On Gordon & Loeb Model for Information Security Investments

Jan Willemson, Cybernetica, Tartu University, Estonia

Voore Theory Days
01.10.2006

Outline

Background

- Even though information exchange is an old concept, the defence decisions are still taken based on heuristics
- Security managers have hard times justifying the necessity of investments to the company boards
- We urgently need some models that would
  - help us analyzing cost efficiency of security investments, and
  - be general enough to be applied in various settings

Previous Work

- Bier and Abhichandani 2003, 2004 – game theory vs reliability theory frameworks
- Kunreuther and Heal 2002, 2003 – interdependent decisions taken by attackers and defenders
- Kannan and Telang 2004 – models to compare community-based vulnerability disclosure and CERT-based vulnerability disclosure mechanisms
- Danezis and Anderson 2004 – study and compare censorship resistance architectures in environments like peer-to-peer networks
- ...

However, these approaches are mostly application area specific

The Model of Gordon & Loeb: Notations

We will consider *information set* threatened by a single vulnerability. We will adopt the following notation introduced by Gordon & Loeb in 2002:

- Let λ be the (monetary) loss suffered when the threat has materialized
- Let t be the probability of the threat occurring
- Let $L = t\lambda$ be the *potential loss* associated with the threat
- Let v denote the *vulnerability*, i.e. success probability of the attack once launched; vL is then the *total expected loss* associated with the threat against the information set
- Let the amount invested into security be z
- Then the remaining vulnerability (called *security breach probability* by G&L) will be denoted by $S(z, v)$

Optimal Level of Investment

Expected benefit from the investment

$(v - S(z, v))L$

Expected net benefit from the investment

$(v - S(z, v))L - z$

Optimal level of investment

is the local optimum $z^*$of the expected net benefit, i.e. solution of the first order equation

$$\frac{\partial}{\partial z}[(v - S(z, v))L - z] = 0 \quad \text{i.e.} \quad -\frac{\partial}{\partial z}S(z^*, v)L = 1$$

Optimal Level of Investment

Expected benefit from the investment

$(v - S(z, v))L$

Expected net benefit from the investment

$(v - S(z, v))L - z$

Optimal level of investment

is the local optimum $z^*$of the expected net benefit, i.e. solution of the first order equation

$$\frac{\partial}{\partial z}[(v - S(z, v))L - z] = 0 \quad \text{i.e.} \quad -\frac{\partial}{\partial z}S(z^*, v)L = 1$$

Optimal Level of Investment

Expected benefit from the investment

$(v - S(z, v))L$

Expected net benefit from the investment

$(v - S(z, v))L - z$

Optimal level of investment

is the local optimum $z^*$of the expected net benefit, i.e. solution of the first order equation

$$\frac{\partial}{\partial z}[(v - S(z, v))L - z] = 0 \quad \text{i.e.} \quad -\frac{\partial}{\partial z}S(z^*, v)L = 1$$

Conditions on $S(z, v)$

- Clearly, one has $0 \leq S(z, v) \leq 1$, $0 \leq z$ and $0 \leq v \leq 1$
- Besides that, G&L define the following restrictions ("axioms")

  A1 $\forall z \, S(z, 0) = 0$

  A2 $\forall v \, S(0, v) = v$

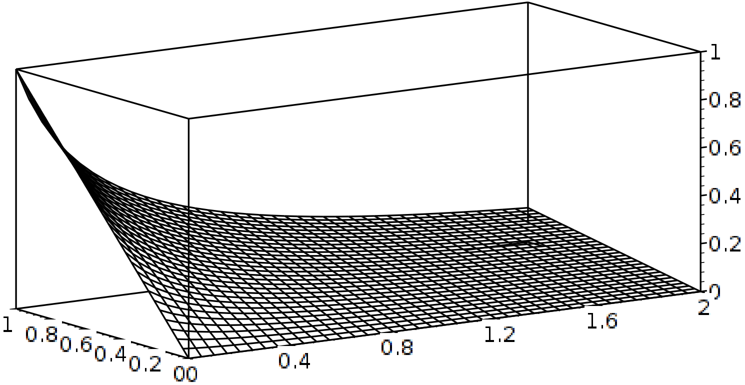
  A3 The function $S(z, v)$ is continuously twice differentiable and for $0 < v$

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

  Additionally,

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

How it Looks Like



Some Examples

Examples

Two functions given by G&L satisfying all the conditions:

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

Assessing the solution

When the optimal level of investment $z^*(v)$ has been found, it is then natural to compare it to the total expected loss vL.

Theorem

$z^{I*}(v) < \frac{1}{e} vL$ and $z^{II*}(v) < \frac{1}{e} vL$.

Some Examples

Examples

Two functions given by G&L satisfying all the conditions:

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

Assessing the solution

When the optimal level of investment $z^*(v)$ has been found, it is then natural to compare it to the total expected loss vL.

Theorem

$z^{I*}(v) < \frac{1}{e} vL$ and $z^{II*}(v) < \frac{1}{e} vL$.

Some Examples

Examples

Two functions given by G&L satisfying all the conditions:

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

Assessing the solution

When the optimal level of investment $z^*(v)$ has been found, it is then natural to compare it to the total expected loss vL.

Theorem

$z^{I*}(v) < \frac{1}{e} vL$ and $z^{II*}(v) < \frac{1}{e} vL$.

Gordon & Loeb Conjecture

The Conjecture

Is it the case that for every $S(z, v)$ we have

$$z^*(v) < \frac{1}{e} vL?$$

Implications

If so, we have a formal proof that it is always optimal to spend less than $\frac{1}{e} \approx 36,8\%$ of the expected loss for protection

Our contribution

We show that this is *not* the case and that it is possible to achieve investment levels of up to 50% staying strictly in the G&L model; and up to 100% by relaxing one minor requirement

Gordon & Loeb Conjecture

The Conjecture

Is it the case that for every $S(z, v)$ we have

$$z^*(v) < \frac{1}{e} vL?$$

Implications

If so, we have a formal proof that it is always optimal to spend less than $\frac{1}{e} \approx 36,8\%$ of the expected loss for protection

Our contribution

We show that this is *not* the case and that it is possible to achieve investment levels of up to 50% staying strictly in the G&L model; and up to 100% by relaxing one minor requirement

Gordon & Loeb Conjecture

The Conjecture

Is it the case that for every $S(z, v)$ we have

$$z^*(v) < \frac{1}{e} vL?$$

Implications

If so, we have a formal proof that it is always optimal to spend less than $\frac{1}{e} \approx 36,8\%$ of the expected loss for protection

Our contribution

We show that this is *not* the case and that it is possible to achieve investment levels of up to 50% staying strictly in the G&L model; and up to 100% by relaxing one minor requirement

Relaxing the G&L Model

- The condition $\frac{\partial}{\partial z} S(z, v) < 0$ implies, that it is impossible to decrease the remaining vulnerability to exactly 0, no matter how large amounts of money we invest
- We will relax the G&L model and allow $S(z, v)$ to become and stay 0, i.e. we will consider the axiom

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,

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

Counterexample in the Modified Model

Example

We define the following family of functions:

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

Theorem

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

Theorem

If the remaining security breach probability belongs to the family $S^{III}(z,v)$, then $z^*(v) < \frac{1}{2}vL$. Further, the optimal investment $z^*(v)$ can be arbitrarily close to $\frac{1}{2}vL$.

Counterexample in the Modified Model

Example

We define the following family of functions:

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

Theorem

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

Theorem

If the remaining security breach probability belongs to the family $S^{III}(z,v)$, then $z^*(v) < \frac{1}{2}vL$. Further, the optimal investment $z^*(v)$ can be arbitrarily close to $\frac{1}{2}vL$.

Counterexample in the Modified Model

Example

We define the following family of functions:

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

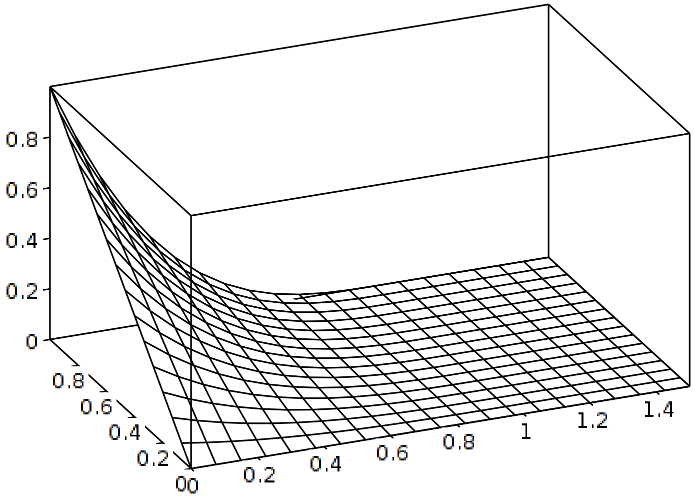
Theorem

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

Theorem

If the remaining security breach probability belongs to the family $S^{III}(z,v)$, then $z^*(v) < \frac{1}{2}vL$. Further, the optimal investment $z^*(v)$ can be arbitrarily close to $\frac{1}{2}vL$.

The Function $S^{III}(z, v)$ for $b = 1$ and $k = 3$



The Family $S^{IV}(z, v)$

To construct a new function family we:

- 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)
- 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

Satisfying the Condition A3

Theorem

*One can choose the parameter $b' < b$ so that the resulting family $S^{IV}(z, v)$ satisfies the conditions **A1**, **A2** and **A3**. Further, the optimal investment $z^*(v)$ for this family can be arbitrarily close to $\frac{1}{2}vL$.*

Extending the Model

- We can see from the proofs that the requirement $k > 2$ was only needed to ensure continuity of the second derivative of $S(z, v)$, which is a somewhat overexaggerated condition. Thus we state a modified axiom.

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,

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

Counterexample Achieving 100% Investment Level

Example

Consider the family

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

- First we relax the condition **A3”** to allow $S(z,v)$ to become 0 again
- Next we prove that the optimal investment $z^*(v)$ for the relaxed family can be arbitrarily close to vL.
- Finally, we go back to the original condition **A3”** using the same trick as for **A3’**→**A3.**

Conclusions

- The conjecture made by Gordon & Loeb concerning the maximal level of investments into (information) security of being less than $\frac{1}{e} \approx 36,8\%$ has been disproved
- However, the counterexamples assume specific forms for the remaining vulnerability $S(z, v)$
- For other function families results may be more promising
- ... or less promising; i.e. Hausken has recently studied *logistic decrease* of the vulnerability and showed that within this model investments of up to 100% may be needed as well
- Still, the Grand Challenge is to determine the exact form of $S(z, v)$ for a given problem setting

Thank You!

Questions?

Logistic Decrease Function