Proceedings of the 2005 IEEE
Workshop on Information Assurance and Security
United States Military Academy, West Point, NY

IA Risk Assessment Process

Kenneth Montry, The Boeing Company (Presenter)
P.O. Box 3707
Seattle, WA 98124-2207
Phone: (253) 657-1221 Fax: (253) 773-5021
kenneth.j.montry@boeing.com
Richard Kelley, The Boeing Company

I. Introduction

When considering the Information Assurance (IA) requirement against a particular program, one must consider the actual risk that needs to be mitigated by any proposed solution. Understanding the actual risk and applying only those solutions deemed necessary will provide a best value approach to the customer. This paper defines one method to gain an understanding of IA risk by exploring the threats applicable to the system, the paths down which those threats can act and the effects of that action on the system given the environment in which the system currently exists. Considering all of those factors will allow a relative risk to be assigned for each applicable intersection.

II. Defining the Process

The steps required to complete this process are:

1. Define the system attributes
    a. Enclaves
    b. Environments
    c. Threat Vectors
    d. Threats
    e. Threat Effects
    f. Scenarios
2. Define the Risk Evaluation Attributes
    a. Probability of Occurrence
    b. Consequence of Occurrence
3. Perform Baseline Risk Analysis
4. Perform Gap Analysis, Part 1
5. Identify Embedded Solutions
6. Perform Embedded Solution Risk Analysis
7. Perform Gap Analysis, Part 2
8. Identify New Solutions
9. Perform Final Risk Analysis
10. Document Residual Risk

The first step in the process is to define the key attributes of the analysis identified in step one above, and described below. Once these are defined, the threat matrix development can begin.

Ken Montry is a Systems Engineer and Rick Kelley is an Associate Technical Fellow, both work for Integrated Defense Systems at The Boeing Company.

0-7803-9290-6/05/$20.00 ©2005 IEEE.

Enclaves – the collection of individual computing environments in the system under the control of a single authority and security policy. There may be more than one enclave in a system. An important aspect is understanding where the external interfaces are defined, often referred to as defining the enclave boundaries.

Environments – the different phases a program may go through during development and deployment. The environments may consist of development, pre-mission, during the mission, post-mission, maintenance, training and sustainment. Any given environment may cross one or more enclave boundaries.

Threat Vector – a path down which a threat may act. This may or may not be a vulnerability of the system. Consider every aspect of the steps that are taken to develop, operate and maintain the system. Threat vectors will likely be applicable to more than one of the environments.

Threats – entities that can act on the system, utilizing one or more of the threat vectors, to cause an IA incident. The threats to a military system may be identified in a System Threat Analysis Report (STAR) or Threat Environment Description (TED), but these may not be the complete set of IA Threats against the system. Additionally, there should be an IT Threat Document listed as being applicable to any system that has IA requirement(s).

Threat Effect – the outcome of an IA incident affecting the availability, integrity, authentication, confidentiality, and non-repudiation of a system. Each of these effects may have either a malicious or accidental intent.

Scenarios – scenarios take into consideration all aspects of the exploitation process: environment, vector, threat and effect. The scenarios are developed in concert with the risk assessment.

A. Initial Threat Matrix Development

Using the information developed above, population of the risk evaluation matrix can begin, evaluating each threat/effect combination for a particular vector. Listing the Threat Vectors vertically (one per row), with each Threat/Effect combination as sub-elements (each in their own row) allows a matrix to be developed to assess the risk of each of these elements.

III. Define The Risk Spectrum

Identify the risk spectrum by determining the scales of both probability of occurrence and consequence of occurrence as described below.

Probability of Occurrence - Relying on government provided data on probabilities of occurrence results in a large amount of overhead. Instead, assigning a probability of occurrence based on a relative scale, where the probability of each scenario occurring is relative to all of the other scenarios is the best approach. Consideration needs to be given to the ability of the scenario to realistically occur, and based on that, what is the likelihood that it will happen to the system being analyzed.

Consequence of Occurrence - The consequence of occurrence is unique to each system. The consequence needs to consider the effect on the system in question as well as impacts to its role in the battle space. In general, consequences are not affected by a mitigation implementation, the consequence could still be realized, the mitigation just lowered the probability of this event occurring.

Risk Factor - The risk factor is the probability of occurrence multiplied by the consequence of occurrence.

IV. Risk Analysis

First determine the relative probability of the event occurring. If doing this at the same time as developing the scenarios, it will help identify why a certain scenario may be weaker than another possible scenario for that intersection. Once the probability has been determined, the consequence rating can be assigned and the risk factor calculated. Not every intersection will have a risk rating. There may be instances where a threat acting down a vector in one environment is not applicable to one or more of the other environments for that vector. It may also be that a certain effect is not applicable to one or more of the environments. Performing the initial risk analysis without taking into consideration features embedded in the baseline system that may mitigate the risk will lead to more comprehensive analysis of the risk to the system, as well as providing potential trade space in the future.

Gap Analysis, Part 1 - This step identifies the areas where additional IA mitigation is required. Evaluating the risks by looking at the threat vectors across each environment will provide a different view than by sorting by threat. It may become apparent that there are some vectors that contain few or zero Very High or High risk rankings, while others contain many. The combination of risks in the vectors themselves may point to certain mitigations that either need to be considered, or can be pushed lower on the priority list. When sorting by Threat, it may become apparent that one or two particular threats acting on the system pose a much greater risk than any of the others.

Evaluation of Embedded Solutions - Consider not only features of the baseline design and architecture, but also procedures and training used by the operational community. Make a list of all the embedded solutions in the system in question and perform second risk assessment to identify the actual IA risk of the system given the baseline design and architecture.

Gap Analysis, Part 2 - essentially identical to the first gap analysis described above. In most cases, compliance with standard security requirements on a program along with application of best business practices in design will mitigate many of the risks. Standard processes and procedures combined with training will mitigate many others, so there should be much less risk to mitigate to achieve an acceptable final solution.

Identification of New Mitigations - identify the new design solutions that will mitigate the residual risk to a level that can be accepted by the DAA. A combination of hardware, software, procedures and training may provide the best value solution. In the selection of mitigation approaches, it is important to consider known and potential vulnerabilities contained in the solution itself. If vulnerabilities are present in the solution, the amount of risk that solution actually mitigates must be understood and adjusted accordingly.

Development of Residual Risk - Allocate the solutions identified above to the remaining risks and make one more pass through the risk matrix. This may be an iterative process to achieve an acceptable level of residual risk.

V. Summary

The IA Risk Analysis Process provides a clear, step-by-step method to achieve a best value Information Assurance solution to the customer for a given program. In completion of the process, the necessary detail is developed to support documentation and justification of a program's IA posture in the SSAA.

Following these steps develops a comprehensive analysis of the Information Assurance risk on the program, and the design solutions required to provide an acceptable level of residual risk to the operational community. The result is a quality product that can be completed with a reasonable amount of effort and in a reasonable amount of time