ATTACK TREE METHODOLOGY

Protecting Critical Business Applications & Assets

Organizations are increasingly grappling with their complex business critical application infrastructure and the changing threat landscape to which it is exposed. Enterprises struggle to quantify their enterprise and operational risk. Lacking a practical alternative, enterprises have turned to a variety of technology point solutions and consulting assessments to identify these threats. However, these common approaches have significant limitations in mission-critical complex environments.

Traceability:
Traditional assessment methodologies fail to map technical risks to operational and business impact.

Practicality:
Standard assessment deliverables list only vulnerabilities and fail to identify realistic (and complicated) attack scenarios that exploit them

Accountability:
Assessed security impacts include only end-point attack consequences. They do not total intermediate consequences that might contribute significantly to the risks resulting from a particular attack scenario.

Reusability:
Deliverables provide only organization and format for future efforts. They do not produce a general model for follow-on analyses.

Temporality:
Traditional assessments fail to provide a “real time” capability to analyze risk under various assumptions about adversarial capability and in-place preventative measures.

Holism:
Most security analyses make artificial distinctions between physical and cyber assets, thus failing to recognize the importance of compensating controls.

Cost:
Ongoing, comprehensive assessment programs require very significant resource commitments; most organizations balance this cost against their need for security mitigation and remediation and cause organizations to close vulnerabilities where actual attack paths may not exist.

Filling the Gap

The team at Network & Security Technologies (N&ST) recognized that there was a need for a systematic holistic methodology that compensated for the above deficiencies. To add value to other empirical methods, this systematic approach needed to:

Facilitate the analysis of causality:
Vulnerability, by itself, does not represent risk. A good security analysis should identify the relationships between vulnerabilities and operational/business consequences.

Construct attack scenarios from the causal relationships:
In general, a realistic attack scenario will consist of cascading cause and effect

...CONTINUED ON NEXT PAGE

ATTACK TREE METHODOLOGY

(e.g., vulnerability and consequence) relationships. Thus, one vulnerability will lead to one or more effects. Each of these, in turn, will lead to higher level vulnerabilities. Any assessment process should capture these attack pathways.

Identify links between the many different low-level compromises and a few higher-level impacts:

The ultimate impact of a simple breach depends on the practicality of the attack scenario. The methodology should assign priority to lowlevel remediation based on the likelihood that a cascade can result in major consequences.

Maintain running totals of intermediate impacts for each attack scenario:

Often, the total cost of a successful attack includes much more than the terminal consequence. The process should total all consequences throughout an attack pathway.

Assert systematic protective measures in each scenario and determine their value:

The decision to devote resources to mitigate a particular security issue should depend upon the incremental reduction of total risk it can produce. A good process facilitates this analysis.

Instantaneously adjust overall risk metrics to proposed changes in protective measure:

A comprehensive assessment weighs the value of a protective measure across all attack scenarios. It should provide an executive risk analysis for the organization as a whole.

Identify "most likely" scenarios when subject to new information about an adversary's capabilities and motivation:

An adversarial profile (or our assumptions about it) can change over time. A dynamic assessment methodology enables the security analyst to modify these assumptions to identify the most likely attack scenarios and their consequences.

The Attack Tree Methodology

N&ST has introduced the Attack Tree Methodology to our clients in the context of:

Cyber/Physical Security Environments

as the line between physical and cyber security thins; both can represent a threat to the availability of your business. Attack Trees allow a holistic view of identifying the most probable exposures. Most of the PDD-63 defined Critical Infrastructure Sectors can benefit from this holistic analysis.

Application reviews

critical applications that facilitate your business and customer interaction may have many inter-working component parts and platforms. Databases, middleware, applications servers, operating systems exposed to internal, external and inherent threats. Examples of this include: Any application involved with financial transactions or containing personal or sensitive business data. Attack Tree mapping can provide an illuminating perspective on where to focus and prioritization of your limited resources.

USE ATTACK TREE TO MAKE INFORMED DECISIONS BASED ON REAL BUSINESS RISKS

Our passion for technical excellence and commitment to our client's business success results in practical solutions to complex problems