PROVISIONING NETWORK SECURITY: TRADEOFF BETWEEN INFORMATION ACCESS AND LEVEL OF SECURITY

Alok Gupta
Associate Professor

Dmitry Zhdanov
PhD Student

Information and Decision Sciences Department
Carlson School of Management
University of Minnesota
Minneapolis, MN 55455

Email: {agupta, dzhdanov}@csom.umn.edu

Last Revised 11/08/04

ABSTRACT

It has been repeatedly pointed out that security problems in multi-agent systems are a manifestation of improper economic incentives provided for agents through mechanisms that are supposed to provide such incentives. This paper provides initial insight on how economics tools of utility theory and welfare economics may be used to analyze the behaviors of economic agents with respect to security choices. We consider a case where security can be produced in organization by using access to information systems as a production factor. There are important tradeoffs between access and security of information that leads to provisioning of additional amount of security being increasingly costly. We provide structural results that characterize these tradeoffs and demonstrate how different security preferences of agents may lead to suboptimal choice for the level of security. We further explore a game-theoretic formulation of the problem, modeling security provisioning in a two-player repeated game with side payments. Our results indicate importance of building long-term trust relationships in order to guarantee proper provisioning of security, as well as ability to find specific and payoff-independent values of payoff discounting factors that induce such trust-building and incentive-compatibility.

1. Introduction

Information security is a growing concern among managers in almost all organizations resulting in increased spending on security solutions from year to year. However, certain types of security incidents repeat themselves time and time again – from virus infections to denial of service attacks to internal compromise of confidential data. It appears that technological solutions in themselves are not enough to provide robust security.

One interesting observation from practice is that new security spending is going into familiar solutions – mostly, antivirus software, intrusion detection systems and firewalls (Schwartz 2004). Patching old systems is also a major part of security-related costs. This implies that provision of additional information security is an increasingly hard problem. Attacks become faster and more sophisticated (CERT 2000), thus making the tracking of these attacks more difficult.

Another source of pressure comes from the need for more, faster and better access to information. However, there is a trade-off between access and information security that is recognized by most managers (Regan 2003). Many e-commerce businesses face tough choices between providing fast transaction processing to their customers and systems security.

In this paper, we look at the tradeoff and its influence on the information security decisions made by organizations and their units. We illustrate why providing additional security is hard for organizations using a stylized economic model of security production and information consumption.

Economic modeling in application to information security problems is still in its nascent stages. Recent research has started to look at the problem of economics of security from a broad scope of economic theories and perspectives. For example, Yemini et al. (1998) try to create a resource access model as a financial market with different currencies used to pay for different services. They claim that such mechanism will provide more security, since an attacker will need a stock of particular currency and may eventually run out. Varian (2002) models systems reliability as a public good, level of which depends on collective effort of individual agents. Ogut et al. (2003) models intrusion detection system where it interacts with a user to determine its type.

We take a somewhat different approach in our analysis and consider the provision of security from the perspective of utility theory and welfare economics. The key insights that we rely upon are that members of organizations may have different incentives and preferences, that access to information systems is a valuable commodity, and that it has to be restricted in order to provide security. Gurbaxani and Kemerer (1989) support the notion of heterogeneous nature of organizations and argue that provision of information services can be market-based. Camp (2002) notes that increasing security requires removing power from users. Therefore, we analyze tradeoffs in security provisioning by modeling security as being an output of a production process using access as input.

2. Modeling setup and notation

Consider an organization that consists of agents using computers. We represent an organization as a collection of agents that are supposed to share a common "security

perimeter" (e.g., a conventional firm; or a company employing consultants or telecommuters, or distributed research group, etc.)

We assume that there is a collection of security policies that are implemented in organization. Let S be the measure of information security to the organization that results from particular set of policies. It can be treated as the "volume" of security that the organization can achieve by implementing a particular configuration of security policies.

Access is another important commodity for agents. In a broad sense, it can be defined as the collection of rights, privileges and policies that enable users to process information. It can be argued that more access leads to more benefits (ability to do job better/faster/more productively, particularly if agent's job is related to data processing). We can think of access as a production factor similar to labor and capital. Let A be the measure of access that users have across the organization.

We can model preferences of agents in terms of access and security – they are, without loss of generality, increasing in access (the more – the better) and decreasing in risk. Also, we may expect that users will have non-decreasing preferences for security.

We assume that choice of security policies S implies associated level of access – A(S). More secure policies tend to restrict users' access privileges (e.g., executing programs remotely), while policies that are less restrictive are less secure.

There may be two viewpoints on the direction of relationship between access and security. On one hand, choice of security policy implies access levels; on another – we may consider "using up" access as agents are "producing" security. This latter approach seems appealing for future analysis, when access can be treated as an input in production of other commodities, with security being one of them, as discussed earlier. We assume

that there is a functional relationship between security and access: S = S(A) and A = A(S).

Without loss of generality, we will assume that there is only one Agent that is producing primary output for the Organization. Security can be produced (provided) by the Organization rather than Agent; however, both have preferences for access and security.

Using the framework defined above we address several interesting questions in this paper:

- What is the optimal composition of security and access in organization?
- If agents act myopically in self-interest, can they reach a level of utility that is acceptable from an organization's viewpoint?
- If the myopic behavior of agents does not result in optimal level of security, what adjustments can be made to market mechanism, so that organizationally-best outcome is achieved?

In the rest of the paper we address these questions from several different perspectives, starting with a special case of lexicographic preferences in section 3.

3. Special case of preferences: conflict between producing agent and security authority

In this section we consider a common situation when goals and preferences of the individual agents are different from those of the Organization.

It has been observed that organizations are not always effective in enforcing security policies among its members. Particularly, in the case of commercial organizations, the primary goal for individual agents, frequently acting as revenue or profit centers, is to increase their output thus requiring more access. Thus, preferences of agents may exhibit a non-continuous, lexicographic type of pattern where more access is always better, however, for the given level of access, increased security is preferred*.

However, from the standpoint of security enforcing entity (Organization), the preferences are exactly opposite, i.e., more security is always better, and only if security level is given, increased access is preferred.

This situation may be modeled by the following Edgeworth box. In this representation, 1 represents producing agent, and 2 represents security authority. Solid lines indicate primary direction of preferences increase and dashed lines indicate secondary direction.

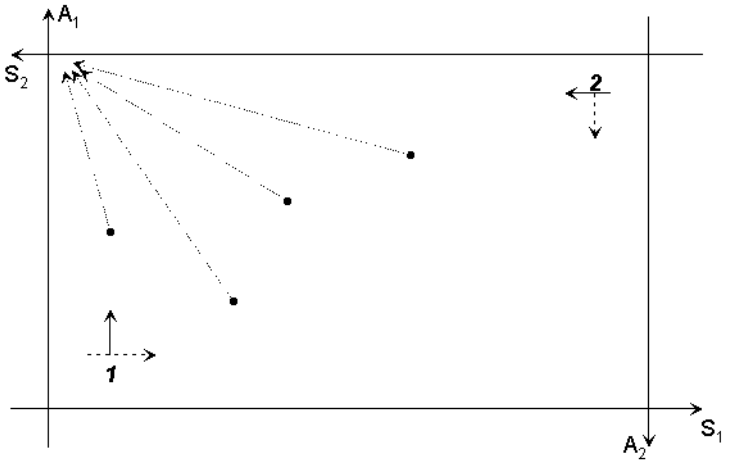

Figure 1.Edgeworth box representing lexicographic security preferences

* Formally, lexicographic preferences for agent i and goods X and Y are defined as follows: if bundle 1 has more good X than bundle 2 (X1>X2), then it is always preferred to bundle 2 by agent I, without considering good Y. Only if both bundles have the same amount of good X (X1=X2), then amount of good Y matters for agent i's preferences.

It is clear from Figure 1 that both parties prefer the northwest corner to any other allocation, which implies that agent wants all access and no security at all.

Fortunately, as discussed earlier, security and access are functionally related, i.e. S = S(A). Also, this function is decreasing in A. Thus, when no access is used to produce security, our Edgeworth box collapses into a vertical line, and its "length" is original endowment of access. Denote this endowment $\overline{A}$. Since both parties care for different commodity, to maximize "society" utility W, we need to maximize:

$W = Pa \cdot A + Ps \cdot S(R),$ (1)

where:

Pa, Ps – positive prices of access and security;

A – amount of access consumed;

$\bar{A}$ – initial endowment of access;

R – restrictions on access used to produce security: $R+A = \bar{A}$;

S(R) – technology (production function), which is continuous and twice differentiable.

Theorem 1 provides a necessary condition for welfare maximization.

Theorem 1: *Welfare maximization problem, as represented by equation (1) , has a feasible solution as long as production function S(R) is concave.*

Proof.

From $R+A = \bar{A}$, expression for W may be rewritten as:

$$W = Pa \cdot A + Ps \cdot S(\overline{A} - A)$$

To seek optimum, we differentiate W with respect to A:

$$\frac{dW}{dA} = Pa - Ps \cdot S'(\bar{A} - A)$$

Setting differential to zero, we find candidate extremum point A^* where

(i) $S'(\bar{A} - A^*) = Pa/Ps > 0$ (since prices are positive)

To ensure that A^* is, indeed, maximum, we need:

$$\frac{d^2W}{dA^2} = Ps \cdot S''(\bar{A} - A^*) < 0,$$

which implies (since Ps is positive) that

(ii) $S''(\bar{A} - A^*) < 0$

From (i) and (ii) it follows that $S(\bar{A} - A^*) = S(R)$ is a concave function, thus being non-increasing returns to scale ***Q.E.D.***

There are two important observations here. First, Theorem 1 applies in a general welfare maximization setting and is not restricted to the case of lexicographic preferences. Second, non-increasing returns to scale is a common shape of production function. Therefore we can consider a broad range of possible production functions for security-producing technologies.

The latter observation also corresponds well with observations from practice. Concavity of production function implies that provision of additional security is increasingly hard, and higher spending does not guarantee a proportional increase in security effectiveness.

4. Producing security from access

In previous section, we modeled security such that it is produced by giving up a fraction of original endowment of access. In this section, we use approaches of welfare economics to further analyze this production economy.

First, let there be a simple economy with one agent and two commodities – access and security, and one firm capable of producing security from access.

Let:

U = U (S, A) – agent's utility from commodities

Pa, Ps – respective prices (positive is a reasonable assumption)

$\bar{A}$ – initial endowment of access

A – access "consumed"

R – "restrictions", access used to produce security

S(R) – production technology

S^p, S^c – security produced and consumed, respectively

Then, competitive equilibrium, if it exists, may be represented as a tuple (Pa, Ps, A, S^c, R, S^p), with third and fourth elements being the consumption set and fifth and sixth elements being the production set.

The equilibrium must satisfy the following conditions:

Max U (A, S^c) (2)

s.t. $Pa \cdot A + Ps \cdot S^c = Pa \cdot \bar{A} + \pi$ – maximization of utility under budget constraint

Max $\pi = Ps \cdot S^p - Pa \cdot R$ (3)

s.t. Sp = S(R) - maximization of profit under technology constraint

$A+R = \bar{A}$; $S^p = S^c$ (4) - what is available is consumed

Since this system can provide enough information to solve for only five of six parameters, it is common in economics to solve it for the ratio of prices Ps/Pa, instead of individual prices.

Note that our simple single-agent economy may be extended to include many agents. To do so, we can specify a rule on how to distribute profits among them (every one will receive some fraction of π, and those shares should add up to one). However, for expository purposes, we focus only on a single-agent economy.

Competitive equilibrium resulting from selfish actions of agents is Pareto-optimal, if certain assumptions are met. These assumptions are (following MasColell et al., ch. 16, pp. 546-548):

- Agent and Firm are price-takers (prices are exogenous)
- Agent is profit-taker (Firm's profits do not depend on her consumption bundle)
- Agent and Firm selfishly maximize their consumption/profit (no externalities)
- Aggregate consumption equals aggregate endowment and production (no free disposal)

It is obvious that all these four assumptions are fulfilled in our formulation of equilibrium. Therefore, By First Fundamental Theorem of Welfare Economics, we know that market allocation is Pareto-efficient.

Numerical example

To make our analysis more illustrative, let us consider a following numerical example:

Let there be two entities: User (representing an aggregation of all users of the information system in an organization), and Organization. User has preferences for access and security that are represented by the utility function $U(A, S^c) = A \cdot S^c$, and

original endowment of access of $\bar{A} = 100$. User delegates R units of access to Organization to produce security using technology $S(R) = \sqrt{R}$. Let us find a Pareto-optimal equilibrium, when both User and Organization are maximizing their utility and profits.

The Organization solves the following problem:

$$\text{Max} \quad Ps \cdot (100 - A)^{1/2} - Pa\,(100 - A), \tag{5}$$

while User solves the problem:

$$\text{Max } A \cdot S^c - \lambda \cdot [Pa \cdot A + Ps \cdot S^c - [Ps \cdot (100-A)^{1/2} - Pa \cdot (100-A)]] \tag{6}$$

where λ is Lagrange multiplier

Writing first-order conditions and imposing that security produced is equal to security consumed, we obtain a system of equations:

$$\begin{cases} S^c = (100-A)^{1/2} \\ A = 100 - Ps^2/(4Pa^2) \\ \lambda = A / Ps \\ S^c = \lambda \cdot Ps / (2 \cdot (100 - A)^{1/2}) \end{cases} \tag{7}$$

Result of solving system (7) is $A = 66\frac{2}{3}$; $S^c = \sqrt{33\frac{1}{3}}$ and price ratio $\frac{Ps}{Pa} = 2\sqrt{33\frac{1}{3}}$.

Thus, a User gives up 33.333 units of access to the Organization to produce 5.75 units of security. This situation can be sustained is price of security is about 11.5 times

higher than price of access. In other words, in this example security is hard to produce, but it is quite valuable commodity.

From a social planner perspective, we can only control prices. The natural question is what will happen if the prices are not set at the optimal level? Consider an example provided in the following graphs:

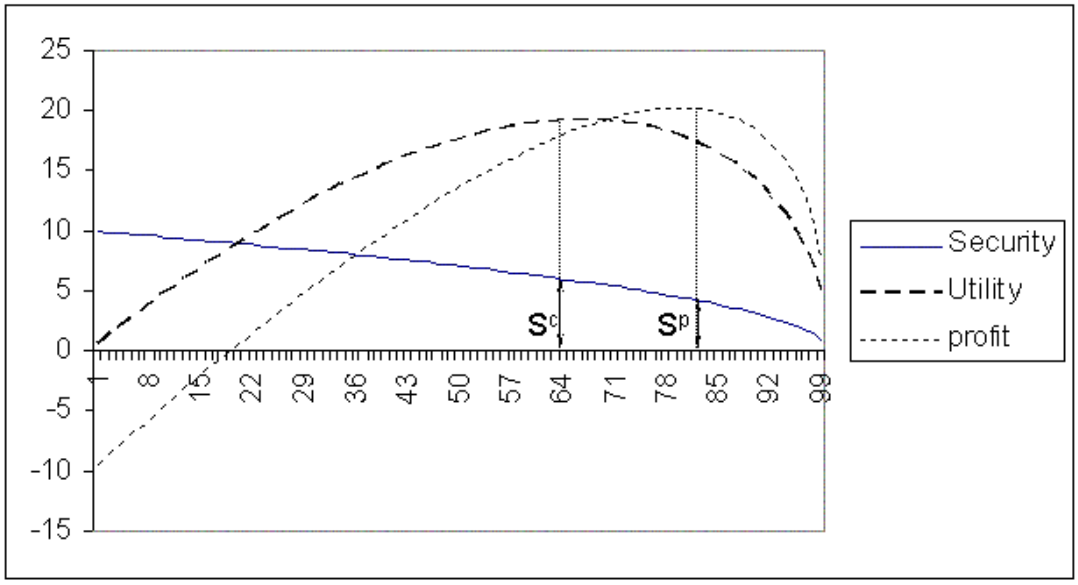

Figure 2a. Optimal myopic choices by User and Organization in terms of access, Ps/Pa = 9

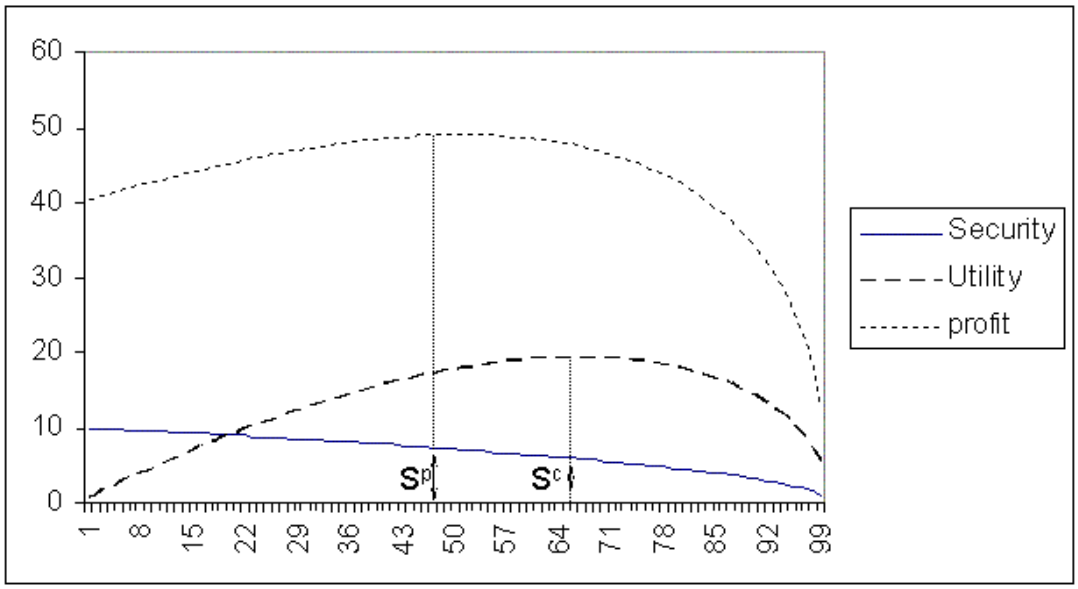

Figure 2b. Optimal myopic choices by User and Organization in terms of access, Ps/Pa =14

In Figures 2a and 2b, the X axis represents the amount of access (A) that our entities want to be used. The remainder (out of 100) is converted into security. The curves represent production technology (solid), User's utility (dashed) and Organization's profit (dotted). Maximization of utility/profit is equivalent to identifying the highest points of these curves.

In Figure 2a, price ratio is 9 (less than equilibrium). We see that in this case, the User wants less access (and, thus, more security). However, it is more profitable for organization to produce less security. Some portion of access that the User is willing to give up may be lost, since the Organization doesn't want that much of resource.

A reverse situation is depicted in Figure 2b. Here, the price ratio of security to access is 14 - greater than equilibrium. In this case, the Organization wants to produce more security than the User wants. Since the User is not inclined to give up access, security is overpriced.

At this point it may be useful interpret what are the implications of security being overpriced. Essentially, it means that if Organization wants the desired level of security and access, it will need to provide higher level of resources. The resources may not necessarily be monetary but may take the form of training users to efficiently use the systems with new security policies. The higher resources also may mean development of new applications to provide users "modified" access to information they need.

Note that these results can be generalized to any conventional utility and production technology.

Suppose user's utility can be represented by a continuous, concave, differentiable utility function, while production technology is represented by continuous, monotonic differentiable production function. Also, let r^* be the optimal price ratio, resulting in market equilibrium. Then, if in maximization problem specified by equations (2) and (3), price ratio is different from equilibrium, provision of security will not be optimal. Particularly, when security is underpriced (relative to access), it will be underproduced; if it is overpriced it will be under-demanded. Proposition 1 formally specifies this result

Proposition 1. *Supply and demand for security are dependent on price levels of Security and Access. Specifically,*

If $Pa/Ps > r^*$, *then* $Sp < Sc$

If $Pa/Ps < r^*$, *then* $Sp > Sc$

If $Pa/Ps = r^*$, *then* $Sp = Sc$

Proof.

We will study the dynamics of decisions by User and Organization as functions of price ratio Pa/Ps.

First, consider Organization. It solves the following optimization problem:

Max $\pi = Ps \cdot S^p - Pa \cdot R$

s.t. $S^p = S(R)$. (and $R = \bar{A} - A$)

Substituting for S^p and R and differentiating, we get first order condition

$\frac{d\pi}{dA} = - Ps \cdot S'(\bar{A} - A) + Pa = 0$, equivalent to $S'(\bar{A} - A) = Pa/Ps$.

Thus, "restrictions" R, demanded by the Organization as production input are:

$R = (S')^{-1}(Pa/Ps)$, where $(S')^{-1}$ denotes an inverse function of the first derivative of production technology S.

Since S (R) is concave and monotonic, then its derivative S' (R) is decreasing. Therefore, $(S')^{-1}$ is also decreasing.

Thus, as Pa/Ps goes up (security is underpriced), optimal R decreases, leading to decreased production of security. If Pa/Ps is greater than equilibrium, security will be underproduced.

Now, consider User. It solves the following optimization problem:

Max $U(A, S^c)$

s.t. $Pa \cdot A + Ps \cdot S^c = Pa \cdot \bar{A} + \pi$

(note that π is defined by Organization, and thus, is a parameter for User)

Lagrangian for this problem is:

$L = U(A, S^c) + \lambda \cdot [Pa \cdot \bar{A} + \pi - Pa \cdot A - Ps \cdot S^c]$

Differentiation gives the following first-order conditions:

$\frac{\partial L}{\partial A} = \frac{\partial U(A,S)}{\partial A} - \lambda Pa = 0$

$$\frac{\partial L}{\partial S} = \frac{\partial U(A,S)}{\partial S} - \lambda \mathrm{Pa} = 0$$

$$\frac{\partial L}{\partial \lambda} = \mathrm{Pa}\cdot \bar{\mathrm{A}} + \pi - \mathrm{Pa}\cdot \mathrm{A} - \mathrm{Ps}\cdot \mathrm{S}^{c} = 0$$

From the first two of them, we get that

$$\frac{U'_A}{U'_S} = \frac{Pa}{Ps}$$

Therefore, as Pa/Ps decreases (security is overpriced), the User can redistribute his budget to get more utility from access, and security gets under-demanded ***Q.E.D.***

The economic rationale behind this result is intuitive: an Organization wants to set price of resource (access) equal to its marginal productivity, while a User want to have prices of access and security be equal to their marginal utilities. Misbalance of the prices leads to results described above.

A natural question is what can a regulator adjust in such a case? It is reasonable to assume that preferences of agent are beyond control. Price of access (since it is a production input in some other process used by the agent) is also probably set externally, e.g., as a marginal productivity of access in producing whatever final good. But that means that regulator, particularly if it is security-producing authority, may try to manipulate production function and price of security. However, some of these adjustments make First Welfare Economics Theorem inapplicable, and there is a need to find an "aggregate" equilibrium in a separate analysis.[†]

[†] One of important assumptions is absence of externalities. Obviously, this is an important direction for future research, since externality is naturally present in allocating security in an organization. Further, agents can manipulate prices of access as well as security and make deceptive statements about their true preferences, which make room for game-theoretic approaches.

Our analysis indicates that though the provision of adequate security is a difficult problem, a production function approach has a potential to provide insights in the reasons for failure of security incentives. While the solution of a system towards equilibrium is beyond the scope of this paper, the described approach indicates directions for potential actions. Next section discusses cases when there are ways to finding a path to equilibrium even though the price ratio is not specified correctly.

5. Incentives for mechanism design and Game-theoretic formulation

We started our analysis with a supposition that there is an organization that is "security aware" and that it consist of users that might not be as "security cautious" as the organization wants them to. In previous section we showed that independent producer and consumer of security will not always interact to provide efficient amount of security.

However, it is reasonable to think that "security aware" organization is the "producer" of security. Then, the imperfect outcomes indicated above can be somewhat avoided.

First, let's reconsider the case of underpriced security. Here, users want more security, but profit-maximizing producer does not provide it. However, if the producer is the same organization that tries to impose security (and for which security is a primary concern), it will be willing to provide sufficient security, even if it means departing from optimal profits. Further, firms may have different capabilities to produce security, resulting in situations when under the same conditions, more efficient firms will provide higher levels of security than their less efficient counterparts.

To illustrate this situation, consider a modification of numeric example in previous section. Suppose there is another firm – Firm 2 – that has a better technology to

produce security: $S_2(R) = 2\sqrt{R}$. If all other parameters are kept the same, solving an equivalent of system of equations (7) will result in an equilibrium solution of $A = 66\frac{2}{3}$; $S^c = 2\sqrt{33\frac{1}{3}}$ and price ratio $\frac{Ps}{Pa} = \sqrt{33\frac{1}{3}}$. Note that Firm 2 uses the same amount of access as Firm 1 in equilibrium, but provides twice as much security as Firm 1. Additionally, the equilibrium price ratio for Firm 2 is twice smaller than that for Firm 1.

Therefore, if we have these two firms with different production technologies, we can mitigate some of the inefficiencies resulting from off-equilibrium prices. Consider Figures 3a and 3b below. Both of them represent optimal myopic choices by Firms and Users in case of off-equilibrium price ratio $\frac{Ps}{Pa} = 7$. Recall that for Firm 1, equilibrium price ratio is about 11.5, therefore it will under-produce security compared to what its users want. It wants to keep Access at about 88, while users need only about 67 units.

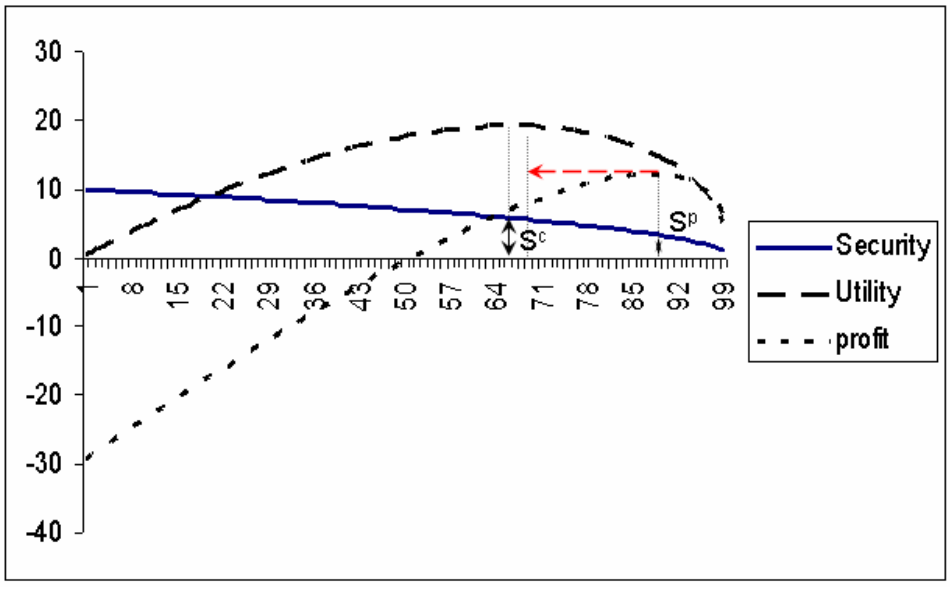

Figure 3a. Optimal myopic choices by Firm 1 (less efficient) in terms of access, Ps/Pa =7

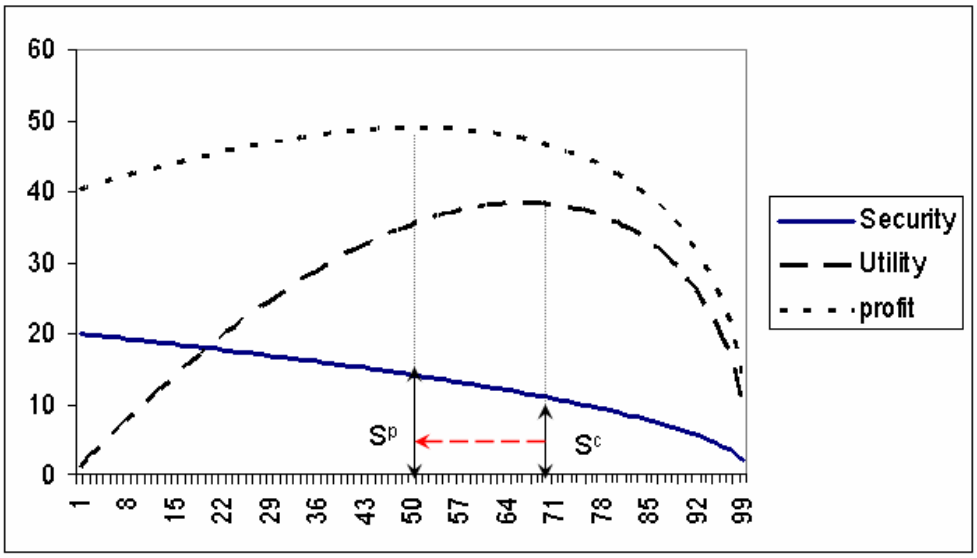

Figure 3b. Optimal myopic choices by Firm 2 (more efficient) in terms of access, Ps/Pa =7

On the contrary, Firm 2's equilibrium price ratio is about 5.8, therefore it is in the situation of under-demanded security. It would like to have 51 units of access, and convert remaining 49 into security, while users want to keep about 67 units of access. Both cases are inefficient in themselves, but combined together, they can improve total social welfare by canceling out individual inefficiencies.

In case of Firm 1, there are about 21 units of access that its users are willing to give up to produce security (and that Firm 1 does not want to use). On another hand, Firm 2 has unused capacity of about 12 units of access that it would like to obtain to produce security (and users of Firm 2 do not want that security). Therefore, a transfer of 12 units of access from users of Firm 1 to Firm 2 will improve social welfare, as Firm 2 will be able to achieve its maximum profit, while users of Firm 1 get closer to their optimal level of security. Such transfers are indicated with red dashed arrows in Figures 3a, 3b.

There are two important observations in this situation. First, we are generally not guaranteed to achieve maximum social welfare with these transfers, but we definitely can

improve over inefficient allocations of individual firms. Second, such approach to security provisioning implies that organizational boundaries in terms of security are not the same as structural ones. In the example above, several functional units of Firm 1 get their security provided by Firm 2. This is an important business world phenomenon of recent days which is clearly present in cases of managed security service providers, telework, web services, etc. Such "blurring" organizational boundaries with regards to security provisioning is called "deperimeterization" (Saran 2003). We develop a detailed treatment of deperimeterization in a separate paper.

As discussed above, underpriced security problem may be partially overcome by leveraging resources of firms with different production technologies. Situation is more problematic when security is overpriced for all firms. In this case, users just don't give up access to produce enough security. The organization can try to take access forcefully, or implement a more subtle scheme, described below.

Consider a simple game between User and Organization. If security is underproduced because User does not give up access, Organization can try to provide "bonus" to the User to give up enough access.

User is happy with relatively "low" level of security. If this state is maintained, his payoff is zero. If Organization can persuade the User to give up amount of access needed to implement "high" level of security, it will cost him $c (opportunity cost of lost access).

On Organization's side, "low" level of security means an opportunity cost of $z (cost of desired, but unattained security). If "high" level is implemented, Organization enjoys that benefit of $z of security.

Organization can decide to provide a side payment or "bonus" to the User to opt for "high" security with a payment of $b. Amount of $b should be less than $z (for Organization to have incentive to provide bonus and still have a benefit of increased security), and should also be greater than $c (for User to have incentive to take the bonus).

Normal form of this game is represented below (payoffs of User are first):

Org. / User	Bonus	No Bonus
Choose Low	+b; -z-b	0; -z
Choose High	+b-c; z-b	-c; z

Obviously, the Nash Equilibrium of this game is (Choose low, No bonus) – our familiar state of underprovision of security. If this game is played just once, high security level will not be achieved.

However, it is not unreasonable to think that some security decisions are made repeatedly over time. Then this game can be repeated infinitely. Now it is possible to check if outcome (Bonus, Choose high) can be sustained as a subgame-perfect equilibrium using Nash reversion strategies, which is a traditional approach to analyzing repeated games. The outcome of (Bonus, Choose high) is more beneficial for both players and leads to provision of the desired level of security, but is never achieved in a one-time game.

In Nash reversion strategy, both players will play (Bonus, Choose high) in some period t, if both of them played the same in previous period t-1. If one of the players

deviates, in period t+1 the opponent will start "punishing" this player by forcing the mutually inefficient outcome (No bonus, Choose low) thereafter.

Incentive to deviate once is present to both players: User may choose to take the bonus and still choose low level of security; Organization can skip payment hoping User will still choose high level of security. In making such decisions, players will compare two streams of payments from period t thereafter: one with same payments as before, another with a higher "deviation" payment in period t, but lower "inefficient" payments thereafter.

It is conventional to use a model similar to "discounted cash flow". Let g ($0 < g < 1$) be a "time value of money" factor – from perspective of period t, one dollar received in period t+1 is worth \$g, in period t+2 – \$$g^2$, … in period t+x - \$$g^x$, and so on. Now it is possible to analyze which values of g can sustain (Bonus, Choose high) using Nash reversion strategies.

First, consider User. If he doesn't deviate, his payment stream is:

$(b-c) \cdot (1+g+g^2+g^3+\ldots) = (b-c)/(1-g)$

If he deviates (takes the bonus, but doesn't choose High), his payment stream is:

$b + 0 \cdot (g+g^2+g^3+\ldots) = b$

He has no incentive to deviate if $(b-c)/(1-g) > b$, or $g > c/b$. (8)

Thus, as User's cost of implementing high security is close to the amount of bonus, he will not deviate if sustainability of future payments is high.

Now, from Organization's perspective, payments from non-deviation are:

$(z-b) \cdot (1+g+g^2+g^3+\ldots) = (z-b)/(1-g)$

If it chooses to deviate (don't pay the bonus once and thereafter), the payments are:

$$z + (-z) \cdot (g+g^2+g^3+\ldots) = z \cdot (1-2g)/(1-g)$$

Organization will not deviate if $(z-b)/(1-g) > z \cdot (1-2g)/(1-g)$; or $g > b/2z$[‡] (9)

Therefore, as amount of bonus increases compared to Organization's value of additional security, it will not deviate if sustainability of future payments is high.

We have seen that higher level of security can be sustained if both players are sure that future payments can be sustained. This is an interesting implication that is not apparent in the initial problem formulation: *for security to be provided at higher level, parties needs to be assured that their relationship will be continued in the future.* Therefore, building trust is very important. In practical terms, this can be thought of as, for instance, building a sense of job security in employees, so that they have a lesser incentive to expose a company's confidential data.

It is also worth noting that in our setting, deviation for Organization has negative payoffs for any $g>½$. However, deviation might still be a better option for User if amount of bonus payment is close to the cost of opting for higher security. Thus, subjectively, User's incentives to deviation seem to be stronger, and we can expect to see more attempts to breach a contract (of provisioning higher level of security) on the side of User rather than Organization. It seems that User can extort almost any amount of bonus payment from the Organization.

However, there is a limit to the power of User. This result is presented in Theorem 2.

[‡] Technically, from previous inequality, deviation brings negative profit if $g > ½$. However, since $b < z$, this inequality also includes the case $g > ½$.

Theorem 2. **(Characterization of feasible bonus amount)** *Suppose that providing a bonus in the amount of b is feasible. Then, if the choice of reward b is inducing incentive compatibility (voluntary adherence with security policy), it may be characterized as follows:*

Inf (b) = c/g; Sup (b) = 2zg

Proof.

Assumption of incentive compatibility implies that there is no need to deviate from equilibrium outcome for either User or Organization. Thus, conditions (8) and (9) hold. Rearranging those inequalities and combining them, we obtain

$c/g < b < 2zg.$ (10)

Since reaching an exact value at any end of this interval creates an indifference condition for one of the parties involved (and, thus a non-zero probability of deviation), we need to use the upper/lower bound notation for the feasible set of values of b. Still, actual values of b may be infinitely close to the ends of intervals without violating feasibility. ***Q.E.D.***

Corollary. **(Existence of guaranteed discount rate that induces incentive compatibility).** *Suppose that provisioning of bonus is feasible. Then, there exist a lower bound on time value of money factor g that induces mutual incentive compatibility. This critical value of g is* $1/\sqrt{2}$.

Proof.

If provision of bonus is feasible, then double inequality (10) holds. From it, we can write that $c/g < 2zg$, or $g^2 > c/(2z)$. (11)

However, by formulation of the problem, c is smaller than z to induce feasibility. Thus, c/(2z) < ½ . Substituting this result into (11), we conclude that *all* time value of money factors that satisfy the inequality $g^2 \geq ½$ (or, equivalently, $g \geq 1/\sqrt{2}$), automatically induce incentive compatibility. ***Q.E.D.***

Note that there may be *some* values of g^2 below ½ that still induce incentive compatibility, but we are guaranteed to have this result if g is above $1/\sqrt{2}$,which is approximately 0.707 – suggesting a reasonably large range of practically useful values[§]. For example, it is common in financial analysis of net present value of money to use the discount rates in the range of 0.01-0.20 (corresponding to g values of 0.80-0.99 – contained in our interval.

Results of Theorem 2 and its Corollary suggest that despite all uncertainty and threat of opportunistic behavior, there is a practically significant range of potential values of discount factors for which it is possible to build trust relationships between User and Organization and insure the provision of appropriate level of security. Moreover, such cutoff level is independent of a particular configuration of agents' payoffs.

6. Conclusions

We consider the problem of provisioning information security in organizations from a viewpoint of welfare economics. We introduce the notion of access as an important production factor and consider tradeoffs between access and information security. We also model market equilibrium for access and security for agents with different incentives and preferences.

[§] Note, again, that Organization has no incentive to deviate for any g > 0.5. Thus, operating in the range of g > 0.707 assures that both User and Organization have no incentive to deviate.

Production approach to security has not been considered before in the literature. However, this approach allows us to analyze the security/access tradeoff that has been identified as an important factor both by practice and academic literature.

One of the results of our model is that security production function is likely to be concave. From the theoretical perspective, it allows to consider a wide and well-known range of particular functional forms as candidates for producing security. From the practice perspective, it supports the notion that provision of additional security is increasingly hard because of the decreasing returns to scale.

Another interesting result states the relationship between prices of access and security that leads to different states of market equilibrium or disequilibrium. For practice, it means that information security, as other information services in organizations, may be assigned transfer prices, which need to be carefully selected. From theory viewpoint, it provides ground for further analysis of incentives for agents that will lead to socially optimal choices of security rising from individual behavior.

As a first step of exploring such situations, we have developed a game-theoretic model of User-Organization interaction in provisioning security. Two important results derived from this model are i) need to establish a long-term trust relationships to ensure security provisioning, and ii) identification of payoff-independent values of time value of money factors that induce such trust building and incentive compatibility.

References:

[1] L.J. Camp "Marketplace incentives to prevent piracy: an incentive for security?" *Presentation at Workshop on Information Security Economics*, UC-Berkeley, May 2002. CERT Coordination Center. "Overview of Attack Trends", 2000.

[2] E. Galor, A. Ghose. "The Economic Consequences of Sharing Security Information", *Presentation at 2nd Workshop on Information Security Economic,* University of Maryland, May 2003

[3] V. Gurbuxani, C. F. Kemerer. An Agent Theoretic Perspective on the Management of Information Systems. In *Proceedings of the Twenty-Second Annual Hawaii International Conference on System Science*, Kailua-Kona, Hawaii, 1989.

[4] A. MasColell, Winston, Green. "*Microeconomic Theory",* 1995, paperback ed.

[5] H. Ogut, S. Ragunathan, H. Cavusoglu. "Intrusion Detection Policies for IT Security Breaches", *Proceedings of WITS-2003,* Seattle, WA, December 2003, pp. 25-30.

[6] K. Regan. "Is Internet Security Killing E-Business?" *Ecommerce Times,* May 8, 2003.

[7] C. Saran, "FTSE Firms in Security Quest Offer Different Approaches to "Deperimeterization"", *ComputerWeekly.com,* November 18, 2003.

[8] M. Schwartz "Top Three Security Problems Remain Despite Increased Spending", *Enterprise Systems Journal,* February 18, 2004.

[9] H. Varian. "System Reliability and Free Riding"; *Presentation at Workshop on Information Security Economics*, UC-Berkeley, May 2002.

[10] Y. Yemini, A. Dailianas, D. Florissi, G. Huberman. "MarketNet: Market-based Protection of Information Systems*"*, In *Proceedings of ICE'98, First International Conference on Information and Computation Economies*, Oct. 1998, Charleston, SC