Is Coalition a Remedy?

The Full Disclosure Problem:

Dmitri Nizovtsev, Ph.D. candidate
Marie Thursby, Burton D. Morgan Chair of International Management and Policy

*CERIAS sponsored project
• What is socially desirable?
• Feasible solutions?
• Why disclose?
• Why the controversy?
Commonly believed motives for full disclosure:
• fame (reputation building);
• educating other end users;
• putting pressure on vendor.

Our explanation:
Self-interest
(minimizing expected loss)
Three types of “agents”:

- **Black Hats**: attack other users when they can
- **White Hats**: choose whether to disclose or not
- **Vendors**: choose when to issue a fix

Independent discoveries of the same bug are possible.
Methodology

- Game theoretic approach
- Agents minimize their expected losses
- Society minimizes the damage from attacks

Exogenous parameters

- Size of the population
- Share of black hats in the population
- Damage from each attack
- Difficulty of developing a fix
- Chances of independent discovery
5

Decision Tree

Bug discovered

Y  Disclose?  N

Choice of effort, $X_W$

N  Game ends

Choice of effort, $X_N$

Y  Patch installed?

Patch installed?

N  Game ends (no loss)

Massive attack

Fix provided by vendor

Game ends

Game continues…
Loss Structure

NON-DISCLOSING AGENT

 Period

0 1 2 3 4 5 6 7 8 9

25 20 15 10 5 0

DISCLOSING AGENT

 Period

0 1

25 20 15 10 5 0

Absolute Loss
Discounted Loss
Expected loss

Equilibrium

Proportion of agents disclosing

$W$ – agents disclosing to the World
$N$ – agents Not disclosing
$N1$ – loss from massive attack (result of FD)
$N2$ – loss from occasional attacks (result of discoveries)
Results

There are cases (and we may deal with one) when

**Full Disclosure** is

- Inevitable
- Desirable

Comparative statics:

Full disclosure occurs more often as
- Bugs become easier to discover
- Population increases
  - It *possibly* occurs more often as
    - Software gets more complex
    - Average damage from an attack decreases
    - Portion of black hats in the population decreases
Suppose we have a coalition of agents anyone can disclose information to.

- Does it change incentive structure?

- What happens to aggregate damage from attacks?
Bug discovered

Disclose?

Choice of effort

Patch installed?

- Yes (X_w)
  - Massive attack
  - Game ends

- No (N)
  - Moderate size attack
  - Game ends (no loss)

Choice of effort

Patch installed?

- Yes (X_c)
  - Moderate size attack

- No (N)
  - No attack

Next discoverer?
A coalition may improve the situation only if…

Software is not too complex

Coalition members are willing to work on a patch

Otherwise, a coalition has no effect!
We recommend:

Target the cause, NOT the effect!!!
Approach A

• Reduce average size of damage from an attack
• Reduce portion of black hats in the population
Approach B

- Improve quality of software products
- Accelerate the fixes
Towards a perfect model

Issues deserving further study:

- Mechanism of vendors’ decisions
- Different schemes of disclosure
- End users’ reluctance to patch
- Heterogeneous population
- Data available, anyone?