

Optimally securing interconnected information systems and assets

Vineet Kumar, Rahul Telang and Tridas Mukhopadhyay
(vineetk, rtelang, tridas @andrew.cmu.edu)
Carnegie Mellon University

Keywords: Mechanism design, Decision rights, Interdependent systems

1 Introduction

Despite information security being a priority issue of many enterprises, the evaluation of investments in information security as well as how to determine firm policies is poorly understood. There are diverging views on whether decision rights for security be placed with the divisions, or with a central group responsible for security. This critically depends on the strategic nature of countermeasures and the type of loss. We develop an analytical model that takes into account the heterogeneous information systems present in a multi-division enterprise, the various threats it faces to its information systems and assets, the kinds of losses these information assets can be targeted for, as well as the types of countermeasure technologies available to protect against different threats. We characterize how losses of confidentiality and availability are different and provide a rigorously derived framework to help firms design optimal mechanisms to deploy both protection and cryptographic countermeasures to combat threats.

Strategically informed analysis of security is crucial in determining how security technologies are deployed in the real world, as our results indicate. We seek to explicitly model the technology and show how this affects strategic interaction between the decision makers. In addition, this work is distinguished from previous work along the following dimensions: (1) Heterogeneity of the information systems of the enterprise's divisions - each division is likely to have different systems and ability to effectively deploy countermeasures (2) Different kinds of losses faced by information assets (availability and confidentiality) (3) Multiple types of countermeasures that are available to decision makers (protection and cryptography).

The motivation for modeling contagious threats ¹ is driven by real-world examples of computer viruses and Internet worms, both of which are dangerous threats to the availability and confidentiality of information assets and enterprises spend a lot of resources protecting against them as detailed by [3]. The model we consider reflects the nature of risk they pose to interconnected systems. A contagious threat source launches \mathbf{T} attacks per time period, which is taken to be a random variable (since we assume risk-neutrality of the decision maker, we can replace it by its mean λ). The threat source is external to the enterprise network, and attacks each division in the enterprise separately. The information systems of the divisions are potentially vulnerable to this (external) attack, with the probability of a successful breach of division j is given by $p_j(s) = v(\alpha_j, s_j)$ depending on the susceptibility (α_j) of the division's systems as well as the level of protection countermeasures deployed by the division (s_j). Suppose that a division's information system gets breached (and consequently infected) by this threat - it turns into a threat source and becomes an internal threat to the network, which is capable of further attacks and breaches leading to losses, with an internal attack leading to a breach with probability η .

¹We do not specifically model attacks by hackers, in general. However, this framework readily extends to hackers who cannot observe the security deployments at the divisions and are not motivated by financial gains

The nature of losses suffered upon a breach depends on the kind of breach that has occurred. Consider a virus attack that takes down a company’s web servers. This represents a loss of availability and can happen multiple times, once via a direct attack and again via another infected division’s systems. Each incidence of breach costs division j $\$l_j$ due to the loss of availability. In addition, most enterprises have confidential data assets that need to be secured, and breach (or unauthorized use) of these data assets causes monetary as well as reputation losses to them. There are several threats like Spyware, Trojan horses, as well as hackers that seek to steal information, and there are countermeasures that protect against these threats to varying degrees. These threats are designed with data theft in mind and cause confidentiality losses. To protect against such losses, firms can use both protection countermeasures (like firewalls) as well as cryptographic countermeasures (like SSL). In order to access an encrypted confidential document one must perform the following operations in sequence: (1) breach the information system and obtain access to the document (2) break the cryptographic security protecting the document to access its contents. The probability of (1) depends on the susceptibility α_j and the level of protection countermeasures (s_j), while the likelihood of (2) depends on the level of cryptographic countermeasures (χ_j). The key aspect of confidentiality losses is that for each attack, if a division ‘ j ’ has been breached via a direct attack and has a loss of L_j , a further breach via an internal attack does *not* lead to an additional loss. This is because the attacker (spyware or worm/trojan horse) has already gained access to the sensitive information via the direct breach. Firms can have leaks of confidential customer data, medical data, documents of strategic importance etc. Campbell and Zhou [2] show that the change in stock market value of a breached company is higher if the breach involved confidential information as compared to a loss of availability.

This paper draws from two streams of research. The first explores investment in countermeasures for interdependent systems, where the security of each entity depends on the decisions of the other entities in the system - as modeled by Kunreuther and Heal [4] and Bier et al[1]. The second stream deals with the allocation of decision rights as well as design of optimal mechanisms. Our modeling of decision structures and mechanisms is similar in spirit to the well known papers by Mendelson [5] and Whang [6] which look at decision structures for information systems, albeit in different contexts. To the best of our knowledge, our paper is the first research effort in information security that has focused on explicitly characterizing the strategic aspects of different threats and types of countermeasures. We make actionable recommendations to managers regarding the allocation of decision rights and implementation of optimal incentive mechanisms to minimize the overall loss faced by the enterprise.

2 Model Components

Susceptibility The susceptibility of a division reflects the characteristics of its information systems as well as the capabilities of its IT staff in configuring and maintaining the system, for example by closing backdoors or timely patching or disabling dangerous programs. Divisions with low susceptibility are less likely to be breached than those that have higher values for this parameter. This essentially captures the heterogeneity in information systems and staff capabilities of different divisions of a large enterprise. For each division j , α_j is a random variable with support $[\underline{\alpha}, \bar{\alpha}]$. The realization of α_j is denoted by α_j and is known to the division manager but not to the CIO. In general, we denote $E[\alpha_j] = \tilde{\alpha}$, $Var[\alpha_j] = \sigma^2$ for $j = 1, 2$ and $cov(\alpha_i, \alpha_j) = \rho\sigma^2$ for $i \neq j$. We denote the marginal distributions of α_j by $\phi_j(\cdot)$ and the joint distribution as $\phi(\cdot, \cdot)$.

Countermeasures These include security software and hardware products that minimize the chances of a successful attack. This can be achieved by mitigating the vulnerability of systems or by reducing the likelihood of a breach of data with cryptographic measures. Each division’s protection and cryptographic countermeasure deployment can be set independently of the other divisions. s_j and χ_j denote the levels of protection and cryptography at division j .

Vulnerability This denotes the probability of a successful breach (given that an attack has occurred) of division j 's information systems, given that its protection countermeasures are of level s_j . The vulnerability to an external attack is given by $p_j = v(\alpha_j, s_j)$. When the attack originates from within the network, the vulnerability is η and this is referred to as *internal vulnerability*. A loss of confidentiality only occurs when the encryption is also breached in addition to the information system breach. The conditional probability of breach of the cryptography given that the information system has been breached is denoted by the function $\psi(\chi_j)$ where χ_j refers to the level of cryptographic countermeasures deployed by division j .²

Loss This represents the monetary loss caused to the firm when it is subject to an attack that successfully exploits a vulnerability in its systems and/or policies. We consider two different kinds of losses to the *information systems and assets* of an enterprise: loss of *availability* (e.g. a DoS attack), and loss of *confidentiality* (e.g. theft of confidential data).

Costs of security countermeasures There are monetary and non-monetary costs of implementing both policy-based and product-based security countermeasures. $C(s, \chi) = c' \cdot s + c'_c \cdot \chi$ denotes the cost³ to a division of deploying protection countermeasures of a level s and cryptographic countermeasures to a level χ .

We consider in table 1 the various events that may occur when the firm is attacked by a threat source. Briefly, we distinguish between losses of availability and confidentiality as well as what divisions are breached via external and internal attacks. A breach of division j via a direct attack is listed as j_D while its breach by internal attack is denoted j_I . A "✓" indicates that the division was breached while a "×" indicates that it was not.

Table 1: Scenarios for availability and confidentiality losses with contagious threats

	probability of event	1_D	2_D	1_I	2_I	Expected loss for each type of loss		
						Availability	Confidentiality	Confidentiality with cryptography
1	$\eta^2 p_1 p_2$	✓	✓	✓	✓	$2l_1 + 2l_2$	$L_1 + L_2$	$\psi(\chi_1)L_1 + \psi(\chi_2)L_2$
2	$p_1 p_2 (1 - \eta)^2$	✓	✓	×	×	$l_1 + l_2$	$L_1 + L_2$	$\psi(\chi_1)L_1 + \psi(\chi_2)L_2$
3	$p_1 p_2 \eta (1 - \eta)$	✓	✓	✓	×	$2l_1 + l_2$	$L_1 + L_2$	$\psi(\chi_1)L_1 + \psi(\chi_2)L_2$
4	$p_1 p_2 \eta (1 - \eta)$	✓	✓	×	✓	$l_1 + 2l_2$	$L_1 + L_2$	$\psi(\chi_1)L_1 + \psi(\chi_2)L_2$
5	$p_1 (1 - p_2) \eta$	✓	×	×	✓	$l_1 + l_2$	$L_1 + L_2$	$\psi(\chi_1)L_1 + \psi(\chi_2)L_2$
6	$p_1 (1 - p_2) (1 - \eta)$	✓	×	×	×	l_1	L_1	$\psi(\chi_1)L_1$
7	$(1 - p_1) p_2 \eta$	×	✓	✓	×	$l_1 + l_2$	$L_1 + L_2$	$\psi(\chi_1)L_1 + \psi(\chi_2)L_2$
8	$(1 - p_1) p_2 (1 - \eta)$	×	✓	×	×	l_2	L_2	$\psi(\chi_2)L_2$
9	$(1 - p_1) (1 - p_2)$	×	×	×	×	0	0	0

The decision problem for the CIO and division managers

For availability losses, the firm's overall loss when the realization of susceptibilities is α_1 and α_2 is given by:

$$Loss_{avail}(\alpha_1, \alpha_2) = v(\alpha_1, s_1)(l_1 + \eta l_2) + v(\alpha_2, s_2)(l_2 + \eta l_1) + c[s_1 + s_2]$$

²This reflects the situation that internal and external traffic are often treated differently in practice by enterprise networks, and information systems are configured to trust internal traffic and not employ filtering mechanisms against it.

³These are generalizable to most convex cost functions, as detailed in the full paper.

Each division manager does not consider the losses of the other division (or its costs), while making his decisions. So, for division 1's objective function we set $l_2 = 0$.

With confidentiality losses, both protection and cryptographic measures can be employed. So, the loss in this case is:

$$\begin{aligned} Loss_{conf}(\alpha_1, \alpha_2) = & (\alpha_1 h(s_1) + \eta \alpha_2 h(s_2) - \eta \alpha_1 h(s_1) \alpha_2 h(s_2)) \psi(\chi_1) L_1 + (\alpha_2 h(s_2) \\ & + \eta \alpha_1 h(s_1) - \eta \alpha_1 h(s_1) \alpha_2 h(s_2)) \psi(\chi_2) L_2 + c [s_1 + s_2] + c_c [\chi_1 + \chi_2] \end{aligned}$$

In all cases, the decision problem for the CIO is to minimize the expected loss by determining the level of investments in protection and cryptographic measures. When the divisions have decision rights, they are engaged in a game of incomplete information. We solve in each case, for the Bayesian Nash equilibrium. We compare the second best with the optimal full information case. Below, we assume that the vulnerability is multiplicatively separable (for confidentiality losses only) or that $v(\alpha, s) = \alpha h(s)$. The level of countermeasures at each division is given by s_j^{CIO} and χ_j^{CIO} when the CIO is the decision maker (with full information) and s_j^{DIV} and χ_j^{DIV} when the division managers are vested with decision rights.

A mechanism design solution

Since the CIO cannot observe the realized susceptibilities, we use mechanism design to design an optimal bayesian direct revelation mechanism for the case of confidentiality losses. This achieves the first best, since within an enterprise, transfers do not have an effect on the overall loss of the firm.

The standard three step process for this is:

1. The CIO offers a set of contracts to each division $(s_j(\hat{\alpha}_j, \hat{\alpha}_k), \chi_j(\hat{\alpha}_j, \hat{\alpha}_k), \tau_j(\hat{\alpha}_j))$ that depends on the reported susceptibility of each of the divisions
2. Each division j sends a report $\hat{\alpha}_j$ of its true susceptibility α_j
3. The CIO observes the reports of all the divisions, and allocates the security countermeasure level for each division and the transfer amounts based on the reports

3 Summary of main results

1. For availability losses, we find that a constant subsidy for each unit will achieve first best levels of deployment - this result is valid for any functional form satisfying the basic regularity condition. the subsidy is increasing with level of internal vulnerability (η) and as $(\eta \rightarrow 1)$, the CIO allocates both divisions the same protection levels even if their losses are very different.
2. For confidentiality losses, the expected loss is decreasing in correlation of susceptibilities (which means that have a standard platform will actually help compared to heterogeneous systems). We illustrate the strategic effects of each countermeasure type and show that protection countermeasures are strategic complements. One might expect that in an interconnected network, if the protection measures at one division are reduced, the other division will in some sense try to make up by increasing its protection. We show that the exact opposite response is optimal - if protection is increased at one division, it is optimal to increase the deployment at the other division. This result holds no matter whether the decision rights are vested with the CIO or the division managers. We also find that subsidies cannot achieve the first best unless the vulnerability function is of an exponentially decreasing form. For this class of vulnerability and identical losses for the divisions, the optimal subsidy for confidentiality losses ranges between 0% and 75% while the corresponding range for availability losses is 0%- 50%, and the subsidy increases with internal vulnerability η .

3. When only cryptographic countermeasures are used, there is no goal divergence between the divisions and the CIO and their goals are aligned with the CIO. However the CIO must enable communication between the divisions so that each division knows the other's susceptibility in order to implement the first best level of cryptographic countermeasures.
4. When both protection and cryptographic countermeasures can be used and the divisions are vested with decision rights, in general they invest less in protection but more in cryptographic countermeasures when compared with the case where the CIO with complete information makes the decision. Therefore, in the presence of multiple types of countermeasures, over-deployment of (cryptographic) countermeasures by the divisions occurs - we detail the underlying strategic interactions that cause this. Such a result has not been shown in prior work because multiple types of countermeasures have not been modeled in information systems.
5. We also derive the optimal bayesian mechanism that will result in the divisions deploying the first best levels of both protection and cryptographic security measures in the case of confidentiality losses.

4 Limitations and Future research

Our paper has examined how an enterprise should optimally secure itself against contagious threats. Further research efforts could consider explicitly the motivations of strategic attackers and various methods of deterrence and protection. Also, modeling losses of integrity would be a valuable contribution to this area of research. Another useful extension or possibly a separate research effort would be to look at the effect of minimum security standards.

The reader is invited to read the complete version of this paper with all propositions and proofs. It is available from:

<http://www.andrew.cmu.edu/user/vineetk/wise2006-fullpaper.pdf>

References

- [1] V. Bier, A. Nagaraj, and V. Abhichandani. Protection of simple series and parallel systems with components of different values. *Reliability Engineering and Systems Safety*, 10(27), 2004.
- [2] K. Campbell and L. Zhou. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, 11:431–448, 2003.
- [3] Lawrence A. Gordon, Martin P. Loeb, and William Lucyshyn. 2005 csi/fbi computer crime and security survey, 2005.
- [4] Howard Kunreuther and Geoffrey Heal. Interdependent security. *Journal of Risk and Uncertainty*, 26(2):231–49, 2003.
- [5] Haim Mendelson. Pricing computer services: queueing effects. *Commun. ACM*, 28(3):312–321, 1985.
- [6] S. Whang. Alternative mechanisms of allocating computer resources under queueing delays. *Information Systems Research*, 1(1):71–88, 1990.