

Risk Assessment: A Game Theoretic Approach

**Vicki Bier, Aniruddha Nagaraj,
Vinod Abhichandani**

University of Wisconsin-Madison

Background



- ◆ **Game theory is a useful model for security risk assessment:**
 - ◆ Appropriate when protecting against intelligent and adaptable adversaries
 - ◆ Recognizes that defensive strategies must take attacker behavior into account
 - ◆ Can identify qualitative properties of optimal solutions (e.g., randomization)

Background...

- ◆ **Game theory is only beginning to be used in security risk assessment**
- ◆ **Military analogies (Schneier):**
 - ◆ **“The defender has to defend against every possible attack”**
 - ◆ **“The attacker...only has to choose one attack, and he can concentrate his forces on that one attack”**

Background...



- ◆ **Most applications are still exploratory:**
 - ◆ Illustrative applications to the choice of attack and defense strategies (Cohen)
 - ◆ Experiments demonstrating relevance of game theory to information warfare (Burke)
 - ◆ Application of game theory to financial institution risks (Chaturvedi et al., Gupta)
 - ◆ Importance of perverse incentives (Anderson)

Outline of this work

- ◆ **Games between attackers and defenders:**
 - ◆ **Simple series/parallel systems**
 - ◆ **Components with inherent values, and also a value to system function**

Overall goal

- ◆ **Study optimal allocation of resources for protection of series and parallel systems against intentional attacks**
- ◆ **Protective investment c_i reduces the probability of successful attack against component i to $p_i(c_i)$:**
 - ◆ **$p_i(c_i)$ convex, decreasing, twice differentiable and invertible**

Cases being considered

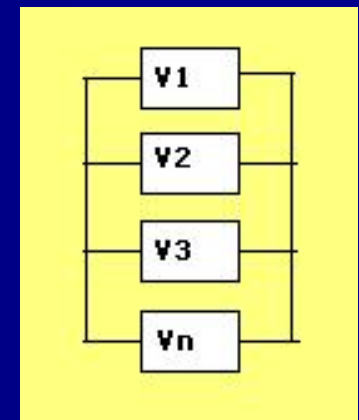
- ◆ **Results to date:**
 - ◆ **Components in parallel**
 - ◆ **Components in series**
 - ◆ **“Additive” models**
(Components have different “values” v_i)
- ◆ **In process:**
 - ◆ **Arbitrary series/parallel structures**
(NP-hard, may use heuristic approaches)
 - ◆ **Other configurations**
(Explore merits of perimeter defense, etc.)

Assumptions

- ◆ **Realistic levels of defensive investment will not deter attacks:**
 - ◆ Models applicable to determined attackers
- ◆ **Attacks against different components succeed or fail independently:**
 - ◆ Models applicable to functionally diverse and spatially separated defenses
- ◆ **Likely to apply to most serious threats against security-critical systems**

Components in parallel

- ◆ Defender wishes to maximize (expected value of system) – (defense cost), or equivalently:
 - ◆ Choose c_i to minimize $\alpha [\Pi p_i(c_i)v + \Sigma p_i(c_i)v_i] + \Sigma c_i$ where α is probability of an attack on the system, v is the value of the system functionality, and v_i is the inherent value of component i
- ◆ Optimum occurs when
 - ◆ $p_i'(c_i) \geq -1/\alpha[v_i + v \Pi_{j \neq i} p_j(c_j)]$, and
 - ◆ $c_i [\alpha v_i p_i'(c_i) + \alpha v p_i'(c_i) \Pi_{j \neq i} p_j(c_j) + 1] = 0$
- ◆ Multiple local optima are possible



Components in parallel...

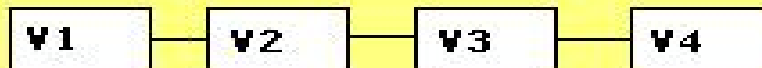
- ◆ Local optimum is unique when $p_i(c_i)$ are **log convex**:
 - ◆ Success probability decreases “faster than exponentially” in c_i
- ◆ This seems unlikely to be the case

Components in parallel...

- ◆ **General insights:**
 - ◆ **Optimal defense strategy depends on the cost-effectiveness with which components can be improved**
 - ◆ As measured by the $p_i'(c_i)$
 - ◆ **and on the values of the components**
 - ◆ As measured by the v_i
 - ◆ **Components that are too costly to defend (relative to their value) will not be hardened**

Components in series

- ◆ **Can occur for many reasons:**
 - ◆ **Physically in series (e.g., pipelines)**
 - ◆ **Multiple failure modes**
 - ◆ **Attacker can afford only one target**
 - ◆ **First successful attack is much more serious (e.g., for symbolic reasons)**



Components in series...

- ◆ **Attacker has a choice of targets**
- ◆ **Two bounding cases:**
 - ◆ **Attacker has no knowledge of defensive investments**
 - ◆ **Attacker can obtain perfect knowledge about defensive investments at no cost**

Components in series...

Perfect knowledge

- ◆ **Assumption of perfect knowledge may not always be unrealistic:**
 - ◆ Due to the openness of our society
- ◆ **Public demands knowledge of defense**
 - ◆ **Even when this weakens its effectiveness!**
- ◆ **This increases the difficulty of defense:**
 - ◆ E.g., anthrax protection

Components in series...

Perfect knowledge

- ◆ Assume attacker has only one attempt (multiple attacks are considered later)
- ◆ Attacker objective is to:
 - ◆ Choose i to maximize $[p_i(c_i) v_i]$
- ◆ For optimal allocation of defensive resources:
 - ◆ Defense must equalize the expected values of attacks against all targets
 - ◆ “Each of the defended targets [must] yield the same payoff to the attacker” (Dresher)

Components in series...

Perfect knowledge

- ◆ Unlike in defending against accidents or acts of nature:
 - ◆ **Optimal allocation does not depend on cost-effectiveness of investments!**
- ◆ **Defender is deprived of flexibility:**
 - ◆ **Must defend all targets of comparable expected value equally (regardless of cost)**

Insight

- ◆ **“Investment in defensive measures,
◆ unlike investment in safety measures,
saves a lower number of lives” (Ravid)**

Components in series...

Perfect knowledge

- ◆ Now, assume that the attacker can attack **each component** once (multiple attacks)
- ◆ Attacker objective is to:
 - ◆ Choose i to maximize
$$\alpha [\sum p_i(c_i) v_i + v \{1 - \prod [1 - p_i(c_i)]\}] + \sum c_i$$
- ◆ For optimal allocation of defensive resources:
 - ◆ Defense need not focus exclusively on components that cause highest expected damage
 - ◆ Investment in other components may pay off, if attacks against such “first-choice” targets fail
 - ◆ Optimal defense strategy again depends on the cost-effectiveness with which components can be improved

Components in series...

Perfect knowledge

- ◆ **Insights:**
 - ◆ **Properties of the optimal solution for series systems with multiple attacks are similar to those for parallel systems (e.g., multiple optima)**
 - ◆ **If one component dominates the risk, then the optimal solution with multiple attacks will be similar to that with a single attack**

Components in series...

No knowledge

- ◆ **Assume:**
 - ◆ Attacker targets component i with constant probability q_i (regardless of defense c_i)
 - ◆ Attacker has only one attempt
- ◆ **Defender objective similar to previous:**
 - ◆ **Choose $\{c_i\}$ to minimize $\sum q_i v_i p_i(c_i) + \sum c_i$**
- ◆ **Optimum occurs when $p_i'(c_i) \geq -1/(q_i v_i)$**
 - ◆ and $c_i [q_i v_i p_i'(c_i) + 1] = 0$
- ◆ **Expenditure c_i is increasing in $q_i v_i$**

Arbitrary Structures

- ◆ **Find defensive strategy when optimal attack strategy is NP-hard (joint work with Cox, Azaiez):**
 - ◆ **Cox's work on least cost diagnosis (1989, 1996) suggests near-optimal heuristic attack strategies**
 - ◆ **Identify optimal (or near-optimal) defenses against near-optimal attacks**
 - ◆ **Determine when heuristic attack strategies are in fact optimal**

Conclusions

- ◆ Protection of series systems from knowledgeable adversaries is a **fundamentally different** challenge:
 - ◆ Investments less cost-effective (since attacks can be deflected to other targets)
 - ◆ Defender loses flexibility to allocate resources cost-effectively
 - ◆ Importance of redundancy, secrecy (and deception) as defensive strategies

Conclusions...

- ◆ Defender should consider the **success probabilities** of attacks against various components:
 - ◆ Not only their inherent values
- ◆ Some high-value targets with a low probability of being successfully attacked may not merit any investment:
 - ◆ Lower-value, more vulnerable targets may merit defense
- ◆ Contrast this to the heuristic proposed by Brookings (2002):
 - ◆ Protecting only the most valuable assets