SAND2009-4306C

Quantifying the Degree of Balance in Physical Protection Systems

Presented to:

50th Annual Meeting of the Institute for Nuclear Materials Management

July 13-16, 2009

By Gregory D. Wyss, Ph.D.

Security Systems Analysis Department
Sandia National Laboratories

Contact: ☎ (505) 844-5893 gdwyss@sandia.gov

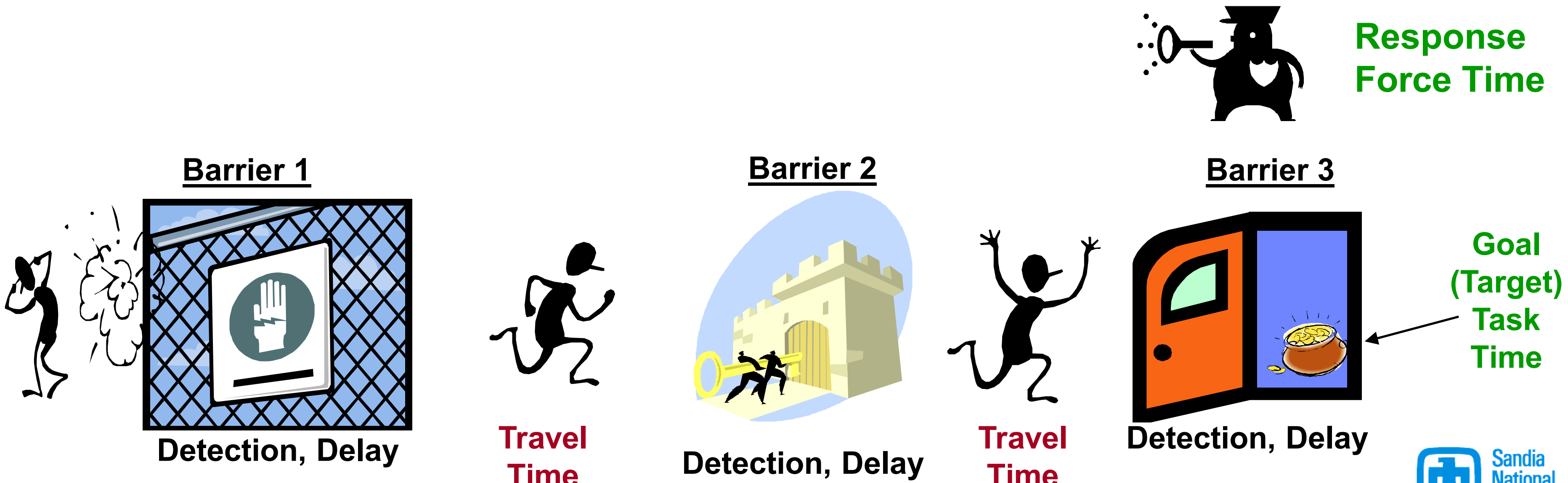
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.
Approved for Unlimited Release as SAND2009-XXXXP

Risk Assessment of Physical Security Systems

- **Evaluation is based on "timely detection"**

  P_E = Probability that the good guys can respond and neutralize bad guys before they accomplish their goal

  - **Each barrier has a task time (delay) and probability of detection**
  - **Bad guys' optimal attack path depends on which elements can be defeated, given their physical attack skills and tools**
  - **An attack path is attractive to an adversary if P_E is small**



What is a "Balanced Security System?

- Balance: "A facility should not have tightly-locked doors but wide-open windows"
- A physical protection system is balanced when every attack path presents a similar level of difficulty, *e.g.,*
  - similar adversary resources required
  - similar probability of timely detection
  - similar likelihood of being neutralized…
- Mathematically: P_E for the 1-2 most advantageous attacks should not be dramatically lower than it is for the next several most attractive attack paths.
  - Simple in concept: Applied as a heuristic by scanning P_E for the several most attractive attack paths.
  - No accepted metric to express "balance" by calculation

Sandia National Laboratories

Desirable Characteristics for a Balance Metric

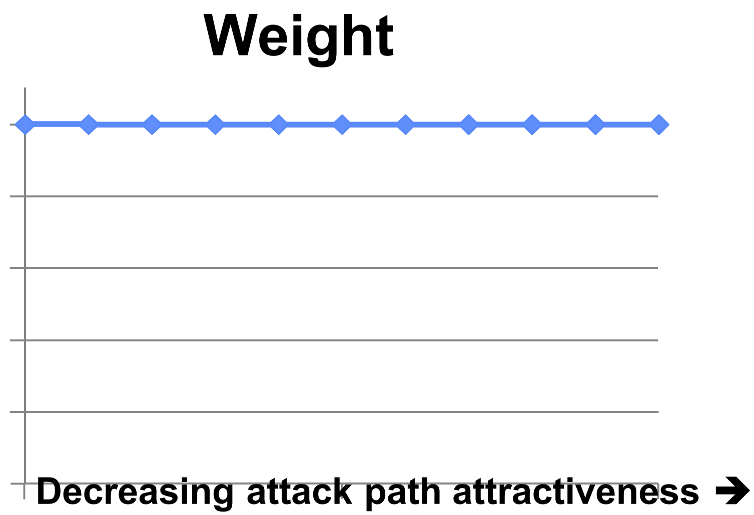
- **Should be based on existing, accepted security attack path attractiveness metrics (*e.g.*, P_E)**
  - **Should also support other attack path attractiveness metrics**
- **Consider several most attractive attack paths, but discount the multitude of unattractive attack paths**
- **Relatively independent of level of detail used in physical protection system analysis**
  - **The metric should be relatively insensitive to the *total* number of attack paths identified in the system analysis**

Sandia National Laboratories

Simple Average

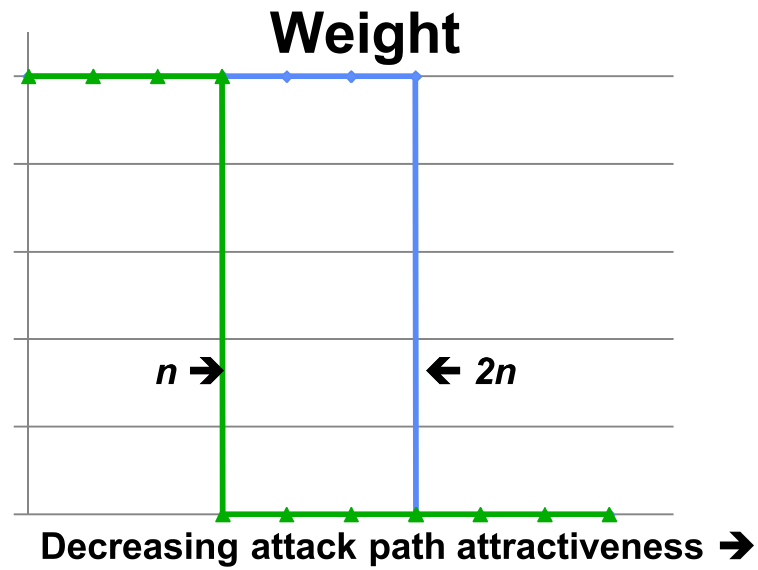
- Mean P_E over all attack paths
  - Unweighted average P_E value
- Advantages:
  - Simple to calculate and understand
  - Works with all known attack path attractiveness metrics
- Disadvantages:
  - Does not discount the multitude of unattractive attack paths, so…
  - Could be gamed by simply looking at more unattractive attack paths, and…
  - Sensitive to the total number of attack paths identified

Relative contribution of each value to the overall average



Simple Moving Average

- Mean P_E over *n* most attractive attack paths
  - Unweighted average P_E value, but using only *n* most attractive attack paths
- Advantages:
  - Simple to calculate and understand
  - Works with all known attack path attractiveness metrics
  - Discounts the multitude of unattractive attack paths (harder to game)
  - Insensitive to the total number of attack paths identified
- Disadvantages:
  - Very sensitive to the value selected for the parameter *n*

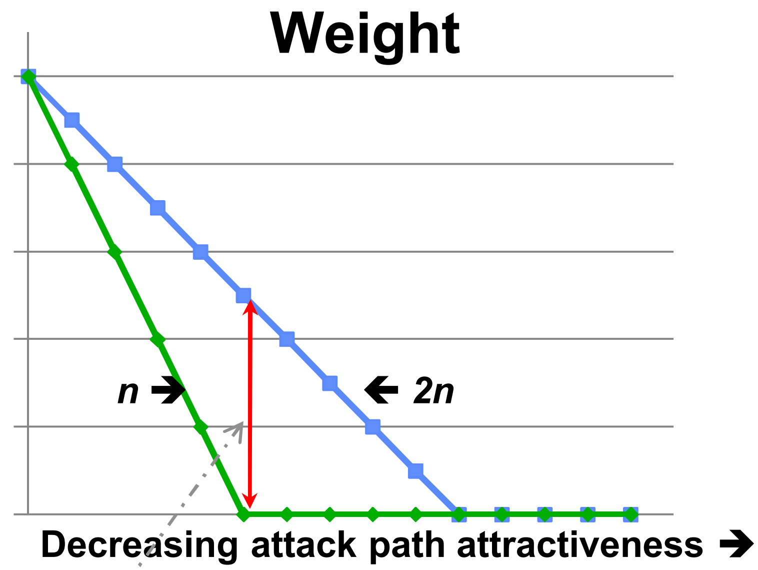


Attack paths are sorted from most to least attractive to the adversary

Curves represent change in relative weighting factors as n is doubled

Linear-Weighted Moving Average

- **Weight decreases arithmetically for less attractive attack paths**
  - **Weighted average P_E value; weight decreases over first n attack paths**
- **Advantages:**
  - Works with all attractiveness metrics
  - Discounts unattractive attack paths
  - Insensitive to total number of attack paths identified
  - **Less sensitive to the value selected for the parameter *n***
- **Disadvantages:**
  - **Relative weights of specific attack paths can change radically as *n* is changed**

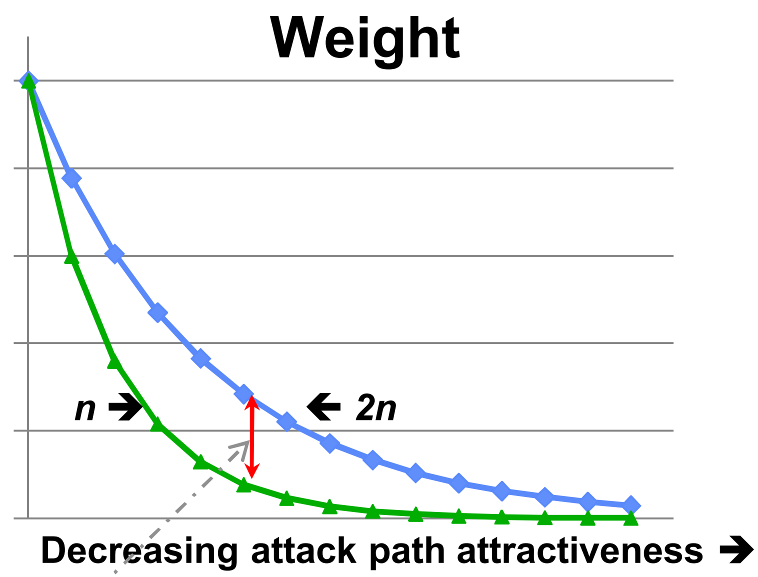


Curves represent change in relative weighting factors as n is doubled

Sandia National Laboratories

Exponentially-Weighted Moving Average

- Weight decreases exponentially for less attractive attack paths
  - ***All*** attack paths contribute to the metric, but most at a very low level
- Advantages:
  - Works with all attractiveness metrics
  - Discounts unattractive attack paths
  - Insensitive to total number of attack paths identified
  - Least sensitive to the value selected for the parameter *n*
  - Relative weights of specific attack paths do not change dramatically as *n* is changed
- Disadvantages:
  - Harder to explain to the uninitiated



Curves represent change in relative weighting factors as n is doubled

The weighting factor for the k^{th} term is

$$w = \alpha \cdot (1 - \alpha)^{(k-1)}$$

$$\text{where } \alpha = \frac{2}{n+1}$$

Application

- DOE Graded Security Protection Policy can be viewed as measuring *security balance* at Category I sites.
  - P_E is averaged over 6 attractive attack scenarios
  - This is a simple moving average with $n = 6$
- Comparing highest P_E to averaged P_E evaluates balance
  - Can be strongly sensitive to the value of n selected – averaged P_E would change significantly if n were 4, or 20, or…
- Using another weighted average reduces sensitivity…

  … but may have other policy implications
- Averaging adversary $P_S = 1 – P_E$ would be a more robust metric for balance
  - Now, less attractive attack paths have higher P_E and lower weight
  - Using P_S, less attractive attack paths would have *both* lower P_S and lower contribution to weighted average calculation

Sandia National Laboratories

Summary

- A security system should provide balanced protection
  - Currently assessed heuristically – no mathematical measure
- Linear- or exponentially-weighted averages are good metrics for balanced protection
  - Greater weight for most attractive attack paths ➔ discount unattractive attack paths
  - Less sensitive to changes in weighting parameter
  - Works with P_E and other attractiveness metrics
- DOE Graded Security Protection Policy can be viewed as measuring security balance at Category I sites
  - Current metric highly sensitive to number of attack paths averaged
- A robust balance metric can help inform risk management decisions both within a site and across multiple sites