MP 180675
MITRE PRODUCT

MITRE

TRACE Analytics

Project No.: 10AOH810-JF

Lexington Park, MD

Authors:

S. Ricks
N. Huston
F. Lynam

Peer Review:

L. Oringer
R. McInnes
M. McFarren

October 2019

Abstract

This paper discusses various formulations of TRACE graphs and how those unique cases require different analytics in order to capture information about a system that can influence decision making. Specifically, probability and expectation value of compromise and involvement are defined and illustrated. This paper is intended to provide a more detailed mathematical understanding of TRACE graphs analytics to analysts with basic familiarity with TRACE.

Overview

This paper discusses important considerations in what the TRACE (Traversal-drive Risk Assessment of Composite Effects) analysis should measure, addressing the influence of both the stochastic space (such as the network architecture in a cyber offensive process) and the deterministic space (the functional or mission dependency model). Simplifying assumptions of the methodology and critical edge cases are discussed to help define the analysis requirements that shape the TRACE algorithm and the consequent analytics it provides.

This paper will focus on the example problem of cyber effects, where a system can be decomposed into both a functional model of how a system is used and a physical model of how a system is built. Generally, a functional model is deterministic and a physical model is stochastic, but in practice characteristics such as known software vulnerabilities can result in the physical model containing deterministic features. In the construction of a system representation, component functions provide the interface between the physical and functional models, and understanding that interconnection is essential to derive actionable information about cyber weapon effects in particular. By convention, the flow of cyber weapon effects is defined by attack paths which start in the cyber space at entry points, transition from cyber to the functional space via end effects, and end at a particular loss condition of interest to the analysis.

Expected Emergent Behaviors

TRACE models are meant to provide a useful representation of reality in capturing these physical and functional models. Consequently, the quantitative values that a TRACE analysis produces from those models should be expected to be consistent with the intuitive expectations of subject matter experts with regard to whatever is being modeled by TRACE. This section introduces a few nuanced ideas about how cyber risk should be expected to change when different options are taken to reduce it. These provide expectations or constraints on what the TRACE algorithm should be expected to illustrate under these conditions.

Firstly, design changes that alter the relationship between the cyber and function models should impact the overall risk appropriately. For example, assigning a single required function to redundant physical nodes can reduce risk (assuming the nodes are not subject to common mode vulnerability) by forcing an adversary to successfully execute more attacks in order to impact functionality. Conversely, combining functions into a single node can increase risk by reducing the number of unique attacks and adversary must execute. However, changes to the abstract structure of the functional model that do not alter the physical space or how the system is actually used by human operators (for example, splitting a complicated function into two simpler ones that accomplish the same function and link to the larger graph in the same manner) should not be expected to change risk.

Secondly, all possible real world attack paths and effects need to be able to be captured. Exhaustively searching these possibilities can present real computational challenges, especially for attacks which leverage multiple simultaneous end effects. A weapon's path can start from multiple nodes, and fork along the way, and might only ever converge at the very end of the functional model with "mission defeat." For example, if two diverse physical nodes provide backup capability, in the event of a failure of either node, there is not necessarily any mission impact. Consequently, weapon path analysis in TRACE must be able to encompass paths which diverge to defeat any set of concurrent end effect nodes.

Central Simplifying Assumptions

To focus specifically on how these nuances are captured by the TRACE analytics, two core simplifying assumptions are made throughout this paper. It is recognized that in practice additional labor must be expended to ensure these assumptions are met.

The first assumption is that the model is representative and understood with full confidence. This is primarily for convenience of the overall discussion. Well-practiced methods to accommodate statistical uncertainty can be incorporated in practice with no necessary change to these basic analytics beyond inclusion of confidence bounds.

The second assumption is that the adversary has access to the same model as the analyst. This means that the TRACE graph is explicitly representative of the decision making options available to an adversary. If perfect intelligence on adversary knowledge is available, it would be reasonable to adjust the graph accordingly to account for what information it is expected the adversary is making decisions using. However, this second assumption is conservative and allows for optimization against a highly intelligent and capable adversary.

Understanding why these assumptions are made and what their impact might be is illustrated through three core types of path interactions: serial, divergent and intersecting paths. Each helps account for different aspects of the amount of marginal risk presented by each node in complex path interactions.

Attack Paths

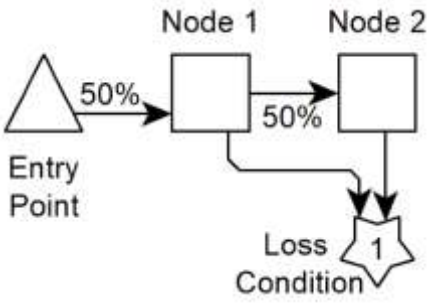
TRACE analytics primarily address the effect of attack paths, but the analytics themselves are about individual nodes in a graph. An attack path is an important concept in threat analysis because it captures the accessibility of mission risk to an adversary. Attack paths in TRACE are defined as any set of steps that takes an adversary from a foothold or point of entry in a system to the point where they can cause a change in how the system operates in such a way as to make it unable to complete some task that the outside world is relying on it for.

However, analyzing individual attack paths presents a substantive and limiting challenge to understanding the integration effects of system architecture. In a system of even moderate complexity, TRACE analysis on real-world systems has found hundreds of thousands or millions of mission-defeating attack paths of relative ease. If TRACE used analytics focused on mitigating those specific attack paths directly, it would struggle to efficiently address the full scope of system risk, or possibly even fail to meaningfully address that risk at all. Thus, TRACE analytics are about how all of the attack paths in a system relate to each individual node. This lets the analyst understand each component's relationship to both adversary access and mission risk.

Serial Paths

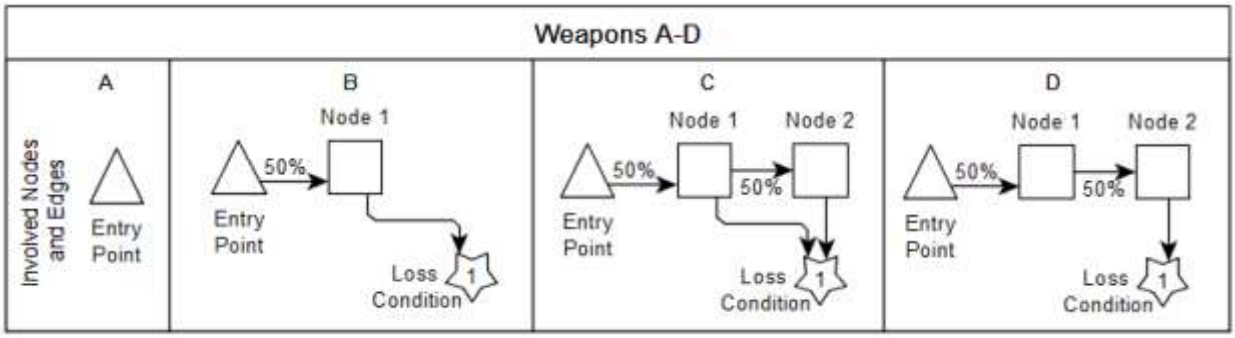
For the second assumption, this kind of information asymmetry between our self-knowledge and the adversary's knowledge about our system and functional allocation would be extremely difficult to collect sufficient evidence to credibly substantiate. Consequently, it would be challenging to take credit for the assumption that our enemy's understanding contains any specific flaws relative to our own. Thus, we are constrained to assume information symmetry, and once any one path is able to propagate via any

set of nodes to some loss condition of interest, no additional steps should be added to the path as the adversary knows as well as we do that they present no additional likelihood of success.



However, this approach results in misleading information about offensive trade space. First, consider the model to the left. In a TRACE cyber analysis, traversal from adversarial space (triangles) through the physical space (squares) is a function of the probability of developing novel cyber weapon capabilities. In contrast, traversal through the functional space (diamonds and stars) is implemented using basic logic functions, "and" or "or," represented here as simple coincidence logic where compromise of any 1 input results in compromise of the function. The analysis is focused around compromise of a specific function, the loss condition of interest to the analysis in question (star).

In this example system with two serially linked physical nodes, compromise of either can result in the loss condition of interest. However, as compromise of Node 2 is dependent on compromise of Node 1, the above discussion on information symmetry would suggest that analysis for the compromise of Node 1 would indicate no residual risk is present due to the presence of a path through Node 2, which is not a valid conclusion. Upon resolution of the risk in Node 1, it's entirely possible the residual risk of Node 2 would become dominant. This results in two necessary risk concepts to illustrate: the analysis must be able to both determine the total risk of attaining the loss condition of interest, as well as illustrate that the second node has some additional risk factor requiring resolution.



Consider that the above example contains four options for an adversary to execute. Weapon A is the trivial solution: no weapon is developed. The risk presented by this choice is zero. Weapon B is a weapon which traverses only Node 1 and presents an end effect in Node 1, which results in mission defeat. Weapon B has a 50% probability of attaining the loss condition of interest. Weapons C and D traverse both Node 1 and Node 2, resulting in a probability of 25%. Weapon C is the intuitive case where an end effect is presented in both nodes, and Weapon D is the unintuitive case where an end effect is solely leveraged in Node 2.

$$P_{L,B} = P[N1|E1] = 50\%$$

$$P_{L,C\ or\ D} = P[N1|E1]P[N2|N1] = 25\%$$

Each weapon is one potential option for an adversary to select, however it's unclear which should be explicitly involved in the calculation of risk and how that calculation should be performed. For TRACE, overall risk can be thought of as an adversary investing in every possible option. Weapon A presents no

risk and is of no concern. Weapon B is similarly straightforward: this seems most likely to achieve the desired loss condition and should be represented in the computation.

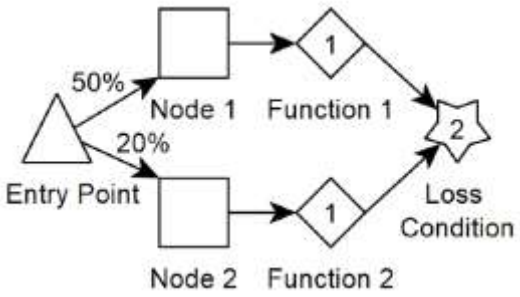
Weapons C and D are less obvious candidates for inclusion. Both are dependent on the prior success of Weapon B. Consequently, they provide no contribution to the overall risk of attaining the loss condition: the probability of attaining the loss condition via Weapons C or D is fully contained within the probability of Weapon B and is solely dependent upon adversarial selections which we fundamentally cannot anticipate. Thus, the probability of involvement ($P_I[N1]$) of Node 1 and of reaching the loss condition (P_L) is bounded at 50% regardless of weapon selection.

$$P_L = P_{L,B} = 50\%$$

While not contributing to the overall loss condition rate, Weapons C and D both provide adversaries an additional option for achieving the loss condition which involves Node 2. The only tangible difference between the total weapon paths for Weapons C and D is in the functional space. Consequently, the probability of executing these weapons fully overlaps in the physical space, and neither contributes any more probability of involving Node 2 than the other. Thus, the probability of involvement ($P_I[N2]$) of Node 2 in a weapon is bounded at 25%.

$$P_I[N2] = P_{L,C\ or\ D} = P[N1|E1]P[N2|N1] = 25\%$$

Divergent Paths



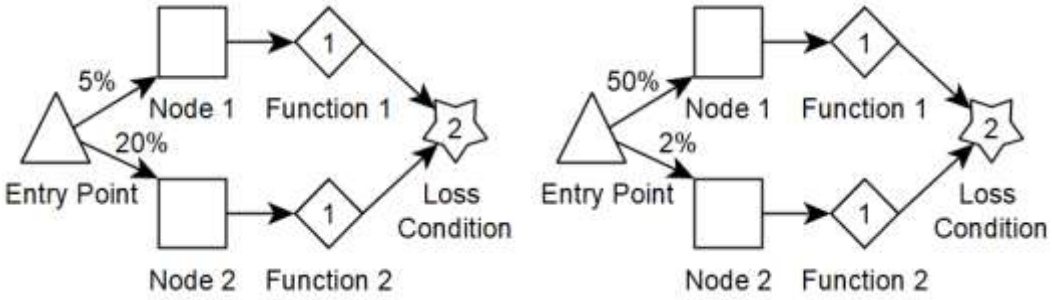
Consider in contrast an example system with only one feasible weapon path that leverages a divergent physical path to compromise nodes for concurrent defeat. Here, the loss condition requires compromise of two incoming paths, both Functions 1 and 2. Given the two physical nodes are diverse technologies, the probability of achieving the loss condition is 10%, which is the probability of achieving the two independent events of compromising both Nodes 1 and 2.

$$P_L = P[N1|E1]P[N2|E1] = 10\%$$

The probability of compromise of Node 1 is 50%, but the probability of Node 1 being involved in an effective weapon is only 10%. Likewise, the probability of compromise ($P_C[F1]$) of Function 1 is 50%, but the probability of that compromise resulting in the loss condition of interest is only 10%. This presents a challenge to what data to illustrate in the analysis, as it may be desirable to indicate that Function 1 is at higher risk independent of its involvement in the loss condition of interest.

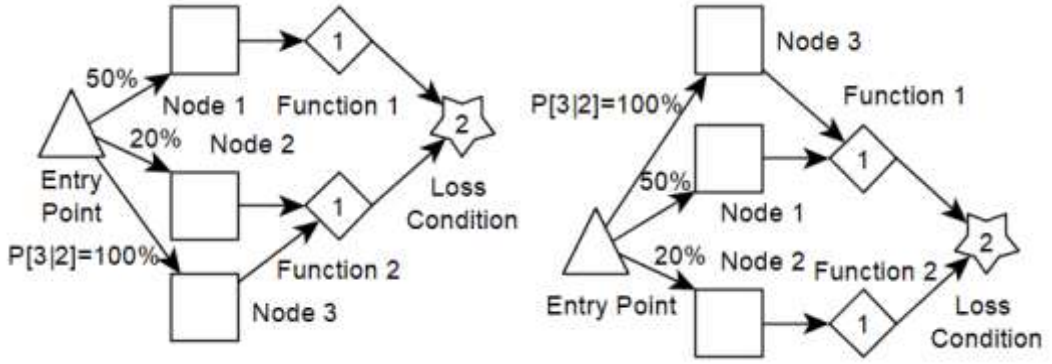
$$P_C[F1] = P_C[N1] = P[N1|E1] = 50\%$$

$$P_I[F1] = P_I[F2] = P_I[N1] = P_I[N2] = P_L = 10\%$$



For mitigation effects measured in terms of fractional gains (like monitoring) with no structural alteration to the underlying model (like redundancy), there is no clear value in understanding the relative loss rate for Function 1 alone, as illustrated above. The marginal reduction to the probability of attaining the loss condition of interest due to a 90% effective mitigation applied to either Node 1 or Node 2 would be equivalent, with both cases resulting in an overall probability of attaining the loss condition of interest and of Function 1's loss being involved of 1%.

$$P_L = (10\% * P[N1|E1])P[N2|E1] = P[N1|E1](10\% * P[N2|E1]) = 1\%$$



However, some mitigation effects do involve structural alteration to the fundamental nature of the model, such as by rearchitecting the functional allocation to add additional redundancy to a critical function as shown above. The effect of such changes may vary in a non-fractional manner, resulting in a misleading indicator if solely the involvement in the loss condition of interest is identified. In this example, consider the addition of Node 3 which is identical in design to Node 2 and thus susceptible to common mode failure. The probability of compromise of Node 3 given compromise of Node 2 is 100%.

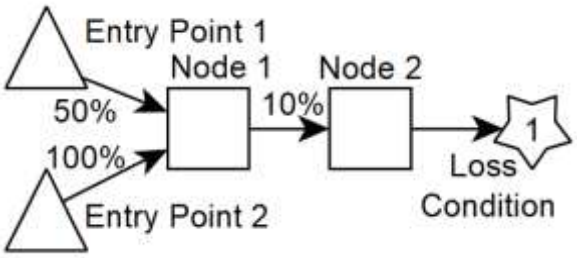
This would result in an increase in the probability of attaining the loss condition of interest when placed functionally in parallel to Node 1 but no change when placed functionally in parallel to Node 2. Here, the asymmetrical impact of this architectural change could be anticipated if the probability of a node's individual compromise was also shown. Methods to reduce overall risk via the architectural trade space are poorly understood in the context of this analysis method at this time, but leveraging such methods has clear ramifications as this example illustrates.

$$P_{L,3||1} = P[N2|E1] = 50\%$$

$$P_{L,3||2} = P[N2|E1]P[N1|E1] = 10\%$$

This results in an important observation: every node in the physical and functional space is, independently, a potential loss condition worthy of interest for the architectural trade space. Thus it is

relevant to understand both the probability of each node's involvement in the loss condition of interest to the overall analysis as well as its own independent probability of compromise. Both values should be computed by any risk calculation algorithm.



Intersecting Paths

Consistent with the previous discussions, this example system presents two weapon paths which traverse from entry points to the loss condition of interest. The weapon originating from Entry Point 1 has a probability of 5% of reaching the loss condition, and the alternate weapon has a probability of 10%.

However, these paths overlap, and the probability of traversing to the loss condition of interest is not the simple Boolean OR of 5% and 10%. Rather, the probability of reaching the loss condition is the probability of traversing to Node 2 after traversing to Node 1 from either Entry Point 1 or Entry Point 2 (in Boolean set notation):

$$P_L = P[N2|N1](P[N1|E1] + P[N1|E2]) = 10\%$$

Thus the probability of involvement of Node 2 and of the loss condition of interest is 10%. As can be observed from the diagram, the probability of reaching Node 1 is 100%. The probabilities of these nodes being involved in reaching the loss condition of interest are all 10%. However, there is no information in these results whatsoever reflecting the impact of Entry Point 1 on risk, as can be illustrated by removal of Entry Point 1 resulting in no change to these figures:

$$P_L = P[N2|N1]P[N1|E2] = 10\%$$

If Entry Point 2 is mitigated but Entry Point 1 remains, residual risk that is not otherwise illustrated in any of the measures identified thus far is present:

$$P_L = P[N2|N1]P[N1|E1] = 5\%$$

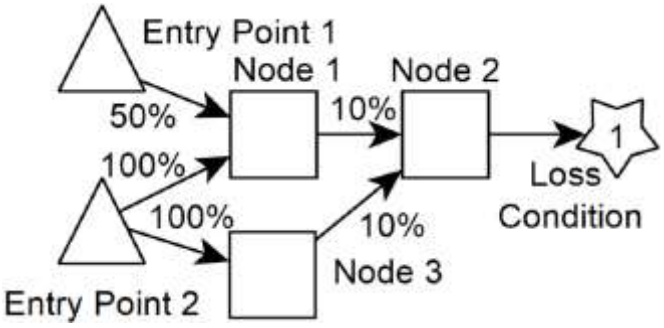
The presence of this residual risk can actually be gleaned from the base model without having to search through the mitigation options by assessing a second factor on both of the measures above: expectation value. Expectation value would need to be computed both for node compromise and for node involvement in a loss condition. Expectation value in this context captures the total number of times the node would expected to be compromised in a given trial where an adversary attempted every available options at every opportunity.

In this example, expectation value for Node 1's compromise is 1.5, as we expect to compromise Node 1 50% of the time from Entry Point 1 and 100% of the time from Entry Point 2. For Node 2 and the loss condition of interest, the expectation value follows as 0.15. The expectation value for any node's involvement in the loss condition of interest (other than the entry point nodes) is, likewise, 0.15 for all nodes.

$$EV_C[N1] = EV[N1|E1] + EV[N1|E2] = 1 + 0.5 = 1.5$$

$$EV_C[N2] = EV_L = EV_I[N1] = EV_I[N2] = EV[N2|N1](EV[N1|E1] + EV[N1|E2]) = 0.15$$

This issue is most relevant for analysis with many values near 100%. For very small probabilities, the expectation value is generally very close to the probability. For most analyses performed to date, many probabilities are very near 100%, making expectation value a useful indicator of risk reduction priorities. Consider how expectation value illustrates additional information in the following modification to the above example:



In this case, an additional path is now available in parallel with Node 1. Given solely the probabilities of compromise or involvement, there is no means to distinguish whether Node 1 or Node 3 pose a greater risk, or more explicitly, whether mitigations against either node would result in less residual risk. However, with the additional computation of expectation value as shown above, it can be observed that Node 1 contains more effective complete paths per trial than Node 3, meaning it is involved in more potential adversary options than Node 3. In a model with potentially millions of design trades to be made, this nuance can provide useful insight in where to start making changes first.

Conclusion

This paper introduces four main analytics: probability and expectation value of compromise and involvement. In practice, the probability values are a function of time and are most usefully expressed in terms of the mean time before an event is expected to occur. However, the core concepts and particular edges cases which each analytic covers remain just as relevant in a time-variant TRACE model, and are important to understand when attempting to assess the composite nature of multiple, overlapping threat vectors in a particular problem.