Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Protection testing: What protection testing should we do?

Protection testing is often taken as a haphazard exercise in seeking out known vulnerabilities and repairing them. But this approach has proven problematic for may enterprises in that it (1) tends to break things that are important to keep working, (2) tends to reveal large numbers of vulnerabilities that are not equally important, (3) tends to measure vulnerabilities against known vulnerabilities, that form a moving target, and (4) are not well related to meaningful metrics for the enterprise.

The problems with breaking things are particularly insidious, because many people seem to claim that if things are that breakable they need to be tested and repaired before the bad guys break them. But it's not that simple. For example, SCADA systems may control large complex and expensive machinery that cannot be immediately replaced or repaired and that can be broken if the control mechanism is disabled by a test vector. The test in this case may be as harmful as the worst-case attack.

In seeking to mitigate these problems, five approaches that we standardly consider in our enterprise protection architecture studies are thought of relative to the risks posed by the systems under test. The five approaches are:

- Protection testing provides verification that protection does what it is supposed to do.
- Fault models are used to generate and evaluate tests.
- Coverage of tests are measured against the fault model.
- Testing periods are based on system risk levels.
- Systems with authoritative high-valued content are NOT tested during operation.

The decision table we use s a default starting point is codified in Table 1 below:

Issue	***High risk***	***Medium risk***	***Low risk***
Protection testing provides verification that protection does what it is supposed to do.	Yes	Yes	No
Fault models are used to generate and evaluate tests.	Yes	Yes	No
Coverage of tests are measured against the fault model.	Yes	Yes	No
Testing periods are based on system risk levels.	Yes	Yes	Yes
Systems are NOT tested during operational periods.	Yes	No	No

Table 1 - The default security decision for protection testing

Protection testing provides verification that protection does what it is supposed to do.

Protection testing has the objective of matching the defined goals of the controls in place with the reality of the controls in place. As such, its purpose is not to determine whether the program is what it should be, but rather to try to refute the assertion that the protection program does what it claims to do. The other approaches to "protection testing" are not in fact testing at all. They are typically something like known vulnerability scanning, verification, and so forth. All of value in their own right, but often mislabeled as testing.

We advise this approach for all but low risk situations. The reason we don't advise this approach for low risk situations is that the cost of doing this testing may exceed its utility.

Fault models are used to generate and evaluate tests.

Fault models are developed to create the basis for identifying the difference between a desired and undesired test outcome and to identify the class of faults that tests might be able to uncover. Without a fault model, testing is shooting in the dark without a clear target. With a fault model, it is possible to determine whether or not the tests are meaningful, redundant, and to what extent they provide "coverage".

We advise this for all but low risk situations, for the same reason - cost versus utility.

Coverage of tests are measured against the fault model.

Coverage is a measurement against the fault model used to express the percentage of faults that the tests would detect if present or determine not to be present if they were not present. As such, it allows the tester to gain and provide clarity around the diagnostic utility of the tests for determining that the controls are in fact working as desired.

We advise this for all but low risk situations, for the same reason - cost versus utility.

Testing periods are based on system risk levels.

The time taken to perform a test depends on the coverage of the test, the size of the test set, and the time per test. Since complete coverage of most fault models in most cases takes a very long time, periodicity of testing is traded off with coverage and test complexity. The tradeoff is inherently limited by the risk of the control failing without that failure being noticed. Hence, the periodicity of the test process is driven by the exposure from undetected control failure which then limits the coverage for the fault model and test times.

This we advise in all cases, with the rate of testing increased for higher risk systems and situations, subject to the limitations imposed by the last case...

Systems with authoritative high-valued content are NOT tested during operation.

Because systems with high consequences of failure can fail because of a test, testing is often limited to test systems that are as close as possible to operational systems, limited to testing during non usage periods such as maintenance windows, or non-authoritative content systems of a similar type.

When the consequence of a test damaging a system is high, the test should not be performed except during defined maintenance windows, and then only if proper backups are in place.