TITLE

Diverging economic incentives caused by innovation for security updates on an information network

RESEARCHER

Kin Sing Leung, Ph.D. Candidate, Management Science & Engineering, Stanford University

Contact info: kleung@stanford.edu

ABSTRACT

In this paper, I develop a simple economic model to explain how innovation creates diverging incentives for adopting new security updates on an information network. Innovation affects an individual firm's investment in information security as well as how this investment affects the welfare of the other network participants. On one hand, frequent security updates can improve the overall protection of the network for all participants. On the other hand, frequent security updates become progressively less cost-effective to a firm as the expected number of technology updates increases.

Security updates can improve the overall protection of the network by reducing the magnitude of the under-investment in socially cost-effective security. This under-investment occurs because the firm fails to recognize the external costs of its security to other participants, for example, the transmission of a computer virus to other network participants, the hijacking of a computer system to assist in a denial-of-service attack, and the identity theft of a participant on a trusted network. Under certain conditions, I show that this incentive failure can be reduced if the firm updates its security whenever a new technology is made available. Furthermore, as the rate of security innovation increases, the consequences of the under-investment can be decreased with more frequent investments in security updates.

While security innovations can improve the overall protection of the network, frequent security updates are not always privately cost-effective for the firm. More so, as the number of innovations grows, the individual firm finds periodic security updates less and less cost-effective. This result can be best explained by the fixed cost that a firm incurs whenever it assesses new

security innovations on its existing information system. This fixed *assessment cost* includes the costs to identify the new technologies, the costs to evaluate integration issues, and other administrative costs. Because the assessment cost is incurred whenever a security update is made available, the firm will find security updates to be cost-effective only up to a certain number of innovations. Beyond this point, the firm will not update its security. The complexity of today's information systems suggests that this assessment cost may be fairly high. In the model, I demonstrate that this assessment cost, in conjunction with the innovation rate, dictates the frequency of security updates by the firm.

A policy implication is that the government can improve the overall protection of the network by making frequent security updates more cost-effective for the individual participants. This improvement becomes more significant as the rate of innovation increases. One way that the government can help to encourage more timely security updates is by lowering the assessment cost faced by a participant. For example, the government can centralize information on new security practices and network vulnerabilities and effectively lower the information-gathering cost faced by the firm. CERT[1] and Common Criteria[2] are examples of such government-sponsored organizations that are already in practice. Also, improving the risk assessment methodologies would further reduce the evaluation cost for integrating a new technology.

This model demonstrates that innovation creates diverging incentives for the individual firm and for the network community. More importantly, it illustrates the importance of the assessment cost in improving overall network protection. With further development, the model can evaluate the effects of different government actions on the frequency of security updates and overall network protection. This evaluation would involve analyzing the tradeoff between private cost-effectiveness for the firm and social cost-effectiveness of overall network protection. In future work, I hope to identify the conditions when government interventions are warranted.

[1] www.cert.org
[2] www.commoncriteria.org