

# Attacker-Defender Investment Strategies in Cybersecurity

## 1. Motivation

Malicious cyber activity cost the US economy between \$57 and \$109 billion in 2016. Consequently, there has been considerable investments and research on cybersecurity, especially in technical defenses (encryption, intrusion detection, etc.). Yet there remains a significant need to better understand how firms should allocate these investments.

Our contributions are *two-fold*:

- Generalize from a one-shot optimal investment allocation for cyber defense to an iterative framework between attackers and defenders.
- Extend existing models<sup>1,2</sup> of optimal investments to protection of multiple assets in more realistic network structures..

## 2. Gordon & Loeb Model

- Defines a *security breach probability function*,  $S(z, v)$ , indicating how investments in information security,  $z$ , can decrease the vulnerability of the information,  $v$ .
- Optimal investments depend on the information's **value**.

$$z^* = \arg \min_{z \geq 0} L \cdot S(z, v) + z \quad (1)$$

- Shows that optimal investments may not always increase with increasing vulnerability.
- Provides guidelines for firms investing in information security to avoid paying more than ~37% of the information's expected loss.

## 3. Generalization to Networks

How might we extend the Gordon & Loeb model to account for multiple vulnerabilities and assets?

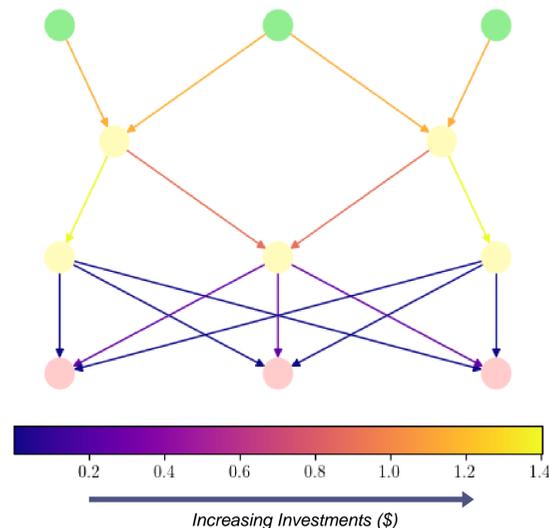
- *Represent network as a directed acyclic graph defining entry, intermediate, and leaf nodes.*

Let  $\mathcal{R}$  be the set of all paths from entry node to leaf, and  $\mathcal{E}$  be the set of all edges in the graph. For  $r \in \mathcal{R}$  and  $e \in \mathcal{E}$ :

- $L^{(r)}$  is the loss associated with the leaf node in path  $r$ .
- $S^{(r)}(z, v)$  defines how investments along path  $r$  decrease its vulnerability.
- $p_e$  is the probability of taking edge  $e$  at a node.

$$\begin{aligned} \min_{\mathbf{z}} \quad & u \\ \text{subject to} \quad & L^{(r)} \cdot S^{(r)}(\mathbf{z}, \mathbf{v}) \leq u \quad r \in \mathcal{R} \end{aligned}$$

$$\mathbf{1} \cdot \mathbf{z} = I_{MAX} \quad \mathbf{z} \succeq 0 \quad \rightarrow \quad S^{(r)}(\mathbf{z}, \mathbf{v}) = \prod_{e \in \mathcal{R}} p_e \cdot S_e(z_e, v_e)$$



**Figure 1:** Optimal network investments. Entry nodes in green, leaf nodes in red.

## 4. Attacker-Defender Model & Results

- Allow attackers to invest in *increasing* breach likelihood.
  - $S_D(z, v)$  vs.  $S_A(z, v)$

$$z_A^* = \arg \max_{z \geq 0} G \cdot S_A(z, v) - z \quad (2)$$

- Attackers and defenders take turns investing under rational constraints.
- Given defenders allocate  $T_D \leq L$  and attackers  $T_A \leq G$ , the state of the system at iteration  $i$  is a 3-tuple  $(v_i, R_{D,i}, R_{A,i})$  representing the current vulnerability, and remaining funds for defenders and attackers, respectively.

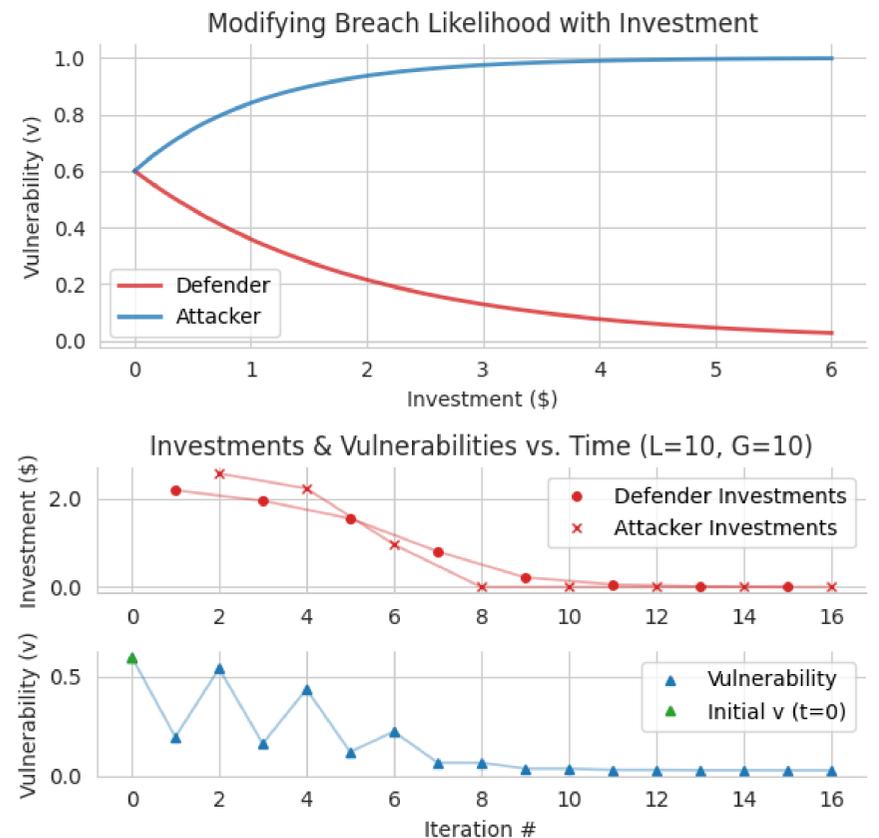
*Iterative Process:*

- For  $i = 1, 2, 3 \dots$

$$\begin{aligned} v_{D,i} &= S_D(z_{D,i}^*, v_{A,i-1}) \\ v_{A,i} &= S_A(z_{A,i}^*, v_{D,i}) \end{aligned}$$

- Where  $z_{D,i}^*$  and  $z_{A,i}^*$  result from solving Eq. (1) for  $z \in [0, R_{D,i}]$  and Eq. (2) for  $z \in [0, R_{A,i}]$  respectively.
- We then update the remaining funds for each party as:

$$\begin{aligned} R_{D,i+1} &= R_{D,i} - z_{D,i}^* \\ R_{A,i+1} &= R_{A,i} - z_{A,i}^* \end{aligned}$$



**Figure 2:** Investments and Vulnerabilities

## 5. Further Work

- *Strategic Optimization* – How might defenders invest non-optimally in the short-term to lead to a more optimal long-term result?
- *Parameter Estimation* – Can we infer future behavior of attackers based on the past? An opportunity for machine learning or multi-armed bandit methods.
- *Generalizations of the Attacker-Defender model to networks* – Just as we have generalized the Gordon & Loeb model, is it possible to extend our attacker-defender model to interactions and strategies in arbitrarily large networks?

## 6. Acknowledgements

We thank Vladimir Marbukh (NIST) for his insights and the benefit of discussions. DM acknowledges the support of NIST.

## 7. References

1. Lawrence A. Gordon and Martin P. Loeb (2002) "The economics of information security investment.", ACM Trans. Inf. Syst. Secur. 5, 4 (November 2002), 438–457.
2. Y. Liu and H. Man, "Network Vulnerability Assessment Using Bayesian Networks," Proc. SPIE, vol. 5812, pp. 61-71, 2005.