Market for Software Vulnerabilities? Think Again*

Karthik Kannan† Rahul Telang ‡

December 12, 2004

Electronic Companion

*Authors would like to thank Charalambos Aliprantis, Ashish Arora, Jonathan P. Caulkins, Prabuddha De, Ramayya Krishnan, Drew Saunders, the AE and the two anonymous reviewers for providing valuable suggestions. We also thank seminar participants at Purdue University, Carnegie Mellon University, HICSS 2004 and WEIS 2004 for their feedback. We notably appreciate the effort of Hao Xu in the making of this paper.

†Purdue University, kkarthik@mgmt.purdue.edu

‡Carnegie Mellon University, rtelang@andrew.cmu.edu

1 Proofs

1.1 Constraint on $\beta^{\text{leak}}_{\text{MARKET}}$

Consider the constraint $\beta^{\text{leak}}_{\text{MARKET}} \geq 0$. We know that $\frac{\overline{\theta}}{8M}$ is always greater than zero. Therefore, $\beta^{\text{leak}}_{\text{MARKET}} \geq 0$ would be the case so long as

$$\begin{aligned} 1 - \frac{(8M - \overline{\theta})\, 27M}{(216M^2 - \overline{\theta}^3)} &\geq 0 \\ \overline{\theta} &\leq \sqrt{27\, M} \end{aligned}$$

Consider the constraint $\beta^{\text{leak}}_{\text{MARKET}} \leq 1$. That would be the case so long as

$$\frac{\overline{\theta}}{8M} \leq \frac{(8M - \overline{\theta})\, 27M}{(216M^2 - \overline{\theta}^3)}$$

If we refer to the left hand term as a and the right hand term as b for this explanation, we are interested in showing $a \leq b$ for valid M and $\overline{\theta}$. $a \leq b$ holds good if $ac \leq b$ for $c \geq 1$. c, in our case, corresponds to $\frac{216M^2}{(216M^2 - \overline{\theta}^3)}$. Therefore, $ac \leq b$ becomes

$$\begin{aligned} \frac{216M^2}{(216M^2 - \overline{\theta}^3)} \frac{\overline{\theta}}{8M} &\leq \frac{(8M - \overline{\theta})\, 27M}{(216M^2 - \overline{\theta}^3)} \\ \overline{\theta} &\leq 4M \end{aligned}$$

This constraint holds good for the CERT-type mechanism. This implies that $\beta^{\text{leak}}_{\text{MARKET}} \leq 1$ for valid M and $\overline{\theta}$. Therefore as long as $\overline{\theta} \leq 4M$ and $\overline{\theta} \leq \sqrt{27M}$, $0 \leq \beta^{\text{leak}}_{\text{MARKET}} \leq 1$.

1.2 Multiplicative Form for Identifier Efforts

In our model, we assume that the benign identifier and the attacker exert an effort of α and β respectively. Their efforts increase their respective probabilities of finding the vulnerability to $\alpha + \gamma$ and $\beta + \gamma$. Note that the effort exerted – α or β – is added to the probability of discovering the vulnerability without exerting any effort, γ. This additive form is adopted only for the sake of simplicity. In this Appendix, we show that our results are robust even when we assume multiplicative form.

Let the benign identifier's and the attacker's effort respectively be α and β. Let this effort increase the probability of discovering the vulnerability to $\alpha\gamma$ and $\beta\gamma$. Following the same procedures as in Section

3, we obtain the following probabilities: K_{reported}, $K^{\text{no leak}}_{\text{prevented}}$, $K^{\text{leak}}_{\text{prevented}}$ and K_{hacker}. Those functional forms, which have not been shown explicitly, are found to satisfy all the intuitive criteria discussed in Setion 3. Based on these functional forms, we compute the optimal effort levels for the benigin identifier and the hacker: $\alpha^* = \frac{16\ M\overline{\theta} - \gamma\ p_b\ \overline{\theta}}{32\ M^2 - \gamma^2 p_b\ \overline{\theta}}$ and $\beta^* = \frac{8\ M\ p_b - \gamma\ p_b\ \overline{\theta}}{32\ M^2 - \gamma^2 p_b\ \overline{\theta}}$ Note that α^* increases in p_b while β^* decreases in p_b.

Using these expressions, we also solve for optimal pricing p_b and p_s under the unregulated market-based mechanism. We have $p_s^* = \frac{4\ K^{\text{leak}}_{\text{prevented}} \overline{\theta}^2}{9}$ and $p_b^* = -\frac{32 M^2 \overline{\theta}^3}{192\ M^2 - \gamma^2\ \overline{\theta}^4}$

These optimal levels of efforts and prices are then substituted in the expressions for UL and IL. We observe the same results as in the additive form. We omit the details concerning welfare metrics for the similarity in the derivation and results obtained.

1.3 Oligopoly Benign Identifiers

Note that in the model we implicitly assumed the existence of only one benign identifier who optimizes the effort of discovering the vulnerability to maximize her profit. In this Appendix, we demonstrate that even when competition arises among benign identifiers, results presented in the paper would continue to hold.

Let there be n identical benign identifiers each of which exerts the same level of effort, α_0, in equilibrium. Hence, each identifier increases its probability of finding the vulnerability to $\gamma + \alpha_0$. We also assume that each identifier's corresponding cost is $f(\alpha_0)$, which is convex in α_0.

We denote the probability that at least one benign identifier finds the vulnerability within time T by P. We have:

$$P = 1 - (1 - \alpha_0 - \gamma)^n \tag{1}$$

Therefore, collectively, all n identifiers increase their probability of finding the vulnerability to $1-(1-\alpha_0-\gamma)^n$. In other words, the collective efforts of all oligopoly identifiers has the equal effect as a monopolist benign identifier (one bening identifier) exerting effort, $\alpha = 1-(1-\alpha_0-\gamma)^n-\gamma$. Further, if each individual identifier's discovery is uniformly distributed, so is the collective probability α.

The total cost of all identifiers' effort is as follows:

$$C(\alpha) = n\ f(\alpha_0) = n\ f(1 - (1 - \alpha - \gamma)^{\frac{1}{n}}) - \gamma \tag{2}$$

It is easy to show that $C(\alpha)$ is convex in α. Recall that we only assume in 3 that monopolist identifier exerts an effort α and the corresponding cost function is convex. In the oligopoly case, the collective effort

is equivalent to α exerted by one identifier and the total cost of this effort is convex in α accordingly. Hence, as long as we may consider the collective level of efforts and costs of oligopoly identifiers as the effort and cost of a monopolist identifier, all the results we have reached in the monopolist model should follow in the oligopoly case.

1.4 Monotonic Change: CERT versus Regulated Market

First note that the binding constraint for α even in this case is same as previous case, i.e. $\overline{\theta} \leq \sqrt{27M}$. To see this note that we require $\alpha + \gamma \leq 1$. Substituting the value for α and simplifying leads to $\frac{\overline{\theta}^3 + 4\gamma M(27M+\overline{\theta}^2)}{216M^2+\overline{\theta}^3}$. Since this is increasing in γ if the constraint holds for $\gamma = 1$ it will hold for all $\gamma \leq 1$. Substituting $\gamma = 1$ and solving leads to $\overline{\theta} \leq \sqrt{27M}$. Since CERT mechanism imposes restriction of $\overline{\theta} \leq 4M$, all our constraints described in the manuscript hold.

Also note that since Δ' is a quadratic function of γ, demonstrating that $\frac{\partial \Delta'}{\partial \gamma} > 0$ is the same as showing $\frac{\partial^2 \Delta'}{\partial \gamma^2} > 0$ for all γ and $\frac{\partial \Delta'}{\partial \gamma} > 0$ at $\gamma = 0$.

We compute the second derivative on Δ' as

$$\frac{\partial^2 \Delta'}{\partial \gamma^2} = \frac{\overline{\theta}^2}{1296M}\left[\underbrace{54(8M-\overline{\theta})}_{RHS_1} - \underbrace{\frac{8M(756M^2+28M\overline{\theta}^2)(432M^2-27M\overline{\theta}+\overline{\theta}^3)}{(216M^2+\overline{\theta}^3)^2}}_{RHS_2}\right] \tag{3}$$

For $\frac{\partial^2 \Delta'}{\partial \gamma^2}$ to be positive, it is sufficient enough to show that the term in the square brackets is positive for all feasible values of M and $\overline{\theta}$. Consider RHS_2 to obtain its maximum value. The denominator is lowest when $\overline{\theta} = 0$, therefore, if we show the result by substituting $\overline{\theta} = 0$ in the denominator, then it holds good for all higher $\overline{\theta}$

$$RHS_2' = \frac{7(27M+\overline{\theta}^2)(432M^2-27M\overline{\theta}+\overline{\theta}^3)}{1458M^2}$$

Let us characterize RHS_2' with respect to $\overline{\theta}$.

$$\begin{aligned}\frac{\partial RHS_2'}{\partial \overline{\theta}} &= \frac{7}{1458M^2}\left(5\overline{\theta}^4 + 27M^2(-27+32\overline{\theta})\right)\\ \frac{\partial^2 RHS_2'}{\partial \overline{\theta}^2} &= \frac{7}{1458M^2}\left(20\overline{\theta}^3 + 864M^2\right)\end{aligned}$$

Since the first derivative is negative at $\overline{\theta} = 0$ and the second order derivative is positive for all positive $\overline{\theta}$, it

is clear that there is one minima for RHS_2' occurring at $\overline{\theta} > 0$. This also means that the maximum value of RHS_2' can occur only at the extremes – either at $\overline{\theta} = 0$ or depending on the binding constraint at $\overline{\theta} = \sqrt{27M}$ or at $\overline{\theta} = 4M$.

First consider the case where $M \geq \frac{27}{16}$, the corresponding binding constraint is $\overline{\theta} \leq \sqrt{27M}$. To determine the maximum value of RHS_2', we compute RHS_2' at $\overline{\theta} = 0$ to be equal to $56M$ and at $\overline{\theta} = \sqrt{27M}$, to be equal to $112M$. From this, RHS_2' is maximized at $\overline{\theta} = \sqrt{27M}$. But the term, RHS_1 is clearly minimum at $\overline{\theta} = \sqrt{27M}$. If at $\overline{\theta} = \sqrt{27M}$, the difference between RHS_1 and RHS_2' is positive, then $RHS_1 - RHS_2$ must be positive at all values of $\overline{\theta}$. Substituting, $\overline{\theta} = \sqrt{27M}$ in $RHS_1 - RHS_2'$ and simplifying, we get $320M - 162\sqrt{3M}$. This is clearly positive for all $M \geq \frac{27}{16}$ and therefore, $\frac{\partial^2 \Delta'}{\partial \gamma^2} > 0$ for all $M \geq \frac{27}{16}$.

Next consider the case when $M < \frac{27}{16}$, when the binding constraint on $\overline{\theta}$ is $0 \leq \overline{\theta} < 4M$. RHS_1 is always minimized at $\overline{\theta} = 4M$ and the value is $216M$. RHS_2' at $\overline{\theta} = 0$ is $56M$ while at $\overline{\theta} = 4M$ is $42M + \frac{896M^2}{27} + \frac{3584M^3}{729}$. Note that since both these expressions are increasing functions of M, we compute RHS_2' for both combinations $(\overline{\theta} = 0, M = \frac{27}{16})$ and $(\overline{\theta} = 4M, M = \frac{27}{16})$. It is easy to observe that under both cases, $216M - RHS_2' > 0$ for all $M < \frac{27}{16}$. Therefore, $\frac{\partial^2 \Delta}{\partial \gamma^2} \geq 0$ for all M and $\overline{\theta}$.

Next we show that first derivative is positive at $\gamma = 0$. Taking the first derivative and substituting $\gamma = 0$ leads to

$$\frac{\partial \Delta'}{\partial \gamma} = \frac{4\overline{\theta}}{(216M^2 + \overline{\theta}^3)^2}\left[863136M^4 - 17712M^3\overline{\theta}^2 + 10206M^2\overline{\theta}^3 - 68M\overline{\theta}^5 + 27\overline{\theta}^6\right]$$

It is very easy to see that the term in square brackets is positive for all valid M and $\overline{\theta}$. The first expression minus the second expression is always positive for all $\overline{\theta} \leq \sqrt{27M}$ and $M \geq \frac{27}{16}$ and $\overline{\theta} \leq 4M$ and $M \leq \frac{27}{16}$. Similarly, the third expression minus the fourth expression is positive for all $\overline{\theta} \leq \sqrt{27M}$ for $M \geq \frac{27}{16}$ and $\overline{\theta} \leq 4M$ and $M \leq \frac{27}{16}$. Thus, $\frac{\partial \Delta}{\partial \gamma} > 0$. **QED**