On the Gordon&Loeb Model for Information Security Investment

Jan Willemson[*†‡]

Abstract

In this paper we discuss a simple and general model for evaluating optimal investment level in information security proposed by Gordon and Loeb [5]. The authors leave an open question, whether there exists some universal upper limit for the level of optimal security investments compared to the total cost of the protected information set. They also conjecture that if such a level exists, it could be $\frac{1}{e} \approx 36,8\%$. In this paper, we disprove this conjecture by constructing an example where the required investment level of up to 50% can be necessary. By relaxing the original requirements of Gordon and Loeb just a little bit, we are also able to show that within their general framework examples achieving levels arbitrarily close to 100% exist.

1 Introduction

Even though information security problems are as old as information exchange, the decisions about the respective defense measures are mostly still taken based on heuristics and experience. There is a definite lack of general, reliable and rigorous models one could use in order to make such decisions.

Several models are proposed that view spending on information security as an investment and try to model the result using some existing framework. For example, Bier and Abhichandani discuss in [2, 1] the pros and cons of game theory vs reliability theory frameworks and use game-theoretic models to analyse the security of systems consisting of parallel components. Kunreuther and Heal note that if attackers and defenders are considered

[*]Cybernetica Ltd, Aleksandri 8a, Tartu, Estonia

[†]Institute of Computer Science, University of Tartu, Liivi str 2, Tartu, Estonia, `jan@ut.ee`

[‡]This research is supported by Estonian Science Foundation grant #6096

as players of a game, their decisions are actually interdependent. They develop a respective general model for several classes of problem settings in [9] and use it to deal with the case of identical agents in [8]. Kannan and Telang build economical models to compare community-based vulnerability disclosure and CERT-based vulnerability disclosure mechanisms in [7]. In [4], Danezis and Anderson study and compare censorship resistance architectures in environments like peer-to-peer networks.

However, all of these models are quite application area specific and mostly also rather complicated. In 2002, Gordon and Loeb proposed a simple and very general model for evaluating vulnerability decrease as a result of increased investments [5]. They consider two concrete function families that represent possible decrease scenarios and come to the conclusion that for both of them, the optimal level of investments does not exceed $\frac{1}{e} \approx 36,8\%$ of the total value of the informational assets. They leave an open question whether this constant is universal among all the functions that satisfy certain constraints, or may larger investments be necessary.

The first counterexamples breaking the $\frac{1}{e}$ barrier were given by Hausken [6]. However, Hausken's results deviate considerably from the original model of Gordon&Loeb by replacing the requirement of convex vulnerability decrease with concave logistic decrease and other decrease functions, dropping the conditions concerning continuity of the first and second derivatives, etc.

In this paper, we will demonstrate that following strictly Gordon&Loeb framework, there exist vulnerability decrease functions that require investments up to 50% of the asset value. We will also show that scenarios requiring investments up to 100% can be constructed if we drop just the requirement of continuity of the second derivative of the vulnerability decrease function.

The paper is organised as follows. First, Section 2 presents an outline of Gordon&Loeb model. Next in Section 3 we introduce a slightly modified model that achieves the required investment level of 50%. Then, in Section 4 we show how to go back to the original Gordon&Loeb framework without decreasing the investment level. We also point out an unnecessary condition of Gordon&Loeb, which, when relaxed, leads to required investments up to 100%. Finally, Section 5 draws some conclusions and sets directions for future work.

2 The Model of Gordon and Loeb

In order to estimate the optimal level of information security investment for protecting some information set, Gordon and Loeb consider several parameters of the set in [5], and we will accept similar, though a bit more formal notation.

First, let L denote the *potential loss* associated with the threat[1] against the information set, i.e. $L = t\lambda$, where t is the probability of the threat occurring and λ is the (monetary) loss suffered. Further, let v denote *vulnerability,* i.e. the success probability of the attack once launched; vL is then the total *expected loss* associated with the threat against the information set.

If a company invests z dollars into security, the remaining vulnerability (called *security breach probability* in [5]) will be denoted by $S(z, v)$. The expected benefit from the investment can then be computed as $(v - S(z, v))L$ and the expected net benefit as $(v - S(z, v))L - z$. Under suitable differentiability assumptions (see the condition **A3** below), we can see that the optimal level of investment can be found by computing the local optimum z^* of the expected net benefit, i.e. by solving the first order equation

$$\frac{\partial}{\partial z}[(v - S(z, v))L - z] = 0$$

and obtaining the following condition for $z^* = z^*(v)$:

$$-\frac{\partial}{\partial z}S(z^*, v)L = 1. \tag{1}$$

Of course, the remaining vulnerability function can not be arbitrary. Clearly, since $S(z, v)$ is a probability, we must have $0 \leq S(z, v) \leq 1$. Its first argument is an investment and the second one another probability, so $0 \leq z$ and $0 \leq v \leq 1$. Besides that, the following restrictions are defined in [5]:

A1 $\forall z\, S(z, 0) = 0$, i.e. if initially the attack success probability is 0, it stays so after every possible investment.

A2 $\forall v\, S(0, v) = v$, i.e. if we invest no money, there will be no change in the attack success probability.

[1] Following the ideology of Gordon and Loeb, we consider here the simplified scenario of a single threat and leave considering the (more realistic) case of several (interdependent) threats for future studies. A natural framework for such a study would be using the threat tree approach proposed by Schneier [10] in the fashion similar to the analysis done by Buldas and Saarepera in [3].

A3 The function $S(z,v)$ is continuously twice differentiable and for $0 < v$

$$\frac{\partial}{\partial z} S(z,v) < 0 \quad \text{and} \quad \frac{\partial^2}{\partial z^2} S(z,v) > 0.$$

Additionally,

$$\forall v \lim_{z \to \infty} S(z,v) = 0.$$

The condition **A3** is postulating that with increasing investments it is possible to decrease the vulnerability level, but at a decreasing rate. Nevertheless, investing larger and larger amounts it is possible to make the attack probability arbitrarily small.

In their paper, Gordon and Loeb give two examples of function families that satisfy the conditions **A1**-**A3**, namely

$$S^I = \frac{v}{(\alpha z + 1)^\beta},\ (\alpha > 0, \beta \in \mathbb{R}) \quad \text{and} \quad S^{II} = v^{\alpha z + 1},\ (\alpha > 0).$$

Applying the first order condition (1) we can find the optimal level of investments, $z^{I*}(v)$ and $z^{II*}(v)$, respectively. Next, it is a natural idea to compare the optimal investment level to the total expected loss vL. It is proved in [5] that $z^*(v) < vL$ for all functions $S(z,v)$ satisfying the conditions **A1**-**A3**, and even more interestingly, that $z^{I*}(v) < \frac{1}{e} vL$ and $z^{II*}(v) < \frac{1}{e} vL$.[2]

It is left as an open problem in [5] whether the constant $\frac{1}{e}$ is universal for all possible functions $S(z,v)$ meeting the conditions **A1**-**A3**. If it were so, it would mean that we have the first formal evidence that in order to defend some property (say, information), it is always *optimal* to spend considerably less than the value of the property is.

On the other hand, it is in principle also possible that the above functions are just two concrete examples achieving the same constant by coincidence. Can it happen that there exist other functions $S(z,v)$ such that the corresponding optimal investment level $z^*(v)$ can be larger than $\frac{1}{e} vL$? The aim of the next sections is to show that the latter is actually the case and that there exist functions $S(z,v)$ such that the corresponding optimal investment level $z^*(v)$ can be arbitrarily close to $\frac{1}{2}$ of the total expected loss vL.

In order to give a concrete example of a suitable family of functions, we first extend the model of Gordon and Loeb a little bit in Section 3. Later in Section 4 we argue that we can also construct a similar example within the

[2] There are actually more classes of functions not mentioned in [5] but giving the same asymptotic bound $\frac{1}{e} vL$, for example $S(z,v) = v\alpha^z$ $(1 > \alpha > 0)$. The proof of the respective bound is similar to the one given in [5].

original model. Finally we will see that relaxing the condition **A3** a little bit more we can achieve that the optimal investment level $z^*(v)$ becomes arbitrarily close to the total expected loss vL.

3 A modified Model

Note that the inequality $\frac{\partial}{\partial z}S(z,v) < 0$ from the condition **A3** implies, that unless originally we had $v = 0$, it is impossible to decrease the attack probability to exactly 0, no matter how large amounts of money we invest.[3] Whereas this may be a good approximation of some real world threat situations, there definitely exist threats that can completely be removed investing enough into improving security measures.[4] Thus we propose extending the condition **A3** to the following form.

A3' The function $S(z,v)$ is continuously twice differentiable and

$$\frac{\partial}{\partial z}S(z,v) \leq 0 \quad \text{and} \quad \frac{\partial^2}{\partial z^2}S(z,v) \geq 0.$$

Additionally,

$$\forall v \lim_{z\to\infty} S(z,v) = 0.$$

Essentially, besides the functions allowed by the condition **A3**, we also allow the functions (viewed as functions of the variable z) that strictly decrease to 0 and then stay 0.

The class of functions that we will next construct will be exactly of this nature. We will introduce a parameter b that represents the maximal amount of investment that is required to completely secure our information set, i.e. $S(z,v) = 0$ if $z \geq b$. For $0 \leq z < b$ we have to find a suitable function so that the conditions **A1**, **A2** and **A3'** would be satisfied. We claim that the following family of functions

$$S^{III}(z,v) = \begin{cases} v(1-\frac{z}{b})^k, & \text{if } 0 \leq z < b \\ 0, & \text{if } z \geq b \end{cases} \quad (b > 0, k > 2) \tag{2}$$

satisfies all the required properties.

---

[3]To see this formally, assume to the contrary that for some values $v_0 > 0$ and z_0 we would have $S(z_0, v_0) = 0$. Since $\frac{\partial}{\partial z}S(z,v) < 0$, we would have $S(z, v_0) < 0$ for all $z > z_0$, which is clearly impossible as $S(z, v_0)$ is a probability.

[4]For example, if the threat is a possible attack from a specific person, it is possible to get rid of this person by paying to a hit man and having this person killed.

Proposition 1 *The functions $S^{III}(z,v)$ satisfy the conditions **A1**, **A2** and **A3'**.*

Proof. The conditions of **A1** and **A2** are straightforward to verify. For the condition **A3'** we compute

$$\frac{\partial}{\partial z}S^{III}(z,v) = \begin{cases} -\frac{kv}{b}(1-\frac{z}{b})^{k-1}, & \text{if } 0 \le z < b \\ 0, & \text{if } z \ge b \end{cases}$$

and

$$\frac{\partial^2}{\partial z^2}S^{III}(z,v) = \begin{cases} \frac{k(k-1)v}{b^2}(1-\frac{z}{b})^{k-2}, & \text{if } 0 \le z < b \\ 0, & \text{if } z \ge b \end{cases} .$$

Now, clearly $\frac{\partial}{\partial z}S(z,v) \le 0$ and $\frac{\partial^2}{\partial z^2}S(z,v) \ge 0$. Besides this we need continuity of the function itself, its first and second derivatives. The only position where these functions can in principle be non-continuous is $z = b$. But we see that they are continuous since

$$\lim_{z\to b-} S^{III}(z,v) = 0, \ \lim_{z\to b-} \frac{\partial}{\partial z}S^{III}(z,v) = 0 \ \text{ and } \lim_{z\to b-} \frac{\partial^2}{\partial z^2}S^{III}(z,v) = 0$$

(the latter equality holding due to $k > 2$ and the second one due to implied $k > 1$). The only remaining condition

$$\forall v \ \lim_{z\to\infty} S^{III}(z,v) = 0$$

holds trivially and this concludes the proof. ■

Now we are ready to state and prove the main result.

Proposition 2 *Suppose that the remaining security breach probability can be represented in the form of function $S^{III}(z,v)$ given by (2). Then $z^*(v) < \frac{1}{2}vL$. Further, the amount of required investment $z^*(v)$ can be arbitrarily close to $\frac{1}{2}vL$.*

Proof. We first solve the equation (1) under the restriction $z < b$ (since investments exceeding the level b give perfect security anyway). We rewrite the equation (1) as follows.

$$\begin{aligned} -\frac{\partial}{\partial z}S^{III}(z^*,v)L &= 1 \\ \frac{kv}{b}\left(1-\frac{z^*}{b}\right)^{k-1} L &= 1 \end{aligned}$$

$$\begin{aligned}\left(1-\frac{z^*}{b}\right)^{k-1} &= \frac{b}{kvL} \\ z^* = z^*(v) &= b\left(1-\left(\frac{b}{kvL}\right)^{\frac{1}{k-1}}\right)\end{aligned}$$

Next we will find the maximum for the function $\frac{z^*(v)}{vL}$ and prove that it approaches $\frac{1}{2}$ from below. Denoting $x = \frac{b}{vL}$ we must analyse the function

$$\frac{z^*(v)}{vL} = \frac{b}{vL}\left(1-\left(\frac{b}{kvL}\right)^{\frac{1}{k-1}}\right) = x\left(1-\left(\frac{x}{k}\right)^{\frac{1}{k-1}}\right). \tag{3}$$

We compute the first derivative

$$\frac{d}{dx}\left[x\left(1-\left(\frac{x}{k}\right)^{\frac{1}{k-1}}\right)\right] = 1-\frac{k}{k-1}\left(\frac{x}{k}\right)^{\frac{1}{k-1}}$$

and use it to find the extremum point of the function (3):

$$\begin{aligned}1-\frac{k}{k-1}\left(\frac{x_0}{k}\right)^{\frac{1}{k-1}} &= 0, \\ x_0 &= k\left(\frac{k-1}{k}\right)^{k-1}.\end{aligned}$$

One may verify that the value of the second derivative at the point x_0 is $-\frac{k^{k-2}}{(k-1)^k}$. This quantity is strictly negative for $k > 1$, so we have x_0 as a maximum point. Substituting its value to the expression (3) we get

$$k\left(\frac{k-1}{k}\right)^{k-1}\left(1-\left(\left(\frac{k-1}{k}\right)^{k-1}\right)^{\frac{1}{k-1}}\right) = \left(\frac{k-1}{k}\right)^{k-1}.$$

This expression is known to decrease as a function of k approaching the value $\frac{1}{e}$ from *above*.

Since the family $S^{III}(z,v)$ of the remaining vulnerability functions was defined for $k > 2$, we have

$$\left(\frac{k-1}{k}\right)^{k-1} < \left(\frac{2-1}{2}\right)^{2-1} = \frac{1}{2}$$

and we can approach this value as $k \to 2$. This concludes the proof. ■

4 Discussion

4.1 Satisfying the Condition A3

The family $S^{III}(z,v)$ of the remaining vulnerability functions does not satisfy the condition **A3** of Gordon and Loeb. In this section we first modify the family $S^{III}(z,v)$ a little bit so that the original condition **A3** is also met, but the Proposition 2 still holds. This way we will have constructed a full counterexample to the conjecture about the universality of the constant $\frac{1}{e}$ made in [5]. We will not give an explicit analytical construction, but rather explain a possible construction method.

Consider the graph of one concrete function from the family $S^{III}(z,v)$ with $b = 1$ and $k = 3$ (see Figure 1). We see from the Figure and from (2) that if $z < b$ and $v > 0$ then $S^{III}(z,v) > 0$. From (2) it is also straightforward to verify that under the same restrictions on z and v we get $\frac{\partial}{\partial z}S^{III}(z,v) < 0$ and $\frac{\partial^2}{\partial z^2}S^{III}(z,v) > 0$.

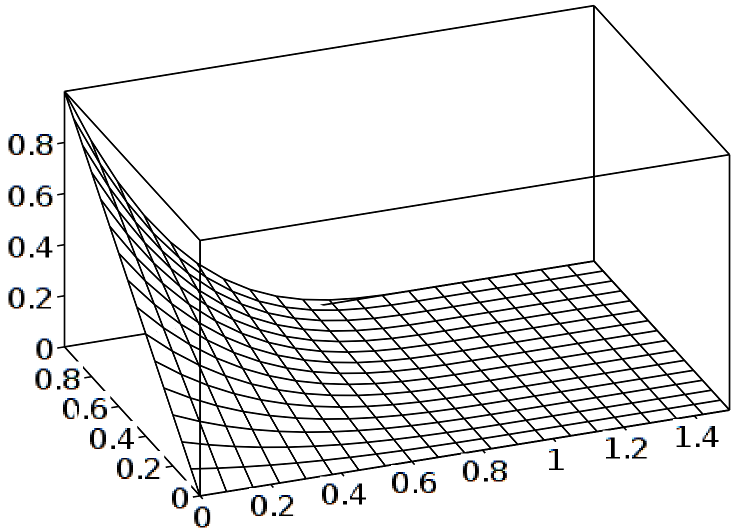

Figure 1: The graph of the function $S^{III}(z,v)$ with $b = 1$ and $k = 3$; $z \in [0, 1.5]$, $v \in [0, 1]$

To construct a new function we will first fix a number $b' \in (0, b)$ and define $S^{IV}(z, v)$ such that $S^{IV}(z, v) = S^{III}(z, v)$ for $z \leq b'$. Next consider the values $S^{III}(b', v)$, $\frac{\partial}{\partial z} S^{III}(b', v)$ and $\frac{\partial^2}{\partial z^2} S^{III}(b', v)$ (remember that they are strictly positive, negative and positive, respectively). It remains to choose the continuation of $S^{IV}(z, v)$ for $z > b'$ so that it would retain continuity and strict inequalities for the function and its first and second derivatives, and additionally would converge to 0 as $z \to \infty$. It is clear that such functions exist, and we will not give an explicit analytical example here.

It remains to understand why the result of Proposition 2 still holds for the functions of the form $S^{IV}(z, v)$. Going back to the proof of the Proposition 2 we see that the maximum is achieved when $z = \left(\frac{k-1}{k}\right)^{k-1} vL$ and $\frac{b}{vL} = k\left(\frac{k-1}{k}\right)^{k-1}$, which imply $z = \frac{b}{k}$. Since $k > 1$, we can retain the optimum of $S^{III}(z, v)$ for the function $S^{IV}(z, v)$ by choosing the cutting point b' to be within the range $\left(\frac{b}{k}, b\right)$.

4.2 Extending the Model

Going back to the proofs of Propositions 1 and 2, we see that the restriction $k > 2$ was actually needed only for continuity of the second derivative of the function family $S^{III}(z, v)$. On the other hand this restriction limited the value of $\frac{z^*(v)}{vL}$ to be upper bounded by $\frac{1}{2}$.

Is continuity of the second derivative of the remaining vulnerability function really essential in the model of Gordon and Loeb? When stating the condition **A3** in [5], the authors say: "This is, as the investment in security increases, the information is made more secure, but at a decreasing rate." This principle translates to the inequalities in the condition **A3**. The continuity of the first derivative is required for the existence of the second derivative, but there is actually no reason for the latter to be continuous.

Thus we may state the extended condition **A3"** as follows:

A3" The function $S(z, v)$ is twice differentiable and for $0 < v$

$$\frac{\partial}{\partial z} S(z, v) < 0 \quad \text{and} \quad \frac{\partial^2}{\partial z^2} S(z, v) > 0.$$

Additionally,

$$\forall v \lim_{z \to \infty} S(z, v) = 0.$$

Similar to the Section 3 we can relax the strict inequalities and then prove that the family of functions

$$S^V(z, v) = \begin{cases} v(1 - \frac{z}{b})^k, & \text{if } 0 \leq z < b \\ 0, & \text{if } z \geq b \end{cases} \quad (b > 0, k > 1)$$

satisfies the resulting requirements. Exactly as in Proposition 2 we can now show that the constant c in the inequality $z^*(v) < cvL$ is upper bounded by the value $\left(\frac{k-1}{k}\right)^{k-1}$, but since now we can let $k \to 1$, we get $\left(\frac{k-1}{k}\right)^{k-1} \to 1$ as well, which means that for the remaining vulnerability functions from the family $S^V(z, v)$ it may be necessary to spend almost the information set's value for its protection. Using the technique presented in Subsection 4.1, functions with the same property and satisfying **A3"** can be constructed.

5 Conclusions and Further Work

In this paper we reviewed a recent model proposed by Gordon and Loeb allowing one to evaluate the potential vulnerability decrease as a result of investments into information security. Even though it is clear that the amount of investments can not exceed 100% of the value of the assets, the first study of the model suggested that there might actually exist some lower optimal level. In this paper we showed that the candidate level of $\frac{1}{e} \approx 36,8\%$ conjectured by Gordon and Loeb is not correct in their model, and that by dropping one minor and a bit too strict requirement we can achieve concrete examples of vulnerability decrease functions approximating the level of 100%.

This does not mean that Gordon and Loeb model is unusable. In fact, it is very a general and simple one and therefore deserves deeper studies. This generality is also its weak point – the form of the underlying vulnerability decrease function is left open, thus in order to obtain any real results some concrete function must be plugged in. In [5], Gordon and Loeb considered two specific function families, but actually there is no reason to assume that any function in any of these families corresponds to any real vulnerability decrease scenario. Thus, the main direction in the further work is to look for functions reflecting changes in vulnerability for some real situations. Clearly, such functions are strongly application area specific.

There are also possibilities to extend the model in other directions. For example, currently it only considers the drop in vulnerability as a result of investment. However, there are other effects of security investments, e.g. increase in the price of attack for the attacker. It is not immediately clear, how the investment (i.e. the defender's money) can be converted to the cost of attack (i.e. attacker's money), and this study will be the topic for future research as well.

6 Acknowledgments

The author would like to thank professor Ahto Buldas for proof-reading the paper.

References

[1] Vicky M. Bier. Should the model for security be game theory rather than reliability theory. In *Communications of the Fourth International Conference on Mathematical Methods in Reliability: Methodology and Practice*, Santa Fe, New Mexico, June 2004.

[2] Vicky M. Bier and Vinod Abhichandani. Optimal allocation of resources for defense of simple series and parallel systems from determined adversaries. In Eugene Z. Stakhiv Yakov Y. Haimes, David A. Moser, editor, *Risk-Based Decisionmaking in Water Resources X*, pages 59–76. American Society of Civil Engineers, 2003.

[3] Ahto Buldas and Märt Saarepera. Electronic signature system with small number of private keys. In *2nd Annual PKI Research Workshop*, pages 96–108, NIST Gaithersburg MD, USA, April 2003.

[4] George Danezis and Ross Anderson. The economics of censorship resistance. In *The Third Annual Workshop on Economics and Information Security (WEIS04)*, 2004.

[5] Lawrence A. Gordon and Martin P. Loeb. The economics of information security investment. *ACM Transactions on Information and System Security*, 5:438–457, November 2002. Reprinted in *Economics of Information Security*, 2004, Springer, Camp and Lewis, eds.

[6] Kjell Hausken. Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability. *Information Systems Frontiers*, 5(8), 2006. To appear.

[7] Karthik Kannan and Rahul Telang. An economic analysis of market for software vulnerabilities. In *The Third Annual Workshop on Economics and Information Security (WEIS04)*, 2004.

[8] Howard Kunreuther and Geoffrey Heal. Interdependent security: The case of identical agents. NBER Working Paper No. W8871. Available at SSRN: `http://ssrn.com/abstract=306405`, April 2002.

[9] Howard Kunreuther and Geoffrey Heal. Interdependent security. *Journal of Risk and Uncertainity*, 26(2–3):231–249, 2003.

[10] Bruce Schneier. Attack trees. In *Dr. Dobb's Journal*, December 1999.