hackers in the vulnerability discovery process. This aspect is not considered in our current model. In all, our model is a simplified and preliminary one. Only the impact of private intermediary on vulnerability disclosure timing is considered, where we focus on customer’s reduced expected loss. And our model doesn’t control for the quality of patch. Additional resource allocated to patch investment could result in higher quality patch than a patch that is released sooner.
5. REFERENCES


