MITRE: Proposal to Formalize Test and Evaluation Activities Within the Forensic and Law Enforcement Communities

By

Mark Hirsh

Presented At

The Digital Forensic Research Conference

DFRWS 2004 USA Baltimore, MD (Aug 11th - 13th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

DC3

AFRL DFRWS

Formalizing Forensic Test & Evaluation Activities

Mr Mark Hirsh
DoD Cyber Crime Institute
August 2004

Topics

DC3

- Discuss rationale for conducting T&E
- Describe DCCI T&E process and procedures
- Discuss findings
- Provide rationale for creating a centralized repository of T&E results

Testing : User Perspective

DC3

- Support ASCLD accreditation
- Provide guidelines on the use of products
- Identify anomalies
- Support product selection process
- Lend credence to testimony
- Provide an independent assessment

ASCLD = American Society of Crime Laboratory Directors

Reduce the risk of surprises!

Testing: Developer Perspective

DC3

- If product does well
  - Provides marketing support
  - Influences customer decisions
- If product fails to meet expectations
  - Identifies areas needing improvement
  - Provides feedback on customer requirements

Customers may require it!

DCCI Test Procedures

DC3

Customer Requests

- Obtain product from customer
- Become familiar with product
- Identify verification hardware and software to use in testing
- Send test plan to customer
- Conduct tests
- Document results
- Allow vendor to review/comment on test results if necessary
- Add vendor comments as appropriate
- Sign report and add to DCCI catalog

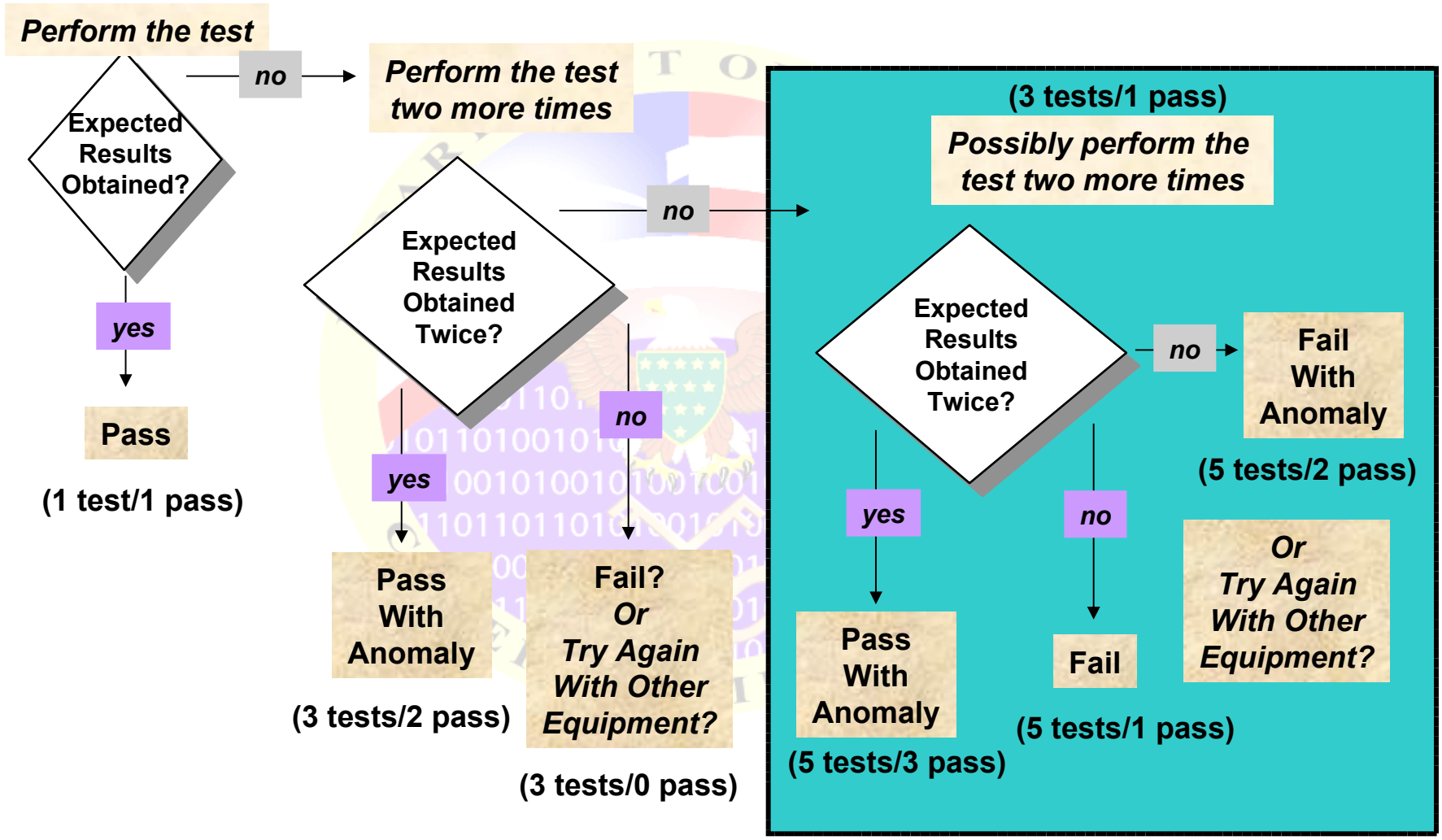
Vendor Requests*

- Obtain product from vendor
- Become familiar with product
- Identify verification hardware and software to use in testing
- *Send test plan to vendor*
- ***Allow vendor to run tests and if necessary develop new version of product***
- ***Have vendor sign Product Test Agreement (send new version to DCCI if necessary)***
- Conduct tests
- Document results
- Allow vendor to review/comment on test results
- Add vendor comments as appropriate
- Sign report and add to DCCI catalog

**** = Approach currently being evaluated***

Conduct Tests: General Process/Procedures

DC3



Sample Findings

DC3

- Some products perform as advertised
- Sometimes advertised features/capabilities do not work as expected
- Platform dependencies
  - Product works on some platforms, not on others
- Hard drive dependencies
  - Some products cannot access very large drives
  - Some products have problems reading from/writing to relatively small drives

Word of Advice: Use Products That Provide Sector Counts!

T&E Limitations

DC3

- Testing does not guarantee a product will work
  - Cannot always exercise all features and capabilities
  - Cannot test on all platforms
  - Can only test with equipment that is available
- Testing performed on particular product version / release

Does not tell you whether you should or should not use a product!

Current State

DC3

- Many products / few testers
  - Need more test organizations
  - Formal testing done at NIST, DCCI, AFRL, FBI – *others?*
  - Informal testing done by some
    - Processes/procedures uneven, inconsistent, and fragmented
- No central repository for test reports
  - Users do not have ready access to all reports
  - Reports not developed to meet minimum standard
    - Repeatable
    - Understandable
    - Easy to interpret
- No message board for community discussion of test results

Next Steps

DC3

- Contact DCCI if interested in performing formal testing
- Share test procedures
- Investigate whether DCCI Web site could serve as a repository for test reports (with links to other sites)
  - Currently DCCI Web site contains product descriptions
  - DCCI is looking into providing access to reports using login vice using email to request the report
- Investigate feasibility of message board
  - Facilitate discussion of reports
  - Login to restrict access

Contact Information

DC3

DCCI:
Commercial: (410) 981-1018
Email: DCCI.Director@dc3.gov

DC3 Main Office:
Commercial: (410) 981-1627
DSN: 923-2595
Toll Free: (877) 981-3235

DoD Cyber Crime Center

DC3

QUESTIONS ?