An analysis of the coverage of some cryptographic aspects in the Common Criteria

Vittorio Bagini, Franco Guida, Renato Menicocci

Fondazione Ugo Bordoni (FUB)
Organismo di Certificazione della Sicurezza Informatica (OCSI)

Thanks to Massimiliano Orazi (FUB, OCSI) for presenting this at 9th ICCC

Fondazione Ugo Bordoni

OCSI
Organismo di Certificazione della Sicurezza Informatica

Summary

- Five aspects have been explored
  1. *Strength of cryptography*
  2. *Enforcement of selected cryptography*
  3. *Side Channel Attacks*
  4. *Fault Attacks*
  5. *Consideration of Direct Attacks against Cryptographic Mechanisms*
- Hereafter, CC v3.1 consists of
  - Part 1, Release 1 (September 2006)
  - Parts 2, 3 and CEM, Release 2 (September 2007)

Summary of *Strength of cryptography*

1. *Strength of cryptography in CC v3.1* (5 slides)
   - Statements from CC v3.1 and precise comparison with CC v2.3 (notice that the relevant aspect was explicitly covered in CC v2.3)
   - Respective implications and/or observations
2. *Additional comparison with CC v2.3* (2 slides)
   - Relevant statements from CC v2.3 that have no corresponding statement in CC v3.1

Strength of cryptography in CC v3.1 (1/5)

- **Statement:** *The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. Should independent assessment of mathematical properties of cryptography be required, the evaluation scheme under which the CC is applied must make provision for such assessments.* (CC v3.1 Pt.1, Sec.2, Par.6)
- **Comparison with CC v2.3:** This text was already in CC v2.3 (CC v2.3 Pt.1, Sec.2, Par.6) with the only difference that *cryptography embedded in a TOE* has been replaced by *cryptography*. Notice that in CC v3.1 no relevant example of such an assessment is given. An example was given in CC v2.3 but it has been eliminated (see below*)

Strength of cryptography in CC v3.1 (2/5)

- **Implication:** As in CC v2.3, the scheme must provide an independent assessment of mathematical properties of cryptographic functionalities (algorithms, protocols, etc.) if this is explicitly required
- **Observation:** For the type of assessment that the scheme should provide, the following text seems to be relevant. Notice that total freedom is left to the scheme in specifying the relevant guidance
- **Statement:** *The matters that schemes may choose to specify include:* […] *any specific guidance in dealing with cryptography;* […] (CEM v3.1, Ann.A.5, Par.1871)
- **Comparison with CC v2.3:** This text was already in CC v2.3 (CEM v2.3, Ann.A.9, Par.1864)

Strength of cryptography in CC v3.1 (3/5)

- **Statement:** *Direct attacks reliant upon a weakness in a cryptographic algorithm should not be considered under Vulnerability analysis (AVA_VAN), as this is outside the scope of the CC. Correctness of the implementation of the cryptographic algorithm is considered during the ADV and ATE activities.* (CEM v3.1, Ann.B.2, Par.1894)
- **Comparison with CC v2.3:** This text is completely new with respect to CC v2.3, where AVA_VAN family was not defined
- **Implication 1:** During vulnerability analysis, the evaluator should not consider direct attacks against cryptographic mechanisms (in this presentation, such attacks must be understood as based on logical vulnerabilities of the cryptographic functionalities implemented in the mechanisms)

Strength of cryptography in CC v3.1 (4/5)

- **Implication 2:** The evaluator must consider the correctness of the implementation of the cryptographic mechanisms during ADV and ATE activities
- **Observation:** The text *Direct attacks reliant upon a weakness in a cryptographic algorithm should not be considered* […] seems to be inconsistent with the following statement, where a direct attack against cryptographic mechanisms is considered in some way

Strength of cryptography in CC v3.1 (5/5)

- **Statement:** […] *For example, where an experiment reveals some bits or bytes of a confidential data item (such as a key), it is necessary to consider how the remainder of the data item would be obtained (in this example some bits might be measured directly by further experiments, while others might be found by a different technique such as exhaustive search).* […] (CEM v3.1, Ann.B.4, Par.1956)
- **Comparison with CC v2.3:** This text is completely new with respect to CC v2.3, where AVA_VAN family was not defined
- **Implication:** It seems that, during vulnerability analysis, the evaluator should also consider direct attacks against cryptographic mechanisms (such as exhaustive key search)

Additional comparison with CC v2.3 (1/2)

- **Note:** In CC v2.3 additional statements about strength of cryptography were included in the coverage of AVA_SOF family, which is no longer defined in CC v3.1
- **Statement 1** (*example of scheme assessment announced before): *SOF analysis is performed on mechanisms that are probabilistic or permutational in nature, such as password mechanisms or biometrics. Although cryptographic mechanisms are also probabilistic in nature and are often described in terms of strength, AVA_SOF.1 Strength of TOE security function evaluation is not applicable to cryptographic mechanisms. For such mechanisms, the evaluator should seek scheme guidance.* (CEM v2.3, Sec.12.9, Par.838; Sec.13.10, Par.1170; Sec.14.10, Par.1610)

Additional comparison with CC v2.3 (2/2)

- **Statement 2/3:** *The strength of cryptographic algorithms is outside the scope of the CC. Strength of function only applies to probabilistic or permutational mechanisms that are non-cryptographic. Therefore, where an PP contains a minimum SOF claim this claim does not apply to any cryptographic mechanisms with respect to a CC evaluation. Where such cryptographic mechanisms are included in a TOE the evaluator determines that the PP/ST includes a clear statement that the assessment of algorithmic strength does not form part of the evaluation.*(CEM v2.3, Sec.9.3, Par.240 / Sec.10.3, Par.422)

Summary of *Enforcement of selected cryptography*

1. *Enforcement of selected cryptography in CC v3.1* (2 slides)
   - Statement from CC v3.1 and precise comparison with *previous practice* (notice that the relevant aspect, though not explicitly covered in CC v2.3, has been considered in previous practice, as resulting from PPs and STs conformant to CC v2.x)
   - Implication and observations
2. *Additional comparison with previous practice* (2 slides)
   - An approach used in previous practice that is not considered in CC v3.1
   - A note on the impact on the evaluation of the enforcement of selected cryptography

Enforcement of selected cryptography in CC v3.1 (1/2)

- **Statement:** *In some cases, an ST writer may wish to refer to an external standard, such as a particular cryptographic standard or protocol. The CC allows three ways of doing this:*
  - *As an organisational security policy (or part of it).* […]
  - *As a technical standard (for example a cryptographic standard) used in a refinement of an SFR.* […]
  - *As a technical standard (for example a cryptographic standard) mentioned in the TOE summary specification.* […]

  (CC v3.1 Pt.1, Ann.A.13. Par.355)

Enforcement of selected cryptography in CC v3.1 (2/2)

- **Comparison with previous practice:** The first two ways have already been used in practice [see our 8th ICCC presentation]. The third way has not already been used (as far as we know)
- **Implication:** An ST writer is allowed to refer to a cryptographic standard only in one of the ways described in the statement above
- **Observation 1:** The first two ways may be used also for PP writing
- **Observation 2:** The third way cannot be used for PP writing, as a PP does not include a TOE summary specification

Additional comparison with previous practice (1/2)

- There is also a fourth way to enforce a cryptographic standard which has not been included in CC v3.1 even though it has already been used in practice [see our 8th ICCC presentation]

  This way consists in referring to the cryptographic standard in a TOE Security Objective

  Notice that this way is equivalent to the first one stated in CC v3.1 if the relevant TOE Security Objective is generated by an OSP that also refers to the standard

  Notice that this way is generally not allowed in CC v3.1 and this seems to be a positive fact because it eliminates a potential problem (see below*)

Additional comparison with previous practice (2/2)

- Enforcement of cryptography: impact on the evaluation
  - Apparently no impact in CC v3.1
  - *Potential problem announced before: Notice that the enforcement of cryptography had a possible impact on the sufficiency analysis of evaluations conformant to CC v2.x [see our 8th ICCC presentation], especially where
    - The cryptographic standard is referred to in a TOE Security Objective (**no longer allowed in CC v3.1!**)
    - And the TOE Security Objective is originated by Threats that explicitly address cryptanalytic attacks (brute-force and/or other)
    - And the evaluation process is executed within a scheme scrupulously providing *specific guidance in dealing with cryptography*

Summary of *Side channel attacks*

1. *Definition of side channel attacks* (1 slide)
   - Limited to cryptographic devices with a note on generalization
2. *Side channel attacks in CC v3.1: ADV_ARC** (5 slides)
3. *Side channel attacks in CC v3.1: AVA_VAN** (3 slides)

   [*Notice that in CC v3.1 *side channel attacks* are only covered in ADV_ARC and AVA_VAN]
4. *Side-channel attack potential* (4 slides)
   - Statements from CC documents: implications and observations
5. *Comparison with previous practice* (2 slides)
   - Notice that this *side channel attacks*, though not explicitly covered in CC v2.3, have been considered in previous practice, as resulting from PPs and STs conformant to CC v2.x

Definition of Side channel attacks

- **Note:** The following definition is limited to cryptographic devices. Notice anyway that side channel attacks may exist against any device that processes sensitive data, even though it does not perform any cryptographic operation
- Physical attacks against cryptographic devices (called *Observation attacks* in *CCDB-2006-04-007 Requirements to perform Integrated Circuit Evaluations*)
  - These attacks do not modify the cryptographic device
  - They aim at recovering sensitive data (e.g., secret and/or private keys) by observing the physical behavior (e.g., execution time and/or power consumption) of the cryptographic device
  - Several analytic techniques are used to recover sensitive data from physical measurements (e.g., execution time and/or power consumption)

Side channel attacks in CC v3.1: ADV_ARC (1/5)

- **Statement:** […] *ADV_ARC.1.5C* ***The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.***

  ADV_ARC.1-5 The evaluator ***shall examine*** *the security architecture description to determine that it presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.* (CEM v3.1, Sec.11.3, Par.537)

- **Observation:** These are the respective definitions of the requirement ADV_ARC.1.5C and of the related work unit ADV_ARC.1-5. The following statements are included in the CEM v3.1 description of ADV_ARC.1-5

Side channel attacks in CC v3.1: ADV_ARC (2/5)

- **Statement:** *Another example of bypass is when the TSF is supposed to maintain confidentiality of a cryptographic key (one is allowed to use it for cryptographic operations, but is not allowed to read/write it). If an attacker has direct physical access to the device, he might be able to examine side-channels such as the power usage of the device, the exact timing of the device, or even any electromagnetic emanations of the device and, from this, infer the key.* (CEM v3.1, Sec.11.3, Par.543)
- **Observation 1:** This text emphasizes side channel attacks as a way to bypass a security functionality (notice that the text also gives a definition of side channel attacks, which are also defined in *Evaluator construction of a Vulnerability Analysis* (CEM v3.1, Ann.B.2) (see below*))

Side channel attacks in CC v3.1: ADV_ARC (3/5)

- **Observation 2:** In ADV_ARC side channel attacks are considered as a way by which an attacker may bypass security enforcement. Anyway, based on the following definition, a side channel attack is an example of *monitoring attack* (see also the definition of side channel attacks given in *Evaluator construction of a Vulnerability Analysis* (CEM v3.1, Ann.B.2) (see below*))

  ***monitoring attacks** – a generic category of attack methods that includes passive analysis techniques aiming at disclosure of sensitive internal data of the TOE by operating the TOE in the way that corresponds to the guidance documents.* (CC v3.1 Pt.1, Sec.4.4, Par.150)

Side channel attacks in CC v3.1: ADV_ARC (4/5)

- **Statement:** *If such side-channels may be present, the demonstration should address the mechanisms that prevent these side-channels from occurring, such as random internal clocks, dual-line technology etc. Verification of these mechanisms would be verified by a combination of purely design-based arguments and testing.* (CEM v3.1, Sec.11.3, Par.544)
- **Implication:** When examining the security architecture description provided by the developer, the evaluator must check that the mechanisms that make side channels ineffective are addressed

Side channel attacks in CC v3.1: ADV_ARC (5/5)

- **Observation 1:** The details of the verification required to the evaluator (*Verification of these mechanisms would be verified by a combination of purely design-based arguments and testing*) are not clear in the text
- **Observation 2:** In practice, there is also a corresponding implication for the developer, even though this is not made explicit in CC v3.1

Side channel attacks in CC v3.1: AVA_VAN (1/3)

- **Note:** The statements reported in the following are included under the heading *Monitoring* of the *Generic vulnerability guidance* in *Evaluator construction of a Vulnerability Analysis* (CEM v3.1 Ann.B.2)
- **Statement:** […] *An **unenforced** signalling channel carrying information under control of the information flow control policy can also be caused by monitoring of the processing of any object containing or related to this information (e.g. side channels).* […] (CEM v3.1, Ann.B.2, Par.1897)
- **Observation:** Side channels are mentioned as an example of ***unenforced** signalling channels,* as opposed to ***enforced** signalling channels* that include covert channels. The utility of this statement is not clear

Side channel attacks in CC v3.1: AVA_VAN (2/3)

- **Statement** (*the definition of side channel attacks announced before): *Side Channel Analysis includes crypt analytical techniques based on physical leakage of the TOE. Physical leakage can occur by timing information, power consumption or power emanation during computation of a TSF. Timing information can be collected also by a remote-attacker (having network access to the TOE), power based information channels requires that the attacker is in the near-by environment of the TOE.* (CEM v3.1, Ann.B.2, Par.1900)
- **Implication:** When constructing an independent Vulnerability Analysis (action element AVA_VAN.2.3E, AVA_VAN.3.3E or AVA_VAN.4.3E), the evaluator should take side channels into account

Side channel attacks in CC v3.1: AVA_VAN (3/3)

- **Observation:** The AVA_VAN definition of side channel attacks emphasizes the implementation of the attacks, whereas the ADV_ARC definition emphasized their result

Side-channel attack potential (1/4)

- **Note 1:** The following statement, included in *Calculating attack potential* (CEM v3.1 Ann.B.4), seems to be the only concrete example of how side channels could be considered in the evaluator's Vulnerability Analysis
- **Note 2:** Recall that attack potential is calculated as a function of several *factors*, one of which is the *equipment*

Side-channel attack potential (2/4)

- **Statement:** ***IT hardware/software or other equipment*** *refers to the equipment required to identify or exploit a vulnerability.* […] *Specialised equipment is not readily available to the attacker, but could be acquired without undue effort. This could include purchase of moderate amounts of equipment (e.g. power analysis tools, use of hundreds of PCs linked across the Internet would fall into this category), or development of more extensive attack scripts or programs. If clearly different test benches consisting of specialised equipment are required for distinct steps of an attack this shall be rated as bespoke.* […] (CEM v3.1, Ann.B.4, Par.1970)
- **Implication:** When calculating the potential of an attack using power analysis, the evaluator should rate the factor *Equipment* at least as *Specialised*. This is explicitly confirmed in a CC supporting document (see below*)

Side-channel attack potential (3/4)

- **Observation:** Other information about side channel attacks may be found in *CCDB-2008-04-001 Application of Attack Potential to Smartcards*, which in particular includes
  - Identification of Factors
  - Examples of attack methods

  Anyway, this document is not intended to be a complete guide to calculating attack potential, since […] *only a general outline of the attacks is given. For more detailed descriptions and examples, please refer to the certification bodies. They can also provide examples as reference for rating.* (Sec.4, Par.72)

  Notice that here the scheme is required to provide guidance to calculating attack potential

Side-channel attack potential (4/4)

In *CCDB-2008-04-001* it is precisely confirmed (*as announced before) that, for a power analysis attack, the factor *Equipment* should be rated as *Specialised*. In fact, *a digital sampling oscilloscope* is mentioned as the basic tool for power analysis and in a specific table such a tool is categorised as *Specialised*

Comparison with previous practice (1/2)

- Side channel attacks were not explicitly covered in CC v2.3 but they have been considered in practice, as resulting from PPs and STs conformant to CC v2.x
- Three approaches have been used [see our 8th ICCC presentation]
  - Approach 0: A specific Assumption is defined to have the Environment take care of the problem (no specific Threats for the TOE are defined)
  - Approach 1: The problem is solved by Standard SFRs
  - Approach 2: The problem is solved by Extended SFRs

Comparison with previous practice (2/2)

- **Previous practice:** Only when above approaches 1 or 2 are used, the evaluator is required to assess both sufficiency and correctness of the countermeasures against side channel attacks implemented within the TOE
- **CC v3.1:** New ad hoc SFR have not been included in the CC Pt.2 catalogue, but side channel attacks are explicitly considered in the CEM. In particular
  - In ADV_ARC the developer is required to document the countermeasures implemented against side channel attacks and the evaluator is required to verify such countermeasures
  - In AVA_VAN the evaluator is required to consider side channel attacks among monitoring attacks and to calculate the relevant attack potential

Summary of *Fault attacks*

1. *Definition of Fault attacks* (1 slide)
   - Limited to cryptographic devices with a note on generalization
2. *Fault attacks in CC v3.1* (1 slide)
   - Statement from CC v3.1: implication
3. *Fault attack potential* (1 slide)
   - Statements from a CC supporting document
4. *Comparison with previous practice* (2 slides)
   - Notice that *fault attacks*, though not explicitly covered in CC v2.3, have been considered in previous practice, as resulting from PPs and STs conformant to CC v2.x

Definition of Fault attacks

- **Note:** The following definition is limited to cryptographic devices. Notice anyway that fault attacks may exist against any device that processes sensitive data, even though it does not perform any cryptographic operation
- Physical attacks against cryptographic devices (called *Perturbation attacks* in *CCDB-2006-04-007 Requirements to perform Integrated Circuit Evaluations*)
  - These attacks modify the cryptographic device in a transient way (the impact of the induced fault is not permanent)
  - They aim at recovering sensitive data (e.g., secret and/or private keys) by exploiting the modified operation of the cryptographic device
  - Transient faults are induced by suitably perturbating the cryptographic device (e.g., by using power glitches and/or electro-magnetic radiation)

Fault attacks in CC v3.1

- **Note:** The statement reported in the following, which describes fault attacks, is included under the heading *Tampering* of the *Generic vulnerability guidance* in the *Evaluator construction of a Vulnerability Analysis* (CEM v3.1, Ann.B.2)
- **Statement:** […] *Physical manipulation can be with the TOE internals aiming at internal modifications of the TOE (e.g. by using optical fault induction as an interaction process), at the external interfaces of the TOE (e.g. by power or clock glitches) and at the TOE environment (e.g. by modifying temperature).* […] (CEM v3.1, Ann.B.2, Par.1888)
- **Implication:** When constructing an independent Vulnerability Analysis (action element AVA_VAN.2.3E, AVA_VAN.3.3E or AVA_VAN.4.3E), the evaluator should take into account fault attacks

Fault attack potential

- **Observation 1:** During Vulnerability Analysis the evaluator should calculate fault attack potential, but no detail has been found in CC v3.1 of this calculation
- **Observation 2:** Other information about fault attacks (*Perturbation attacks*) may be found in *CCDB-2008-04-001 Application of Attack Potential to Smartcards*. Recall that this document is […] *only a general outline of the attacks is given. For more detailed descriptions and examples, please refer to the certification bodies. They can also provide examples as reference for rating.* (Sec.4, Par.72)

  Notice that, again, the scheme is required to provide guidance to calculating attack potential

Comparison with previous practice (1/2)

- Fault attacks were not explicitly covered in CC v2.3 but they have been considered in practice, as resulting from PPs and STs conformant to CC v2.x
- Two approaches have been found to be used [see our 8th ICCC presentation]
  - Approach 0: A specific Assumption is defined to have the Environment take care of the problem (no specific Threats for the TOE are defined)
  - Approach 1: The problem is solved by Standard SFRs

Comparison with previous practice (2/2)

- **Previous practice:** Only when above approach 1 is used, the evaluator is required to assess both sufficiency and correctness of the countermeasures against fault attacks implemented within the TOE
- **CC v3.1:** New ad hoc SFR have not been included in the CC Pt.2 catalogue, but fault attacks are explicitly considered in the CEM. In particular
  - In AVA_VAN the evaluator is required to consider fault attacks among tampering attacks and to calculate the relevant attack potential

Summary of *Consideration of Direct Attacks against Cryptographic Mechanisms*

1. *Direct Attacks against Cryptographic Mechanisms in CC v3.1* (1 slide)
   - Recall of relevant statements from CC v3.1
2. *Recall of Trinh and Arnold presentation at 8th ICCC* (1 slide)
   - Focus on the part suggesting to consider direct attacks against cryptographic mechanisms
3. *Support to Consideration* (4 slides)
   - Possible arguments for including direct attacks against cryptographic mechanisms in CC evaluation
4. *Our Proposal* (6 slides)
   - A possible approach for including direct attacks against cryptographic mechanisms in CC evaluation

Direct Attacks against Cryptographic Mechanisms in CC v3.1

- **Statement:** *Direct attacks reliant upon a weakness in a cryptographic algorithm should not be considered under Vulnerability analysis (AVA_VAN), as this is outside the scope of the CC.* […] (CEM, Ann. B.2, Par. 1894)
- **Statement:** […] *For example, where an experiment reveals some bits or bytes of a confidential data item (such as a key), it is necessary to consider how the remainder of the data item would be obtained (in this example some bits might be measured directly by further experiments, while others might be found by a different technique such as exhaustive search).* […] (CEM v3.1, Ann.B.4, Par.1956)

Recall of Trinh and Arnold presentation at 8th ICCC

- Q. Trinh and J. Arnold presented at 8th ICCC an investigation of Vulnerability Analysis for Cryptographic Mechanisms
  - They remarked that during Vulnerability Analysis the evaluator **must** consider all those *aspects of cryptographic mechanisms that are not based on cryptographic strength and, hence, are not outside the scope of the Common Criteria*
  - They proposed a method by which the evaluator may identify the aspects of cryptographic mechanisms that must be considered during Vulnerability Analysis
  - **They suggested that during Vulnerability Analysis the evaluator could also consider some direct attacks against cryptographic mechanisms**

Support to Consideration (1/4)

- **Hypothesis:** The position that declares direct attacks against cryptographic mechanisms *outside the scope of the CC* may be reviewed (at least partially)
- In the next slides, we give a contribution to this revision (we are aware that the addressed question is quite tricky; nonetheless, we think that the feasibility analysis of Trinh and Arnold proposal is worth an effort)

Support to Consideration (2/4)

- **Hypothesis:** Only direct attacks are based exclusively on logical weaknesses of cryptographic mechanisms
- Then, as long as direct attacks are not considered during evaluation, there is a substantial risk that logical weaknesses of cryptographic mechanisms included in the TOE will be ignored (it is debatable the value of evaluating the correct and robust* implementation of a cryptographic mechanism that could be logically weak: an attacker always looks for the simplest way of violating the security objectives) [*Resistant to non direct attacks]

Support to Consideration (3/4)

- To keep its current position, CC could
  1. Affirm that a careful user is/should be aware of the previous risk
  2. Recall that each scheme could autonomously protect itself against the previous risk
  3. Choose to require a TOE to include only cryptographic mechanisms whose logical weaknesses are negligeable (in terms of corresponding attack potential)
- As for solutions 1 and 2, we note that considering direct attacks in a way that is, as more as possible, scheme independent would increase the significance of the evaluation and therefore the protection provided even to a careless user

Support to Consideration (4/4)

- Notice that any shift from the current CC position would make it necessary to assess, at some extent, the logical weaknesses of cryptographic mechanisms

Our Proposal (1/6)

- **Hypothesis:** Direct attacks have been declared outside the scope of CC to avoid requiring the evaluator to have an **advanced** cryptologic expertise
- Notice that the evaluator, as an ICT security expert, should have an (at least) **elementary** cryptologic expertise
- Including direct attacks should be done by taking into account the cryptologic expertise of the typical evaluator (This approach could even be extended to a full consideration of direct attacks against cryptographic mechanisms. Notice that, if needed, the evaluator could resort to external cryptologic expertise)

Our Proposal (2/6)

- According to the previous considerations, direct attacks against cryptographic mechanisms could be classified in three categories, each of which should be managed in a different way
  - Direct attacks based on *structural* vulnerabilities of the mechanisms, as inadequate dimension and statistical quality of the security parameters
  - Direct attacks based on *known* vulnerabilities in the logic of the mechanisms
  - Direct attacks based on *new* vulnerabilities (to be searched in the logic of the mechanisms)

Our Proposal (3/6)

- Direct attacks based on structural vulnerabilities can obviously always be considered (**elementary** cryptologic expertise is required), provided that the input/output behaviour of the mechanism is known
  - Example of attack: exhaustive key search
- Direct attacks based on known vulnerabilities could also be considered*, provided that both public and adequate documentation exists [*Notice that the relevant evaluator's task is the attack potential computation, for which an **elementary** cryptologic expertise is required, and not the execution of the attack itself!]
  - Example of attack: specific collision search for MD5 hash function

Our Proposal (4/6)

- Direct attacks based on new vulnerabilities could be excluded from the evaluation, because searching new vulnerabilities in the logic of the mechanism requires **advanced** cryptologic expertise, which can be considered beyond the cryptologic expertise of the typical evaluator

Our Proposal (5/6)

- The Certification Report should clearly indicate the performed analysis of susceptibility of cryptographic mechanisms to direct attacks, right in terms of
  - Structural vulnerabilities
  - Known vulnerabilities
  - New vulnerabilities
- CCRA should provide guidance about structural and known vulnerabilities by tables analogous to those published for side channel attacks in *CCDB-2008-04-001 Application of Attack Potential to Smartcards*

Our Proposal (6/6)

- Notice the following two cases (recall again that *any* relevant action of the evaluator should be clearly stated in the Certification Report)
- **Well known cryptographic mechanisms:** Direct attacks based on structural and known vulnerabilities are expected to be well considerable
- **Non well known cryptographic mechanisms (proprietary mechanisms, customized standard mechanisms, ...):** It may result impracticable to consider direct attacks based on known vulnerabilities and even those based on structural ones. Possible evaluator actions are
  - Avoid any consideration of direct attacks
  - Resort to external cryptologic expertise