



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN
 - ❑ Dans les critères*: succinct mais objectif !



LES CRITÈRES COMMUNS

➤ Le niveau AVA_VAN

- ❑ Dans les critères: succinct mais objectif !
 - *“The developer shall provide the TOE for testing”*



LES CRITÈRES COMMUNS

➤ Le niveau AVA_VAN

- ❑ Dans les critères: succinct mais objectif !
 - *“The developer shall provide the TOE for testing”*
 - *“The TOE shall be suitable for testing”*



LES CRITÈRES COMMUNS

➤ Le niveau AVA_VAN

❑ Dans les critères: succinct mais objectif !

- *“The developer shall provide the TOE for testing”*
- *“The TOE shall be suitable for testing”*
- *“The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE”*



LES CRITÈRES COMMUNS

➤ Le niveau AVA_VAN

□ Dans les critères: succinct mais objectif !

- *“The developer shall provide the TOE for testing”*
- *“The TOE shall be suitable for testing”*
- *“The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE”*
- *“The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE”*



LES CRITÈRES COMMUNS

➤ Le niveau AVA_VAN

□ Dans les critères: succinct mais objectif !

- *“The developer shall provide the TOE for testing”*
- *“The TOE shall be suitable for testing”*
- *“The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE”*
- *“The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE”*
- *“The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing **Basic / Enhanced-Basic / Moderate / High** attack potential”*



LES CRITÈRES COMMUNS

➤ Le niveau AVA_VAN

□ Dans les critères*: succinct mais objectif !

- *“The developer shall provide the TOE for testing”*
- *“The TOE shall be suitable for testing”*
- *“The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE”*
- *“The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE”*
- *“The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing **Basic** / **Enhanced-Basic** / **Moderate** / **High** attack potential”*

↑
AVA_VAN.3

↑
AVA_VAN.4

↑
AVA_VAN.5

↑
AVA_VAN.1
AVA_VAN.2



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puce
 - ❑ Comment définir le potentiel d'attaque (Basic – enhanced-basic, moderate et High) ?



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment définir le potentiel d'attaque (Basic – enhanced-basic, moderate et High) ?
 - ❑ Table de cotation*

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

Table 11: Rating of vulnerabilities for CC v3



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment définir le potentiel d'attaque (Basic – enhanced-basic, moderate et High) ?
 - ❑ Table de cotation

AVA_VAN.1-2 →

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

Table 11: Rating of vulnerabilities for CC v3



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment définir le potentiel d'attaque (Basic – enhanced-basic, moderate et High) ?
 - ❑ Table de cotation

	Range of values*	TOE resistant to attackers with attack potential of:
	0-15	No rating
AVA_VAN.1-2 →	16-20	Basic
AVA_VAN.3 →	21-24	Enhanced-Basic
	25-30	Moderate
	31 and above	High

Table 11: Rating of vulnerabilities for CC v3



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment définir le potentiel d'attaque (Basic – enhanced-basic, moderate et High) ?
 - ❑ Table de cotation

	Range of values*	TOE resistant to attackers with attack potential of:
	0-15	No rating
AVA_VAN.1-2 →	16-20	Basic
AVA_VAN.3 →	21-24	Enhanced-Basic
AVA_VAN.4 →	25-30	Moderate
	31 and above	High

Table 11: Rating of vulnerabilities for CC v3



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment définir le potentiel d'attaque (Basic – enhanced-basic, moderate et High) ?
 - ❑ Table de cotation

	Range of values*	TOE resistant to attackers with attack potential of:
	0-15	No rating
AVA_VAN.1-2 →	16-20	Basic
AVA_VAN.3 →	21-24	Enhanced-Basic
AVA_VAN.4 →	25-30	Moderate
AVA_VAN.5 →	31 and above	High

Table 11: Rating of vulnerabilities for CC v3



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment définir le potentiel d'attaque (Basic – enhanced-basic, moderate et High) ?
 - ❑ Table de cotation

	Range of values*	TOE resistant to attackers with attack potential of:
AVA_VAN.1-2	0-15	No rating
AVA_VAN.3	16-20	Basic
AVA_VAN.4	21-24	Enhanced-Basic
AVA_VAN.5	25-30	Moderate
	31 and above	High

Table 11: Rating of vulnerabilities for CC v3





LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment coter une attaque ?



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment coter une attaque ?
 - ❑ 5 critères*



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment coter une attaque ?
 - ❑ 5 critères:
 1. Temps passé



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment coter une attaque ?
 - ❑ 5 critères:
 1. Temps passé
 2. Niveau d'expertise



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment coter une attaque ?
 - ❑ 5 critères:
 1. Temps passé
 2. Niveau d'expertise
 3. Connaissance du produit



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment coter une attaque ?
 - ❑ 5 critères:
 1. Temps passé
 2. Niveau d'expertise
 3. Connaissance du produit
 4. Accessibilité au produit



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment coter une attaque ?
 - ❑ 5 critères:
 1. Temps passé
 2. Niveau d'expertise
 3. Connaissance du produit
 4. Accessibilité au produit
 5. Equipement nécessaire



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment coter une attaque ?
 - ❑ 5 critères:
 1. Temps passé
 2. Niveau d'expertise
 3. Connaissance du produit
 4. Accessibilité au produit
 5. Equipement nécessaire
 - ❑ A chaque critère une table de cotation



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment coter une attaque ?
 - ❑ 5 critères:
 1. Temps passé

	Identification	Exploitation
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*

Table 1: Rating for Elapsed Time



LES CRITÈRES COMMUNS

➤ Le niveau AVA_VAN pour les Cartes à puces

❑ Comment coter une attaque ?

❑ 5 critères:

2. Niveau d'expertise

	Identification	Exploitation
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6

Table 4: Rating for Expertise

- *Layman: pas d'expertise particulière*
- *Proficient: connaissance d'attaques classiques et concepts de sécurité*
- *Expert: connaissances des algorithmes, protocoles, structures HW, principes et concepts de sécurité – techniques et outils pour définir de nouvelles attaques*
- *Multiple Expert: niveau « expert » sur différents niveaux d'attaque (par exemple manipulation HW et crypto)*



LES CRITÈRES COMMUNS

➤ Le niveau AVA_VAN pour les Cartes à puces

❑ Comment coter une attaque ?

❑ 5 critères:

3. Connaissance du produit

	Identification	Exploitation
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA

Table 5: Rating for Knowledge of TOE

- **Public:** information dans le domaine publique
- **Restricted:** information utilisé lors du développement de la puce (spécifications, guides, documents de préparation...)
- **Sensitive:** information HLD et LLD
- **Critical:** implémentation (design et code source)
- **Very critical:** informations et outils spécifiques et propre au produit



LES CRITÈRES COMMUNS

- Le niveau AVA_VAN pour les Cartes à puces
 - ❑ Comment coter une attaque ?
 - ❑ 5 critères:
 - 4. Accessibilité au produit

	Identification	Exploitation
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*

Table 6: Rating for Access to TOE



LES CRITÈRES COMMUNS

➤ Le niveau AVA_VAN pour les Cartes à puces

❑ Comment coter une attaque ?

❑ 5 critères:

5. Equipement nécessaire

	Identification	Exploitation
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8

Table 9: Rating for Equipment

- **Standard:** oscilloscope de base, lecteur de carte, PC, logiciel d'analyse ou de génération de signal...
- **Specialized:** oscilloscope haut de gamme, microscope UV, équipement lazer, micro sonde, outils de gravure chimique...
- **Bespoke:** FIB (Focused Ion Beam), SEM (Scanning electron microscope), AFM (Atomic Force Microscope)...
- **Multiple Bespoke:** équipements « bespoke » sur différents niveaux de l'attaque



Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA



Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	0
Restricted	2	2
Sensitive	4	4
Critical	6	6

TOTAL

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

Table 11: Rating of vulnerabilities for CC v3



Exemple

Pour une DPA ?

Layman: pas d'expertise particulière

Proficient: connaissance d'attaques classiques et concepts de sécurité

Expert: connaissances des algorithmes, protocoles, structures HW, principes et concepts de sécurité – techniques et outils pour définir de nouvelles attaques

Multiple Expert: niveau « expert » sur différents niveaux d'attaque (par exemple manipulation HW et crypto)

Standard: oscilloscope de base, lecteur de carte, PC...

Specialized: oscilloscope haut de gamme, microscope UV

Bespoke: FIB (Focused Ion Beam), AFM (Atomic Force Microscope)...

Multiple Bespoke: équipements « bespoke » sur différents niveaux de l'attaque

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA



Exemple

Pour une DPA ?

Layman: pas d'expertise particulière

Proficient: connaissance d'attaques classiques et concepts de sécurité

Expert: connaissances des algorithmes, protocoles, structures HW, principes et concepts de sécurité – techniques et outils pour définir de nouvelles attaques

Multiple Expert: niveau « expert » sur différents niveaux d'attaque (par exemple manipulation HW et crypto)

Standard: oscilloscope de base, lecteur de carte, PC...

Specialized: oscilloscope haut de gamme, microscope UV

Bespoke: FIB (Focused Ion Beam), AFM (Atomic Force Microscope)...

Multiple Bespoke: équipements « bespoke » sur différents niveaux de l'attaque

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA



Exemple

Pour une DPA ?

Layman: pas d'expertise particulière

Proficient: connaissance d'attaques classiques et concepts de sécurité

Expert: connaissances des algorithmes, protocoles, structures HW, principes et concepts de sécurité – techniques et outils pour définir de nouvelles attaques

Multiple Expert: niveau « expert » sur différents niveaux d'attaque (par exemple manipulation HW et crypto)

Standard: oscilloscope de base, lecteur de carte, PC...

Specialized: oscilloscope haut de gamme, microscope UV

Bespoke: FIB (Focused Ion Beam), AFM (Atomic Force Microscope)...

Multiple Bespoke: équipements « bespoke » sur différents niveaux de l'attaque

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA



Exemple

Pour une DPA ?

Layman: pas d'expertise particulière

Proficient: connaissance d'attaques classiques et concepts de sécurité

Expert: connaissances des algorithmes, protocoles, structures HW, principes et concepts de sécurité – techniques et outils pour définir de nouvelles attaques

Multiple Expert: niveau « expert » sur différents niveaux d'attaque (par exemple manipulation HW et crypto)

Standard: oscilloscope de base, lecteur de carte, PC...

Specialized: oscilloscope haut de gamme, microscope UV

Bespoke: FIB (Focused Ion Beam), AFM (Atomic Force Microscope)...

Multiple Bespoke: équipements « bespoke » sur différents niveaux de l'attaque

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA



Exemple

Pour une DPA ?

Layman: pas d'expertise particulière

Proficient: connaissance d'attaques classiques et concepts de sécurité

Expert: connaissances des algorithmes, protocoles, structures HW, principes et concepts de sécurité – techniques et outils pour définir de nouvelles attaques

Multiple Expert: niveau « expert » sur différents niveaux d'attaque (par exemple manipulation HW et crypto)

Standard: oscilloscope de base, lecteur de carte, PC...

Specialized: oscilloscope haut de gamme, microscope UV

Bespoke: FIB (Focused Ion Beam), AFM (Atomic Force Microscope)...

Multiple Bespoke: équipements « bespoke » sur différents niveaux de l'attaque

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA



Exemple

Pour une DPA ?

Layman: pas d'expertise particulière

Proficient: connaissance d'attaques classiques et concepts de sécurité

Expert: connaissances des algorithmes, protocoles, structures HW, principes et concepts de sécurité – techniques et outils pour définir de nouvelles attaques

Multiple Expert: niveau « expert » sur différents niveaux d'attaque (par exemple manipulation HW et crypto)

Standard: oscilloscope de base, lecteur de carte, PC...

Specialized: oscilloscope haut de gamme, microscope UV

Bespoke: FIB (Focused Ion Beam), AFM (Atomic Force Microscope)...

Multiple Bespoke: équipements « bespoke » sur différents niveaux de l'attaque

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA



Exemple Pour une DPA ?

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

Table 11: Rating of vulnerabilities for CC v3

TOTAL = 15 points !

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA



LES CRITÈRES COMMUNS

➤ Le niveau AVA_VAN pour les Cartes à puces

