A Comparative Analysis of Software Liability Policies

Introduction

In the current network environment, there are serious incentive problems among various actors whose decisions impact the overall security of the cyber infrastructure: the risks associated with attacks on this infrastructure are growing in number and potential impact; and the importance of the role of regulation is increasingly understood and debated.

However, answering how regulation can actuate a shift toward preferable outcomes, such as an increasingly secure cyber infrastructure and higher social surplus associated with these public resources, is not well understood and requires formal analysis. We begin to explore this important question by analyzing an economic model that captures both security interdependence and the primary underlying incentives of actors.

One corrective means to address the underlying incentive problems which has received intense debate in the security community is the ownership of liability for network security losses. We investigate how liability policies can be used to increase Internet security considering the effects of interconnectivity and the resulting interdependence of users’ security actions on one another.

Research Questions

1. In the short run, when the security level of a software product is fixed, what role should software liability play? What form of liability is most effective?
2. Given significant negative externalities associated with software patching and security attacks, what shapes vendor incentives to invest in software security?
3. In the long run, with vendor investment, can security liability be effective? If so, what is the best approach to vendor liability?
4. How do other policies such as software security standards compare to traditional liability?

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. CNS-0954234.

Model

- Consumer valuation space: $v \in V = [0, 1]$
- Security losses: $\xi(v)$
- Cost of patching: $c_p > 0$
- Probability of security attack on patchable vulnerability: $\pi_a$
- Probability of security attack on zero-day vulnerability: $\pi_z$

Consumer Strategy Set: $S = \{B, NB\} \times \{P, NP\} - (NB, P)$

Consumer’s Problem:

$$C(v, \sigma) = \left\{ \begin{array}{ll}
\pi_a w(0) 1(v = 0) + \pi_z w(1) & \text{if } \sigma = (B, NP) \cap S
\\
\pi_a w(v) & \text{if } \sigma = (B, P) \cap S
\\
0 & \text{if } \sigma = (NB, P) \cap S
\end{array} \right.$$

Cost of patching function: $c(v) = c_p 1(\text{patched}) + c_n 1(\text{not patched})$

Max Valuation threshold above which consumers purchase $V_p$

Vendor’s share of zero-day losses: $\lambda_z$

Vendor’s share of patching costs: $\lambda_p$

Policy in question: $\tau \in \{p, z\}$

Security losses:

$$L_v = \int_{v(z)}^{v(p)} c_p dv \quad \text{if } \tau = p$$

Security investment cost: $C(\beta)$

Vendor Profit: $\Pi(p, \beta, \lambda_p) = p(1 - v_b) - \lambda_p L_v - C(\beta)$

Vendor’s Problem: Sets price and investment level $\max_{p, \beta, \lambda_p} \Pi(p, \beta, \lambda_p)$ s.t. $(v_b, v_p)$ satisfy $\sigma^{*}(p, \beta, \lambda_p)$

Regulator’s Problem: Sets loss and patch liability shares $\max_{\lambda_p} W(\lambda_p, \beta^*(\lambda_p))$ s.t. $(v_b, v_p)$ satisfy $\sigma^{*}(p, \lambda_p, \beta^*(\lambda_p))$ ($p^*(\lambda_p, \beta^*(\lambda_p))$ solve $[\xi]$)

Consumer Market Structure

- Non-users
- Patched users
- Unpatched users

Equilibrium Equations

1. $v_b = p + \pi_a (v_p - v_b) + \pi_z (1 - v_b) = v_p$
2. $c_p = \pi_a (v_p - v_b) + c_p$

Economic Agents / Incentives

- Information Security Risk (ISR)
- Users
- Government
- Software Firms

Discussion

- Software vendors naturally have substantial incentives to invest in security
  - Investments are being made, but they are also quite costly
  - The role of liability is to encourage more “efficient” outcomes (not necessarily larger investments)
- Loss liability policies tend to be ineffective
  - Do not create incentives to boost vendor security investments
  - In fact, they can reduce these investments in many cases
- Utilizing security standards leads to the greatest level of security but is primarily useful in less risky environments where the vendor lacks strong investment incentives
- Patch liability (or sharing of patching costs) works best in risky environments
  - Provides greater incentives for users to protect the entire network
  - Patch liability is actually a substitute to security investment (i.e., it is more efficient to address user behavior than the inherent attack likelihood)
  - Easy to implement as a price discount because patching status is readily communicated

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 - 29th 2012
National Harbor, MD