THE ASSESS OUTSIDER MODULE WITH MULTIPLE ANALYSES

Mark K. Snell, Alfred E. Winblad
Sandia National Laboratories
Albuquerque, New Mexico USA

SAND--90-0714C
DE90 013312

Bryan Bingham, Brad Key, and Scott Walker
Science & Engineering Associates, Inc.
Albuquerque, New Mexico USA

ABSTRACT

The Analytic System and Software for Evaluating Safeguards and Security (ASSESS) includes modules for analyzing vulnerabilities against outsider and insider adversaries. The ASSESS Outsider Analysis Module has been upgraded to allow for defining, analyzing, and displaying the results of multiple analyses. Once a set of threat definitions have been defined in one Outsider file, they can be readily copied to other Outsider files. This multiple analysis, or batch, mode of operation provides an efficient way of covering the standard DOE outsider threat spectrum. A new approach for coupling the probability of interruption, P(I), values and values calculated by the ASSESS Neutralization module has been implemented in Outsider and is described. An enhanced capability for printing results of these multiple analyses is also included in the upgraded Outside module.

DISCLAIMER

INTRODUCTION

The ASSESS Outsider Analysis (Outsider) Module is part of the Analytic System and Software for Evaluating Safeguards and Security (ASSESS) developed under contract to the U.S. Department of Energy [1]. Outsider calculates the vulnerability of facilities defined in the ASSESS Facility Description (Facility) module to intrusion by outsiders. All ASSESS modules run on IBM-PC compatible computers within Microsoft Windows(TM), a graphical user interface. More information on ASSESS is found in some earlier references [2-6].

The Outsider Analysis Module has been upgraded to make it easier to set up and run the many outsider analyses required to determine protection levels and to identify and test potential upgrades against a realistic spectrum of threats.

SCOPE OF AN ASSESS OUTSIDER ANALYSIS

Before running Outsider, the analyst uses the ASSESS Facility module to define a file describing protection around a target. Each target requires a separate facility file.

For a given facility file, Outsider calculates the probability of interruption, P(I) for different types of outsider intruders. In ASSESS the probability of system win, P(W), for outsider adversaries is currently determined by conditioning on the interruption event: P(W) is the product of the probability of

interruption, P(I), and the probability of neutralization, P(N). P(I) is the probability that the security force at a facility can respond to an alarm and interrupt intruders before the complete their mission, while P(N) is the probability the response force can neutralize the intruders once interruption occurs.

A considerable number of outsider analyses may be required for each facility file. Adversary attacks can be classified as overt or covert. Adversaries attacking a facility covertly minimize detection until they are detected; they then minimize their delay along the rest of their path. There are 10 types of adversaries included in ASSESS, each requiring a separate analysis for covert attacks. Adversaries are defined by the kind of equipment they carry and use to penetrate the facility. Equipment includes hand tools, power tools, high explosives, small arms, light anti-tank weapons, land vehicles, and helicopters. Adversaries attacking overtly attempt to kill as much of the security force as possible and to disable the protection system with no regard for detection; two additional analyses are required to cover overt attacks.

These 12 analyses should be repeated when protection changes such as from day shift to off-shift. Each facility file carries information about two facility states, each with different protection such as day and night-shift so this doubles the number of analyses to 24 for a given facility file.

Further analyses beyond this basic 24 are generally required. As we shall see below, several analyses must be performed to produce better P(W) estimates for each of the basic 24 analyses.

Additionally, the analyst may also wish to perform analyses to compare denial or containment response strategies for protecting the target. Denial means the response force must interrupt adversaries before they reach the target - successful denial prevents sabotage. Containment means the response force must interrupt adversaries sometime before they leave the facility - successful containment prevents adversaries from stealing the target.

MEASURING SYSTEM EFFECTIVENESS

The measure of protection system effectiveness against a given adversary type is the probability of system win, P(W) for the most-vulnerable path through the facility. For outsider threats, P(W) is the probability that adversaries are detected, correctly assessed, interrupted, and neutralized before they can complete their mission. The most-vulnerable path is the path with the lowest P(W).

Outsider computes P(I) for a path as the probability of timely detection, that intruders are detected early enough on that path so that time left after detection exceeds the response force time (RFT). RFT measures how long it takes after an intrusion is correctly assessed for the response force to deploy and interrupt the forward progress of the intruders. Detection must occur at or before the Critical Detection Point (CDP) in the path, or else the intruders can complete their mission because the response force cannot deploy fast enough to interrupt them.

Figure 1 shows how the RFT, CDP, and P(I) are related. RFT is measured back from the end of the path by summing the delays (t_6+t_5+t_4...) provided by barrier safeguards and transit times. The point in the path where the adversaries require greater than RFT seconds to complete is the CDP. Detection safeguards (p_1, p_2, etc.) at CDP and back up the path to the beginning provide useful detection; their accumulated probability of detecting the intruders is P(I). The difference between the actual time, TR, to finish the mission starting at CDP and the RFT is called the Time Remaining After Interruption (TRI).

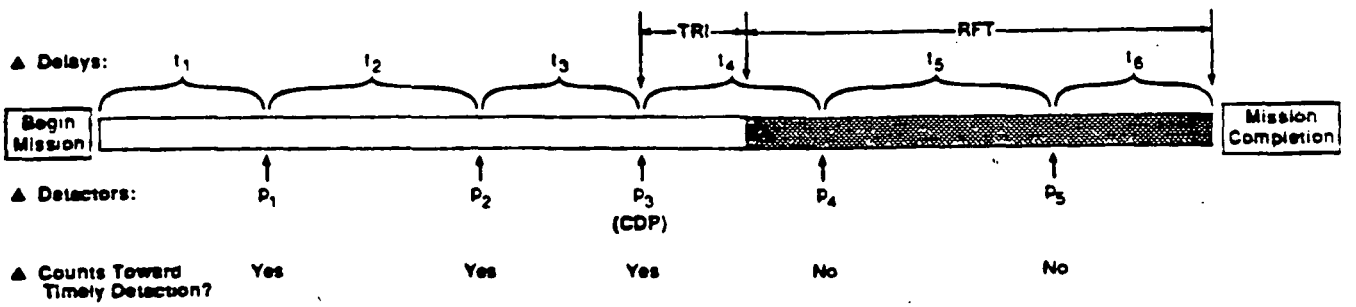

Figure 1. Timely Detection Timeline

Outsider determines the path through the facility with the lowest P(I), while the ASSESS Neutralization Analysis (Neutralization) Module computes P(N). These two modules do not necessarily find the path with the lowest P(W) because P(N) is also a function of the path taken: as the path varies different responders may be engaged and different numbers of adversaries may be busy defeating barriers or detectors. Therefore, the path with the lowest P(I) is not necessarily the path with the lowest P(I)*P(N) product.

It has been pointed out [7] that the engagement model in Neutralization is best used for modeling neutralization for a

specific scenario along a specific facility path because the analyst can more clearly determine where and when combatants can engage.

Focusing on a scenario allows a better estimate of P(W) by conditioning on when the adversary is detected and assessed on the path, which is more specific than conditioning on timely detection. Let P(Ei) denote the probability that the adversary is first detected and correctly assessed at the ith detection location on a path and P(Ni) be the probability that the adversary is neutralized given first correct assessment at the ith detection location. If there are m detection locations along a path,

$$P(W) = P(E1)*P(N1) + P(E2)*P(N2) + \ldots + P(Em)*P(Nm). \quad (1)$$

1-P(Ei) is the probability that the adversary is not detected, or if detected not correctly assessed, at detection locations 1,...,i. This is usually computed as a product of nondetection or assessment probabilities for each of the locations 1 to i. P(Ni), determined in Neutralization, will vary with i because the earlier the adversary is detected the longer he must stay at the facility to complete his path, allowing more response forces to arrive. Thus, P(Ni) is a function of the remaining path delay given first correct assessment at the ith detection location. For instance in Figure 1, if an adversary is detected at P1, then he can not leave the site before $t_2+t_3+t_4+t_5+t_6$ seconds have gone by but if detection occurs at P5 then he can leave after just t_6 seconds.

Harris et al.[7] suggest simplifying the calculation in (1) by including only 1 to 3 detection locations with the highest detection probabilities before the CDP.

The ideal solution to finding the most-vulnerable path is to compute P(W) for each path in the facility directly using (1) or some simpler variant and then report the most-vulnerable path as the path with the lowest P(W). This is often impractical however.

If the facility protection is unbalanced and there are only a few paths with a low P(I), the analyst could first determine the low-P(I) paths using Outsider and then use (1) to determine P(W) along each of these low-P(I) paths. As facility protection improves this becomes more and more difficult. A more general solution is necessary.

Suggested Approach for Obtaining a Practical P(W) for each Threat

When it is impractical to determine the most-vulnerable path and its P(W) directly, we suggest using a simple but conservative estimate of P(W) based on the equation P(W) = P(I)*P(N). The analyst first determines a P(N) from Neutralization that is conservative for all paths. The most vulnerable path is then that path Outsider has determined as having the lowest P(I); P(W) is the product of P(I) for this path and this "worst-case" P(N). Though this method produces adequate P(W) estimates, these will underestimate P(W) because P(N) is "worst-case."

The analyst could improve on this P(W) estimate by requiring P(N) to be conservative only for paths with a low-P(I), rather than all paths. Another approach for obtaining a more realistic P(W), outlined below, is to vary the RFT used to calculate P(I).

Before showing how P(W) is determined for different RFTs, we will show how RFT is related to the model used in Neutralization. Neutralization models a two-sided small-arms engagement between adversaries and response forces using a different timeline called the engagement timeline. The engagement timeline (Figure 2) begins when an alarm is received. It then accumulates assessment, communications, and deployment times to determine the arrival times of response forces. Figure 2 shows the engagement timeline for two contingents, each contingent being formed by one or more Security Inspectors that arrive at the same time. The first contingent arrives at T3 and the second T4. The arrival time for a contingent defines the beginning of an engagement event, with Event 1 starting when the first contingent arrives.

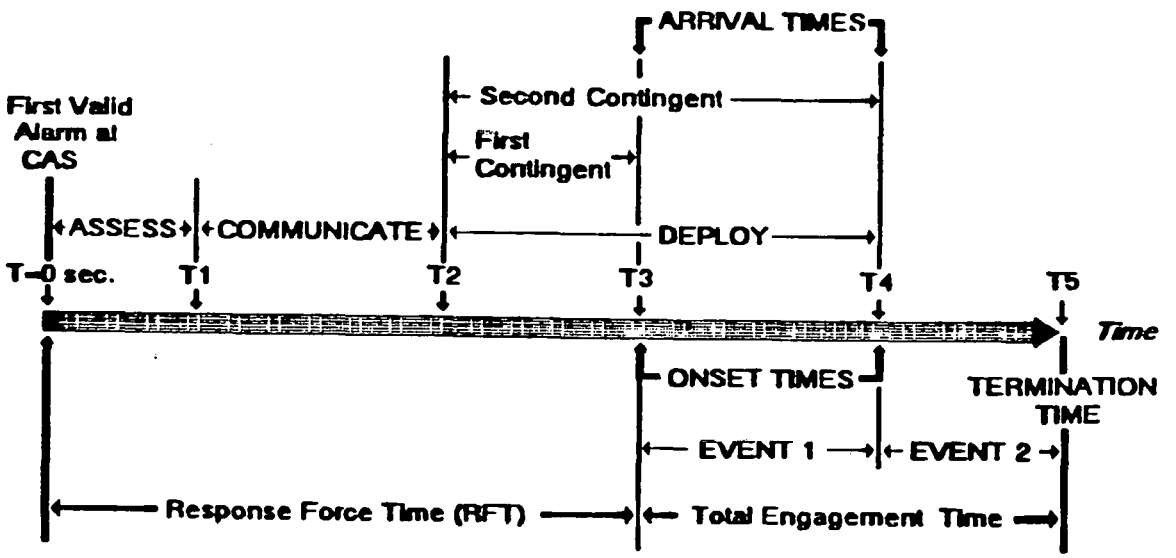

Figure 2. Neutralization Engagement Timeline

Neutralization makes certain assumptions about when adversaries and response forces engage. Adversaries engage the first contingent arriving at the beginning of event 1 and stay engaged until they are neutralized or successfully complete their mission. Contingents arriving later reinforce the first contingent and are engaged as they arrive, at the beginning of later events.

To set up a Neutralization analysis the analyst enters the timeline data and describes how many adversaries there are and the size of the response contingents, along with armament, tactics, and exposure. Different threats will therefore need different Neutralization analyses.

RFT is generally equal to the arrival time of some contingent because interruption occurs when just enough response forces have deployed to impede the forward progress of the intruders. In this particular example, there are two possible RFTs, RFT 1 (T3 time units) and RFT 2 (T4). RFT 1 is indicated in Figure 2.

When there are several possible RFTs, the analyst can produce better global P(W) estimates by calculating P(I)*P(N) for the various RFTs and choosing P(W) as the best product. This is illustrated in Figure 3. At the larger RFT, RFT 2, P(I) is lower because detection at P3 is no longer timely. However, as RFT becomes larger, the longer adversaries will take to complete their mission after correct assessment at the CDP, resulting in a generally larger P(N). In the example, the adversary must remain for at least $t_3+t_4+t_5+t_6$ for RFT 2 versus $t_4+t_5+t_6$ for RFT 1. P(N) may change drastically if the first contingent is very easy

to defeat while the second is more formidable. Then detection at the CDP for RFT 1 (P3) would allow the adversaries to defeat the first contingent easily and escape before the second contingent arrived. For RFT 2, detection at the CDP (P2) or before would give the second contingent time to arrive before the adversary completed his mission; the adversary could not quit early even though the first contingent was defeated.

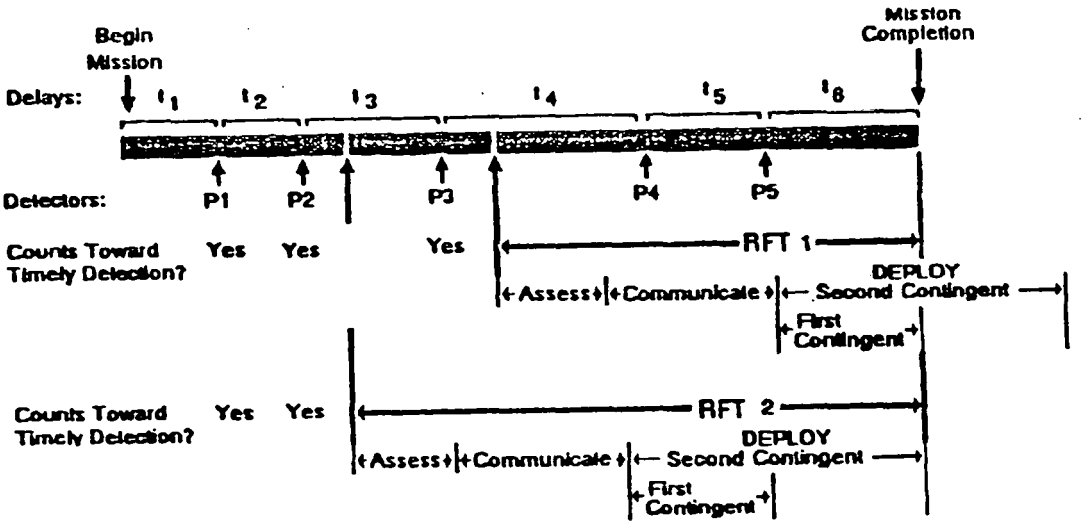

Figure 3. Calculating P(I)*P(N) for Several RFTs

Define P(N|t) as the probability of neutralization given that the adversary cannot quit the engagement until time t along the engagement timeline. Then for the example in Figure 3, P(W) could then be set as the greater of P(I|RFT 1)*P(N|RFT 1) and P(I|RFT 2) *P(N|RFT 2). To do so, the analyst would first calculate P(N|RFT 1) and P(N|RFT 2) in Neutralization by specifying that the

adversaries could not quit until time RFT 1 and RFT 2 respectively. Table 1 shows the two Outsider analyses that would then be defined for the given threat, a terrorist group on foot. Each P(N) would be tied to a separate analysis. Once these analyses were finished, Outsider would display P(I)*P(N) for each and the analyst could pick the best product as P(W). If there had been three possible RFTs, the analyst would look at the larger of P(I|RFT)*P(N|RFT) for the three RFTs.

Table 1

Analyses Compared to Find Best P(I)*P(N)

Analysis	Threat	Number of RFTs	RFT Range	P(N)
1	Terrorist on Foot	1	RFT 1	P(N|RFT 1)
2	Terrorist on Foot	1	RFT 2	P(N|RFT 2)

Other, less conservative estimators of P(W) exist that use the same data (P(I) and P(N) for the different RFTs) but these are more complicated and do not necessarily allow the user to identify a most vulnerable path.

In producing a "worst-case" P(N) estimate, note that the analyst should not reduce the adversary attack team size to account for adversaries defeating barriers or detectors. In some cases this is an unrealistic assumption but the Neutralization model cannot model this detail in a general fashion across several paths.

Certain paths may have Security Inspectors stationed on them and others not; to be conservative, the analyst should not include these inspectors in the Neutralization model because the adversary might attack along a path bypassing these posts that has a P(I) close to the minimum but a much lower P(N).

THE OUTSIDER ANALYSIS MODULE

The new Outsider allows the user to define, conduct, and save the results of up to 99 analyses in each outsider file. This vastly reduces the effort of creating and tracking ASSESS outsider files: previously, a different outsider file had to be defined for each analysis. Several analyses can now be defined at one time, leaving the analyst free to do other tasks while the analyses are being performed.

If a site building has several targets, each with the same response strategy, then the analyst can define a common set of analyses to be used at all targets in that building. These common analysis settings can be imported for use with each facility file, relieving the analyst from having to re-enter this data.

Each outsider analysis can be thought of as a layer, with the analyst only being able to see one layer at a time. Figure 4 shows the Outsider application as it might look after analysis has been completed. The current analysis, analysis 1, is being displayed. A Control Panel displays analysis settings, and three support windows, Diagram, Results and Graphs, display analysis results for analysis 1. Each support window can be moved and

sized independently inside the main window. Outsider provides both mouse and keyboard control.

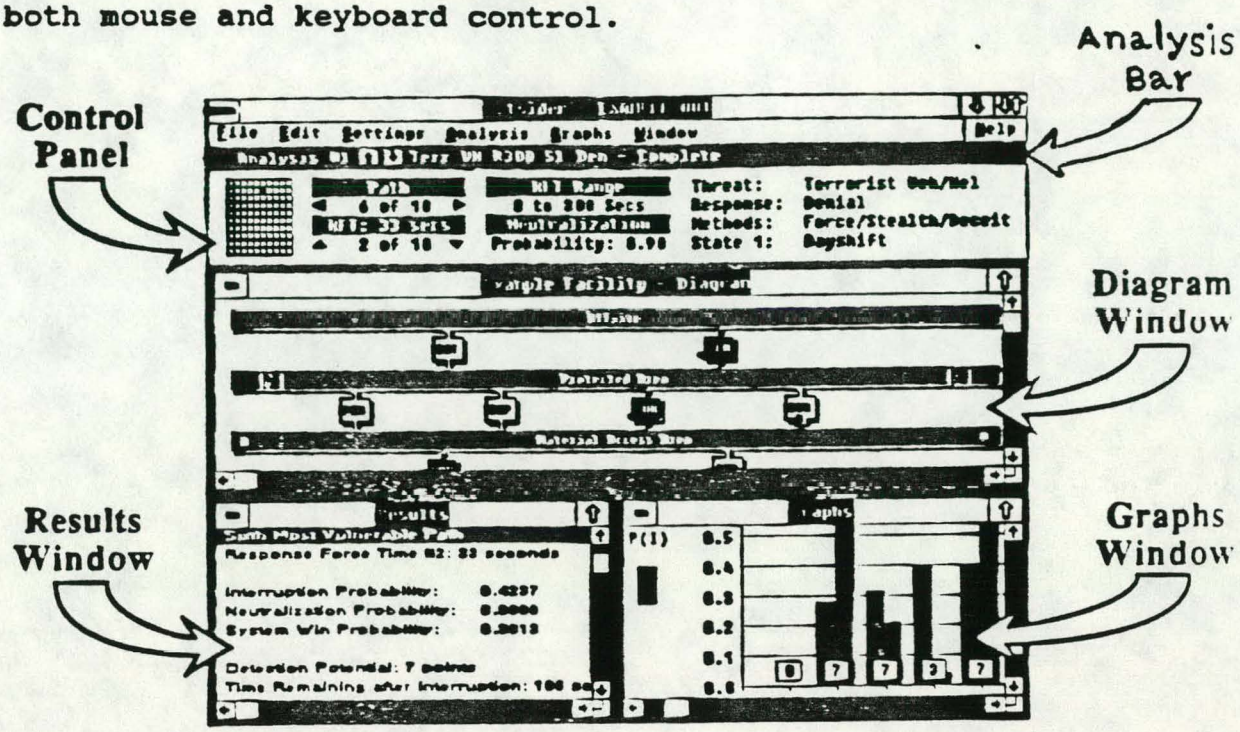

Figure 4. The Main Outsider Analysis Screen

After starting Outsider, an analyst can load a physical protection system description (facility file) created in the ASSESS Facility module or a previously saved outsider file. The protection system, in the form of an Adversary Sequence Diagram (ASD), appears in the Diagram window. After analysis settings have been defined, the desired analyses can be run. When an analysis is complete, the Control Panel (Figure 5) is used to select any path and see it highlighted on the Diagram. A detailed textual description of the path including intrusion methods and individual safeguard performance values is shown in the Results window. The Graphs window displays user-selectable information about sets of paths for a single analysis, including a graph of the protection

system's sensitivity to response force deployment time. After reviewing the analysis results, the analyst can save them to a file, print reports, create a collusion analysis support file, or modify settings and re-analyze.

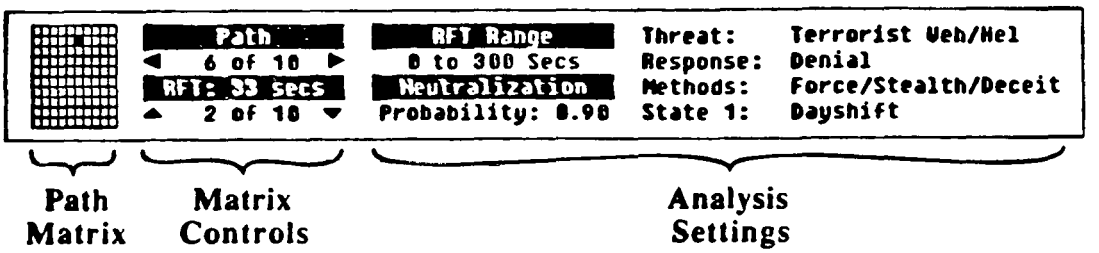

Figure 5. The Outsider Analysis Control Panel

Entering Analysis Data

To define a new analysis, the analyst selects the Define Analysis dialog box (Figure 6), and selects the new button. An Analysis dialog box then appears (Figure 7) that has all the analysis variables for the user to edit. The user can name each analysis and include a short memo to describe it further. The name entry serves as a convenient place to summarize analysis data.

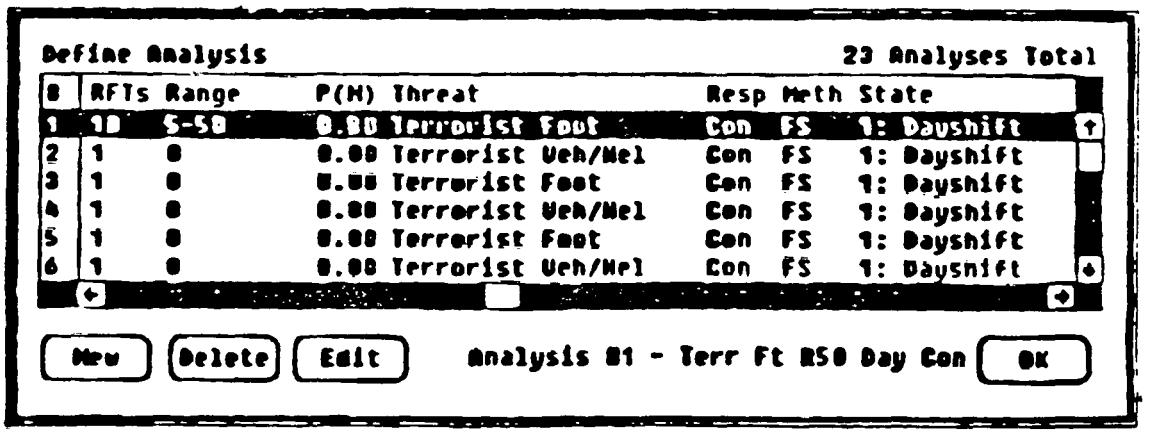

Figure 6. Define Analysis Dialog Box

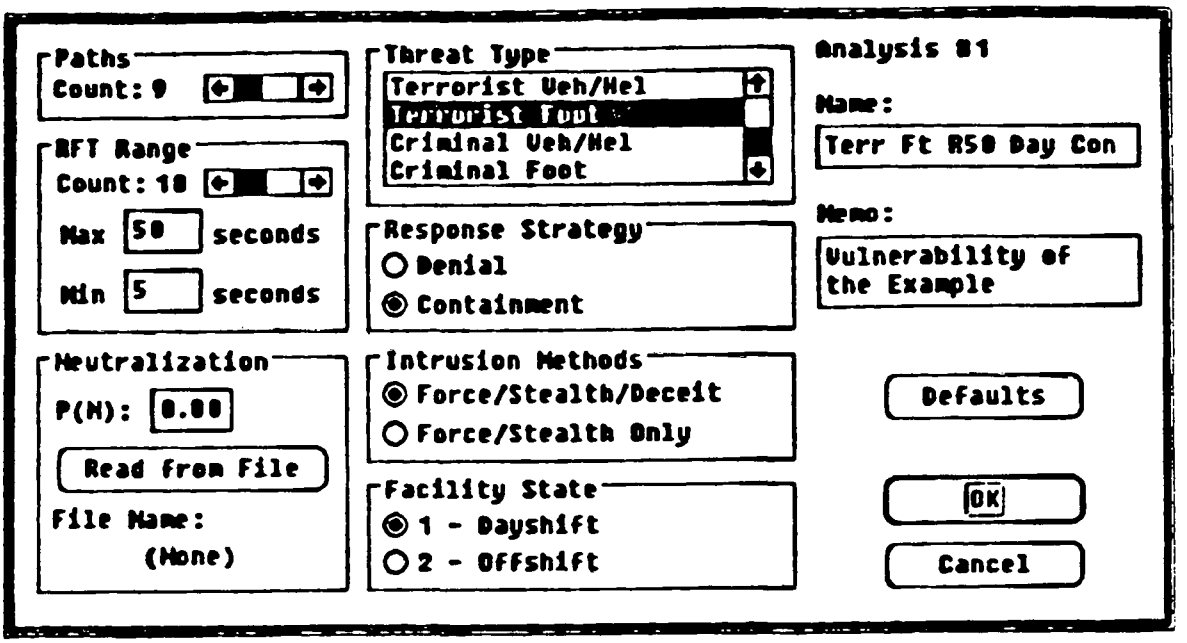

Figure 7. Analysis Dialog Box

The analyst can also specify how many of the most-vulnerable paths to collect, ranging from just the most-vulnerable path up to the 10 most-vulnerable paths. Results can be calculated for up to 10 RFT values, equally spaced between the minimum and maximum values.

A single Neutralization P(N) can be entered for each analysis so that P(W) can be calculated automatically once P(I) is computed. This P(N) can be imported from a specific neutralization file or the analyst can type it in directly. Note that if P(N) differs for different RFTs separate analyses should be defined for each different P(N).

The analyst also chooses from a list of ten adversary types and specifies the Response strategy as denial or containment. Either Facility State 1 or 2 can be specified for analysis.

The Methods setting indicates the methods the intruders can use to penetrate the facility. The two choices are Force/Stealth and Force/Stealth/Deceit. Force/Stealth means intruders use violence, tools, and explosives to penetrate the facility; Force/Stealth/Deceit means intruders can also attempt to penetrate the facility using falsified credentials and smuggling contraband equipment, whenever it is to their advantage to do so.

Settings for an existing analysis can be redefined by selecting that analysis in the Define Analysis dialog box and selecting the Edit button or by moving to that analysis using the up and down arrows on the analysis bar (Figure 4) and using the Control Panel or menu to alter parameters.

Reviewing Results

The user can move between completed analyses by using the up and down arrows on the analysis bar or can move directly by using the select dialog box.

Once the desired analysis is on the screen, the Control Panel's Path Matrix can be used to select from the most vulnerable intrusion paths for a completed analysis. The Path matrix columns represent the most vulnerable intrusion paths. The analyst may request that up to 10 of the most vulnerable paths be identified.

Each row of the matrix represents a single response force time from the specified range, which may also have as many as 10 RFTs. Therefore, the Path Matrix can be as large as 10 by 10. The Path matrix controls indicate the number of requested paths and RFTs as well as the current highlighted path in the matrix. All data associated with the highlighted path is displayed automatically in the Diagram, Results, and Graphs windows. Using these controls, the analyst can efficiently review the vulnerability of all paths in the matrix.

The Results window shows a detailed description of the selected path, including which path elements have been defeated, the intrusion method (force or deceit) at each element, the delay and/or detection at each safeguards component at a path element, and how the adversary defeated each component. In this new version of Outsider we also show which safeguards were not installed, but could have been, to help the analyst upgrade the facility.

Printing has also been improved. The analyst can ask for a vulnerability summary to be printed out that displays P(I), P(N), and P(W) for the different analyses. The analyst has more control over the level of detail to print about each path description, there being three levels of detail: 1) just P(I), P(N), P(W) level of information; or 2) description down to the path elements in the adversary path; or 3) description down to the level of which components are defeated at each path element.

The analyst can also control which paths for a given analysis will be included in the vulnerability summary or path description. All paths can be printed for a given analysis or just one (most-vulnerable or user-selected).

Other New Features

ASSESS contains another module that analyzes protection against hand-off collusion [6] by insiders and outsiders, where a non-violent insider moves material from a target to some other facility area where the material is hidden for later pickup by an intruding outsider group. One other function of Outsider is to produce vulnerability data for this Collusion module. Previously, preparing this collusion data in Outsider would overwrite the normal analysis, destroying data if the analyst had not saved it previously; now this calculation is done separately.

SUMMARY

The ASSESS Outsider Module has been upgraded so that up to 99 analyses can be stored in one Outsider file, drastically reducing the file management problem and allowing the analyst to set up sets of analyses at one time. Analysis settings from one file can be imported to another, to cut down on re-entering data.

An analysis process was also described for finding conservative estimates of the Probability of System Win for the most-vulnerable path through a facility.

REFERENCES

[1] An Overview of ASSESS - Analytic System and Software for Evaluating Safeguards and Security, T.D. Cousins, R.A. Al-Ayat, and J.C. Matter, INMM 30th Annual Meeting Proceedings, 1989.

[2] The ASSESS Facility Descriptor Module, Sabina Erteza Jordan, Alfred Winblad, Brad Key, Scott Walker, Therese Renis, and Richard Saleh, INMM 30th Annual Meeting Proceedings, 1989.

[3] A Comprehensive Method for Evaluating Safeguards Against the Insider Threat, R.A. Al-Ayat, T.A. Renis, R. Saleh, and C.J. Patenaude, INMM 30th Annual Meeting Proceedings, 1989.

[4] The ASSESS Outsider Analysis Module, Alfred Winblad, Mark Snell, Sabina Erteza Jordan, INMM 30th Annual Meeting Proceedings, 1989.

[5] The ASSESS Adversary Neutralization Module, Bill Paulus, Sabina Erteza Jordan, Martha Moore, and Junko Mondragon, INMM 30th Annual Meeting Proceedings, 1989.

[6] The Hand-Off Collusion Module of the ASSESS Program, Bill Paulus, Sabina Erteza Jordan, Martha Moore, and Junko Mondragon, INMM 30th Annual Meeting Proceedings, 1989.

[7] Neutralization for SAVI Evaluation of Security System Effectiveness, L. Harris, Jr., L.A. Goldman, G.D.Smith, K.J.Anderson, INMM 30th Annual Meeting Proceedings, 1989.