SAND2015-0989R

Department of Homeland Security

This page left blank intentionally

Homeland Security

Science and Technology

TRANSITION TO PRACTICE (TTP)

Path Scan

OPERATIONAL DATA-BASED TEST REPORT

VERSION 2.0.1

U.S. Department of Homeland Security (DHS)
Science and Technology Directorate (S&T) Cyber Division
CM/LANL/Path Scan/PI&E/TR/R2.0.1/2015

February 13, 2015

Points of Contact:
DHS Sciences and Technologies Transition to Practice Program Manager
Mike Pozmantier

T&E Report prepared by
Sandia National Laboratories
Steven Hurd

United States Department of Homeland Security

Science and Technology Directorate

Transition to Practice Test and Evaluation Program

This document is owned by DHS S&T Cyber Division. Modifications to this document should be provided to S&T for their concurrence and release. Distribution of this document must be approved by DHS S&T.

Technical Document Disclaimer

THIS REPORT DOES NOT CONSTITUTE CERTIFICATION OF THE TECHNOLOGY BY THE DHS S&T CYBER SECURITY DIVISION OR BY SANDIA NATIONAL LABORATORIES.

Table of Contents

Table of Figures

Table of Tables

1 EXECUTIVE SUMMARY

1.1 TTP Program Overview

The TTP program is managed by DHS S&T Cyber Division and facilitates the transition of technology from the research lab to the Homeland Security Enterprise. It serves as a connection point for cyber security researchers, the Federal Government, and the private sector. Technologies targeted are those that are likely to transition successfully to the commercial market and expected to have notable impact on the cyber security of our Nation's networks or systems. The test element of the TTP program aids in the technology transfer process and is not intended to be adversarial. Additional information on the TTP program and the iterative process used can be found in Appendix A - TTP Program Overview.

1.2 Technology Tested

The technology to be tested is Path Scan, provided by Los Alamos National Laboratory [1].

1.3 Testing Results

With only one notable exception, Path Scan performed well in detecting these anomalous inserted connections. The exception can be considered to be a "corner case", where other tools may identify the anomaly.

Table 1: Summary of Test Results

Test Case Number	Test Case Title	Test Case Status	
		Complete	Type
TC1.1	Adding sequential paths	Y	F
TC1.2	Create an inbound star	Y	F
TC1.3	Create an outbound star	Y	F
TC1.4	Add sequential paths that terminate into a created outbound star	Y	F
TC1.5	Add sequential paths that terminate into a created inbound star	Y	F
TC1.6	Adding Sequential Paths, using specified types of hosts	Y	F

Table 2: Legend of Symbols and Abbreviations

Symbol	Description
Y	Test goal complete Yes, or use %
TBD	To be determined
N/A	Not applicable
Test Case Number	Test case number is a link to testing information
%	When a numerical % is provided in the Complete column this represents an estimate of how much of a test was able to be performed
U, F, P, & S	Type of testing, Usability, Functionality, Performance, and Security

1.4 Conclusion and Recommendations

These tests focused on how well Path Scan detects inserted anomalous traffic. Path Scan clearly performed very well in this regard. The test team makes no recommendations with respect to improving Path Scan's efficacy.

However, the test team misunderstood changes made to Path Scan relative to an earlier version and made initial errors with respect to how Path Scan runs were configured. This serves to underscore the point that Path Scan is a complex system and to receive these valuable results, great care should be taken with respect to Path Scan configuration and operator training. If Path Scan is ultimately deployed without expert assistance, the test team recommends developing test cases that can be used to verify Path Scan is working as expected.

1.4.1 Post-Test Interactions

None

1.4.2 Potential Follow-On Testing

At this time, the test team makes no recommendations with respect to follow-on testing.

However, at such time that Path Scan is ready for large-scale deployment, the test team would recommend conducting usability testing.

2 Overview of Testing Components

2.1 Criterion

Technology criteria identify the desirable information needed to inform the decision making process. Technology criteria are the basis of the Test and Evaluation objectives for which test processes and procedures are to be created. While some criteria will be subjective (qualitative) in nature, the goal of the test team is to make these as specific and quantitative as possible. Where this is not possible, test processes and data collection will be clearly documented such that others can analyze the information to form their own conclusions. The testing criteria below will investigate the technology provider’s claims as listed below:

- Identify capabilities
  - Ability to identify anomalous connections.

The scope of the test activity will be driven by cost, schedule, and the success of previous test activities. The criteria selection drives the test process and procedures. Therefore, prioritization occurs with the selection of the test criteria. The criterion guidance provided below is neither exhaustive nor required for each technology being evaluated. Its purpose is to provide consistency within the TTP program for test and evaluation activities.

2.2 Test Cases

Test cases are comprised of procedures that evaluate criterion and provide the results and support data required by the decision making process. While some test cases will produce qualitative results that require interpretation, the goal of the test team is to make these specific, producing quantitative results. Where this is not possible, results from test cases will be clearly documented such that others can analyze the results to form their own conclusions.

2.3 Test Results

Test results are the output from executing the test procedures. A summary of these results is provided in a table in the executive summary and the details can be found in Section 5 where it is grouped with the corresponding test criteria and procedures.

3 Stake Holders, Responsibilities, and Intellectual Property Protection

This section addresses primary points of contact, their responsibilities, and intellectual property protection.

3.1 Points of Contact

Point of Contact (lead) for technology provider

Curt Hash
Los Alamos National Laboratories
chash@lanl.gov
505-570-2079

Point of Contact (lead) for test and evaluation team

Steve Hurd
Sandia National Laboratories
sahurd@sandia.gov
925-294-1224

Point of Contact (lead) for DHS S&T

Mike Pozmantier, Program Manager
DHS Sciences and Technologies Transition to Practice
Michael.pozmantier@hq.dhs.gov
(202) 254-2366

3.2 Responsibilities

One of the most important success factors is the timely exchange of information between stakeholders. Accurate and clear installation instructions and operation documentation will accelerate the schedule and provide a smooth collaboration between T&E and technology stakeholders.

The technology provider POC is responsible for ensuring timely delivery of:

- Preliminary documentation
- Technology package
- Facilitation of information exchange between developers and evaluators

The technology evaluator POC is responsible for ensuring timely delivery of:

- Preliminary test plan
- Facilitation of information exchange between developers and evaluators
- Timely evaluation schedule

3.3 Intellectual Property Protection

This section provides a place for all parties to communicate their specific legal needs and constraints. It allows testers and other stakeholders to understand legal restrictions and associated guidance with a specific technology.

- Not applicable

4 TEST PREPARATION

This section describes the testing environment and necessary resources. Providing the technology provider the test team's perception prior to testing allows for the developers to correct misconceptions prior to testing.

4.1 Technology Functional Overview

The following is a summary of the purpose, functions, and benefits of PathScan as described by Los Alamos National Laboratory [1].

- PathScan targets the traversal behavior of hackers by building behavioral models to reflect normal activity, followed by passively monitoring network traffic and comparing it with the behavioral models.
  Note: PathScan continually updates behavioral models as new information is received.

4.1.1 Prerequisite Technology Requirements

The prerequisite hardware and software requirements for the client's and server are listed below:

- Server System Requirements:
  - For testing purposes, must be running 64-bit Ubuntu Linux Server. Version 12.04 LTS was used for testing.

4.1.2 Technology Provider Hardware, Software and Documentation

The technology provider provided the following to the testing team:

- Software
  - Pathscan v0.2 (pathscan_0_2_amd64.deb)

4.2 Overview of Test Activity

4.2.1 Objective of Testing

Determine whether Path Scan can detect anomalous connections inserted into existing operational data.

4.2.2 Testing Scope

The scope of testing is limited to testing Path Scan functionality through a series of scenarios jointly agreed to by the Path Scan team and representatives of Sandia's red team. All scenarios will use 11 months of anonymized network connections from operational data collection for training and additional data for the test runs.

4.2.3 Test Assumptions

Throughout the test process assumptions are made. Documenting these assumptions provided stakeholders the opportunity to correct misunderstandings in documentation and communications.

- Assumption 1: The primary assumption is that the operational anonymized data is representative of a "real network". The test team is confident this is the case and the test results were consistent with that assessment.

4.2.4 Testing Team

The test team initially consisted of representatives from Sandia's red team. After scenarios were defined jointly with the Path Scan development team, additional staff from Sandia implemented the latest version of Path Scan, prepared the operational data, and ran the defined scenarios.

4.2.5 Testing Environment

The testing environment was limited to a single server. Operational data was copied to the server and Path Scan was installed as per instructions.

5 Test Criteria, Test Cases, Test Procedures and Test Results

This section focuses on the screening and familiarization criterion and test cases. The criterion for screening and familiarization was developed by reviewing the documentation, installation, and initial operation of the technology. From initial review, the test team identified the appropriate subject matter expertise and was able to execute the test cases below to address the criterion that they developed. The testing overview is described above in Table 1: Summary of Test Results. Below is each test case that was conducted.

All tests used a methodology that included gathering connection records from an operational network over the period of one year, and inserting specified connection records to determine whether Path Scan would report one or more of the inserted connection records as anomalous.

Specifically, the test team used the information gathered January through November as the baseline for testing. These records can be considered the training set. The test team used the existing connection records for December 1st for the actual test. When no additional connection records were added to the December 1st data, Path Scan identified no anomalous connections. Thus, the test team believed that adding connection records within a 30-minute window during December 1st would yield a fair assessment as to whether Path Scan was operating as expected.

Details of the Path Scan configuration that was used as well as the command line used to invoke Path Scan can be found in Appendix B. In every case, Path Scan was configured to identify anomalous 3-paths (such as IP1->IP2, IP2->IP3, and IP3 -> IP4). In addition, Path Scan was configured such that on average, Path Scan would identify approximately one anomalous connection per day.

All IP addresses used to construct the inserted connection records existed in the training set. However, the inserted connection records (such as IP1->IP2) did not exist in the training set.

Terms used in specific test cases

Sequential Paths: A series of sequentially linked connection records. Example: IP1->IP2, IP2->IP3, IP3->IP4, etc.

Inbound Star: A set of connection records, such that all records have the same destination address. Example: IP1->IP10, IP2->IP10, IP3->IP10, etc.

Outbound Star: A set of connection records, such that all records have the same source address. Example: IP10->IP1, IP10->IP2, IP10->IP3, etc.

Desktop: An address that during the training set had a low number of inbound connections and a high number of outbound connections.

Server: An address that during the training set had a high number of inbound connections and a low number of outbound connections.

Server Hub: An address that during the training set had a high number of both inbound and outbound connections.

TC1.1 Adding Sequential Paths

Description

This test case involves inserting a series of sequentially linked connection records into the existing data set, running Path Scan, and analyzing any anomalous 3-paths identified by Path Scan.

Criterion

C1.1) When a series of sequentially linked connection records are inserted into the existing data, one or more 3-paths, which could contain a combination of inserted and existing records, are identified as anomalous. Also, all of the 3-paths identified as anomalous include at least one inserted connection.

Procedure(s)

1. Select 4 node addresses at random, and add a total of 3 connection records (creating a sequential path) within a 30-minute window of time. Run Path Scan and review resulting output. Repeat 10 times.
2. Select 8 node addresses at random, and add a total of 7 connection records (creating a sequential path) within a 30-minute window of time. Run Path Scan and review resulting output. Repeat 10 times.
3. Select 12 node addresses at random, and add a total of 8 connection records (creating a sequential path) within a 30-minute window of time. Run Path Scan and review resulting output. Repeat 10 times.

Results

- C1.1. SUCCESS. This criterion was satisfied in all 10 experimental runs for each of the 3 procedures. In every instance, Path Scan identified at least one anomalous 3-path that included one or more of the inserted connection records. In addition, all anomalies that were reported included at least one inserted record.

Observations

- None

Recommendations

- None

TC1.2 Create an inbound star

Description

This test case involves inserting connection records into the existing data set, such that all inserted connections have the same destination address then running Path Scan, and analyzing any anomalous 3-paths identified by Path Scan.

Criterion

C1.2) When connection records, making up an inbound star are inserted into the existing data, it is possible but not guaranteed that one or more of the 3-paths are identified as anomalous. However, any three paths identified as anomalous must include at least one connection that was inserted.

Procedure(s)

1. Select 8 node addresses at random from among the addresses classified as being a “desktop” and add a total of 7 connection records (creating an inbound star) within a 30 minute window of time. Run Path Scan and review resulting output. Repeat 10 times.
2. Select 8 node addresses at random from among the addresses classified as being a “server” and add a total of 7 connection records (creating an inbound star) within a 30 minute window of time. Run Path Scan and review resulting output. Repeat 10 times.
3. Select 8 node addresses at random from among the addresses classified as being a “server hub” and add a total of 7 connection records (creating an inbound star) within a 30 minute window of time. Run Path Scan and review resulting output. Repeat 10 times.

Results

- C1.2. SUCCESS. This criterion was satisfied in all 10 experimental runs for each of the 3 procedures, as all anomalous 3-paths identified included at least 1 inserted connection record.
  For procedure 1, choosing desktop nodes, with little or no inbound traffic, means that anomalous 3 paths will only be identified if there are 2 paths emanating from the destination address common to the inserted connection records. In this case, 3 of the 10 runs resulted in identifying anomalous 3 paths.
  For procedure 2, choosing server nodes, with little or no outbound traffic, means that anomalous 3 paths will only be identified if there are 2 paths terminating at one or more of the source addresses. In this case, none of the 10 runs resulted in identifying anomalous 3 paths.
  For procedure 3, choosing server hub nodes, with both inbound and outbound traffic, means that anomalous 3 paths can be identified in several ways. In this case, 2 of the 10 runs resulted in identifying anomalous 3 paths.

Observations

- None

Recommendations

- None

TC1.3 Create an outbound star

Description

This test case involves inserting connection records into the existing data set, such that all inserted connections have the same source address then running Path Scan, and analyzing any anomalous 3-paths identified by Path Scan.

Criterion

C1.3) When connection records, making up an outbound star are inserted into the existing data, it is possible but not guaranteed that one or more of the 3-paths are identified as anomalous. However, any three paths identified as anomalous must include at least one connection that was inserted.

Procedure(s)

1. Select 8 node addresses at random from among the addresses classified as being a "desktop" and add a total of 7 connection records (creating an outbound star) within a 30 minute window of time. Run Path Scan and review resulting output. Repeat 10 times.
2. Select 8 node addresses at random from among the addresses classified as being a "server" and add a total of 7 connection records (creating an outbound star) within a 30 minute window of time. Run Path Scan and review resulting output. Repeat 10 times.
3. Select 8 node addresses at random from among the addresses classified as being a "server hub" and add a total of 7 connection records (creating an outbound star) within a 30 minute window of time. Run Path Scan and review resulting output. Repeat 10 times.

Results

- C1.3 SUCCESS. This criterion was satisfied in all 10 experimental runs for each of the 3 procedures, as all anomalous 3-paths identified included at least 1 inserted connection record.
  For procedure 1, choosing desktop nodes, with little or no inbound traffic, means that anomalous 3 paths will only be identified if there are 2 paths emanating from one or more of the destination addresses in the inserted connection records. In this case, 3 of the 10 runs resulted in identifying anomalous 3 paths.
  For procedure 2, choosing server nodes, with little or no outbound traffic, means that anomalous 3 paths will only be identified if there are 2 paths terminating at the common source addresses. In this case, 6 of the 10 runs resulted in identifying anomalous 3 paths.
  For procedure 3, choosing server hub nodes, with both inbound and outbound traffic, means that anomalous 3 paths can be identified in several ways. In this case, 6 of the 10 runs resulted in identifying anomalous 3 paths.

Observations

- None

Recommendations

- None

TC1.4 Add sequential paths that terminate into a created outbound star

Description

This test case is essentially a combination of test case 1 and 3, such that a series of sequentially linked connection records are inserted into the existing data set then the destination address of the last connection record is the source address for inserted connections records that make up an outbound star. The test then requires running Path Scan, and analyzing any anomalous 3-paths identified by Path Scan.

Criterion

C1.4) When the combination of a series of sequentially linked connection records and connections records making up an outbound star are inserted into the existing data, one or more three paths, which could contain a combination of inserted and existing records, are identified as anomalous. Also, all of the three paths identified as anomalous include at least one inserted connection.

Procedure(s)

1. Select 3 node addresses at random from among the addresses classified as being a "desktop" and arrange them as a sequential path. Then from the terminus of the sequential path, add a total of 8 connection records (creating an outbound star) within a 30 minute window of time. Run Path Scan and review resulting output. Repeat 10 times.
2. Select 7 node addresses at random from among the addresses classified as being a "desktop" and arrange them as a sequential path. Then from the terminus of the sequential path, add a total of 8 connection records (creating an outbound star) within a 30 minute window of time. Run Path Scan and review resulting output. Repeat 10 times.
3. Select 11 node addresses at random from among the addresses classified as being a "desktop" and arrange them as a sequential path. Then from the terminus of the sequential path, add a total of 8 connection records (creating an outbound star) within a 30 minute window of time. Run Path Scan and review resulting output. Repeat 10 times.

Results

- C1.4 FAILURE (with qualifications). This criterion was satisfied in all but 1 experimental run of the 10 experimental runs for each of the 3 procedures. However, in one instance there was no anomaly detected. The test team's best explanation for this result is that while none of the inserted connections existed in the training set, they were collectively not considered sufficiently unlikely to raise an alarm at the current threshold setting of an average of 1 alarm per day. LANL staff confirmed this result and determined that when the threshold setting was increased to 6 per day, this anomaly was identified. In addition, in the process of increasing the threshold from 1 to 6, no false positives results produced alarms.

Observations

- To be clear, Path Scan was operating as designed in the instance identified as a "failure". There is an inherent trade-off between reducing false positives through the lower threshold value and an increasing in anomalies that would not be detected (false negatives).

Recommendations

- No change to Path Scan is recommended due to these results. However, one recommendation is to focus on educating users as to the criticality of a proper setting from this threshold value. Each implementation can differ with respect to what value is appropriate, and what value is appropriate can certainly change over time for a specific implementation.

TC1.5 Add sequential paths that terminate into a created inbound star

Description

This test case is essentially a combination of test case 1 and 2, such that a series of sequentially linked connection records are inserted into the existing data set then the destination address of the last connection record is also the destination address for inserted connections records that make up an inbound star. The test then requires running Path Scan, and analyzing any anomalous 3-paths identified by Path Scan.

Criterion

C1.5) When the combination of a series of sequentially linked connection records and connections records making up an inbound star are inserted into the existing data, one or more three paths, which could contain a combination of inserted and existing records, are identified as anomalous. Also, all of the three paths identified as anomalous include at least one inserted connection.

Procedure(s)

1. Select 3 node addresses at random from among the addresses classified as being a “desktop” and arrange them as a sequential path. Then to the terminus of the sequential path, add a total of 8 connection records (creating an inbound star) within a 30 minute window of time. Run Path Scan and review resulting output. Repeat 10 times.
2. Select 7 node addresses at random from among the addresses classified as being a “desktop” and arrange them as a sequential path. Then to the terminus of the sequential path, add a total of 8 connection records (creating an inbound star) within a 30 minute window of time. Run Path Scan and review resulting output. Repeat 10 times.
3. Select 11 node addresses at random from among the addresses classified as being a “desktop” and arrange them as a sequential path. Then to the terminus of the sequential path, add a total of 8 connection records (creating an inbound star) within a 30 minute window of time. Run Path Scan and review resulting output. Repeat 10 times.

Results

- C1.5 SUCCESS. This criterion was satisfied in all 10 experimental runs for each of the 3 procedures. In every instance, Path Scan identified at least one anomalous 3-path that included one or more of the inserted connection records. In addition, all anomalies that were reported included at least one inserted record.

Observations

- None

Recommendations

- None

TC1.6 Adding Sequential Paths, using specified types of hosts

Description

This test case involves inserting a series of sequentially linked connection records into the existing data set, running Path Scan, and analyzing any anomalous 3-paths identified by Path Scan. However, in each test procedure, a different sequence of types of hosts will be used.

Criterion

C1.6) When a series of sequentially linked connection records are inserted into the existing data, one or more 3- paths, which could contain a combination of inserted and existing records, are identified as anomalous. Also, all of the 3- paths identified as anomalous include at least one inserted connection.

Procedure(s)

1. Select 6 desktop node addresses and 2 server node addresses at random, and add a total of 7 connection records (creating a sequential path) within a 30 minute window of time. The sequence of hosts will be as follows: Desktop1 -> Desktop2 -> Desktop3 -> Server1 -> Server2 -> Desktop4-> Desktop5 -> Desktop6. Run Path Scan and review resulting output. Repeat 10 times.
2. Select 2 desktop node addresses and 2 server hub node addresses at random, and add a total of 5 connection records (creating a sequential path) within a 30 minute window of time. The sequence of hosts will be as follows: Desktop1 -> Desktop2 -> ServerHub1 -> ServerHub2 -> Desktop2-> Desktop1. Run Path Scan and review resulting output. Repeat 10 times.
3. Select 2 desktop node addresses and 2 server hub node addresses at random, and add a total of 7 connection records (creating a sequential path) within a 30 minute window of time. The sequence of hosts will be as follows: c. Desktop1 -> Desktop2 ->ServerHub1 -> ServerHub2 -> Desktop1 -> Desktop2 -> ServerHub1 -> ServerHub2. Run Path Scan and review resulting output. Repeat 10 times.

Results

- C1.6. SUCCESS. This criterion was satisfied in all 10 experimental runs for each of the 3 procedures. In every instance, Path Scan identified at least one anomalous 3-path that included one or more of the inserted connection records. In addition, all anomalies that were reported included at least one inserted record.

Observations

- None

Recommendations

- None

6 REFERENCES

[1] *Cyber Security Division Transition to Practice Technology Guide*. Vol. 2. U.S. Department of Homeland Security Science and Technology Directorate, 2013. PDF.

APPENDIX A - TTP PROGRAM OVERVIEW

A.1 SUMMARY

Technologies selected for the TTP program come from a wide variety of research and development activities. TTP development activities include those early in the development cycle as well as cutting edge technologies. The broad spectrum of technology maturity makes it difficult to develop test procedures that validate each specific product requirement or specification. Test criterion for TTP technologies are derived through a variety of sources and used to develop test procedures that validate the range of capabilities, maturity, and stability of the technology. As a result, the evaluation process proposed herein is iterative in nature and designed to be tuned to the specific needs of the technology being evaluated. The determination about what needs to be tested and how it will be tested is planned prior to testing and it is essential agreement be reached among stakeholders. In keeping with TTP T&E program goals, the product evaluation guidelines described in this document should be a collaborative effort between DHS S&T, its test organizations, and the technology provider. Additional information from the technology providers' review and comment of the test plan are included and are identified by the nomenclature "TP Note:"

A.2 ITERATIVE EVALUATION

Testing performed within the TTP program is executed by the lead test laboratory, commercial enterprise, or other government laboratories. This flexibility allows for mitigation of Organization Conflict of Interest (OCI) and the incorporation of organizations with specialized capabilities and skill sets.

The evaluation process is the result of experience gained during the program execution of TTP year one technologies. Testing begins with discussions with the technology provider, technology familiarization, qualitative inquiries and initial quantitative observations. After initial familiarization, a cycle of testing, analysis of results and the alignment of results with test goals occurs. Test plan guidelines focus on high-level test objectives and allow the creation of specific test procedures based on technology specifics and expertise gained through familiarization.

Test criterion is aligned with the technology description and mission and sources for this information vary. Source examples are: functional descriptions, the Transition to Practice Technology Guide, provider claims, provider goals, stakeholder requirements, technology familiarization outcomes, current test results, and other information obtained from stakeholder communications. The desire is to validate the technology attributes through an agile test program. Figure 1: Iterative Evaluation Cycle illustrates the agile testing sequence.

The ability to continuously refactor the test scope based on current observations and assessment is an important aspect of the evaluation process. It is essential that testers have the ability to improvise during the test activity. This improvisation allows for fine tuning and resource optimization. Adjustments can be made due to new information, a better understanding of the technologies capabilities, preliminary screening, and test results. Allowing this flexibility is required in order to address the many unknowns from evaluating cutting edge technologies.

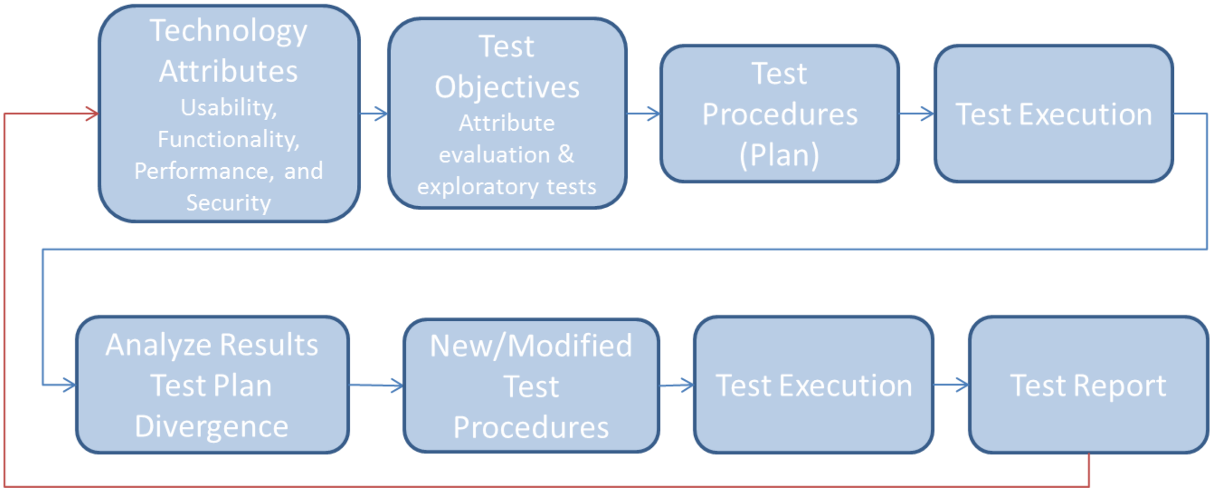
Technology Attributes
Usability, Functionality, Performance, and Security
Test Objectives
Attribute evaluation & exploratory tests
Test Procedures (Plan)
Test Execution
Analyze Results Test Plan Divergence
New/Modified Test Procedures
Test Execution
Test Report

Figure 1: Iterative Evaluation Cycle

In accordance with this test strategy, there is an initial familiarization activity followed by one or more test sequences. This iterative test process is applied as necessary to satisfy the test goals for a given technology. Each previous test activity serves as an input to the future ones. The process is as follows:

- Develop criteria for test and evaluation
- Develop test procedures
- Execute test procedures, analyze results, and report

A.3 Development and Revision Description

The availability of a revision history is optional and dependent on where the technology is in the development and commercialization lifecycle. Complications can arise with testing if multiple versions of a product exist. This information helps to insure the TTP program and test organization are making the best investment and scheduling decisions related to evaluating the best configuration for commercialization.