MP190481
MITRE PRODUCT

MITRE

Traversal-driven Risk Assessment of Composite Effects (TRACE) – An Overview

Project No.: 10AOH810-JF

Lexington Park, MD

Author:

F. Lynam
flynam@mitre.org

October 2019

Abstract

This paper provides a high-level understanding of TRACE, a formal, model-based analysis methodology for asymmetric threat vector problems. TRACE has been applied to both cyber and supply chain effects to support risk-informed decision making. This paper does not provide a detailed explanation of the design of analysis considerations, asymmetric threat theory, mathematics or data science supporting specific applications of TRACE, which is covered in other papers. This paper is intended for a reader aware of the risks posed by non-kinetic adversarial threats, such as cyber or supply chain attacks, but unfamiliar with TRACE. This paper argues that the formal methodology, empirical basis and rapid analysis toolkit provided with TRACE enables better informed, more objective and more repeatable decisions.

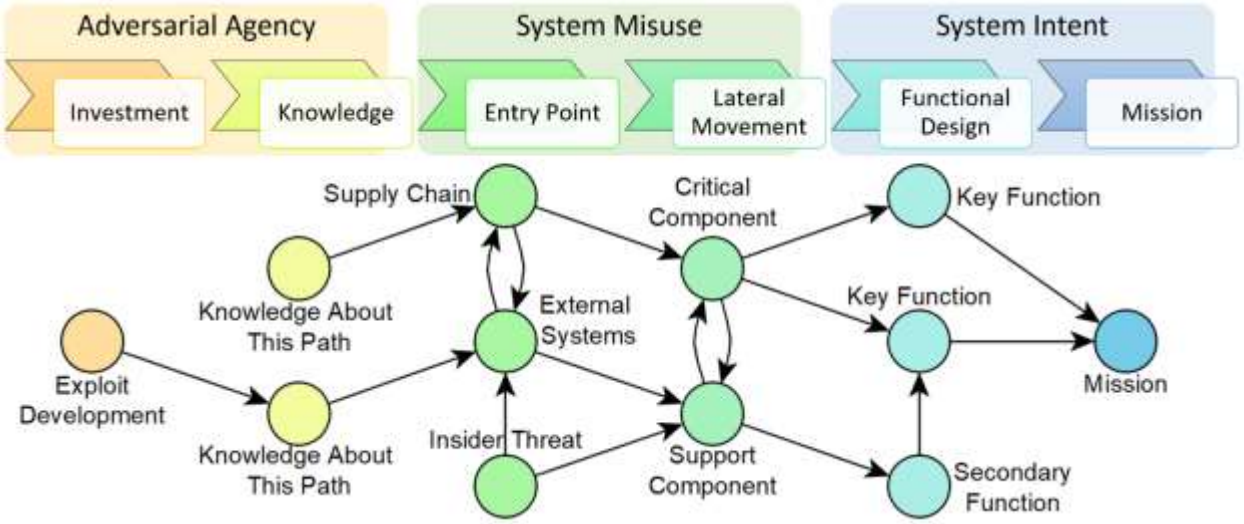
Overview

The systems we rely on for our missions today are more intricate than ever in history. The constituent components of operational systems continue to evolve away from simple human-to-human interactions through the greater and greater employment of technology. Technology enhances and extends human capability, creating a web of socio-technical systems that together can accomplish tasks beyond the capability of any one person or one technical component alone. However, the actual implementations of these systems of systems for the purposes of highly integrated missions often relies on innumerable tiny assumptions about how each of those elements will perform their role. When the wrong one of those assumptions is unexpectedly proven invalid, catastrophe can ensue.

Traversal-driven Risk Assessment of Composite Effects (TRACE) provides a set of standardized modeling and simulation methods designed to rapidly yet exhaustively analyze systems of systems for exactly the kinds of weaknesses that can be exploited to cause systemic failure. TRACE models can be used to rigorously describe internal dependencies within systems, how those systems are vulnerable to failures and attacks, and where to invest in systemic resilience. As a formal modeling technique, TRACE provides a repeatable means to objectively evaluate not just known weaknesses, but the effectiveness of system functional designs and architectures, or alternative designs and architectures, to be resilient in the face of random or induced failures, including accounting for credible advanced cyber, supply chain and insider threat actors.

Threat Vectors

A threat vector consists of any elements that connect adversarial agency to disruption of a system's intended purpose. Threat vectors can be described as containing three essential elements: adversarial agency, system misuse and system intent.



The above diagram illustrates a generic, high-level model of relationships of threat vectors that could be applied to any arbitrary system of systems. TRACE provides a set of methods for describing and analyzing this structure. The TRACE graph for a system can contain thousands of individual nodes (circles) representing each element of every threat vector in a socio-technical system, with edges (arrows) connecting these nodes together to capture their relationships to each other.

In TRACE, the model of system intent represents the design and intended purpose or mission of the system itself. The criticality of any node in this graph is captured explicitly by the relationship between that element and this mission structure. Opportunities for system misuse are informed by the implemented physical system that supports that intended function. Vulnerability of the system can be described by every path between each accessible entry point in the physical system and the structure of the mission model. The simulation of adversarial agency employed across this vulnerable space is built on historical intelligence information. Combining these elements constitutes a threat vector: a complete path that can be articulated from known adversary investments, through their knowledge of system vulnerabilities and into a demonstrable course of action resulting in mission disruption.

TRACE currently employs three standard models to describe this threat vector space: FOXTROT, ECHO and SIERRA. FOXTROT defines a detailed structure for models of system dependencies, providing a simple approach to generate a functional model inherently able to transform into several other standard functional and fault analysis models. ECHO is a generalized model for cyber attacks, leveraging vulnerabilities from numerous sources to predict the mean time to development of zero-day effects given basic information about components in a system, allowing a systems engineer to articulate subtle cyber effects to the same fidelity as a cyber expert. SIERRA is a structured approach to supply chain decomposition, facilitating measurement of the risks introduced by broad and diverse component sourcing channels, using open-source data on real-world suppliers to make better-informed risk inferences based on extrapolation of data from other sources.

Modeling Resilience

TRACE threat vectors are estimates of time. Each edge in a TRACE graph represents a time-varying probability of successful compromise. The more time invested, the greater the probability of success. As individual threat vectors add up to a complete path, the mean time to successfully compromise the entire path can be determined. The resilience of a system of systems to compromise is therefore measured in terms of the mean time to compromise the key mission of that system, whether the initial entry point is an insider threat, a cyber attack or simply random failure. These initiating events can be modeled probabilistically as well, allowing for direct comparison within a single TRACE graph.

Even with TRACE, searching for effective offensive or defensive options is a computational challenge. For example, the mean time before any individual node in a TRACE model gets involved in a threat vector impacting the mission can be numerically solved, but doing so is exponentially more difficult than solving for the mean time to compromise any single node. Compounding the difficulty of solving for the optimal attack vectors, defending against only the most effective offensive strategy often ignores alternative paths that are only marginally less effective offensively. Solving the defensive problem in a manner that effectively reduces risk requires understanding the nature of these competing factors, primarily characterized by estimating and managing the uncertainty they introduce into the result. TRACE analytics are designed to address these issues specifically.

Threat models face three distinct types of uncertainty: systematic, statistical and agent-driven. Systematic uncertainty arises when a model fails to describe an element of a threat vector, and is managed in TRACE through use of the well-defined standard models that bound all possibilities. Statistical uncertainty arises when a model has variability in particular probabilities, resulting in wide bands of possible mean values, and is managed in TRACE through a conservative approach to continued research and data collection. Agent-driven uncertainty arises when the decisions made by the adversary

are unknown, as is always the case. Given these uncertainties, the best way to defend the right set of threat vectors can be challenging to determine.

Each of these sources of uncertainty are amplified by the large numbers of available options in a threat vector space. The farther an action is from the top-level mission node, the greater the number of intermediate steps involved, the greater the number of alternatives available, and the greater the uncertainty in the result. As systems become more complicated and intricate, less confidence can be expressed in the certainty of their security or resilience against attack. The closer to the mission node that defensive alterations are made, the greater the certainty in their effectiveness. In contrast, boundary defense is effectively meaningless if you have systematic uncertainty about what constitutes your boundary. Comparably, defending against the most well-validated attacks which are best suited to our testing capabilities can prove ineffective if a low-confidence, difficult-to-test yet devastating attack later proves feasible. Likewise, cutting off a few of the adversary's shortest paths does nothing if the adversary anticipated that defense and already invested in a few different alternatives. TRACE applies an asynchronous game theory approach across the entire system model to manage these factors.

TRACE Analysis

TRACE analysis is designed to articulate not just key risks, but effective solutions. By conservatively elevating to a systems-level measure of mean time to compromise for the overall mission, TRACE inherently addresses competing sources of uncertainty. Through examination of the entire solution space across all threat vector paths and resiliency options, TRACE maintains the focus of analysis on solving the systems engineering problem, not individual implementation flaws. Component-level solutions driven from a TRACE graph are fully contextualized within the larger scope of adversary capability and mission needs by the design of the analysis. Architectural solutions are validated explicitly through restructuring of the representative TRACE model. TRACE mean time to compromise values are explicit measures of system resilience based purely on empirical data, whose predictions are continuously validated against subject matter expertise.

TRACE analytics aren't just a single value or a single graphic, but rather answer the question asked. If the question is "which entry point presents the greatest vulnerability" to help decide which ties to cut, TRACE analysis can produce a chart of the mean time to compromise for each key mission for attacks starting from each entry point. If the question is "which components play the biggest role in mission defeat" to help decide which components to improve, TRACE analysis can produce an ordered list of every component's mean time to involvement in a successful attack. If the question is "how do I make my system more secure" to help decide how to re-architect the entire design, TRACE analysis can explore design alternatives to fully characterize the cost benefit trade space. Effective analysis, as always, depends on asking the right questions.

Using TRACE

TRACE uses a set of freely available tools, which come with detailed documentation and examples. A portable toolkit built into Excel macros is available for deployment in standalone environments, and a SysML tool plugin interface allows for direct integration into model-based acquisition ecosystems. Our team of developers and analysts is continuously developing the technologies driving TRACE, expanding the capabilities of the application and improving the accuracy and accessibility of the analytics.