

Common Criteria Vulnerability Analysis of Cryptographic Security Mechanisms

*Quang Trinh/
James Arnold*

28 September 2007

- Introduction
- What is Common Criteria Vulnerability Analysis?
- Requirements of Vulnerability Analysis
- Vulnerability Analysis Approach for Cryptographic Security Mechanisms
- FIPS Considerations
- Conclusions

Note that the presentation applies both to Common Criteria version 2.3 as well as version 3.1. The examples were drawn from version 3.1.

- Crypto-analysis is **hard** and outside the scope of the Common Criteria (CC).
 - The CC leaves it to each evaluation scheme to provide guidance regarding the handling of strength of cryptographic mechanisms.
- In the United States – Common Criteria Evaluation and Validation Scheme (CCEVS): A policy has been issued allowing that cryptographic mechanisms can conform to cryptographic standards based on:
 - FIPS certification (relied on third-party analysis)
 - Vendor assertion (relied on vendor analysis)
- ***Problem:*** As a result, cryptographic mechanisms are sometimes all but ignored in the context of evaluations, despite the fact that cryptographic mechanisms may have elements that are not based in cryptographic strength.

- This presentation is intended to identify aspects of cryptographic mechanisms that may not be based on cryptographic strength and, hence, are not outside the scope of the Common Criteria.
- Appropriate, practical, and systematic approaches are offered; in particular, for addressing cryptographic mechanisms in the context of performing a vulnerability analysis in accordance with the Common Criteria.

What is CC Vulnerability Analysis?

- In the context of the Common Criteria, a vulnerability analysis is an assessment activity to determine the existence and exploitability of flaws or weaknesses in the target of evaluation (TOE) in the operational environment.
- Five generic types of vulnerabilities
 - Bypass
 - Tamper
 - Misuse
 - Direct attacks*
 - Monitoring**

* - Direct attacks reliant upon weakness in cryptographic algorithms (i.e., related to the notion of cryptographic strength) are excluded.

** - Medium to high assurance level (covert channel) are excluded from presentation.

- Requirements of Vulnerability Analysis CC v3.1
 - Search public domain to identify potential vulnerabilities in the target of evaluation (TOE)
 - Search proprietary information (design, code, etc.) to identify potential vulnerabilities in the TOE
 - Identify which are exploitable in the TOE operational environment
 - Devise penetration tests based on the exploitable ones
 - Conduct penetration testing
 - Document all exploitable and residual vulnerabilities

- Vulnerability Analysis Approach for Cryptographic Security Mechanisms
 1. Breakdown the cryptographic mechanism into cryptographic components
 2. Analyze each component in order to identify those aspects based in cryptographic strength and those that are not
 3. Perform regular Common Criteria vulnerability analysis any aspects of each component not based in cryptographic strength
 4. Look for well-known or publicly accessible attacks and tools in the public domain for each of the cryptographic components

1. Breakdown the cryptographic mechanism into cryptographic components
 - a) Establishment of the cryptographic keys
 - b) Performing the cryptographic operations
 - c) Storage of the cryptographic keys and data
 - d) Destruction of cryptographic keys

1a. Establishment of the cryptographic keys

- Keys can be generated based on random number generation (RNG)
- Keys can be established using Diffie-Hellman
- Keys can be imported (side channel)
- Keys can be sent using AES key wrap
- Keys can be hard-coded
- Keys can be generated based on user inputs, date and time, passwords, etc.

1b. Performing the cryptographic operations

- Operation is performed transparently (no user action required)
- Operation is not performed transparently (correct user action required)
 - Access to the cryptographic keys
 - Data specified to be signed or encrypted
- Operation can be disabled or enabled

1c. Storage of the cryptographic keys and data

- Keys/data are stored encrypted
- Keys/data are stored in cleartext but access is controlled
- Keys/data are stored in cleartext but location is unknown
- Keys/data are stored in cleartext

1d. Destruction of cryptographic keys

- Keys are overwritten
- Keys are not overwritten

2. Analyze each component in order to identify those aspects based in cryptographic strength and those that are not
 - Examine the design documents, perform source code review, and ask the developer questions
 - Determine which parts are based in cryptographic strength

- Determine which parts are based in cryptographic strength and which are not by applying these questions
 - Establishment of the cryptographic keys
 - Can the cryptographic key be guessed or brute-forced?
 - Can the cryptographic key be intercepted during transmission?
 - Performing the cryptographic operations
 - Can the cryptographic operation be disabled or interrupted?
 - Can the cryptographic operation be performed incorrectly by user?
 - Performing the cryptographic operations
 - Can the cryptographic operation be disabled or interrupted?
 - Can the cryptographic operation be performed incorrectly by user?
 - Storage of the cryptographic keys and data
 - Can the cryptographic key be accessed?
 - Destruction of the cryptographic keys
 - Can the cryptographic key be accessed after being “destroyed?”

3. Perform regular Common Criteria vulnerability analysis on the non-cryptographic components
 - Any potential vulnerabilities not related to cryptographic strength are within scope
 - Ability to simply guess keys are other attributes used in cryptographic operations
 - Unintended disclosure of sensitive data (e.g., keys)
 - Use of user-entered data (e.g., password) upon which to base cryptographic operations
 - Failure to protect cryptographic modules from tamper or bypass

- Vulnerability analysis example
 - While the strength of the DES algorithm is out of scope, the potential to simply guess keys within the relatively small key range is within scope, since guessing keys does not require any crypto-analytical expertise.

4. Look for well-known or publicly accessible attacks and tools in the public domain for each of the cryptographic components
 - Any tool that can be downloaded from the Internet that can exploit a weakness in the cryptographic algorithms is fair game.
 - For example, WEP password-cracking tool
 - Also, while the strength of MD5 is out of scope, the fact that a tool can be readily obtained on the Internet and used to exploit applicable mechanisms without performing any crypt-analysis is within scope.
 - The rationale is that using a tool requires no crypto-analysis skills or even knowledge of the cryptographic algorithm.
 - Similarly, a well-documented attack is very similar to using a tool, though the evaluator would need to account for any additional expertise requirements.

- The results of FIPS certifications should generally address concerns related to the strength of cryptography mechanisms.
 - If there is no FIPS or other third-party certification, then perhaps the relative strength of the mechanism is in doubt.
- However, if a product developer utilizes a FIPS certificate cryptographic mechanism,
 - the evaluation team should determine whether it is used in accordance with its FIPS security policy and, if so,
 - should be able to reference that evaluation as evidence to address applicable aspects of their own evaluation.
 - For example, the FIPS evaluation may have already ensured that key generation is done appropriately.

- Common Criteria (CC) evaluation teams should apply this or a similar approach in order to ensure that all target of evaluation (TOE) security functions are addressed to the extent possible and required by the CC.
- It should be generally unacceptable to simply exclude a cryptographic mechanism from evaluation because it is cryptographic in nature, since even cryptographic mechanisms have aspects that are not based on the strength of cryptography.
- It should, however, be acceptable to reference other cryptographic certifications as they may pertain to aspects of the CC evaluation so that work is not repeated unnecessarily.

Quang Trinh

SAIC Accredited Testing & Evaluation Labs
Common Criteria/FIPS Evaluator

Quang.M.Trinh@saic.com

James Arnold

SAIC Accredited Testing & Evaluation Labs
AVP/Technical Director

James.L.Arnold.Jr@saic.com

<http://www.saic.com/infosec/cctl.html>