Network Security, Vulnerabilities and Disclosure Policy

Jay Pil Choi, (MSU)
Chaim Fershtman (Tel Aviv University, CEPR)
Neil Gandal (Tel Aviv University, CEPR)

May, 2008
Background

• The Slammer, Blaster, and Sobig.F viruses exploited vulnerabilities even though security updates had been released.
• According to the Economist, the vulnerabilities exploited by these viruses were reverse engineered by hackers.
• Time between the disclosure of a vulnerability and an attack exploiting the vulnerability has declined significantly.
• Zero-day vulnerability by the end of 2007?
Introduction

• Vulnerabilities major concern since attackers can cause substantial damages.

• Firms face a disclosure dilemma:
  
  - Disclosing vulnerabilities and issuing updates protects consumers who install updates.
  - Not all consumers necessarily install updates
  - Disclosure facilitates reverse engineering by hackers.
Introduction (Continued)

- Examine the incentives for a firm to disclose software vulnerabilities. Key tradeoff: “disclosure” provides protection, but also increases probability of attack.

- Disclose and issuance of updates changes the value of software, increasing it for high-value users (who will employ updates) and decreasing it for low-value users (who will not employ updates)

- Examine effects of regulatory policy that requires mandatory disclosure (Is it Desirable?)

- Investigate how changes -- in (I) number of vulnerabilities & (II) probability the firm identifies problems before hackers -- affect disclosure policy
Literature

- Anderson (2006) - Nice Review Article
- Arora, Caulkins, and Telang (2007) - when to release a patch
- August and Tunca (2006): We allow for possibility that firm will discover vulnerabilities before hackers
- Polinsky and Shavell (2006) Disclosure of product risk information always beneficial to consumers (no hackers). Firm benefit of disclosure arises from its incentive to acquire more information. Firm can keep silent if the information is unfavorable.
Institutions & Mandatory Disclosure

• Vulnerabilities are often discovered by third-parties and their policies can effectively impose mandatory disclosure.

• CERT/CC acts as an intermediary between those who report vulnerabilities and software vendors. Its policy essentially mandates disclosure of vulnerabilities reported to CERT/CC.

• A private market for vulnerabilities has developed. (e.g., iDefense & Tipping Point/3Com)

• Bug Bounty Programs
### Decisions

**Software Vendor**

- Whether or not to disclose vulnerabilities.
- (If disclose $\Rightarrow$ issue updates)
- Price of the software

**Consumers**

- Whether to buy (license) the software
- Whether to install updates (if available)
Model

- $\alpha$ -- Probability that the firm will find the problems before hackers.

- $\gamma$ -- Probability of attack if no disclosure. If firm discloses the vulnerability (& releases a patch) $\gamma=1$.

- $\theta$ -- consumer heterogeneity uniformly distributed on $[0,1]$.

- Value of software to consumer type $\theta$ is given by $\theta v$.

- Damage from each security breach exploited by hackers: $\theta D$, where $D<v$.

- $n$--Number of security vulnerabilities

- $c$ - cost to consumers of downloading and installing updates
Three possible disclosure regimes

- Firm must disclose vulnerabilities and is “obliged” to release updates.
- Firm does not disclose vulnerabilities nor does it issue updates.
- Firm can either adopt a policy to disclose vulnerabilities or a non-disclosure policy.

Firm’s disclosure policy is known to consumers when they purchase software.
**Consumer Valuations**

**Firm Discloses Vulnerabilities**

\[ W_u \]: consumer value (type \( \theta \)) from buying software and installing update

\[
(1) \quad W_u(\theta) = v_\theta - \gamma(1-\alpha) \theta Dn - \alpha c = Z\theta - \alpha nc
\]

\[ W_{nu} \]: consumer value (type \( \theta \)) from buying, but not installing a patch.

\[
(2) \quad W_{nu}(\theta) = v_\theta - \gamma(1-\alpha) \theta Dn - \alpha Dn = S\theta
\]

**Firm Does Not Disclose Vulnerabilities**

\[ W_{nd} \]: consumer value (type \( \theta \)) from no announcement

\[
(3) \quad W_{nd}(\theta) = v_\theta - \gamma \theta Dn = T\theta
\]

\[ Z > T > S \]
Two Assumptions

• **A1**: We assume that $S > 0$, guarantees that $W_{nu}(\theta) > 0$ for all $\theta$. This assumption also implies that $W_u(\theta)$, $W_{nu}(\theta)$, and $W_{nu}(\theta)$ increase in consumer type $\theta$.

• **A2**: We assume that $\gamma > c/D$. Assumption insures that $W_u(\theta) > W_{nd}(\theta)$ for some consumer types.

When **A2** does not hold, probability of a hacker attack is so small that software vulnerabilities are not a concern and the firm’s optimal policy is non-disclosure of vulnerabilities.
Disclosure Required
Purchase/Update Decision when Marginal Consumer less than $\hat{\theta}$

Figure 1

Do not purchase
Buy but do not install updates
Purchase and install updates
Disclosure Required
Purchase/Update Decision when Marginal Consumer greater than $\hat{\theta}$

Figure 2: Purchase/Updating Decision when Marginal Consumer Type $\theta^*(p) > \hat{\theta}$
When the firm must disclose vulnerabilities... Lemma 3:

- $D/c < 2 - \alpha n_c/Z$: Some consumers do not install updates. Firm serves a “large” market & charges a “low” price.

- $D/c > 2 - \alpha n_c/Z$: All consumers install updates. Firm serves a “small” market & charges a “high” price.

- Greater damage, larger number of vulnerabilities, higher $\alpha$, higher probability of hacker attack, & lower patch costs --- more likely that the firm will serve updaters only.
Figure 3: Effect of an Increase in $\alpha$

Values: $W_u(\theta)$, $W_{nu}(\theta)$

$\theta = c/D$

$\theta^1 = c/D\gamma$

--- High $\alpha$

_____ Low $\alpha$
Firm must disclose Vulnerabilities
Effect of $\alpha$ (Proposition 1)

• Suppose $(2-nc/v)c\leq D<2c$. Exists $\hat{\alpha}$ such that

• When $\alpha$ increases, but below $\hat{\alpha}$, profit maximizing price and equilibrium profits decrease in $\alpha$.

• When initial $\alpha$ such that $\alpha<\hat{\alpha}$, but $\alpha>\hat{\alpha}$ following the increase, regime shift (serve only updaters)

• When $\alpha>\hat{\alpha}$ price increases in $\alpha$. Profits increase in $\alpha$ when $\gamma$ large.

• Corollary 1: When $D$, $\alpha$, or $\gamma$ are small, firm’s optimal policy is to refrain from increasing $\alpha$ even when it is costless for the firm to do so and when it is costless to issue updates
Willingness to pay under disclosure and non-disclosure

Values: \( W_u(\theta) \), \( W_{nd}(\theta) \), and \( W_{nu}(\theta) \)

\[ \theta = \frac{c}{D} \quad \theta^1 = \frac{c}{D \gamma} \]

<table>
<thead>
<tr>
<th>Prefer “nd” - no patch</th>
<th>[ W_{nd}(\theta) ]</th>
<th>Prefer disc - patch</th>
<th>[ W_u(\theta) ]</th>
</tr>
</thead>
</table>

Prefer “nd”, but will apply patches if available
Propositions 2 & 3

• Firm will choose to disclose vulnerabilities if and only if \((D/c)\gamma > 2 - \alpha nc/Z\).

• Firm serves a larger market & charges a lower price when under “no disclosure”

• If \(D > \bar{D}\), Critical probability of hacker attack, \(\tilde{\gamma}\), such that \(\gamma > \tilde{\gamma}\): firm discloses.

• Firm will disclose vulnerabilities in equilibrium when \(D, n, \alpha\), and \(\gamma\) are relatively large and \(c\) is relatively small. (Critical \(\tilde{\gamma}, \bar{D}\) decrease in \(n, \alpha\))
Region I: Suboptimal Disclosure (Firm does not Disclose; Regulator would Disclose)

Region II: Efficient (Firm does not Disclose; Regulator would not Disclose)

Region III: Efficient (Firm does not Disclose; Regulator would not Disclose)

Region IV: Efficient (Firm does Disclose; Regulator would Disclose)

Region V: Efficient (Assumption A2 does not hold; hence neither the firm nor the regulator would disclose)
Welfare

• We consider a regulator that can mandate the disclosure of vulnerabilities.

• **Proposition 4:** The equilibrium disclosure policy of the firm is socially optimal unless the parameters are such that Region I in Figure 5 obtains.

• **Corollary 2:** Mandatory disclosure increases social welfare in Region I, reduces welfare in Regions II & III (V), and has no effect in Region IV.
Effect of Mandatory Disclosure (Corollary 3)

• (i) In Regions I and II in Figure 5, mandatory disclosure decreases the equilibrium price.

• (ii) In Region III, mandatory disclosure increases the equilibrium price and reduces equilibrium number of consumers.

• (iii) In Region IV, mandatory disclosure has no effect on either the price or the number of consumers who purchase software.
Figure 6: Effects of decrease in $n$ on $W_u(\theta), W_{nu}(\theta), W_{nd}(\theta)$

Values: $W_u(\theta)$, $W_{nu}(\theta)$, and $W_{nd}(\theta)$

- High $n$
- Low $n$
Proposition 5 (Ex-ante Investment):

• When $\gamma$ is intermediate and firm discloses, a large decrease in $n$ leads to a switch to non-disclosure and possibly to a lower equilibrium price. ($u \Leftrightarrow nd$)

• Otherwise, a reduction in $n$ leads to an increase in the equilibrium price, profits and consumers welfare, but has no effect on the disclosure policy of the firm.
Corollary 4

- Regime change (u⇒nd) occurs if $n-\Delta n<\tilde{n}$, where

\[
\tilde{n} = \frac{\nu(2c-\gamma D)}{(1-\alpha)\gamma D(2c-\gamma D)+\alpha^2}
\]

- Price of software falls if $\Delta n/n \leq \frac{\alpha(\gamma D - c)}{\gamma D}$
Proposition 6 (Ex-post Investment):

- (Institutions like CERT/CC increase $\alpha$)

(i) When $\gamma > \gamma(n, \alpha)$ and $D > \tilde{D}(n, \alpha)$, a firm would “disclose;” increases in $\alpha$ don’t affect disclosure policy. Price, Profits, welfare increase in $\alpha$.

(ii) Otherwise, the firm does not disclose; a relatively large increase in $\alpha$ may induce regime change to disclosure ($\text{nd} \Rightarrow \text{u}$) Price, Profits, welfare increase in $\alpha$.

- Bounty Program (increase in $\alpha$) is an alternative policy to Mandatory Disclosure. It is Welfare improving
Conclusions

• Mandatory disclosure improves welfare only when the probability of attack is very high and the expected damage is relatively small.

• We find that a Bug Bounty program is a welfare improving policy instrument.

• An ex-ante reduction in the number of vulnerabilities may induce a (welfare-improving) regime shift from disclosure to non-disclosure.

• Ex-post investment (increase in $\alpha$) may induce a welfare-improving regime shift in the opposite direction: from non-disclosure to disclosure.