An Economic Analysis of Market for Software Vulnerabilities

Karthik Kannan, Purdue University
Rahul Telang, CMU

Motivation

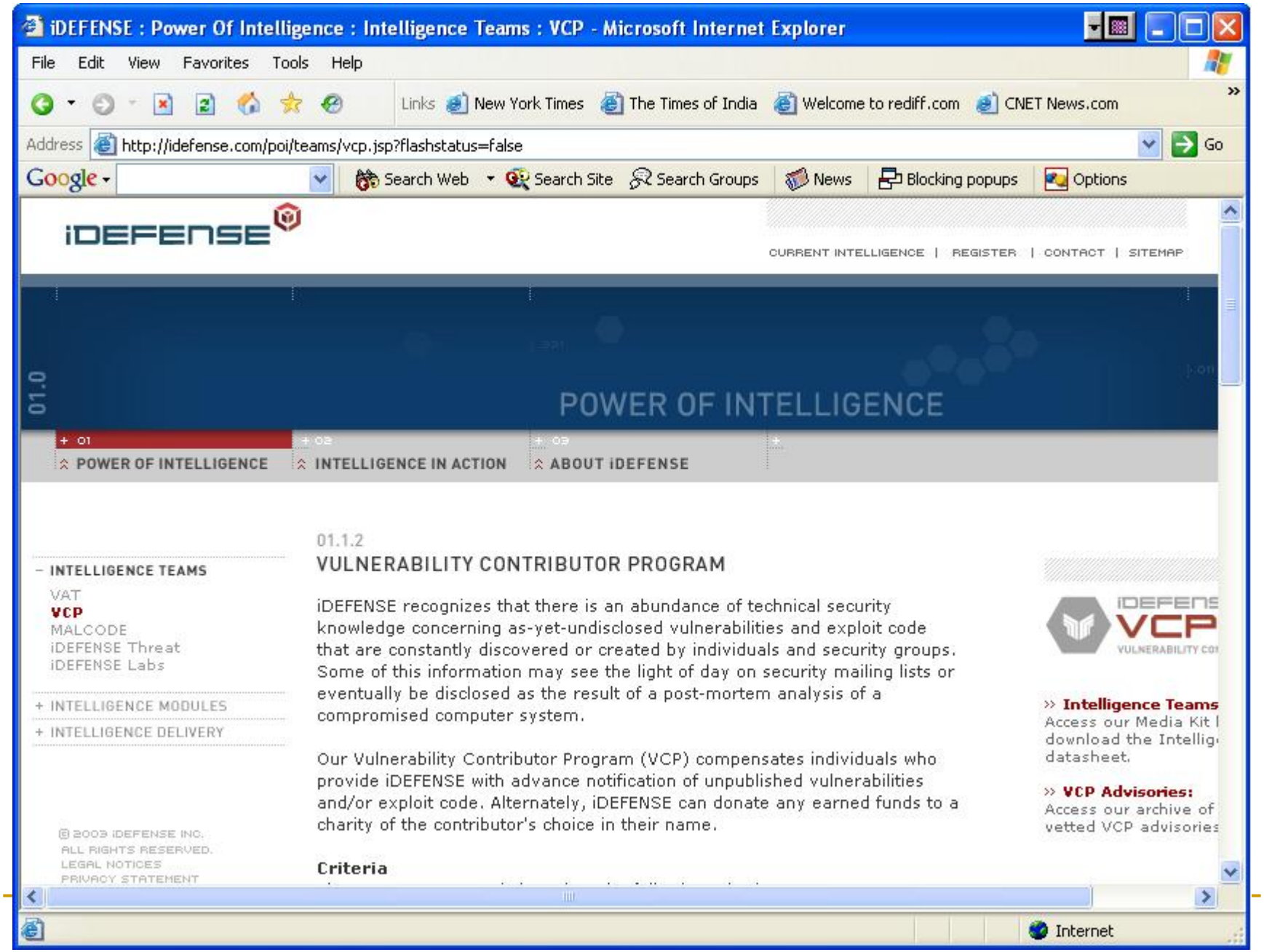
- Significant Economic cost due to exploitation of Software Vulnerabilities.
- CERT/CC reports 319,992 self reported incidences of vulnerability exploitation in last 5 years.
- It also reported 3,784 vulnerabilities in 2003 alone.

Motivation

- In general, users voluntarily report vulnerability information to CERT, Vendors etc.
- CERT then contacts the vendors, provides them with appropriate time window and then releases the vulnerability information along with the patch such that users suffer as little loss as possible.
- But what if there were a market for such vulnerability information?
  - In particular iDefence has opened a market for vulnerability.

Market for Vulnerability

- iDefence buys vulnerability information from identifiers and then help protect its client base by providing them with
  - Timely information
  - Work-around and patches if possible
  - Defense from exploit codes
  - Managing its patching operations


iDEFENSE : Power Of Intelligence : Intelligence Teams : VCP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links New York Times The Times of India Welcome to rediff.com CNET News.com
Address http://idefense.com/poi/teams/vcp.jsp?flashstatus=false
Go
Google
Search Web Search Site Search Groups News Blocking popups Options
iDEFENSE
CURRENT INTELLIGENCE | REGISTER | CONTACT | SITEMAP
01.0
POWER OF INTELLIGENCE
+ 01 POWER OF INTELLIGENCE
+ 02 INTELLIGENCE IN ACTION
+ 03 ABOUT iDEFENSE
01.1.2
VULNERABILITY CONTRIBUTOR PROGRAM
INTELLIGENCE TEAMS
VAT
VCP
MALCODE
iDEFENSE Threat
iDEFENSE Labs
+ INTELLIGENCE MODULES
+ INTELLIGENCE DELIVERY
iDEFENSE recognizes that there is an abundance of technical security knowledge concerning as-yet-undisclosed vulnerabilities and exploit code that are constantly discovered or created by individuals and security groups. Some of this information may see the light of day on security mailing lists or eventually be disclosed as the result of a post-mortem analysis of a compromised computer system.
Our Vulnerability Contributor Program (VCP) compensates individuals who provide iDEFENSE with advance notification of unpublished vulnerabilities and/or exploit code. Alternately, iDEFENSE can donate any earned funds to a charity of the contributor's choice in their name.
Criteria
» Intelligence Teams
Access our Media Kit
download the Intelli
datasheet.
» VCP Advisories:
Access our archive of
vetted VCP advisories
© 2003 iDEFENSE INC.
ALL RIGHTS RESERVED.
LEGAL NOTICES
PRIVACY STATEMENT
Internet

Research Question

- Is a movement towards market based mechanism socially welfare enhancing?
- If yes,
  - then we need to reshape the role of institutions like CERT who have traditionally played an important role in vulnerability dissemination.
  - Create the right policy environment to encourage such a market.
- A formal Analysis for a market mechanism is timely.

Assumptions

- We will analyze the market and the CERT separately.
  - Co-existence is a useful extension but in general, if market maker pays and CERT does not then nobody has an incentive to report to CERT.
- We will focus on Monopoly market maker (Infomediary)
  - Competition will be an interesting future work, but as we will see, like most Information goods market, this market will tip to the dominant firm.

Model Parameters

- Infomediary pays p_b amount for each vulnerability disclosed to it.
  - CERT pays no direct money to identification.
- It charges p_s as the subscriber fees to its customers.
  - CERT does not charge any subscription fee.
- Customer are heterogeneous in the loss they suffer due to vulnerability exploitation. Therefore, high loss customers have stronger incentives to join.

Identifiers and Attackers

- There are benign identifiers and attackers who find the vulnerability in a product with some probability.
- When infomediary pays money p_b, then benign identifiers have an incentive to increase their effort level to find the vulnerability before the attacker.
- This will affect the attacker's incentives as well.
- Clearly, the subscribers to infomediary benefit only when the benign identifiers can find the vulnerability before the attackers.

Model

- So infomediary sets p_b and p_s.
- Based on this p_s, subscribers calculate their expected benefits and join the network
- Based on this p_b, benign identifiers and attackers compete to find the vulnerability.
- If the benign identifier finds it first then attackers can only exploit non subscribers (if it finds the vulnerability at all).
- If attackers find it first then they can exploit all customers.

Profit Functions

- User Utility

$$\theta^2 \text{Prob}(\text{AttackPrevented}) - p_s > 0$$

- Infomediary Profit Function

$$\text{Demand}(p_s, p_b)\, p_s - \text{Prob}(\text{Vulnerability reported})\, p_b$$

- Benign User Effort Level

$$\text{Prob}(\text{Finding Vuln before Attacker})\; p_b - \text{Cost of Effort}$$

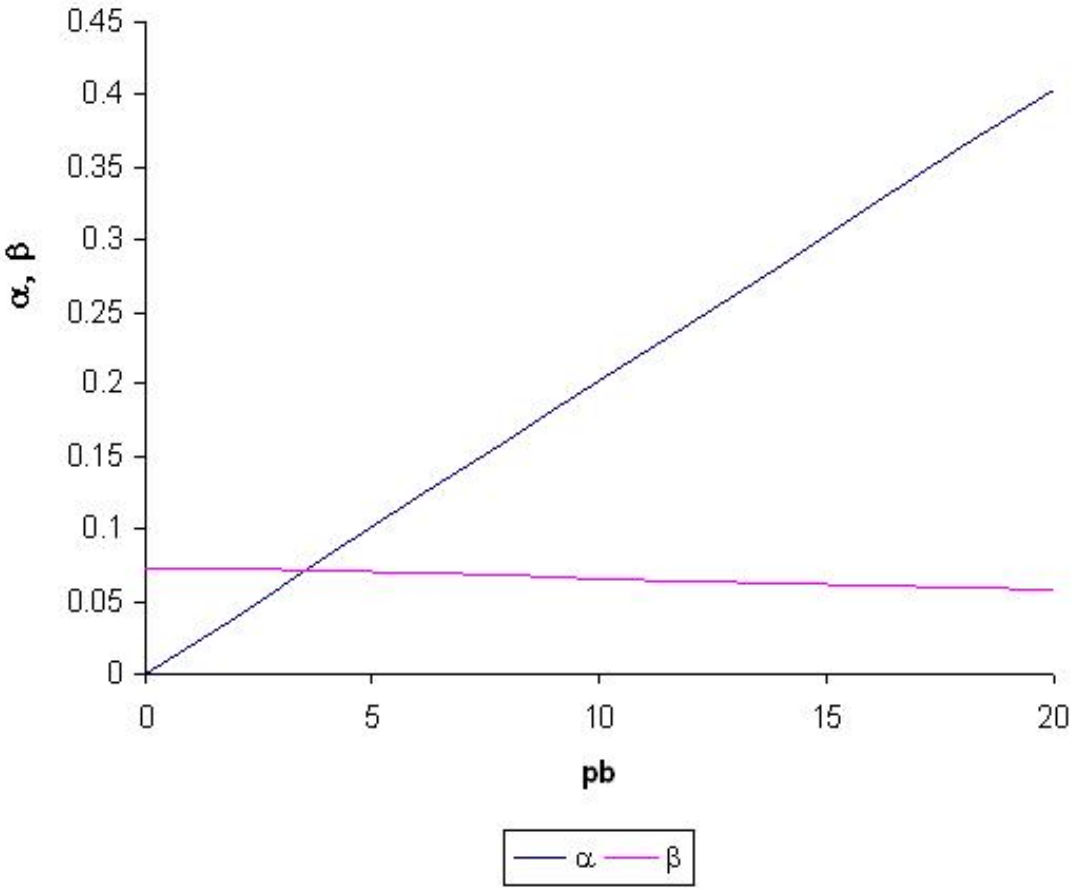
- Attacker Effort Level

$$\begin{aligned} &\text{Prob}(\text{Find before benign}) * \text{Gains from Attacking all} \\ &+ \text{Prob}(\text{Find After benign}) * \text{Gains from Attacking nonsubs} \\ &- \text{Cost of Effort} \end{aligned}$$

- Similarly we can then define our two welfare matrices
  - User Loss
  - Industry Loss

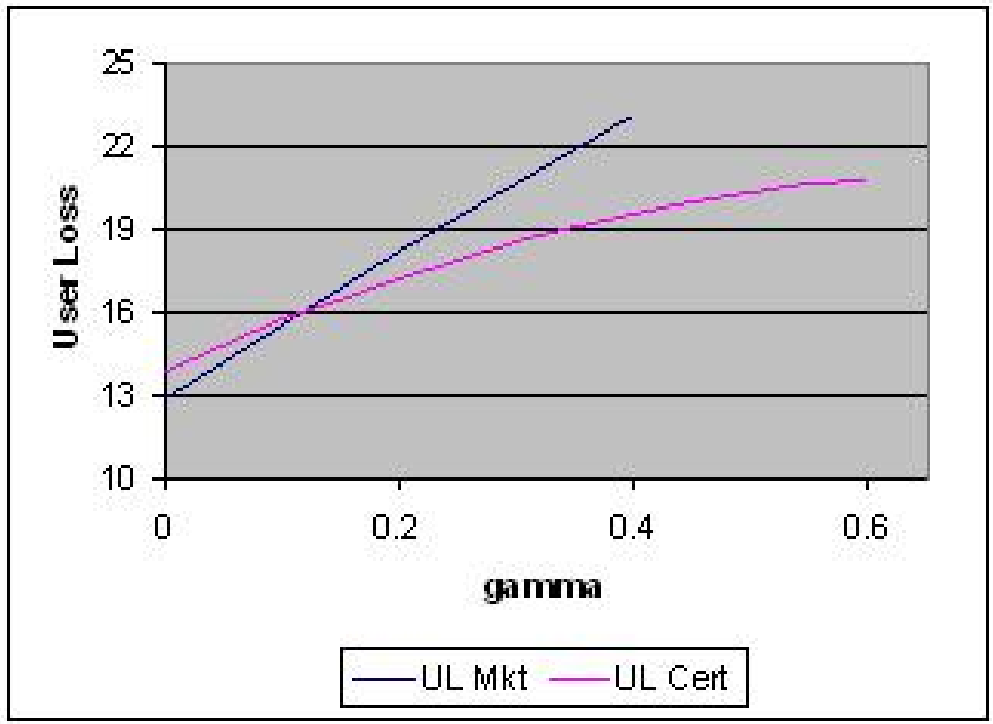
Results

- Benign Identifier exerts negative externality on hackers



Results

- If the default probability of finding vulnerability by benign users is low then
  - Having a market is socially welfare enhancing.

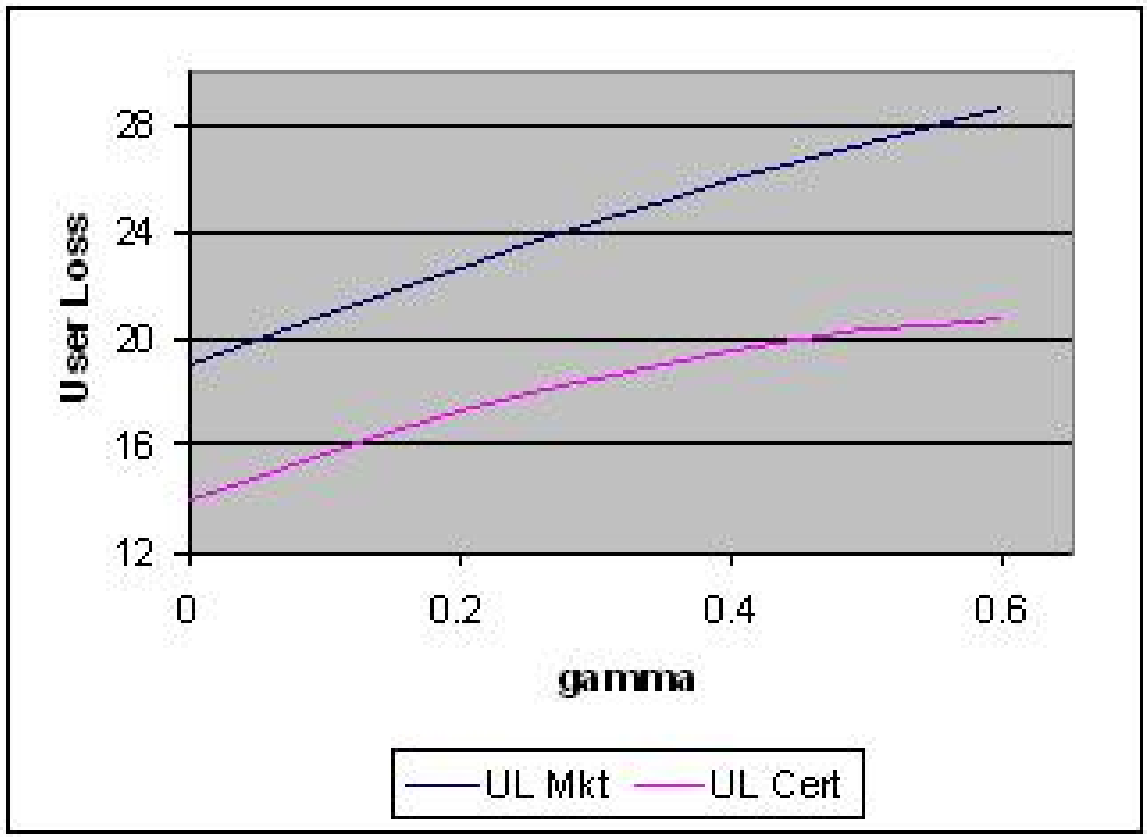


Results

- But will infomediary, after protecting its client, disclose the vulnerability on a public forum?
- If it does so, non-subscribers will be exposed to the risk of exploitation.
- It is easy to see that it would be in the interest of the infomediary to do so.

Result

- Now, user loss is strictly higher under infomediary. In fact, it can be shown that *having a market is worse than no market at all.*



Disclosure Policy

- CERT provides vendors with 45 days and almost never discloses the vulnerability without proper safeguard.
- iDefence provides vendors 5 days to begin the negotiation. If not, it makes the information public.

CERT pays money?

- We find that if CERT can increase the rate of information disclosed to it then it is usually the most beneficial for users. It can do so by payment, recognition, etc.

Conclusions

- Markets can work only if we can be sure that information is handled properly.
- Incorporating competition, diffusion of patching etc will be interesting extensions.
- Analyzing other mechanism would be interesting.