

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

*CC, Part3, V3, R4



- Le niveau AVA_VAN
 - □ Dans les critères: succinct mais objectif!
 - "The developer shall provide the TOE for testing"



- 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"



- 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"

Natalya Robert - ANSSI



- 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"



- 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"



- 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



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

Natalya Robert - ANSSI 78



- ➤ 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 vulnerabilites for CC v3



- ➤ 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	
	21-24	Enhanced-Basic	
	25-30	Moderate	
	31 and above	High	

Table 11: Rating of vulnerabilites for CC v3



- ➤ 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
$AVA_VAN.3 \longrightarrow$	21-24	Enhanced-Basic
	25-30	Moderate
	31 and above	High

Table 11: Rating of vulnerabilites for CC v3



- ➤ 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
$AVA_VAN.3 \longrightarrow$	21-24	Enhanced-Basic
AVA_VAN.4 →	25-30	Moderate
	31 and above	High

Table 11: Rating of vulnerabilites for CC v3



- ➤ 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	
$AVA_VAN.3 \longrightarrow$	21-24	Enhanced-Basic	
AVA_VAN.4 →	25-30	Moderate	
AVA_VAN.5 →	31 and above	High	

Table 11: Rating of vulnerabilites for CC v3



- ➤ 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
$AVA_VAN.3 \longrightarrow \Box$	21-24	Enhanced-Basic
$AVA_VAN.4 \longrightarrow \Box$	25-30	Moderate
$AVA_VAN.5 \longrightarrow$	31 and above	High

Table 11: Rating of vulnerabilites for CC v3





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



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



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



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



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



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



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



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



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



- 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)



- 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



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

Exploitation
0
2
4
6
*

Table 6: Rating for Access to TOE



- 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, equipement lazer, micro sonde, outils de gravure chimique...
- Bespoke: FIB (Focused Ion Beam), SEM (Scanning electron mircroscope), AFM (Atomic Force Microscope)...
- Multiple Bespoke: équipements « bespoke » sur différents niveaux de l'attaque



< one hour 0 < one day 1 < one week 2 < one month 3 > one month 5 Not practical * Expertise * Layman 0 Proficient 2 2 Expert 5 4 Multiple Expert 7 6 Knowledge of the TOE * * Public 0 0 0 Restricted 2 2 2 Sensitive 4 3 3 Critical 6 5 NA design Access to TOE * NA < 10 samples 0 0 0 < 10 samples 1 2 2 < 100 samples 2 4 2 > 100 samples 3 6 Not practical * * Equipment None 0 0 0 Standard 1 2 Specialized (1) 3 4 4 Bespoke 5	Factors	Identification	Exploitation
< one hour 0 0 < one day 1 3 < one week 2 4 < one month 3 6 > one month 5 8 Not practical * * Expertise	Elapsed time		of the second
< one week	< one hour	0	0
< one month	< one day	1	3
Not practical * * *	< one week	2	4
Not practical * * *	124	3	6
Expertise Layman 0	> one month	5	8
Layman	Not practical	*	*
Layman 0 0 0 Proficient 2 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 9 NA design 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	15-4		
Proficient 2		0	0
Multiple Expert 7		2	2
Multiple Expert 7 6 Knowledge of the TOE 0 0 Public 0 0 Restricted 2 2 Sensitive 4 3 Critical 6 5 Very critical hardware design 9 NA Access to TOE 0 0 < 10 samples 0 0 0 < 30 samples 1 2 4 > 100 samples 3 6 Not practical * * Equipment None 0 0 0 0 Standard 1 2 2 4 3 4 Equipment 0 <td>Expert</td> <td>5</td> <td>4</td>	Expert	5	4
None		7	6
Public 0 0 Restricted 2 2 Sensitive 4 3 Critical 6 5 Very critical hardware design 9 NA Access to TOE NA NA < 10 samples	Knowledge of the TOE		8
Sensitive		0	0
Critical 6 5 Very critical hardware design 9 NA Access to TOE 0 0 < 10 samples	Restricted	2	2
Very critical hardware design 9 NA Access to TOE 0 0 < 10 samples	Sensitive	4	3
Access to TOE	Critical	6	5
Access to TOE	Very critical hardware	9	NA
< 10 samples	design		27
< 30 samples			
< 100 samples	< 10 samples	0	0
< 100 samples	< 30 samples	1	2
> 100 samples 3 6 Not practical * * Equipment 0 0 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) NA Public 0 NA Restricted 2 NA Sensitive 4 NA		2	4
Not practical * * * * * * * * * * * * *		3	6
Equipment 0 0 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) NA Public 0 NA Restricted 2 NA Sensitive 4 NA		*	*
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) NA Public 0 NA Restricted 2 NA Sensitive 4 NA	Equipment		
Specialized (1) 3		0	0
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	Standard	1	2
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	Specialized (1)	3	4
Multiple Bespoke 7 8 Open samples (rated according to access to open samples) Public 0 NA Restricted 2 NA Sensitive 4 NA		1.574.000	6
Open samples (rated according to access to open samples) Public 0 NA Restricted 2 NA Sensitive 4 NA		7	8
according to access to open samples) Public 0 NA Restricted 2 NA Sensitive 4 NA			
Public 0 NA Restricted 2 NA Sensitive 4 NA	according to access to open		
Public 0 NA Restricted 2 NA Sensitive 4 NA	samples)		
Restricted 2 NA Sensitive 4 NA		0	NA
Sensitive 4 NA		2	
France Control of the			
		6	CONTRACTOR OF THE PROPERTY OF



	Factors	Identification	Exploita	tion	
	Elapsed time				
	< one hour	0	0		
	< one day	1	3		
100	< one week	2	4		
_	< one month	3	6		
	> one month	5	8	ľ	
100	Not practical	*	*		
8	Expertise				
	Layman	0	0		
100	Proficient	2	2		
	Expert	5	4		
	Multiple Expert	7	6		
200	Knowledge of the TOE		82 86		
	Public	0	0		
	Restricted	2	2		
- 6	Sensitive	4	3		
	Critical	6	5		
186	Very critical hardware	9	NA		
9	design		100		
	Access to TOE				
100	< 10 samples	0	0		
	< 30 samples	1	2		
	< 100 samples	2	4		
100	> 100 samples	3	6		
	Not practical	*	*	**	*
	Equipment			Range of values*	TOE resistant to attackers with attack potential of:
	None	0	0	0-15	No rating
	Standard	1	2	16-20	Basic
	Specialized (1)	3	4	21-24	Enhanced-Basic
	Bespoke	5	6	25-30	Moderate
18	Multiple Bespoke	7	8	31 and above	High
	Open samples (rated	n samples (rated		Tabl	e 11: Rating of vulnerabilites for CC v3
	according to access to open	TOTA	┞ -		
8	samples)				
100	Public	0			
8	Restricted	2	N.		
	Sensitive	4	NA		
e	Critical	6	NA		99



Layman: pas d'expertise particulière

<u>Proficient</u>: 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

<u>Bespoke</u>: FIB (Focused Ion Beam), AFM (Atomic Force Microscope)...

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		8
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware	9	NA
design		5,00000
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



Layman: pas d'expertise particulière

<u>Proficient</u>: 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

<u>Multiple Expert</u>: 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

<u>Bespoke</u>: FIB (Focused Ion Beam), AFM (Atomic Force Microscope)...

<u>Multiple Bespoke</u>: équipements « bespoke » sur différents niveaux de l'attaque

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day		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	3	85
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware	9	NA
design		**************************************
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	1	=
according to access to open		
samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

)1



Layman: pas d'expertise particulière

<u>Proficient</u>: 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

<u>Bespoke</u>: FIB (Focused Ion Beam), AFM (Atomic Force Microscope)...

<u>Multiple Bespoke</u>: équipements « bespoke » sur différents niveaux de l'attaque

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day		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	Y	6
Knowledge of the TOE	3	8
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware	9	NA
design		
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

)2



Layman: pas d'expertise particulière

<u>Proficient</u>: 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

<u>Bespoke</u>: FIB (Focused Ion Beam), AFM (Atomic Force Microscope)...

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day		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	3	
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware	9	NA
design		
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



Layman: pas d'expertise particulière

<u>Proficient</u>: 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

<u>Bespoke</u>: FIB (Focused Ion Beam), AFM (Atomic Force Microscope)...

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day		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	Y	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware	9	NA
design		28
Access to TOE		
< 10 samples	0	0
< 30 samples	T	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



Layman: pas d'expertise particulière

<u>Proficient</u>: 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

<u>Multiple Expert</u>: 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

<u>Bespoke</u>: FIB (Focused Ion Beam), AFM (Atomic Force Microscope)...

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day		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	$\overline{\gamma}$	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware	9	NA
design		8
Access to TOE		
< 10 samples	0	0
< 30 samples	Ĭ	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



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

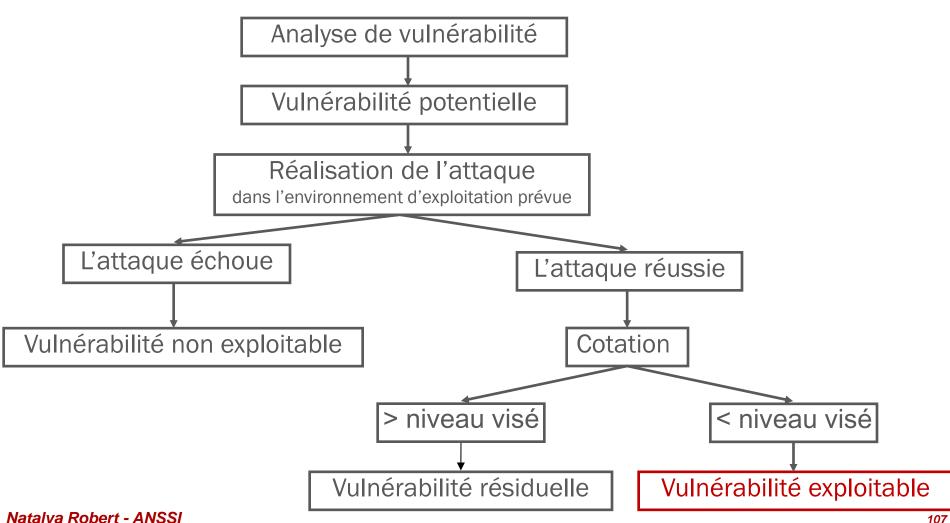
Table 11: Rating of vulnerabilites for CC v3

TOTAL = 15 points!

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day		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	$\overline{\gamma}$	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware	9	NA
design		8
Access to TOE		
< 10 samples	0	0
< 30 samples	Ĭ	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



Le niveau AVA_VAN pour les Cartes à puces



Natalya Robert - ANSSI