Inf Syst Front (2007) 9:531–539
DOI 10.1007/s10796-007-9047-2

An examination of private intermediaries' roles in software vulnerabilities disclosure

Pu Li · H. Raghav Rao

Published online: 6 October 2007

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 patch time increases when the probability of information leakage is low, if not non-existent. In other words, private intermediaries' service decreases a vendor's willingness to deliver quick patches. Empirical evidence with 1493 vulnerability observations from CERT/CC and other 326 different vulnerability observations from iDefense provided support for our analytical results.

Keywords Software vulnerability · Disclosure · Private intermediary

1 Introduction

Information security breaches pose a significant threat to national security and economic well-being. The economics of information security has already become a thriving and fast-moving discipline. Privacy, bugs, and spam are no longer the only topics in this field. System dependability, policy and more general security questions are also being raised (Anderson and Moore 2006). Most such attacks exploit software defects or vulnerabilities. Without doubt, further vulnerabilities will continue to be discovered and disclosed in the future. When a vulnerability is discovered by a malicious hacker, unprotected computer systems are the most likely to be attacked., leaving open the potential of loss of data, sensitive information being stolen, or even worse, the entire computer system being controlled by an outside source. A challenging issue in internet security is how to manage the disclosure of vulnerability information. In the early days of the Internet, the Computer Emergency Response Team (CERT) played an extremely important role as an intermediary where the friendly disclosure of vulnerabilities could be carried out. Upon being alerted of the discovery of a vulnerability, CERT informs the software vendor and provides them a time window to produce a patch. The typical events CERT executes after the discovery of a 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) for patch development. After this window passes, CERT publicly discloses the vulnerability to all users. There are many intensive debates about which policy should be adopted by coordinating agencies such as CERT regarding the multiple disclosure policies in place such as immediate disclosure, non-disclosure, or middle-of-the-road, (Symantec 2003).

In the recent past, the vulnerability marketplace has seen the entry of some new players. Private firms such as iDefense and tippingPoint have now started acting as private intermediaries. They pay the persons who report

The earlier version of this paper was presented at Secure Knowledge Workshop (SKW)-2006 in New York City, and received best student paper award.

P. Li · H. R. Rao (✉)
State University of New York,
Buffalo, NY 14260, USA
e-mail: mgmtrao@buffalo.edu

P. Li
e-mail: puli@buffalo.edu

the vulnerabilities, provide the discovery information to users who have subscribed to the service, and also at times report to the 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 mitigating threats to their information assets, computers, networks functions, and proprietary information before a crisis occurs. In other words, they help to minimize potential disruptions to network and business operations. Their reports are timely and offered 365 days per year (iDefense 2005). Furthermore, they provide monetary rewards to the identifiers of each vulnerability reported. Their clients/subscribers can protect themselves against potential attacks for each specific vulnerability based on the information provided by the private intermediaries. However, the market-based intermediary's incentive to leak the vulnerability information inappropriately is of great concern. This may result in non-subscribers becoming exposed to potential attacks (Kannan and Telang 2005).

With the new private intermediaries in the market, the proper timing to inform vulnerability disclosures becomes complicated and unclear. The disclosure policy affects three major participants. First is the software vendor. After a vulnerability discovery, vendors need to invest in developing and testing patches. In the meantime, they suffer from a loss of reputation, market share, and also customer goodwill. The vendor needs to debate the merits of how to issue the patch; sooner with lower quality, or a higher quality patch at a later time. The second main participant is the user of the vulnerable system. The users may suffer from loss of data, breach of security, and also incur the cost of installing and implementing patches. The third participant is the malicious hacker.

The question "What effect do private intermediaries who provide information to their subscribed users have on optimal disclosure policies?" is an open research topic still under investigation. Monetary incentives to discover vulnerabilities may encourage benign identifiers to invest more effort and time to find them (Kannan and Telang 2005), allowing the clients of those private intermediaries to benefit. Also, the increase in the number of clients who subscribe to the services leads to a negative externality with respect to the effort of the hackers. As a result, the corresponding software vendors suffer *less* loss of reputation, *less* loss of future sales, and *fewer* contractual service obligations and legal liabilities. Thus, the incentive to develop patches quickly is decreased. On the other hand, this same incentive can also lead to a race for vulnerability discoveries between benign users and hackers as pointed out by Kannan and Telang (2005). When the number of vulnerabilities discovered by hackers increases, both vendor and user losses will increase. Furthermore, if the private intermediary leaks information in order to increase their own benefits, the scenario becomes even more complicated. This occurs when the private intermediary leaks the vulnerability information to the public without any safeguards. While the private intermediary's own subscribers are protected, this leaves non-subscribers exposed to more attacks, (Kannan and Telang 2005).

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 the 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 second section discusses some existing research related to the issue of our interest. In section three, we propose our model and discuss empirical evidence that supports our analysis. Finally, we present the concluding remarks and future work in section four.

2 Prior literature

There are many papers addressing problems in the information security field. One approach is to analyze security investments 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 investments in information security for far less than the expected loss incurred from a security breach. They also show that the optimal level of information security spending does not always increase with the expected loss from the attacks. Schechter and Smith (2003) discuss how to take the cost from an intruder breaking-in to the site into account in security investment. Similarly, Choi et al. (2005) model the firm's choice of an upfront investment in quality software to reduce potential vulnerabilities and how to price the software. Some other papers focus on 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. The impact of those non-confidential 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 significantly affects the stock performance of a software vendor in an adverse manner.

Another angle 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 before the time at which it is disclosed to the public. Arora et al. (2003) introduce an economic model to study the 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 fewer vulnerabilities than a socially optimal one. However, they are less willing to patch than one who is socially efficient. Arora et al. (2004b) examines the optimal policy for software vulnerability disclosure. Arora's paper demonstrates that 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. 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: the vulnerabilities can be exploited by hackers only after a benign user discovers it. This assumption ignores the possibility that the vulnerability can be exploited by hackers before it is discovered by a benign user. We will not make this assumption in our model. Additionally, in most research, there are only three main participants—vendors, users, and the policy makers such as CERT. The role of the private intermediaries, such as iDefense, is not considered. In this paper, we do consider the aspect of private intermediaries. Table 1 lists some of the key literatures in the area.

While the above research provides insights into the behavior of various parties involved in the vulnerability issues, none of them examines the role of the private intermediaries in the 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. To our knowledge, this is one of the first studies to measure the influence of private intermediation on public intermediary's decision of optimal disclosure timing and vendor reactions.

Table 1 List of recent relevant literatures

Topic	Description	Source
Security investment	Introduction of a model for optimal information security investment decisions	(Gordon and Loeb 2002)
Security investment	Discussion of taking cost from intruder site to security investment	(Schechter and Smith 2003)
Security investment	Models of firm's choice of an upfront investment in the quality of the software to reduce potential vulnerability	(Choi et al. 2005)
Market impact of security breach	The announcement of a security breach is negatively impact some market return of the firm	(Cavusoglu et al. 2004b)
Market impact of security breach	Comments that only the impact of confidentiality related security breaches is negative and significant	(Campbell et al. 2003)
Market impact of security breach	The examination of the role that financial markets play in determining the impact of vulnerability disclosure on software vendors	(Telang and Wattal 2005)
Policy of vulnerability disclosure	Initialization of a life cycle model to conduct vulnerability analysis	(Arbaugh et al. 2000)
Policy of vulnerability disclosure	Examination of vendor's decision on when to introduce product and how much to invest on patch	(Arora et al. 2003) (Arora et al. 2004b)
Policy of vulnerability disclosure	Examination of the optimal timing of the disclosure policy of software vulnerability	(Arora et al. 2004b)
Policy of vulnerability disclosure	Comparisons of all available disclosure policies	(Cavusoglu et al. 2004a)
Policy of vulnerability disclosure	Analysis of the impact of vulnerability disclosure mechanisms on the decision of stakeholders	(Cavusoglu et al. 2004b)
Policy of vulnerability disclosure	Study on the optimal policy under the scenario that vulnerability affects multiple vendors	(Cavusoglu et al. 2005)
Policy of vulnerability disclosure	Empirical study on the results of the instantaneous disclosure policy with those of the responsible disclosure policy	(Arora et al. 2004a)
Policy of vulnerability disclosure	Re-examination on vendor's response to disclosure policy using the data set from CERT/CC	(Arora 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 2005; Ozment 2004; Schechter 2004; Nizovtsev and Thursby 2005)

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 a software vulnerability, a vendor invests in the development and testing of patches, while at the same time, tries to minimize the costs from loss of reputation, market share, and customer goodwill. A main assumption about a vendor is that they will not publicly disclose vulnerabilities themselves until they release the patch. Customers therefore suffer losses when their vulnerable systems are exploited by attackers. Some of them do nothing to protect themselves until patches are available. Others however subscribe to those private intermediaries who provide discovery information in return. These private intermediaries promise to protect customers' systems to some degree. However, we should also note that customers' own effects are limited, in terms of full vulnerability protection. Only after a vendor's release of a patch can the specific vulnerability problem be solved.

We model the situation such that when the vulnerability is discovered by a benign user, they report it to the private intermediary. The motivation for one to do so is to receive payment from the intermediary for their discovery. In the mean time, they have the choice to report the vulnerability to public planners (e.g. CERT) or not. CERT doesn't pay anything to benign users for the discovery of vulnerabilities, so it entirely depends on the goodwill of the benign user. We also assume that private intermediaries disclose the vulnerability information to the vendor after they receive the information. This summarizes actual practice for most instances (iDefense 2005). For simplicity, we treat the disclosure policy as binary, which means either all or none of the information is disclosed. No partial disclosure of information is involved. In our model, CERT's goal remains the same as in previous literature. Its job is to choose time frame 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 including the participation of a private intermediary.

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

Regarding Fig. 1, point "0" depicts the release of the software. T_0 is the point in time when the benign user finds the vulnerability. One assumption in (Arora et al. 2004a) is that they ignore the possibility that the vulnerability can be exploited by hackers before a benign user discovers it. This implies that the hacker can only exploit the vulnerability after a benign user discovers it with no ability to discover it themselves. This is a strong assumption. Instead we will assume that a hacker can discover the vulnerability either before or after a benign user finds it. These possibilities are shown as case 1 and case 2 in Fig. 1. In other words, a malicious attacker can discover the vulnerability at T_h and immediately exploit it, if he does not find the vulnerability before public disclosure. The reason to assume instant exploitation is based on the report from (Symantec 2003), which states approximately 60% of 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.

We also assume that vendor releases the patches at timeslot $\tau+T_0$. It can be either before or after public disclosure of the vulnerability. In order to effectively examine the impact of the private intermediary's role on vulnerability disclosure policy, we keep all the other assumptions of the model developed by (Arora et al. 2004b) the same. We add an additional player to the model, 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 a vulnerability publicly until it releases the corresponding patch. The second is that when a benign user finds the vulnerability, he or she informs both the public and the private intermediaries. By definition, the benign identifier does not exploit the vulnerability. Table 2 shows the notations used in the model.

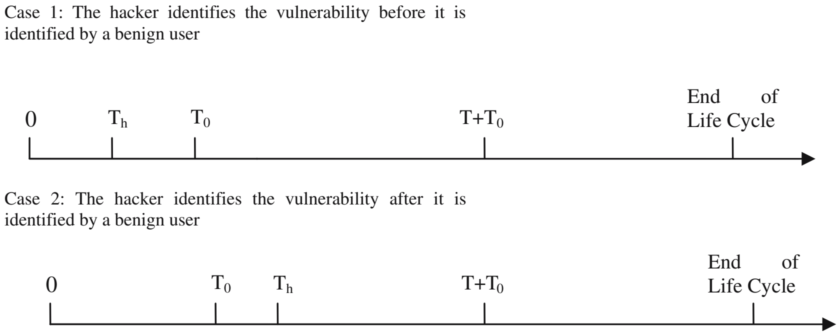
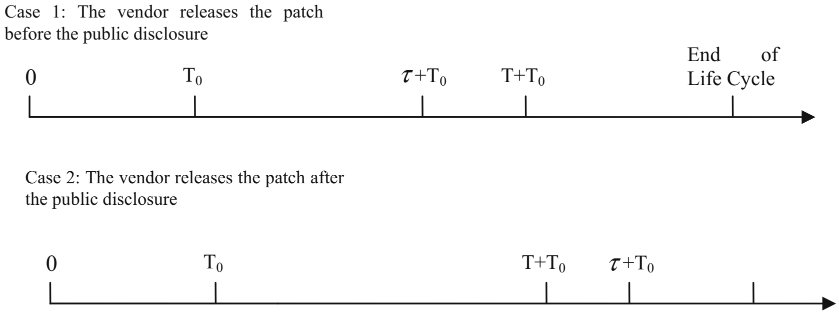

Case 1: The hacker identifies the vulnerability before it is identified by a benign user
0
T_h
T_0
$T+T_0$
End of Life Cycle
Case 2: The hacker identifies the vulnerability after it is identified by a benign user
0
T_0
T_h
$T+T_0$
End of Life Cycle

Fig. 1 Software life cycle (1)

Fig. 2 Software life cycle (2)


Case 1: The vendor releases the patch before the public disclosure
0
T0
τ+T0
T+T0
End of Life Cycle
Case 2: The vendor releases the patch after the public disclosure
0
T0
T+T0
τ+T0

According to Kannan and Telang (2005), there are two possible markets with two different behaviors by the private intermediaries, depending on whether information leakage occurs. In a "regulated" market, private intermediaries do not misuse information, inform the vendor, and disclose the information responsibly. Inappropriate information leakage does not occur in this case. However, in an "unregulated" market, private intermediaries may misuse information. The vulnerability information can be disclosed to the public without proper safeguards. Thus, hackers can easily exploit this vulnerability to attack non-subscribers. The following sections will focus on scenarios where information leakage is low.

3.2 Cost functions

Vendor costs can be characterized into two parts. The first is investment on patch development and testing. This is 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 et al. 2004b), a vendor takes responsibility for a proportion of customer's loss, which can be represented as λ. Originally in their model (Arora et al. 2004b), customer's loss function is represented by $\theta(\tau, T)$, a function of the time window of disclosure of the policy, and the patching itself, which are T and τ. However, in our model, some customers subscribe to private intermediary's vulnerability-disclosure service. 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. In the low information leakage market, non-subscribers do not suffer from private intermediary's misusage and instant disclosure of this vulnerability which cause unexpected attacks from hackers. Overall social welfare loss will decrease due to clients' subscriptions and their self protections. We assume that a proportion of α 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 β, 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:

$$\begin{aligned}\theta_j(\tau, T) &= (1-\alpha)\theta(\tau, T) + \alpha\beta\theta(\tau, T)\\ &= (1-\alpha+\alpha\beta)\theta(\tau, T)\\ &= \delta\theta(\tau, T),\end{aligned} \tag{1}$$

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

The vendor's cost can also be expressed as follows:

$$V_i = C(\tau) + \lambda\delta\theta(\tau, T) \tag{2}$$

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

$$S_i = C(\tau) + \delta\theta(\tau, T) \tag{3}$$

Table 2 Notations

Parameters	Description
T_0	The calendar time that benign user identifies the vulnerability
T_h	The calendar time that the hacker identifies the vulnerability
$C(\tau)$	Vendor's patch development cost
T	The time window of vulnerability disclosure by public intermediary
τ	The time window of patch development by vendor
T^*	The optimal time window of vulnerability disclosure by public intermediary
τ^*	The optimal time window of patch development by vendor
V	Vendor's total cost
$\theta(\tau, T)$	Total customers' cost
S	Total social cost

3.3 Propositions

3.3.1 Proposition 1

Public intermediary's optimal disclosure time T^* does not change with private intermediary's participation.

Recall that from Eq. 3, the first order condition (FOC) for public intermediary's new optimal disclosure policy T_j* is

$$\frac{dS_i}{dT} = \frac{\partial C}{\partial \tau}\frac{d\tau}{\partial T} + \frac{\delta\partial\theta}{\partial \tau}\frac{d\tau}{\partial T} + \frac{\delta\partial\theta}{\partial T} \tag{4}$$

Regarding the vendor, the first order condition (FOC) for vendor's new optimal release policy τ* is

$$\frac{\partial C}{\partial \tau} + \lambda\delta\frac{\partial\theta}{\partial \tau} = 0 \tag{5}$$

Insert Eq. 5 into Eq. 4, we can get as follows:

$$\begin{aligned}\frac{dS'}{dT} &= -\lambda\delta\frac{\partial\theta}{\partial\tau}\frac{d\tau}{\partial T} + \frac{\delta\partial\theta}{\partial\tau}\frac{d\tau}{\partial T} + \frac{\delta\partial\theta}{\partial T}\\ &= (1-\lambda)\frac{\delta\partial\theta}{\partial\tau}\frac{d\tau}{\partial T} + \frac{\delta\partial\theta}{\partial T}\\ &= (1-\lambda)\frac{\partial\theta}{\partial\tau}\frac{d\tau}{\partial T} + \frac{\partial\theta}{\partial T} = 0\end{aligned} \tag{6}$$

Compared to original optimal T*, which is the solution of equation (Arora et al. 2004b)

$$(1-\lambda)\frac{\partial\theta}{\partial\tau}\frac{d\tau}{\partial T} + \frac{\partial\theta}{\partial T} = 0 \tag{7}$$

Arora et al. (2004b) has proved that S is locally convex in T and there exists a point where $\frac{dS}{dT} = 0$. From Eqs. 6 and 7 which are exactly the same, we know that the two optimal T* are the same, which is $T^* = T_j^*$. 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.

3.3.2 Proposition 2

With low information leakage, vendor's optimal patch release time window τ 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

$$V_i = C(\tau) + \lambda\delta\theta(\tau, T) \text{ where } 0 < \delta < 1 \tag{9}$$

Regarding function 8, the original optimal τ* 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 τ_i∗ satisfies

$$\frac{\partial C}{\partial \tau} + \lambda\delta\frac{\partial\theta}{\partial \tau} = 0 \text{ where } 0 < \delta < 1 \tag{11}$$

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 the customer will be.

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

It is easy to see here, when information leakage is low, 0<δ<1, and since τ* satisfies Eq. 10, this means the left site of Eq. 11 is less than zero,

$$\frac{\partial C}{\partial \tau^*} + \lambda\delta\frac{\partial\theta}{\partial \tau^*} < 0 \tag{12}$$

As the release time window τ increases, the increase rate of the investment cost C will become lower. Since the investment cost C will become less sensitive to time window τ as τ becomes larger and larger. Regarding customer loss however, the reverse is true. As the release time window τ 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

$$\frac{\partial^2 C(\tau)}{\partial\tau^2}0$$

So here, as τ increases, $\frac{\partial C}{\partial\tau}$ is less negative, $\lambda\delta\frac{\partial\theta}{\partial\tau}$ is more positive, and together this makes 12 tend to 0.

So we can see that $\tau* < \tau_i*$

The intuition behind the phenomena is the following: When information leakage is low to non-existent, participation of private intermediaries can allow some customers who have subscribed to the service of the intermediary to protect their computer systems to some extent, reducing their losses. The total loss from all customers is reduced. Thus the vendor is liable to face a smaller loss from customers. The vendor will face less pressure to release the patch earlier. This also suggests that vendor's patching time becomes less responsive to the public intermediary's disclosure policy. In the same time, many vendors may have a long and stable relationship with CERT, rather than the third private intermediaries. They may not take their notes very seriously and respond to the same degree as they could have done with CERT. This may also delay its time to patch.

3.3.3 Proposition 3

With low information leakage, as more customers subscribe to the awareness service offered by private intermediaries, the longer the optimal patch release time window τ will tend to be.

Here the assumption is that each customer who subscribes to the service offered by a private intermediary, will carry out self-protection of their own computer systems after they are aware of the software vulnerability when notified by the private intermediary. With low information leakage, the more customers that subscribe, the lower the total customers' loss. This leads to a smaller δ.

We can compare the two functions with different δ, where $\delta_1 > \delta_2$

Vendor's cost function with δ_1 is

$$V_1 = C(\tau) + \lambda\delta_1\theta(\tau, T) \tag{13}$$

Vendor's cost function with δ_2 is

$$V_2 = C(\tau) + \lambda\delta_2\theta(\tau, T) \tag{14}$$

Regarding function 13, the optimal τ_1* can be calculated with FOC (first order condition), which satisfies

$$\frac{\partial C}{\partial \tau} + \lambda\delta_1 \frac{\partial \theta}{\partial \tau} = 0 \tag{15}$$

Regarding function 14, optimal τ_2* satisfies

$$\frac{\partial C}{\partial \tau} + \lambda\delta_2 \frac{\partial \theta}{\partial \tau} = 0 \tag{16}$$

As explained in proposition 2, here we know:

$$\frac{\partial C}{\partial \tau} < 0, \; and \; \frac{\partial \theta}{\partial \tau} > 0$$

It is easy to see here, τ_1* which satisfies Eq. 15, makes the left side of Eq. 16 less than zero, which means,

$$\frac{\partial C}{\partial \tau_1 *} + \lambda\delta \frac{\partial \theta}{\partial \tau_1 *} < 0 \tag{17}$$

Using the same logic as in proposition 2, as τ increases, $\frac{\partial C}{\partial \tau}$ is less negative, $\lambda\delta\frac{\partial \theta}{\partial \tau}$ is more positive, and together makes 17 go to zero.

So, we can conclude that $\tau_1* < \tau_2*$

Based on the same logic, it is easy to see that the result is reversed when $\delta > 1$.

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

Table 3 Two sample *Z* test for means of public release time

	CERT	IDefense
Mean release time	52.44	61.55
Known variance	103.00	64.00
Observations	1493.00	326.00
Hypothesized mean difference	0.00	
Z	−16.88	
P(*Z*<=*z*) two-tail	0.24	

Table 4 *Z* test: two sample for means of patch time

	CERT	iDefense
Mean	55.25	70.33
Known variance	50.00	70.00
Observations	1493.00	326.00
Hypothesized mean difference	0.00	
Z	−35.90	
P(*Z*<=*z*) two-tail	0.00	

3.4 Empirical evidence

CERT/CC published a total of 1,570 vulnerability notes from 2002 to 2006. iDefense published 387 additional vulnerability notes, unique from the CERT/CC notes of the same time period. From these, we dropped the observations wherein either the "vendor patch time window" or the "public disclosure time window" was not available. In other words, we retained only the observations with both attributes "vendor patch time window" and "public disclosure time window" available in our study. This leaves us with 1,819 total vulnerability observations; 1,493 coming from CERT/CC and 326 vulnerability observations from iDefense.

The average *public disclosure time* window for the vulnerabilities published in CERT/CC is 52.44 days. Since those vulnerabilities were not in the notes from iDefense, we could approximate them as the market without the participation of private intermediaries. The average public disclosure time window for the vulnerabilities published in iDefense is 61.55 days. We conducted *Z* test to check whether the difference between the two sample means was statistically significant or not. The reason we choose *Z* test instead of ANOVA or *t* test is because the latter requires the same number of data points and we have a different number of data points from the data sets of iDefense and CERT. The result shows that the difference between the two means is not significant. The detailed *Z* test result is shown in Table 3. The non-significance between the two means provides us the empirical evidence to support proposition 1 (Public intermediary's optimal disclosure time * does not change with private intermediary's participation).

The average *patch time window* is 55.25 days for the vulnerabilities published in CERT/CC. However, the average patch time window is 70.33 days for the vulner-

Table 5 Average patch time in iDefense

Time	2002	2003	2004	2005	2006
Average patch time	25	74	54	75	93

abilities published in iDefense. The Z test result in Table 4 shows that this difference is statistically significant. Extensive queries of Google and other public sources uncovered no previous instances of information leakage from iDefense. Thus it is reasonable that we approximate iDefense as a market with low information leakage. It provides us the empirical evidence to support proposition 2, where the optimal patch release time increased with the participation of private intermediaries (With low information leakage, vendor's optimal patch release time window is increased with the private intermediary's participation).

Furthermore, the average patch time windows for the vulnerabilities published in iDefense are exhibited in Table 5.

Excepting for a drop from 74 in 2003 to 54 in 2004, the average trend is increasing. As reported by iDefense (2005), the number of subscribers has been growing since 2002. This provides us the empirical evidence to support proposition 3, *where the more customers subscribe to the service provided by private intermediaries, the longer the optimal patch time will be*.

4 Conclusions and future research

Recently, some private security organizations (e.g. iDefense, tipplingPoint, ISS Inc.) are actively involved in discovering vulnerabilities. In this paper, we propose an approach to analyze private intermediary's impact on disclosure issues of software vulnerabilities. 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 increases in the market given low information leakage. In other words, private intermediaries' service decreases a vendor's willingness to deliver a patch quickly. Empirical evidence was also provided to support our propositions. To the best of our knowledge, those findings are questions that have not been empirically answered thus far during previous research in this field. Hence, we mark it as a contribution to the literature of economics of information security. Regarding future research, we will extend our analysis to scenarios with extensive information leakage, where private intermediaries may misuse information and the vulnerability information can be disclosed to the public without proper safeguards.

We discussed the private software vulnerability service providers, such as iDefense and tippingPoint as the intermediaries in the current paper. User groups may also have salient impact in this context. People who use similar IT technologies may join together in user groups where they can get know each other, have questions answered, and have fun within the user group. The strong participation involved makes for a good link between the vendor and customers and calls for the study of social networks as a proxy for intermediaries. We will also consider these user groups as another form of intermediary in our future research.

Acknowledgement An earlier version of this paper was presented at the 2006 Secure Knowledge Workshop (SKW) in New York City. We are grateful to the conference participants and three anonymous reviewers for their feedback which helped in developing this research further.

References

Anderson, R., & Moore, T. (2006). The economics of information security: A survey and open questions. *Science, 314*(5799), 610–613.

Arbaugh, W. A., Fithen, W. L., & McHugh, J. (2000). Windows of vulnerability: A case study analysis. *IEEE Computer, 33,* 52–59.

Arora, A., Caulkins, J. P., & Telang, R. (2003). Provision of software quality in the presence of patching technology. Carnegie Mellon University, Working Paper, February.

Arora, A., Krishnan, R., Nandkumar, A., Telang, R., & Yang, Y. (2004a). *Impact of vulnerability disclosure and patch availability—An empirical analysis*. Workshop on Economics and Information Security, May 2004, Minneapolis, MN, USA.

Arora, A., Krishnan, R., Telang, R., & Yang, Y. (2005). *An empirical analysis of vendor response to disclosure policy*. The Fourth Workshop on the Economics of Information Security.

Arora, A., Telang, R., & Hao, X. (2004b). *Optimal policy for software vulnerability disclosure*. Carnegie Mellon Working Paper.

Campbell, K., Gordon, L., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004a). *Analysis of software vulnerability disclosure policies*. CORS/INFORMS Joint International Meeting, Banff, Alberta, Canada.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2005). *Emerging issues in responsible vulnerability disclosure*. The Fourth Workshop on the Economics of Information Security.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004b). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce, 9* (1), 69.

Choi, J. P., Fershtman, C., & Gandal, N. (2005). *Internet security, vulnerability disclosure, and software provision*. The Fourth Workshop on the Economics of Information Security.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*, 438–457.

IDefense (2005). Service overview. http://www.idefense.com.

Kannan, K., & Telang, R. (2005). Market for software vulnerabilities? Think again. *Management Science, 51*(5), 726.

Nizovtsev, D., & Thursby, M. (2005). Economic analysis of incentive to disclose software vulnerabilities. The Forth Workshop on the Economics of Information Security.

Ozment, A. (2004). Bug auctions: Vulnerability markets reconsidered. http://www.dtc.umn.edu/weis2004/ozment.pdf.

Schechter, S. (2004). Computer security, strength and risk: A quantitative approach. http://www.eecs.harvard.edu/~stuart/papers/thesis.pdf.

Schechter, S., & Smith, M. D. (2003). *How much security is enough to stop a thief?* The Seventh International Financial Cryptography Conference, Gosier, Guadeloupe, January.

Symantec (2003). Symantec Internet security threat report. http://www.symantec.com.

Telang, R., & Wattal, S. (2005). *Impact of software vulnerability announcements on the market value of software vendors—an empirical investigation*. The Fourth Workshop on the Economics of Information Security.

Pu Li Ph.D. candidate with Management Science & Systems Division in School of Management, State University of New York, at Buffalo. Her research interests focus on information security and assurance, information sharing and risk management. Her work has been published in journals such as *Journal of Information Technology Management* and *International Journal of Communications*, *Laws and Policy*, and conference proceedings such as *ICIS, HICSS, WITS* and *AMCIS*.

H. R. Rao Ph.D. from Krannert Graduate School of Management at Purdue University. His interests are in the areas of management information systems, decision support systems, e-business, emergency response management systems and information assurance. He has chaired sessions at international conferences and presented numerous papers. He also has co-edited four books of which one is on “Information Assurance in Financial Services”. He has authored or co-authored more than 150 technical papers, of which more than 75 are published in archival journals. His work has received best paper and best paper runner up awards at AMCIS and ICIS. Dr. Rao has received funding for his research from the National Science Foundation, the Department of Defense and the Canadian Embassy and he has received the University’s prestigious Teaching Fellowship. He has also received the Fulbright fellowship in 2004. Prof. Rao is also the recipient of the 2007 State University of New York Chancellor’s award for excellence in scholarship and creative activities.