AVA_VAN.2 – Performing Vulnerability Analysis Under CCv3

Eve Pierre and James Arnold

September 24, 2008

Synopsis

- What is Vulnerability Analysis
- Vulnerability Analysis – Common Criteria v2
- Vulnerability Analysis – Common Criteria v3
- Common Criteria AVA_VAN.2 requirements
- An approach to vulnerability analysis
  - Search of the public domain
  - Search of the evaluation evidence
  - Flaw hypothesis
  - Penetration testing
- Conclusions and recommendations

What is Vulnerability Analysis?

The Common Criteria defines vulnerability analysis as an assessment of whether potential vulnerabilities identified during the evaluation of a product could allow attackers to violate the security functional requirements

Vulnerability Analysis – Common Criteria v2

- The developer was required to research and identify potential vulnerabilities and provide rationale that any vulnerability identified was not exploitable
  - The analysis typically focuses on public domain searches and assertions about not finding vulnerabilities in evaluation evidence.
- The evaluator was required to evaluate the developer's analysis and to perform penetration testing
  - Concerned mostly with whether the developer analysis addresses all information sources identified in the applicable Common Evaluation Methodology (CEM) work units and whether the developer may have missed something in the public domain.
  - Penetration testing was usually directed at confirming information in the analysis.
- Performing vulnerability analysis was a shared task between the developer and the evaluator

Vulnerability Analysis – Common Criteria v3

- There are no requirements that the vendor provides vulnerability analysis evidence.
  - No statement of the developer's bug tracking capabilities
  - No prior developer search of the evaluation evidence or other design information
  - No prior developer search of the public domain to identify vulnerabilities
- The evaluator is responsible to perform an independent vulnerability analysis and to conduct penetration testing.
  - Based on available evaluation evidence materials and all available public domain sources.

Common Criteria AVA_VAN.2 Requirements

- A search of public domain sources to identify potential vulnerabilities
  - The CEM identifies the World Wide Web as the prime source of information via modern search tools.
- Analysis of the evaluation evidence to identify potential vulnerabilities
  - The evaluation evidence is identified as material to analyze to conjecture potential vulnerabilities.
- Penetration testing to reach a conclusion about all identified potential vulnerabilities
  - Tests need be developed only in cases within a Basic attack potential. (EAL2 and EAL3)
    - Vulnerabilities beyond a Basic attack potential are to be documented as ‘residual vulnerabilities’.
  - It seems all potential vulnerabilities must be confirmed via a test in order to be considered an evaluation failure.

An Approach to Vulnerability Analysis

- Search of the public domain
- Search of the evaluation evidence
  - Security Target
  - Functional Specification and Product Design
  - Architecture Description
  - Guidance
- Flaw Hypothesis
- Penetration Testing

Search of the Public Domain

- Perform a search of the public domain, including various vulnerability databases such as:
  - http://nvd.nist.gov/nvd.cfm
  - http://www.cert.org
  - http://cve.mitre.org
  - Among others

    Evaluation schemes should publish guidance in this regard and evaluation labs should accumulate search sites that prove most useful
- Use the following search criteria:
  - Product name (and variants)
  - Vendor's name (and variants)
  - Product type
  - Name of any and all products supported in the TOE environment

    Evaluation Schemes should publish guidance in this regard
- Any potential vulnerabilities returned by this search must be investigated

Search of the Public Domain (cont.)

- Do a cursory review of the potential vulnerabilities returned by the search and categorize them
  - Apply
    - The developer should be queried for input – in many cases, publicly identified vulnerabilities have already been resolved and the public notice has not been amended.
    - The potential vulnerability should be further analyzed to determine whether it might be exploitable and whether it must be subject to penetration testing.
  - Not clear if it applies
    - The developer should be queried for help and/or clarification.
    - Perform additional analysis based upon evidence and other publicly available information to decide whether it remains a potential vulnerability.
  - Does not apply
    - No further consideration should be given to items identified in searches that are obviously or easily determined to be not applicable.

Search of the Evaluation Evidence

- Security Target
  - Target of Evaluation (TOE) Description
    - Examine the descriptions of physical and logical boundaries to determine if they appear to be complete
    - Determine if it is clear how the product is protected and not bypassable in its evaluated configuration
    - Identify things that should be revisited in the security architecture
  - Statement of Security Environment
    - Use the statement of security environment to scope the vulnerability analysis (i.e., perceived vulnerabilities may have already been taken care of with assumptions)
  - TOE Summary Specification (TSS)
    - Review the TSS to determine if it indicates any potential vulnerabilities that need to be investigated in the design (e.g., the TSS may indicate that the TOE uses an insecure mechanism such as a weak cryptographic algorithm)

Search of the Evaluation Evidence (cont)

- Functional Specification and Product Design
  - Study the design to see where the product might be potentially weak
  - Determine how the interfaces get invoked (e.g., are they invoked over unprotected boundaries such as across an insecure network connection)
  - Consider whether any assumptions are unreasonable or impractical
  - Consider the functions of available interfaces and whether documented restrictions seem appropriate or adequate
  - Consider interfaces in terms of the potential for historical vulnerabilities (e.g., time of check to time of use, buffer over runs)

Search of the Evaluation Evidence (cont)

- Architecture Description
  - Identify the security domains of the various product components and examine how they are instantiated and protected
  - Examine the boundaries of the applicable product components and how those components interact
    - For example, unprotected network communication between components might allow data to be observed, modified, or destroyed
  - Where the product relies on supporting components, check that the use of the supporting components does not seem to introduce potential vulnerabilities
  - Consider the product in its intended context to identify whether there may be potential ways to bypass its security functions

Search of the Evaluation Evidence (CONT'D)

- Guidance
  - Examine the guidance to determine whether it allows users to do things that are expressed as threats or counter to the assumptions in the statement of security environment
  - Look at any restrictions on user's permissions

Flaw Hypothesis

- Flaw Hypothesis Methodology
  - Recommended by the Common Evaluation Methodology
  - Well documented
    - **Teaching Security Engineering Principles** (http://cisr.nps.navy.mil/downloads/01paper_securityengineering.pdf)
    - **Security: Where Testing Fails** (http://cisr.nps.navy.mil/downloads/00paper_testingfails.pdf)
    - **CS 392/681 - Computer Security Module 16 - Vulnerability Analysis** (http://isis.poly.edu/courses/cs681/Lectures/module_9.pdf)
    - **Security Risk Analysis** (http://www.ece.uvic.ca/~itraore/elec567-05/notes/elec67-05-3.pdf)
  - Basic process
    - Brainstorm potential vulnerabilities
    - Prioritize and analyze the potential vulnerabilities
    - Re-examine any confirmed vulnerabilities to identify other potential vulnerabilities
    - Remediate confirmed vulnerabilities

Flaw Hypothesis (cont)

- Evaluation Approach
  - Evaluation team meets and brainstorms potential vulnerabilities based on the review of evaluation evidence (and the public search for vulnerabilities)
  - Potential vulnerabilities are prioritized based on an estimate of Time, Expertise, Knowledge, Access, and Equipment each on a simple scoring of 1-4
    - 1 = No perceived impediment of substance
    - 2 = Some impediment but can be reasonably overcome in most cases
    - 3 = Moderate impediment but can be overcome in some cases
    - 4 = High impediment - difficult to impossible to overcome
  - Refine the score to align with CEM guidance in order to determine the actual attack potential in each case.

Flaw Hypothesis (cont)

- Evaluation Approach (cont)
  - The analysis of potential vulnerabilities should conclude for each vulnerability
    - It is not exploitable
      - The analysis should be documented in the evaluation record with suitable rationale
    - It is exploitable
      - The analysis should be documented in the evaluation record with suitable rationale
      - The evaluation team should determine whether a penetration test is necessary since in some cases the issue might be sufficiently obvious that a test is not necessary for conclusive demonstration that the vulnerability is exploitable
    - It remains uncertain
      - The evaluation team should consider whether testing can be performed to draw a conclusion
      - If not, the evaluation team should reconsider the prioritization and also consult the developer for any inputs they may have about the potential vulnerability
      - If the evaluation team is unable to confirm a potential vulnerability using public domain sources, the applicable evaluation, and the product itself (e.g., via testing), the potential vulnerability is not exploitable and should be documented in the evaluation record as such

Penetration Testing

- Evaluation Team Penetration Testing
  - As a result of the vulnerability analysis, the evaluator should devise tests to demonstrate exploitability of confirmed or questionable vulnerabilities
  - Where tests do not demonstrate exploitability, the vulnerability should be considered to not be exploitable unless analysis offers convincing evidence to the contrary and the test was perhaps infeasible to implement (e.g., given the limited time, resources)
  - All tests should be documented so they are repeatable
  - All test results should also be documented to provide rationale for the various conclusions of exploitability
- Remediation
  - The developer should be provided the results of the analysis and testing so that any exploitable vulnerabilities can be addressed
  - At this point, the evaluation will likely need to iterate some activities depending on the specific nature of the exploitable vulnerability remediation

Penetration Testing (cont)

- Tools
  - The evaluators should make use of tools wherever possible while conducting penetration testing
    - They can reduce the difficulty to confirm potential vulnerabilities (e.g., a port scanning tool can readily uncover unexpected network-facing interfaces)
  - Tools are readily available in the public domain and for commercial purchase
    - Evaluation Schemes should publish guidance in this regard and evaluation labs should accumulate tools that prove useful

Conclusions and Recommendations

- The aim of performing Common Criteria vulnerability analysis is to ensure that products with obvious vulnerabilities, do not get certified
- To achieve this, it is recommended that
  - Common Criteria evaluation schemes should publish guidance on the most useful sites to search for vulnerabilities and the search criteria to use. The schemes should also identify and publish lists of tools that should be used for vulnerability testing of various product types.
  - Common Criteria Testing Laboratories should accumulate search sites and testing tools that prove most useful to improve their own capabilities
  - While independently searching for vulnerabilities, evaluators should understand that not every idea can be an exploitable vulnerability within the context of EAL2 or EAL3
- This process should also be extended to apply to higher assurance level evaluations

Contacts

Eve Pierre

SAIC Accredited Testing & Evaluation Laboratories
Common Criteria Evaluator

Marie.e.Pierre@saic.com

James Arnold

SAIC Accredited Testing & Evaluation Laboratories AVP and Technical Director

James.L.Arnold.Jr@saic.com

http://www.saic.com/infosec/common-criteria/