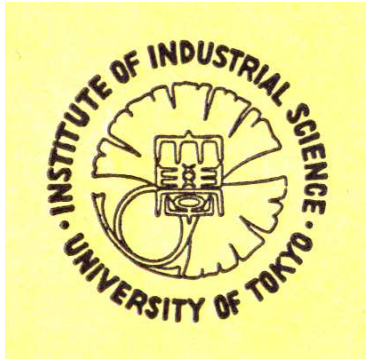
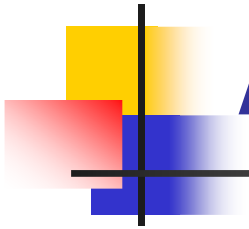
Economic Implications of Light-Weight Security Mechanisms

Kanta Matsuura
(The University of Tokyo)

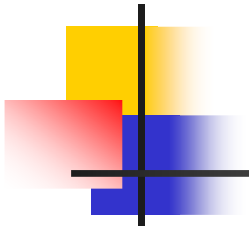


This talk includes results from a project supported by NEDO (New Energy and Industrial Technology Development Organization) of Japan.



Agenda

1. Economics of information security
   - Answers to many questions
   - Analysis and synthesis
2. Economics of light-weight security
   - Security efforts and their impacts
   - Investment models
   - Productivity space and Optimal investment
   - Sensitivity analysis and implications



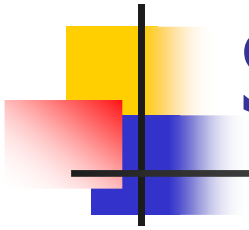
1. Economics of Information Security

Analysis, Analysis, & Analysis.

- Why information security is hard?
- Why free-riding problems happen?
- Why software vendors prefer the patch-after-patch approach?

- Economics of Information Security (EIS) can give possible reasons.
- Early works of raising problems are in 1990's.
- Many early works of the current trend of EIS are between 2000-2004.
- WEIS (Workshop on the EIS) started in 2002.

Next Trend would be: Synthesis



- Interaction between academia and industry (not as a user but as a vendor/provider) is important.
- However, not that active at present.
- Many people are noticing this (e.g. a panel at WEIS2009).
- Some empirical findings (of the insufficient interaction), too.

A role of R&D

- Quick innovation may help.
- Collaboration for innovation.

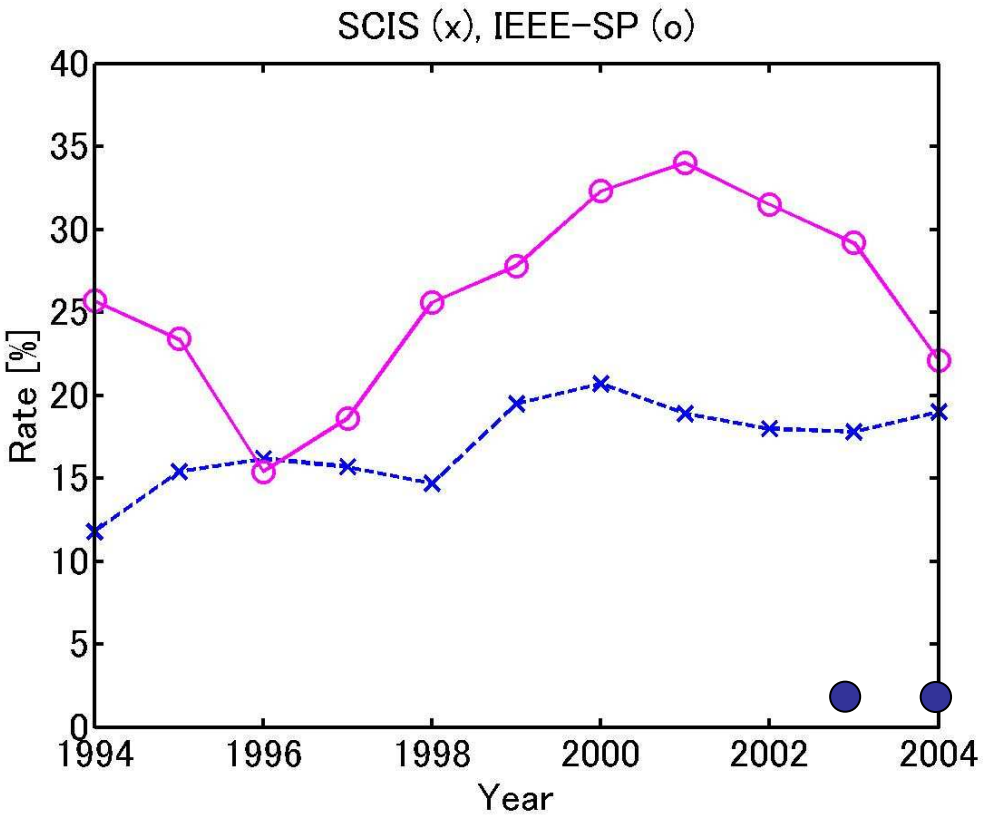
Sophisticated Attacker

Popular Level

How we can shorten the gap?

A Comparison of the rate of inter-sector collaborative papers (3-year moving average)

Presented at IEEE Eng. Management Conf. 2005, where I emphasized that other matured fields (e.g. chemical, mechanical eng.) have much higher rates.

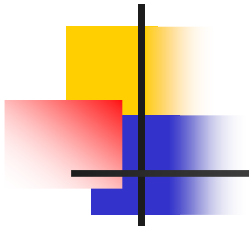


- ○IEEE Symposium on Security & Privacy
- xSCIS (Symposium of Cryptography and Information Security, Japan)
- ●WEIS

Ask "Why?", again.

- Why collaboration is not active?
  - Industry would ask what they can do with the help of such analyses.
  - Academia has not really tried to answer.
- Possible approaches: advanced consulting and mechanism design.
  - Implications from analytical models.
  - Sensitivity analysis.
  - . . .

This lecture.



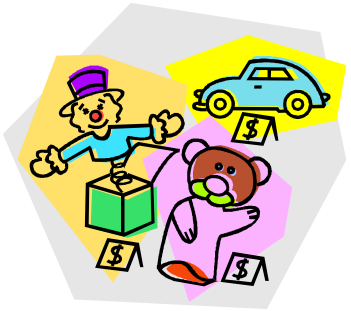
2. Economics of Light-Weight Security

Security efforts and their impacts

- Some countermeasures are provided so that attacks will fail.
  = Vulnerability reduction
- Others are provided so that attacks will not occur.
  = Threat reduction (Research is rather sparse.)
- How the reductions influence the optimal investment strategies and relevant implications?

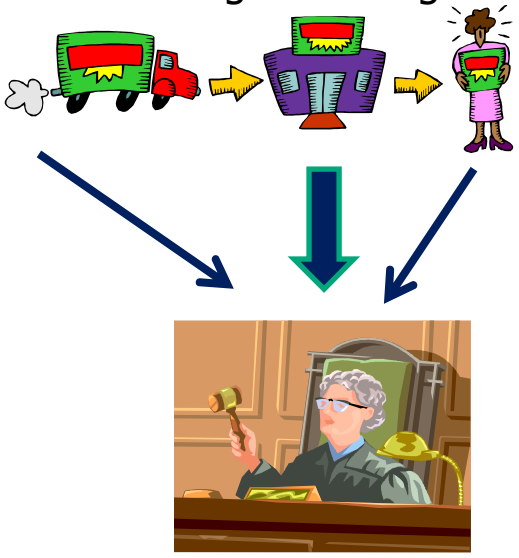
Threat reduction (An example)

- Provable-security lovers may criticize traceability systems if components use nothing but a light-weight security protocols.



- In reality, we can place rigorous countermeasures for dispute settlement and so on (as a deterrent).

E.g. Audit log



Investment models

- Taxonomies (e.g., Rue et al.@WEIS07)
  - Macro-economic input/output models, More traditional econometric techniques, Methods derived from financial markets, Case studies of firms, Heuristic models, Risk management & insurance framework, Game theoretic models, Accounting models.

"A model is supposed to reveal the essence of what is going on: your model should be reduced to just those pieces that are required to make it work." (Varian 1997)

"Clearer insights are provided by models that are less rather than more complex." (Gordon and Loeb 2002)

The Gordon-Loeb model

- Basic theory (Gordon and Loeb 2002)
  - Investigation considering Return-on-Investment in a one-period economic model.
- Empirical supports
  - The optimal investment strategy of focusing on mid-range vulnerabilities (Tanaka et al. 2005).
  - A class of security function (Liu et al. 2007).
- Extensive formulation
  - A model for information sharing and free-rider problem (Gordon et al. 2003).

Parameters & functions in the GL model

- The loss when breached: λ
- The probability of a threat occurring: t
- The potential loss: $L = t\lambda$
- The conditional probability of the threat being successful (conditional on the occurrence), called "vulnerability" in the model: v
- The information-security investment: z
- The conditional probability after the investment (security-breach probability function): $S(z,v)$
  - Class I: $S(z,v) = v/(\alpha z+1)^{\beta}$
  - Class II: $S(z,v) = v^{\alpha z+1}$

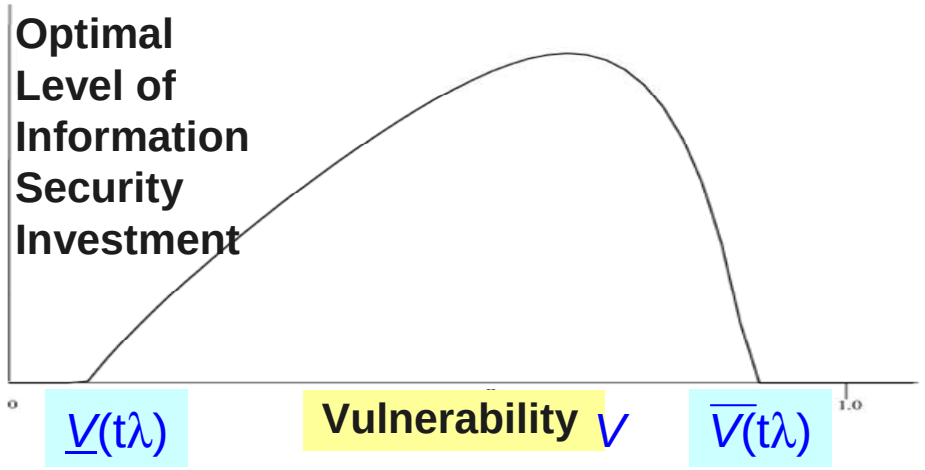
This α is called the productivity of information security.

The optimal investment z^*

- Maximize the ENBIS (Expected Net Benefit of Information Security)

$$ENBIS(z) = \{v - S(z,v)\}L - z \rightarrow \max.$$

- Closed-form solutions:
  - Class I: Focus on high vulnerabilities.
  - Class II: Focus on mid vulnerabilities. ⟶
  (Some empirical supports)



(V could be assessed locally.)

An extension: Matsuura model @WEIS2008

- Let us assume the investment z reduces the threat-occurring probability, t, down to $T(z,t)$.
- Fundamental assumption:
  - The threat reduction depends only on the investment and the current level of threat.
- Additional assumptions:
  - $T(z,0) = 0$ for all z.
  - $T(0,t) = t$ for all t.
  - For all $t \in (0,1)$ and for all z, $T_z(z,t)<0$ and $T_{zz}(z,t)>0$.
  - For all $t \in [0,1)$, $\lim_{z\to\infty} T(z,t) = 0$.

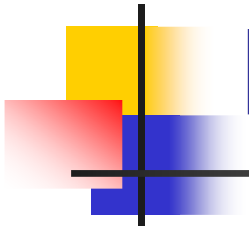
The optimal investment z^* under the risk-neutrality assumption

- Determined by

$$ENBIS(z) = \underbrace{vt\lambda - S(z,v)T(z,t)\lambda}_{=B} - \underbrace{z}_{=C} \rightarrow \max.$$

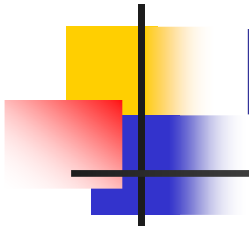
- Note: If the marginal benefit at z=0 is less than or equal to the marginal cost of such investment, z^* equals zero.

$$\left.\frac{\partial B}{\partial z}\right|_{z=0} \leq \left.\frac{\partial C}{\partial z}\right|_{z=0}$$



Risk neutrality

- If someone is risk-neutral, it means that they are indifferent to investments that have the same expected value, even though the investments may have varying amounts of risk.



Example

- A risk-neutral decision-maker would be indifferent to Investment #1 that generates either a net return of $200,000 or a net loss of $100,000 each with probability of 0.5, and Investment #2 that generates a net return of either $40,000 or $60,000 each with probability of 0.5, as both investments have an expected net return of $50,000.

A note for the example

- Notice that Investment #1 has more risk (i.e., larger standard deviation around the expected value, and the possibility of a net loss) than investment #2, and yet the two investments are being considered equal.

Class-II functions

- Hereafter, we consider the class-II functions: $S(z,v)=v^{\alpha z+1}$, $T(z,t)=t^{\beta z+1}$.
- Two productivities
  - Vulnerability-reduction productivity: α.
  - Threat-reduction productivity: β.
- We are going to examine the behavior of z^* in the two-dimensional space formed by the two productivities.

Closed-form solution

- The condition for having a zero investment as the optimum:

$$F(v) \equiv v \ln v + \frac{\beta \ln t}{\alpha} \cdot v + \frac{1}{\alpha L} \geq 0$$

That is, $-\alpha v \ln v - \beta v \ln t \leq \frac{1}{L}$.

- When $F(v)<0$, we have

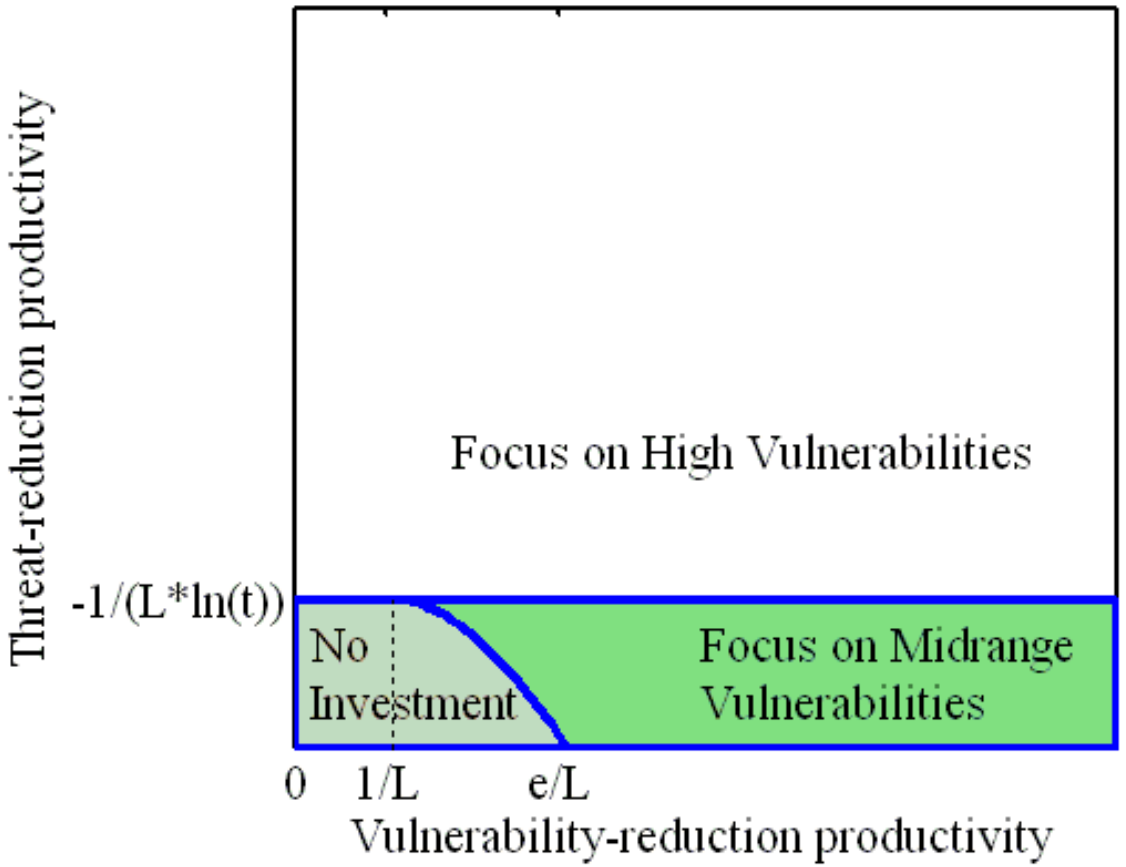
$$z^* = \frac{\ln\{-1/(vt\lambda \ln(v^\alpha t^\beta))\}}{\ln(v^\alpha t^\beta)} = \frac{\ln \frac{1}{-vL\{\alpha(\ln v) + \beta(\ln t)\}}}{\alpha(\ln v) + \beta(\ln t)}$$

Hints for the elementary calculus to obtain the z^*-v curve

- F′(v) is monotonically increasing.
- F′(v)=0 iff $v=v_0=\exp\{-1-\beta(\ln t)/\alpha\}$.
- $F(v_0)>0$ iff $\beta<\alpha\{\ln(\alpha L)-1\}/(\ln t)$.
- F(v) approaches $1/(\alpha L)$ (i.e. a positive constant) when v approaches +0.
- Note that (the conditional probability) v ranges from 0 to 1.

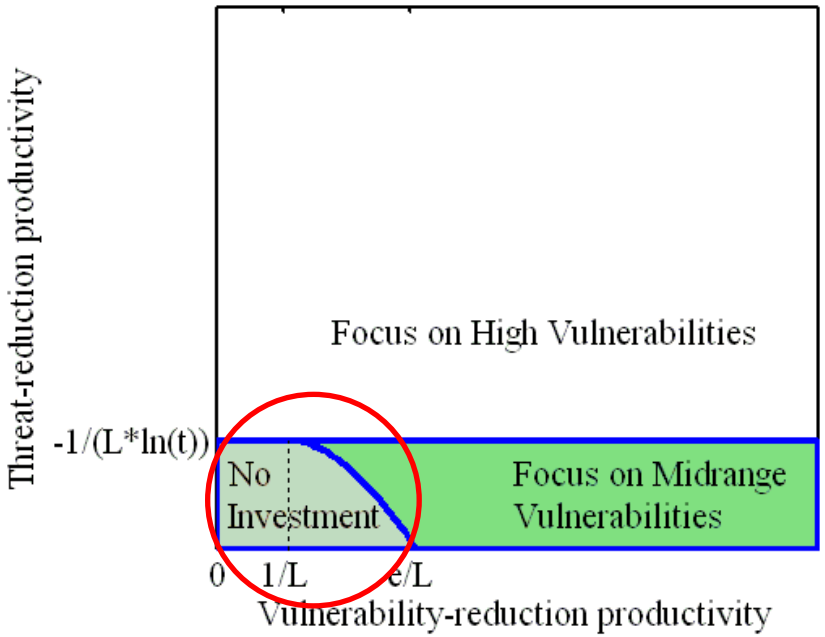
Productivity space and optimal investment

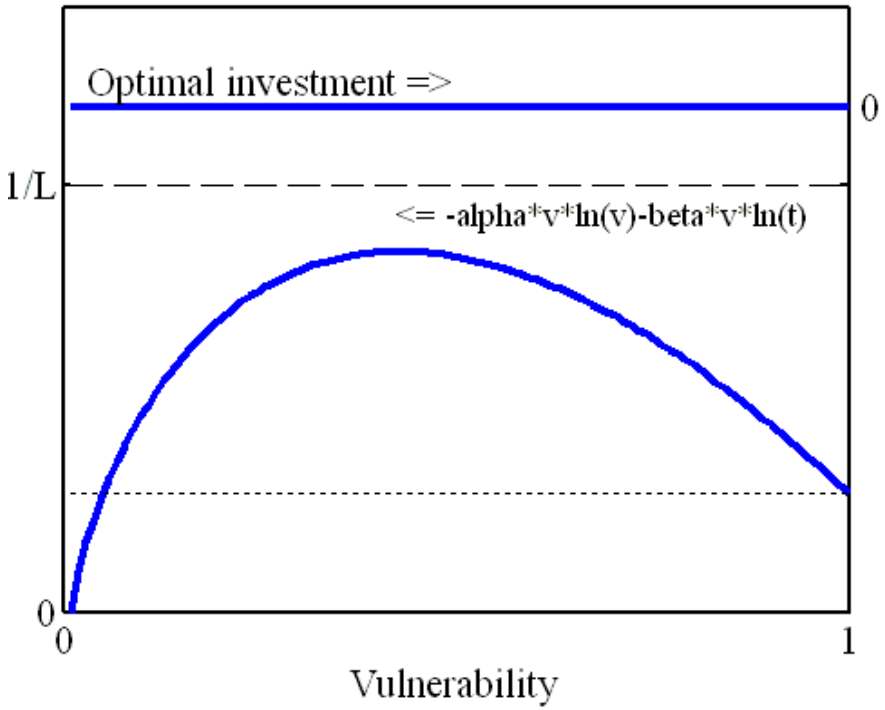
- Divided into three areas



No-investment area

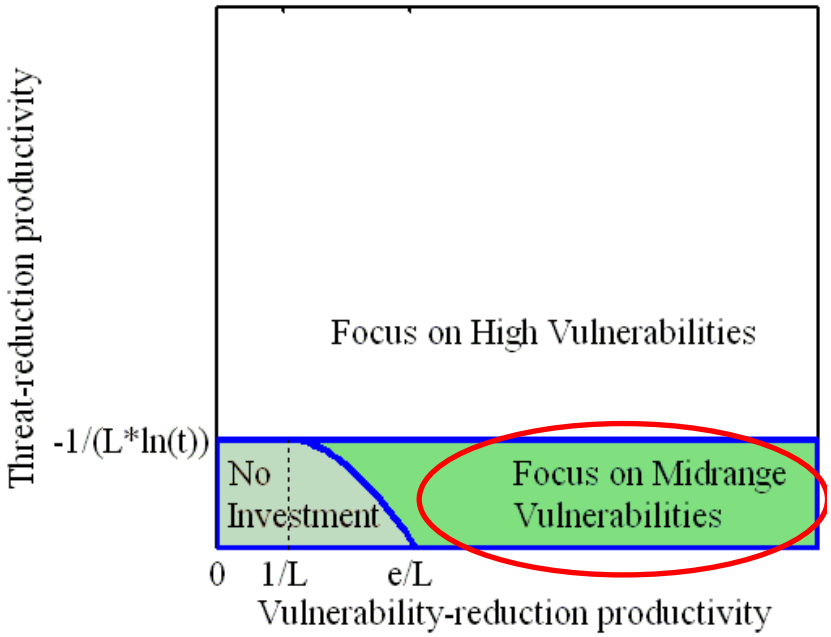
- Simply productivities are too bad.

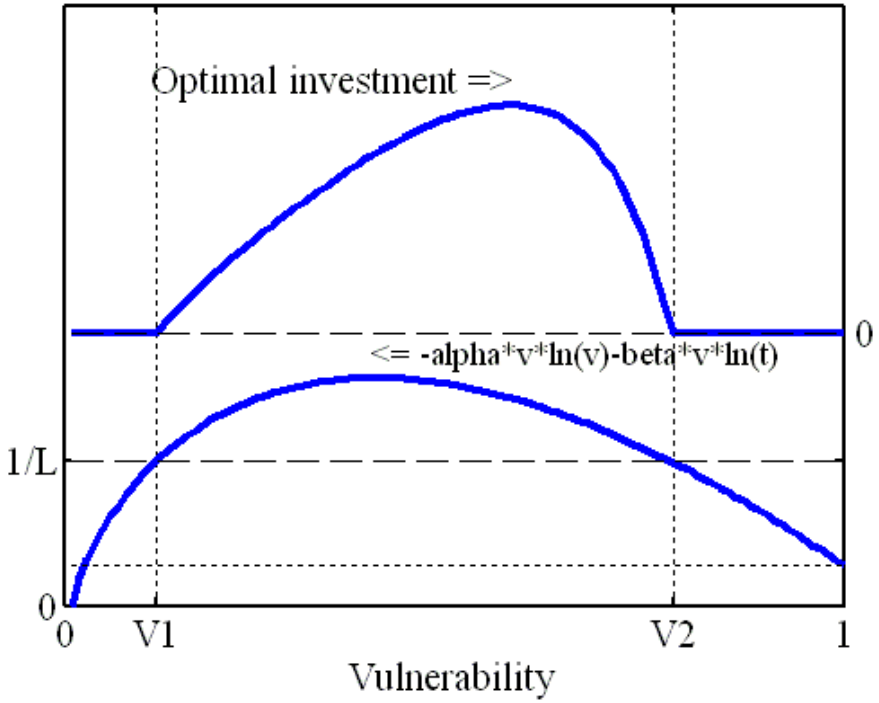




Mid-vulnerability intensive

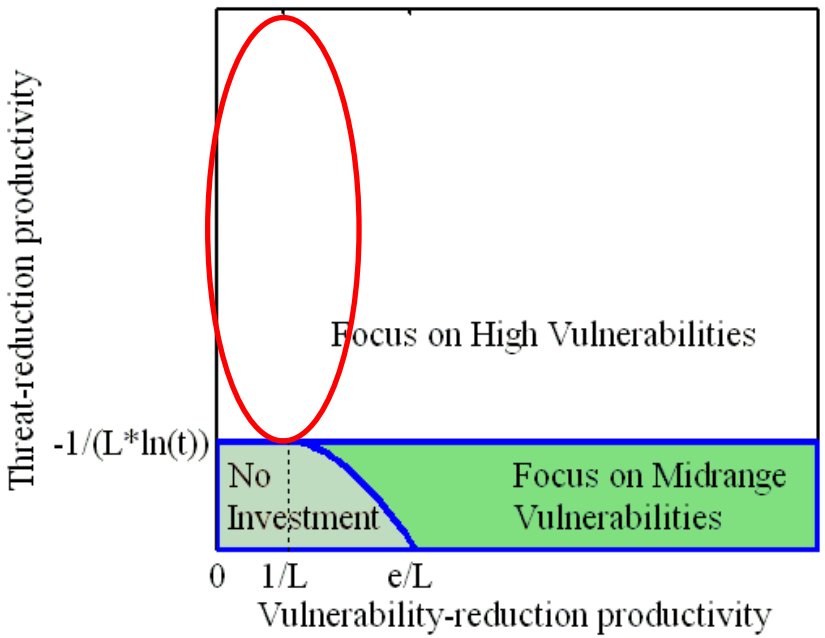
- A firm may be better off concentrating its efforts on midrange vulnerabilities.

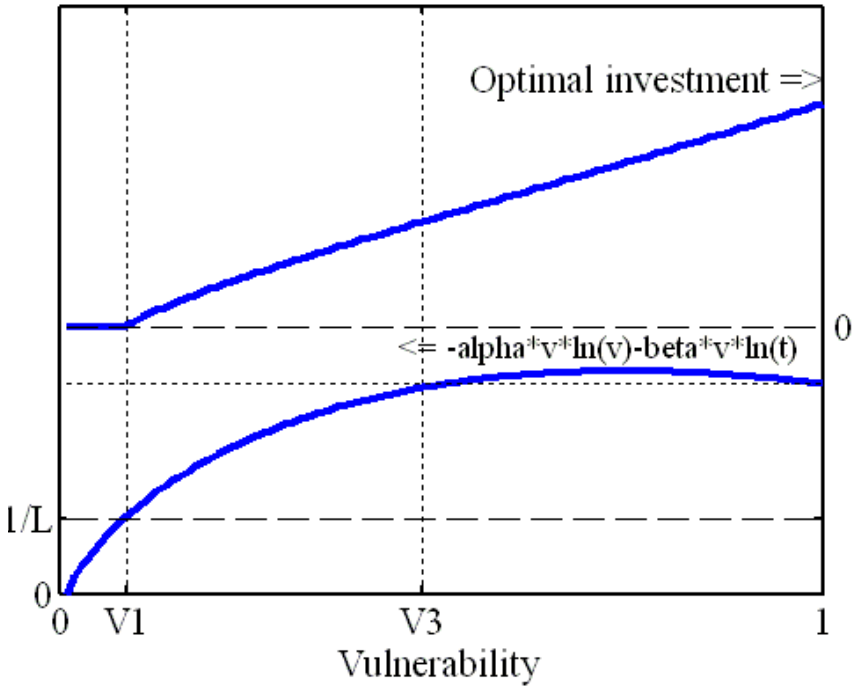




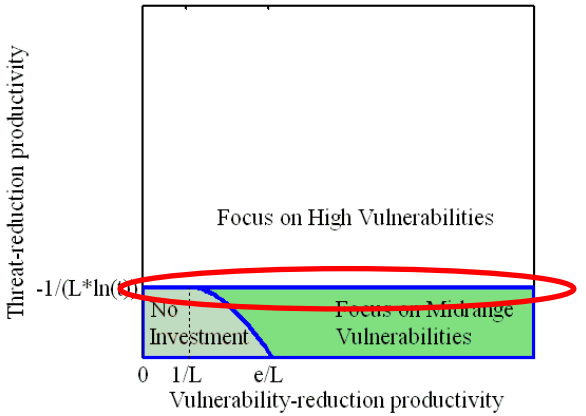
High-vulnerability intensive area

- If the threat-reduction productivity is sufficiently high, a firm should focus on high vulnerabilities.





Sensitivity analysis and implications



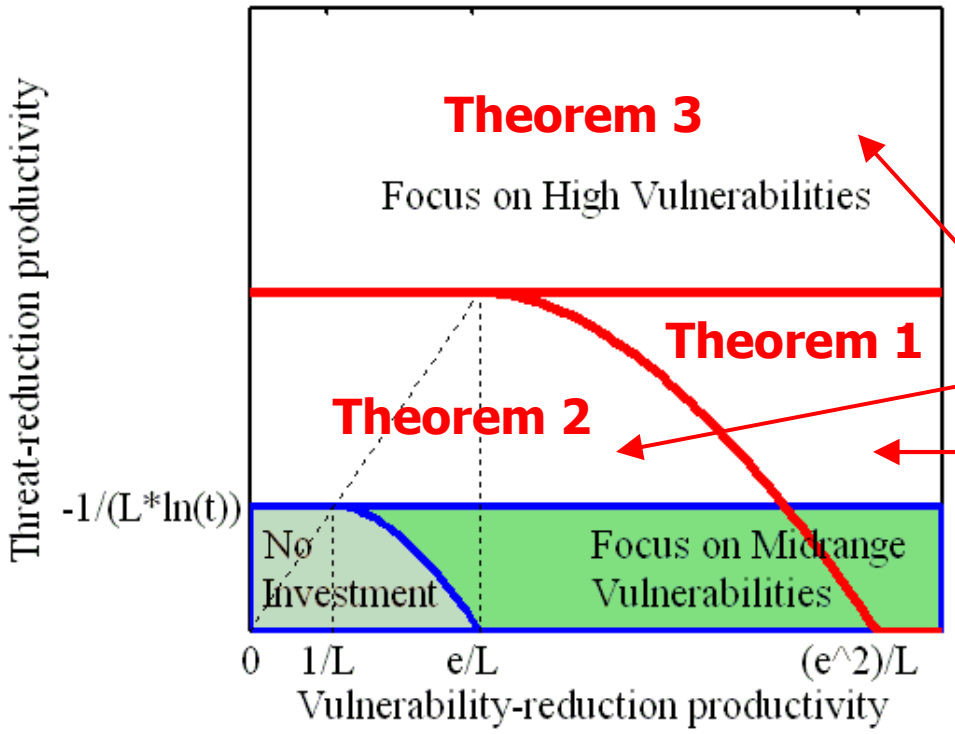
- Recommended investment strategies
  - Differ area by area in the productivity space. (*cf.* In the original GL model, determined by the class of security breach probability functions.)
- Influence of productivity-assessment failures (across the threshold)
  - Failures regarding threat reduction can cause a wrong choice of the strategy.
  - Strategy makers would see whether sufficiently secure. Would NOT see whether perfectly secure.
  - Exploring high-end technologies is important even if we fear implementation blunders and so on.

Sensitivity analysis

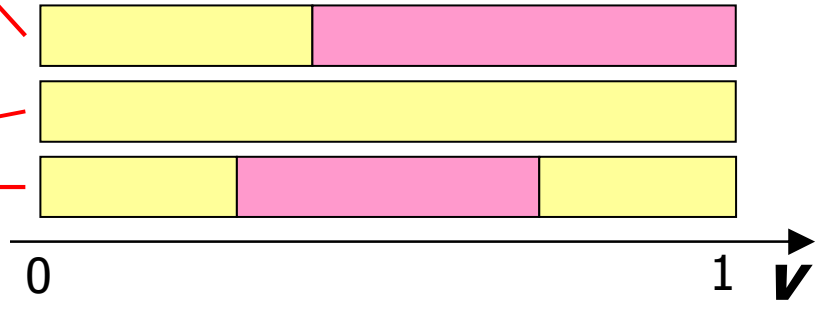
- Influence of innovation
  - How the optimum z^* would change in response to productivity improvements?
- If z* will be reduced, then vendors may have a negative incentive to realize the innovation.
- By the same elementary calculus, we have $\frac{\partial z^*}{\partial \alpha} \geq 0 \Leftrightarrow \frac{\partial z^*}{\partial \beta} \geq 0 \Leftrightarrow -\alpha v \ln v - \beta v \ln t \leq \frac{e}{L}$

Results of the sensitivity analysis

- Partitioned by similar lines and curves.



- As long as $z^* > 0$, the optimal investment increases/decreases as the productivities increase, in the following manner:

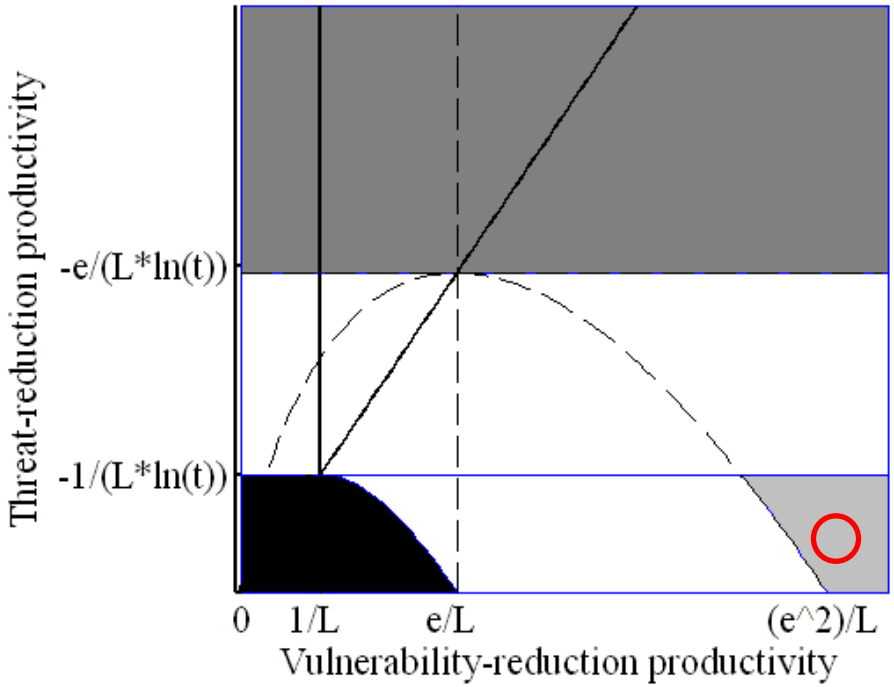


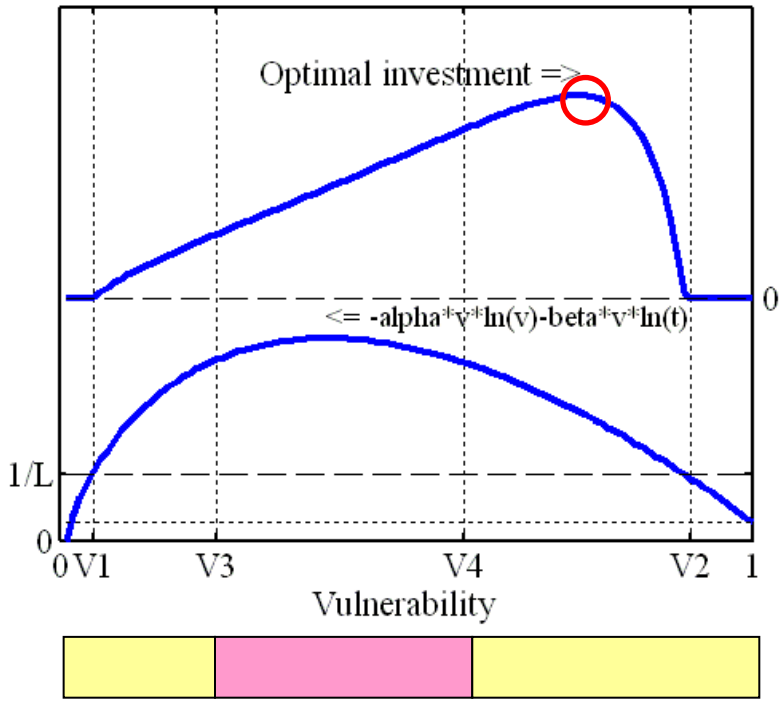
$$\frac{\partial z^*}{\partial \alpha} \geq 0, \frac{\partial z^*}{\partial \beta} \geq 0$$

$$\frac{\partial z^*}{\partial \alpha} < 0, \frac{\partial z^*}{\partial \beta} < 0$$

A note on the peak of the mid-vulnerability intensive z^*-v curve

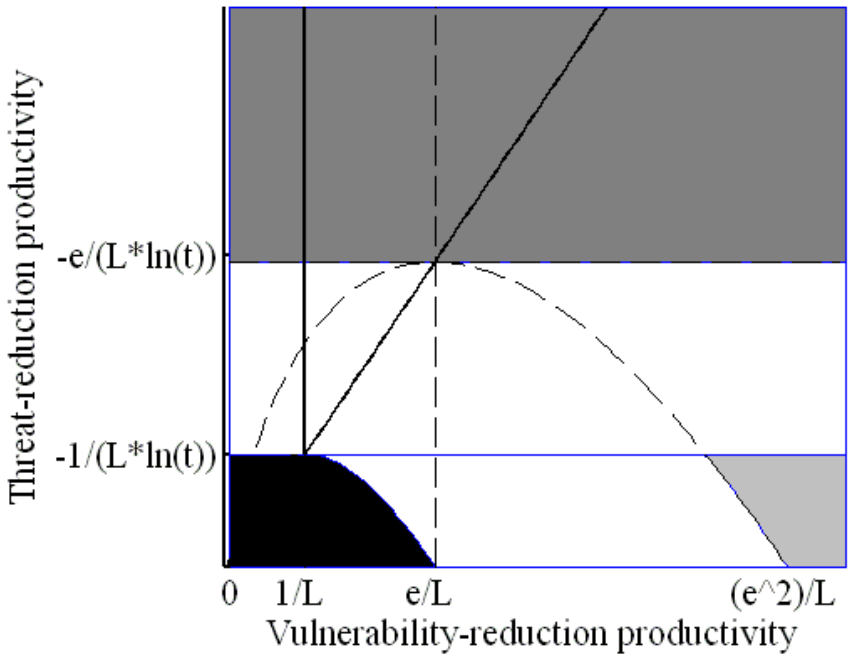
- If one rather chooses a strategy of focusing sharply around the maximum of the z^*-v curve, the focus is outside the vulnerability range for $\frac{\partial z^*}{\partial \alpha} < 0$, $\frac{\partial z^*}{\partial \beta} < 0$.



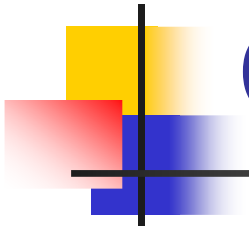


A tradeoff between vulnerability reduction and threat reduction

- When engineers efforts increase the productivities, users' investment may increase (white) or decrease (dark-gray).
- The feature in the light-gray region depends on the interpretation of the mid-vulnerability intensive strategy.
- Some vendors may prefer the former, but others may not.



(A note) My publication in 2008: 50% in cryptography, 27% in network security, 23% in economics of information security.



Concluding comments

- I hope EIS research toward synthesis improves real-world security.
  - A user guideline for JCMVP (Japan Cryptographic Module Validation Program): Draft will appear in May 2010.
- I hope more and more active (efforts for) innovations happen, in all the areas of information security.
- Ask fundamental questions.

References (1/2)

- R. Rue, S. L. Pfleeger, and D. Ortiz: A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making. Workshop on the Economics of Information Security 2007.
- H. Varian: How to build an economic model in your spare time. Part of a collection titled *Passion and Craft: Economists at Work* (M. Szenberg ed.), University of Michigan Press, 1997.
- L. A. Gordon and M. P. Loeb: The Economics of Information Security Investment. *ACM Transactions on Information and System Security* (5:4) pp.438-457, 2002.
- H. Tanaka, K. Matsuura, and O. Sudoh: Vulnerability and Information Security Investment: an Empirical Analysis of e-Local Government in Japan. *Journal of Accounting and Public Policy* (24:1) pp.37-59, 2005.

References (2/2)

- W. Liu, H. Tanaka, and K. Matsuura: Empirical-Analysis Methodology for Information-Security Investment and Its Application to a Reliable Survey of Japanese Firms. *IPSJ Journal* (48:9) pp.3204-3218, 2007.
- L. A. Gordon, M. P. Loeb, and W. Lucyshyn: Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting & Public Policy* (22:6) pp.461-485, 2003.
- K. Matsuura: Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model. Workshop on the Economics of Information Security 2008.
- K. Matsuura: Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model. In *Managing Information Risk and the Economics of Security* (E. Johnson ed.), Springer, pp.99-119, 2009.