SAND2008-7621P

Collect Data to Address Target Metrics

Attack Metrics (1)

Attack-based metrics describe the capabilities and commitment required to undertake a given attack successfully.

- Attack-based metrics
  - imply detailed understanding of the process necessary to perform an attack - the path from adversary discovery to adversary goal completion, and
  - have a significant degree of overlap with *adversary metrics.*
- Example commitment factors*
  - intensity (e.g., willing to risk going to prison),
  - stealth (e.g., detection unacceptable) , and
  - time (e.g., slow vs. fast).
- Attack-based metrics derived from capabilities include those for attack
  - discovery (e.g., knowledge),
  - development (e.g., R&D program for sophisticated exploits), and
  - execution (e.g., access).

*Think of these in both adversary and attack terms.

Attack Metrics (2)

- Attack discovery metrics
  - adversary characteristics, resources, and costs necessary to identify and characterize an attack opportunity, so
  - discovery example: terrorist observes government troop movements; how to measure?
- Attack development metrics
  - adversary characteristics, resources, and costs necessary to develop an attack,
  - breaking commercial encryption example: competitor needs exploit to gain access to sensitive information; how to measure?
- Attack execution metrics
  - adversary characteristics, resources, and costs necessary to execute an attack,
  - access example: insider planted by adversary to enable physical, remote, or both to support successful attack; how to measure?

Attack Metrics (3)

Attack-based metrics

Attack-based metrics describe the capabilities and commitment required to undertake a given attack successfully.

CONSIDERATIONS:

- Take special care to ensure subjectivity and consistency.
- Compare costs of different collection methods.
- Avoid discussions of specifics with decision makers.
- Make sure you know who will see the metrics.

EXAMPLES:

- Knowledge or skill required.
- Time required to perform the attack.
- Probability of detection; likelihood that the defender will detect the attack.

SOURCES:

METHODS:

- Elicit subject matter expertise.
- Measure during execution (time the attackers).
- Execute repeatedly; divide the detections by successes.

Considerations

- **Take special care to ensure subjectivity and consistency** - use elicitation methods, poll multiple SMEs, perform attacks and actually measure.
- **Compare costs of different methods to gather** – actual testing can be expensive, sometimes using SMEs can save money.
- **Avoid discussions of specifics with decision-makers** – decision-makers are just another SME among, hopefully, many you've used so don't let them draw you into arguments about specific values.
- **Make sure you know who will see the metrics** – you may need to rethink how you gather the metrics depending upon who will use them.

Vulnerability Metrics (1)
(aka Weakness-Based Metrics)

Vulnerability-based metrics count vulnerabilities found or weaknesses discovered.

- Examples include
  - Boolean (yes/no - is there a vulnerability?),
  - percentage of vulnerable platforms, and
  - reachability (is the weakness within reach of adversaries?).
- Counting vulnerabilities found or weaknesses discovered is made more relevant when used with adversary metrics to show which vulnerabilities could be exploited by adversary (or adversary model)
- One problem is overcoming unknown vulnerabilities:

"To those things Clausewitz wrote about uncertainty and chance, I would add … Participants in a war game would describe an unknown unknown as unfair, beyond the ground rules of the game. But real war does not follow ground rules, and I would urge that games be "unfair" by introducing unknown unknowns."

-Raymond B. Furlong, Lieutenant General, USAF (Ret.)

Clausewitz and Modern War Gaming: losing can be better than winning

1984, July

Vulnerability Metrics (2)
(aka Weakness-Based Metrics)

- Counting vulnerabilities found or weaknesses discovered is made more relevant when used with adversary metrics to show which vulnerabilities could be exploited by adversary (or adversary model)
  - without the adversary, this set of metrics is all known vulnerabilities,
  - but with the adversary this set of metrics is all known vulnerabilities that a particular adversary could exploit.
- The difficulty is that there is, inherently, an uncounted set of unknown vulnerabilities.
- V-b metrics are useful in conjunction with other metrics as well, such as attack-based metrics to
  - analyze the impact and efficiency of the adversary's attacks, or
  - determine how vulnerabilities should be prioritized for mitigation.

Vulnerability Metrics (3)
(aka Weakness-Based Metrics)

Vulnerability-based metrics

Vulnerability-based metrics count or measure vulnerabilities found or weaknesses discovered.

CONSIDERATIONS:
- Decide in advance when to stop looking for vulnerabilities.
- Do not share vulnerabilities out of context.
- Distinguish between vulnerabilities of technology, processes, and implementation.

EXAMPLES:
- Boolean existence (is there a vulnerability?).
- Percentage of platforms with the vulnerability.
- Reachability (can the attacker reach the vulnerability?).

SOURCES:

METHODS:
- Scan the system.
- Execute attacks against multiple systems.
- Characterize the system.

Considerations

- **Decide in advance when to stop looking for vulnerabilities** – there are always more to find, so you need to know when to walk away from the process. Automated tools make these easy to gather, but the tools will keep on looking long after you should have called a halt.
- **Don't share vulnerabilities out of context** – a vulnerability that the adversary can't use is less important than ones they can – context makes all the difference in whether the adversary can use the vulnerability.
- **Distinguish between vulnerabilities of technology, processes, and implementation** – the vulnerability type plays a large role in how easy it would be to correct – so be sure you know whether the problem is the technology, the way that technology is implemented, or the process in which it is used.

C Consequence Metrics (1)

Consequence-based metrics describe or measure the consequences that attend a successful attack.

- Examples include
  - number of deaths,
  - system downtime, and
  - nightmare consequences*.
- An approach to estimating a target's vulnerability to undesirable consequences is
  - brainstorm attacks, apply filters (key filter is adversary), and analyze countermeasures, then
  - measure security by determining what consequences cannot occur under adversary attack.

* The IDART™ red teaming methodology identifies the need to elicit nightmare consequences from sponsors during red team planning. Sometimes, during the course of an assessment, the red team identifies other previously unknown consequences that are of greater magnitude than what the customer has identified.

C Consequence Metrics (2)

An alternative approach to estimating a target's vulnerability to undesirable consequences:

1. Start with a set of consequences about which the sponsor cares, then determine how those consequences could occur by breaking them down into necessary conditions in an upside down attack tree*.
2. If the defenses preclude one or more necessary conditions for adversary progression or success up a particular attack path in the tree, then the defense can feel secure that the consequence at the top of the pathway is not reachable.
   - In a red team attack graph, this means proving that no path to an adversary goal is achievable - i.e., enough attack steps are proven impossible to preclude any path from attack starting point to objective/goal.

*For more info, see http://www.schneier.com/paper-attacktrees-ddj-ft.html

C Consequence Metrics (3)

Consequence-based metrics C

Consequence-based metrics describe or measure the consequences that attend a successful attack.

CONSIDERATIONS:

- Work with the customer to establish consequences of concern.
- Make sure the consequences can be measured.
- Try to equate different consequences.

EXAMPLES:

- Number of deaths.
- Downtime.
- Nightmare consequences.

METHODS:

- Interview target system staff.
- Assess results from models and simulations.
- Measure response under attack.

SOURCES:

Considerations

- **Work with customer to establish consequences of concern** – every customer and their situation is different and so are the consequences they care about. Even those consequences that are nearly universal can vary greatly in degree among customers.

- **Make sure the consequence can be measured** – some consequences of concern to a customer are nebulous (e.g., public confidence), so try to find a way to measure these consequences.

- **Try to equate different consequences** – consequences tend to be varied in units of measure – try to relate them to a single unit of measure. Even lives and loss of confidence can be translated to dollar costs.

Adversary Metrics (1)

Adversary-based metrics describe the adversary model the red team uses during the red team process.

- Example adversary commitment factors
  - intensity – stealth – time
- Example adversary resources
  - number of team personnel,
  - knowledge (technology, cyber, kinetic, etc.),
  - skill level,
  - quality and sophistication of tools, and
  - insider access.
- Adversaries may acquire specialized resources as required
- Consider money to be a resource multiplier, and not necessarily a stand alone resource
- Adversary metrics have significant overlap with *attack metrics*

Adversary Metrics (2)

- Adversary metrics have a significant overlap with attack metrics:
  - attack discovery metrics
    - adversary characteristics, resources, and costs necessary to identify and characterize an attack opportunity,
  - attack development metrics
    - adversary characteristics, resources, and costs necessary to develop an attack, and
  - attack execution metrics
    - adversary characteristics, resources, and costs necessary to execute an attack.
- Consider money to be a resource multiplier, and not necessarily a stand alone resource
  - money by itself doesn't do anything (except represent potential), and
  - adversary use of money (investments) can result in zero, positive, or negative gains for capabilities (skills, tools, personnel,etc.) and commitments (time, stealth, intensity).

Adversary Metrics (3)

Adversary-based metrics

Adversary-based metrics describe the adversary model the red team uses during the red teaming process.

CONSIDERATIONS:

- Use metrics that are consistent and relative through the adversary continuum.
- Choose metrics that you can find in current adversary intelligence.
- Try to use the same metrics and units as the attack metrics.

EXAMPLES:

- Knowledge or skill level.
- Number of team members.
- Tools or techniques.

METHODS:

- Review adversary intelligence.
- Analyze past activities.
- Compare to known adversaries.

SOURCES:

Considerations

- **Use metrics that are consistent and relative through the adversary continuum** – if your red-teaming will consider more than one adversary, try to use metrics that are common among the range of adversaries rather than pick something to measure that applies to only one adversary.
- **Choose metrics that you can find in current adversary intelligence** – use what is already known about the potential adversaries if you don't have the time, resources, or authority to gather intelligence about adversaries.
- **Ideally, adversary metrics should relate to attack metrics for risk analysis** – try to use the same units and measures as the attack metrics so the two can be related and analyzed against each other.

Protection-Based Metrics (1)

Protection-based metrics count or measure protection systems (extant or posited as countermeasures).

- If unknowns can't be counted, count the known - protections
- Examples include
  - number of security layers,
  - number of systems protected, and
  - number of compromises (e.g., daily, quarterly, annually).
- P-b metrics are perhaps most useful in conjunction with other metrics, particularly attack metrics
- An example of the non-measurable is the mapping between a known protection system and a set of unknown weaknesses

Protection-Based Metrics (2)

More on counting what can be counted, a network security example:

- IT Security might count the following:
  - number of firewalls,
  - the number of firewall rules,
  - the number of open ports in the firewalls,
  - cost of buying the firewalls,
  - the cost of maintaining them, and
  - how many connection attempts are rejected by the firewalls.
- Some objective metrics, like number of firewalls are purely quantitative, while
- Other objective/quantitative metrics, like the number of rejected connections, benefit from qualitative analysis resulting in a mixed metric that is both objective and subjective
- IT Security may attempt to count the quality of their firewall - beware

P Protection-Based Metrics (3)

Protection-based metrics

Protection-based metrics count or measure protection systems (extant or posited as countermeasures).

CONSIDERATIONS:

- Include less obvious, unconventional measures of protection.
- Assess whether the protections actually protect the targets of interest.
- Pay close attention to what, why, and for whom you measure protections.

EXAMPLES:

- Percentage of systems protected.
- Number of protections/layers.
- Number of incidents/ compromises.

METHODS:

- Review interviews and documents.
- Count actual protections.
- Compare red and blue views.

SOURCES:

Considerations

- **Don't rely on just the obvious ways to beat protections** – there's the conventional and then there's the unconventional – calculate the time to pick the front door lock and record the fact that the back door has no lock – count the number of firewalls, and count how many have wide-open policies.
- **Do the protections secure targets of interest?** – early red team experiments showed that placement of network protections make a big difference in effectiveness.
- **Pay close attention to what, why and for whom you measure protections** – protections can be hard to measure correctly for the purpose and audience.

Threat-Based Metrics (1)

Threat-based metrics describe the degree of threat and are calculated using combinations of the other metrics cited here.

- Threat-based metrics imply a composite calculation using *consequence, vulnerability, protection*, and *adversary-based metrics*
- T-b metrics are calculated from the defender's point of view – the assets to be protected are those important to the defender, not necessarily those important to real adversaries
- Examples include
  - expected cost to repair damage,
  - number of systems expected to be affected, and
  - estimated mean time to restore services.

Threat-Based Metrics (2)

- T-b metrics are calculated from the defender's point of view – the assets to be protected are those important to the defender, not necessarily those important to real adversaries
- Cautionary notes:
  - beware the sponsor's view of what metrics need to be collected; the red team may find itself planning to capture data on a target that is of relative unimportance to their customer,
  - the lack of adversary modeling (red teaming w/o an adversary model) could be interpreted by some to mean the threat may not be real, and
  - the red team must be able to communicate
    - that the model adversary may have no intention of attacking an asset important to the defender, and
    - why they think the real adversary would not.

Threat Based Metrics (3)

Threat-based metrics

Threat-based metrics describe the degree of threat and are calculated using combinations of the other metrics cited here.

CONSIDERATIONS:

- Make sure the constituent metrics are consistent and objective.
- Assume the adversaries will apply their resources creatively.
- Ensure the threat is real to the decision makers.

EXAMPLES:

- Expected cost to repair damage.
- Expected number of systems affected.
- Mean time to restore services.

METHODS:

- Repeated simulation of attack.
- Calculation from other collected metrics.

SOURCES:

*All other things being equal, the adversary will choose the path of least resistance - that is what we mean by “lazy adversaries.”

Considerations

- **Make sure the constituent metrics to threat are consistent and objective** – remember: “garbage in, garbage out.”

- **Assume the adversary is creative with their resources** – adversaries are lazy* but creative; they will bypass protections with limited resources.

- **Ensure the threat is real to the decision-makers** – measuring the threat will accomplish nothing if the decision-makers don’t believe it.

Questions?

Section Two Exercise

- As the red team, you collect data to determine which attack path your burglar adversary should pursue.

(Collect data to address the target metrics)

- **Exercise: In your group, determine what data you would collect and how.**