Meaningful Vulnerability Analysis with V3: By-product of evaluation or ***the*** product of evaluation

Denise Cater
BT CLEF

Meaningful vulnerability analysis with v3

- Changes to vulnerability analysis in v3
- When to perform vulnerability analysis
- Affect of vulnerability analysis on other evaluation activities

Objectives of AVA update

- Include a new lowest level of vulnerability analysis component for an evaluator search of the public domain
- At the lowest levels the emphasis should be on evaluator activities rather than developer activities
- The activities to be performed by the evaluator must be clearly specified and capable of consistent application

BT

Objectives of AVA update

- Resolve the issues surrounding the distinction between obvious and low attack potential
- Include any aspects of the misuse analysis family that have not been incorporated into operational guidance family (AGD_OPE)
- Consider dependencies of vulnerability analysis components to provide the necessary flexibility in their application

BT

Vulnerability Analysis in V3

- Incorporating all v2.x AVA families into single v3 family
  - Strength of function now a particular example of direct attack
  - Misuse considered in Guidance (AGD) activity
  - Covert channel analysis added to higher components of vulnerability analysis
    - Also clarified covert channel vs. side channel analysis
- Renaming of activity to AVA_VAN
- Introduced new level of attack potential:
  - Enhanced-Basic

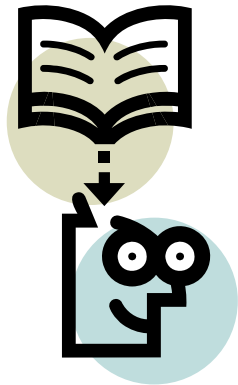
BT

Vulnerability Analysis in V3

- Emphasis on evaluator analysis and ADV_ARC
  - Developer analysis now provided in new ADV_ARC family
- Added new lowest level of vulnerability analysis
  - Evaluator search of public domain material
- Removed ‘obvious’ vulnerabilities
  - Replaced with encountered
- “Encountered” vulnerabilities….

Philosophy of “encountered” vulnerabilities

- Vulnerability analysis is pervasive
- Ongoing activity throughout evaluation
- Continual questioning of evidence and design decisions

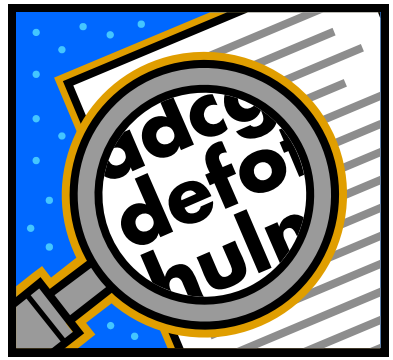


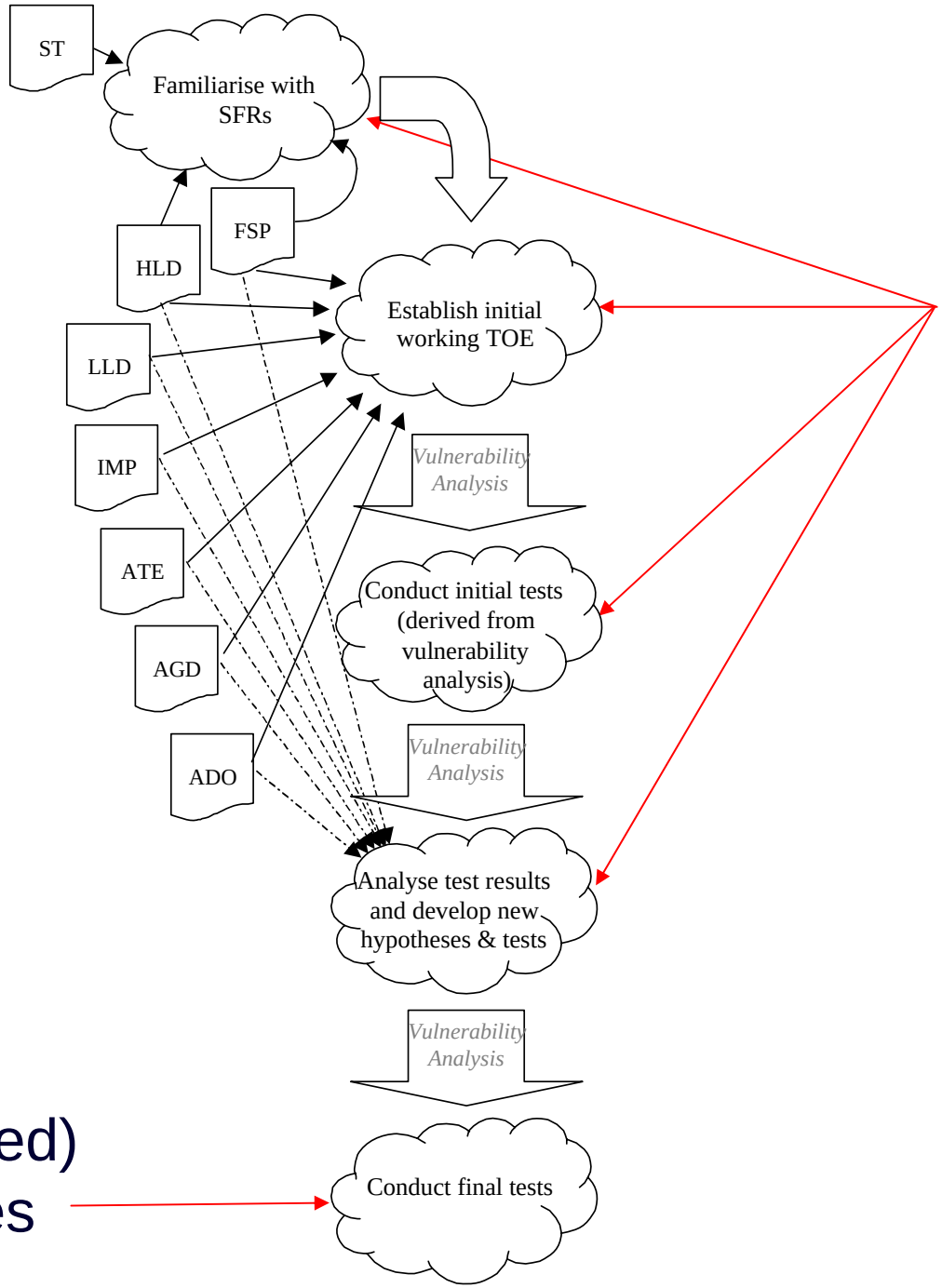
Affect on evaluation activities

- Challenge to the often linear view of activities
  - “must complete [at least the majority of] the functional specification activity before starting the high-level design”
  - “can’t start testing until design is complete”
- Shift in evaluator focus from evidence to goal
  - Increase confidence in security functionality, rather than ensuring that a perfect set of documentation exists.

Result in shift of focus

- An evaluator who is questioning how the product works and where weaknesses may exist from the time they first open the ST.





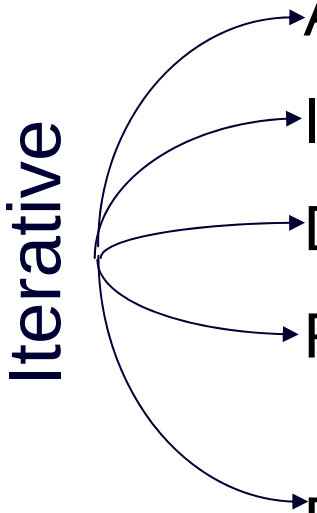
encountered vulnerabilities

(demonstrated) vulnerabilities

Result in shift of focus

Familiarise with product

Get the TOE working



- Analyse design to understand how it works
- Inspect developer testing
- Develop initial tests
- Revisit design/test material for further understanding
- Refine tests

Bring together ideas, thoughts, understanding of potential vulnerabilities

Final testing

Meaningful vulnerability analysis…

- Strong link with ADV_ARC
- Ongoing activity throughout all evaluations
  - From EAL1 through to EAL7
- Should be used to direct every other evaluation activity

…is ***the*** product of evaluation

Thank you

denise.cater@bt.com