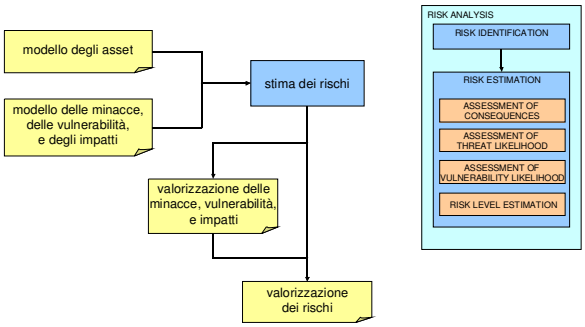
Il processo di analisi dei rischi (parte IV)

Marco Domenico Aime
< m.aime @ polito.it >

Politecnico di Torino
Dip. di Automatica e Informatica

1

2.2. Stima dei rischi (risk estimation)



2

Stima dei rischi

- **stima degli impatti**
  - assegnazione del valore a beni e impatti
- **stima dell'occorrenza delle minacce**
  - assegnazione della probabilità / frequenza delle minacce
- **stima dello sfruttamento delle vulnerabilità**
  - assegnazione della probabilità / facilità di sfruttamento delle vulnerabilità
- **stima del livello di rischio**
  - calcolo del livello di rischio combinando le stime precedenti

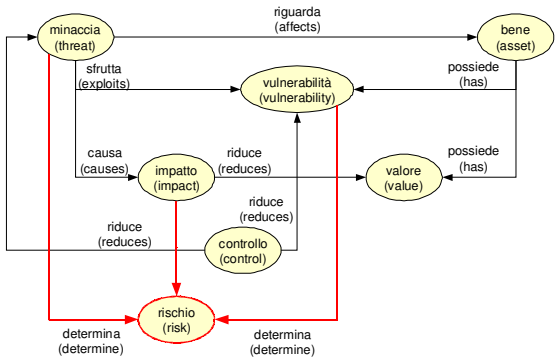
3

Stima dei rischi

- **non tutte le metodologie distinguono chiaramente tutti i passi di stima**
- **la sequenza effettiva dei pessi dipende dalla metodologia**
- **analisi qualitativa vs quantitativa**
  - valgono le osservazioni fatte riguardo il passo di definizione del contesto, e il passo di identificazione dei beni

4

Rischi



5

2.2.1. Stima degli impatti (Assessment of consequences)

- **a partire dal modello dei beni:**
  - stima dei beni (valore) e dipendenze
- **e dal modello degli impatti:**
  - conseguenze delle minacce (danni) e dipendenze
- **si calcola la stima degli impatti identificati:**
  - per dimensione di sicurezza
  - per ogni minaccia
- **si può poi aggregare:**
  - per bene, per minaccia, per dipendenze

6

Stima dei danni

- **la fase di identificazione dei danni identifica i beni che possono essere danneggiati da una minaccia**
- **per la stima, possiamo assegnare un valore alle eventuali degradazioni parziali:**
  - es. danno(Bi,Mj) = 60%
  - spesso difficile assegnare questi valori e/o calcolarli
- **una soluzione più robusta, ove possibile, consiste in:**
  - decomporre ulteriormente il bene
  - definire l'impatto in termini di danni binari
  - eventualmnte aggregare in seguito le stime di impatto

7

Stima degli impatti: esempi

- **esempio di stima dell'impatto:**
  - *impatto(Bi,Mj) = valore(Bi) x danno(Bi,Mj)*
- **esempio di aggregazione per bene:**
  - *impatto(Bi) = valore(Bi) x sum/max(danno(Bi,Mj)) su Mj*
- **esempio di aggregazione per minaccia:**
  - *impatto(Mj) = sum(valore(Bi) x danno(Bi,Mj)) su Bi*
- **esempio di aggregazione per dipendenza:**
  - *impatto(Bi) = valore(Bi) x sum(danno(Bk,Mj) x dipendenza(Bi,Bk)) su Bk*
  - *impatto(Mj) = sum(valore(Bi) x sum(danno(Bk,Mj) x dipendenza(Bi,Bk)) su Bk) su Bi*

8

2.2.2. Stima dell'occorrenza delle minacce (Assessment of threat likelihood)

- **stima molto difficile**
- **approcci:**
  - statistiche fornite dalle assicurazioni e dalle associazioni professionali
  - dai log di sistema
  - stima tabulare approssimata
  - metodo Delphi = stime indipendenti, distribuite, corrette una volta, convergenza o discussione

9

2.2.3. Stima delle vulnerabilità (Assessment of vulnerability likelihood)

- **si determina una stima complessiva della probabilità che una vulnerabilità sia efficacemente sfruttata in relazione a uno scenario di minaccia**
  - e si concretizzi dunque l'associato scenario di impatto
- **definita considerando:**
  - motivazione e capacità della sorgente di minaccia
  - natura della vulnerabilità
- **in seguito aggiornata considerando:**
  - esistenza e efficacia dei controlli

18/05/09 © Marco Domenico Aime (2009) 10

2.2.4. Stima dei rischi (Assessment of risk level)

- **infine si calcolano i livelli di rischio**
  - per bene
  - per minaccia
  - complessivo
    - utile per confrontare soluzioni alternative
- **il livello di rischio è funzione di:**
  - probabilità di occorrenza della minaccia
  - probabilità che la minaccia riesca ad esercitare una vulnerabilità
  - l'impatto conseguente

11

ISO 27005: esempio 1

fonte: ISO 27005

- **matrice con valori predefiniti**
  - assegno valore bene, proabilità minaccia, probabilità sfruttamento vulnerabilità => estraggo il valore di rischio corrisponedente

	Likelihood of occurrence - Threat	Low			Medium			High		
	Likelihood of occurrence - Vulnerability	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

12

Minacce e vulnerabilità in CRAMM

- **minacce:**
  - very low (una volta ogni 10 anni)
  - low (una volta ogni 3 anni)
  - medium (una volta all'anno)
  - high (una volta ogni 4 mesi)
  - very high (una volta al mese)
- **vulnerabilità = probabilità che in caso di incidente si verifichi lo scenario peggiore:**
  - low (probabilità < 33%)
  - medium (probabilità 33-66%)
  - high (probabilità > 66

13

Matrice dei rischi in CRAMM

	threat	VL	VL	VL	L	L	L	M	M	M	H	H	H	VH	VH	VH
	vulner.	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
asset value	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3	
	2	1	1	2	1	2	2	2	3	2	3	3	3	3	4	
	3	1	2	2	2	2	3	2	3	3	3	4	3	4	4	
	4	2	2	3	2	3	3	3	4	3	4	4	4	4	5	
	5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
	6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
	7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
	8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
	9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
	10	5	5	5	5	6	6	6	6	6	6	7	7	7	7	7

14

ISO 27005: esempio 2

fonte: ISO 27005

- **assegno valore impatto e probabilità minaccia => calcolo rischio = impatto x probabilità minaccia**
- **dalle misure di rischio posso ricavare il rank di ogni minaccia**

Threat descriptor (a)	Consequence (asset) value (b)	Likelihood of threat occurrence (c)	Measure of risk (d)	Threat ranking (e)
Threat A	5	2	10	2
Threat B	2	4	8	3
Threat C	3	5	15	1
Threat D	1	3	3	5
Threat E	4	1	4	4
Threat F	2	4	8	3

15

Combinazione minacce e vulnerabilità

- **parametri:**
  - K = n. vulnerabilità totali
  - V_i = vettore vulnerabilità
  - $C_{i,j}$ = correlazione vulner. i-esima / minaccia j-esima
  - M_j = valore minaccia j-esima
- **calcolo la suscettibilità del bene =** $\sum_{i=1}^{K} \left[V_i * \left(\sum_{j=1}^{L} C_{i,j} * M_j \right) \right]$
- **e calcolo il rischio = valore bene x suscettibilità**

16

ISO 27005: esempio 3

fonte: ISO 27005

- **per ogni bene:**
  - assegno il valore di impatto
  - e la probabilità combinando minacce e vulnerabilità
  - calcolo il rischio = imaptto x probabilità
- **sommo per tutti gli asset e ricavo la stima globale della bontà del sistema**

Levels of Threat	Low			Medium			High		
Levels of Vulnerability	L	M	H	L	M	H	L	M	H
Likelihood Value	0	1	2	1	2	3	2	3	4

Asset Value	0	1	2	3	4
Likelihood Value					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

17

Annual Loss Expectancy

- **stima quantitativa della perdita economica:**

  ALE = SLE x ARO

- **SLE = Single Loss Expectancy**
  - perdita causata da un singolo evento
- **ARO = Annual Rate of Occurrence**
  - probabilità annua di evento negativo
- **ALE = Annual Loss Expectancy**
  - perdita annua media

18

SP 800-30: esempio

fonte:
SP 800-30, pp 23-25

- **stima qualitativa**
- **assegno probilità combinata minaccia/vulnerabilità:**
  - tenendo conto di motivazione della sorgente di minaccia, natura della vulnerabilità, efficacia dei controlli esistenti

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

19

SP 800-30: esempio

fonte:
SP 800-30, pp 23-25

- **assegno la stima dell'impatto:**

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

20

SP 800-30: esempio

fonte:
SP 800-30, pp 23-25

- **calcolo la matrice del rischio:**
  - scala di rischio: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

Threat Likelihood	Impact		
	Low (10)	***Medium*** (50)	***High*** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

22

SP 800-30: esempio

fonte:
SP 800-30, pp 23-25

- **interpretazione dei livelli di rischio:**
  - (cfr. fase di classificazione dei rischi)

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

23

MAGERIT: esempio 1

fonte: MAGERIT v2,
techniche (eng version), pp 6

- **analisi con tabelle, qualitativa**
- **assegno valore bene e degradazione causata da una minaccia e ricavo la stima di impatto**

impact		*degradation*		
		1%	10%	100%
value	VH	M	H	VH
	H	L	M	H
	M	VL	L	M
	L	VL	VL	L
	VL	VL	VL	VL

VL: very low
L: low
M: medium
H: high
VH: very high

24

MAGERIT: esempio 1

fonte: MAGERIT v2,
techniche (eng version), pp 7

- **poi assegno la frequenza della minaccia e calcolo il livello di rischio:**

risk		*frequency*			
		PF	FN	F	MF
impact	VH	H	VH	VH	VH
	H	M	H	VH	VH
	M	B	M	H	VH
	L	VL	L	M	H
	VL	VL	VL	L	M

VF: very frequent (daily)
F: frequent (monthly)
NF: normal frequency (yearly)
I: infrequent (every few years)

25

MAGERIT: esempio 2

cfr MAGERIT v2,
tecniche (eng version), pp 8-9

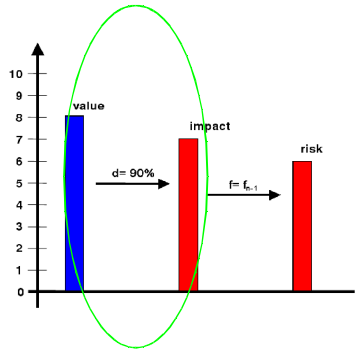
- **analisi algoritmica, qualitativa o quantitativa**

	qualitativa	quantitativa
valori	scala di valori simbolici: V = {...,v0,v1,...,vi,...} negligibile quando =< v0	reali positivi: V in {R+} negligibile quando =< v0
dimensioni	indipendenti tra loro	
dipendenze	dirette: valore booleano, indirette: chiusura transitiva A ⇒ C ⇔ ∃ B, (A ⇒ B) ∧ (B ⇒ C) dirette e indirette trattate allo stesso modo	dirette: reale in [0,1], indirette: dip(A⇒C) = ⅀{ dep(A⇒Bi) × dep(Bi⇒C) } con somme Bayesiane: a+b=1−(1−a)×(1−b)
valori accumulati (accumulated value)	acc_val(B) = max(val(B), {val(Ai)}) dove SUP(B)={ Ai, Ai⇒B } è l'insieme dei beni dipendenti da B	acc_val(B) = val(B) + ⅀{ val(Ai) × dep(Ai⇒B) }
degradazioni (degradation)	(per ogni minaccia) reali positivi: d in {R+}, espresse in percentuale, 0%-100%	
impatto accumulato (accumulated impact)	impact(B) = v_round(v_b × d_b) con Vx_b = acc_aval(B) e d_b la sua degradazione esempio: round(8×0.9) = round(7.2) = 7 => v7	impact(B) = v × d
impatto riflesso (deflected impact)	impact(B) = v_round(v_b × d_a) con Vx_b = acc_val(B) e d_a la degradazione del bene A da cui B dipende	impact(B) = v_b × d_a × degree(B⇒A)

26

MAGERIT: esempio 2

cfr MAGERIT v2,
tecniche (eng version), pp 8-9



27

MAGERIT: esempio 2

fonte: MAGERIT v2,
metodo (eng version), pp 129

- **assegno valore beni e dipendenze => calcolo i valori accumulati**

	[S_T_in person]	[S_T_remote]	[D_exp]	[email]	[archive]	[SW_exp]	[PC]	[SRV]	[firewall]	[LAN]	[ADSL]
[S_T_in person]			√	√	√	√	√			√	
[S_T_remote]			√	√	√			√	√	√	√
[D_exp]					√	√	√	√		√	
[email]								√	√	√	√
[archive]								√	√		√
[SW_exp]											
[PC]											
[SRV]											
[firewall]											
[LAN]											
[ADSL]											

dipendenze

valori

valori accumulati

Security dimensions

Asset	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_T_in person] Processing in person	[5](1)			[7](2)		[6](3)	
[S_T_remote] Remote processing	[3](4)			[7](5)		[6](6)	
[D_exp] Current files		[5](7)	[6](8)		[5](9)		[5](12)

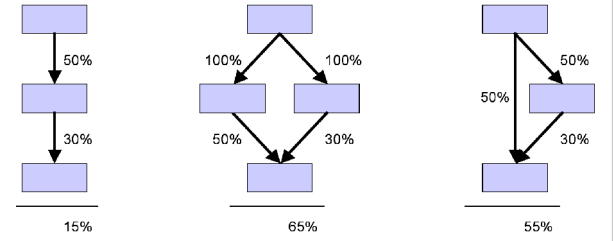
Security dimensions

Asset	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_T_in person] Processing in person	[5]			[7]		[6]	
[S_T_remote] Remote processing	[3]			[7]		[6]	
[D_exp] Current files	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[email] E-mail	[5]			[7]		[6]	
[archive] Central historical archive	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[SW_exp] Proccessing files	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[PC] Working positions	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[SRV] Server	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[firewall] Firewall	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[LAN] Local network	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[ADSL] Internet connection	[5]	[5]	[6]	[7]	[5]	[6]	[5]

MAGERIT: esempio 2

cfr MAGERIT v2, tecniche (eng version), pp 8-9

- **esempio di calcolo delle dipendenze indirette:**



0.5 x 0.3 = 0.15 | 1 - (1 - 0.5) x (1 - 0.15) = 0.65 | 1 - (1 - 0.5) x (1 - 0.15) = 0.575

29

MAGERIT: esempio 2

- **assegno la risk map:**
  - per asset
  - e threat
- **include:**
  - degradazione
  - frequenza

fonte: MAGERIT v2, metodo (eng version), pp 128

asset / threat	frequency	dimensions of security: D	I	C	A_S	A_D	T_S	T_D
[D_exp] Current files		50%	50%	100%	100%	100%	100%	100%
[E.1] Users' errors	10		10%	10%				
[E.2] Administrator errors	1	20%	20%	10%	10%	10%	20%	20%
[E.3] Monitoring errors	1						50%	50%
[E.4] Configuration errors	0,5	50%	10%	10%	50%	50%	50%	50%
[E.14] Information leakage	1			1%				
[E.15] Information alteration	10		1%					
[E.16] Insertion of faulty information	100		1%					
[E.17] Information degradation	10		1%					
[E.18] Destruction of information	10	1%						
[E.19] Disclosure of information	1			10%				
[A.4] Manipulation of the configuration	0,1	50%	10%	50%	100%	100%	100%	100%
[A.11] Unauthorised access	100		10%	50%	50%			
[A.14] Eavesdropping	10			50%				
[A.15] Alteration of information	10		50%					
[A.16] Entry of false information	20		50%					
[A.17] Corruption of information	10		50%					
[A.18] Destruction of information	10	50%						
[A.19] Disclosure of information	10			100%				

MAGERIT: esempio 2

fonte: MAGERIT v2, metodo (eng version), pp 130

- **calcolo l'impatto accumulato:**

example: accumulated impact

asset	D	I	C	A_S	A_D	T_S	T_D
ASSETS							
[FS] Functions of the information system							
[S_T_presenciali] Processing in person	[4]			[7]		[6]	
[S_T_remota] Remote processing	[2]			[7]		[6]	
[D_exp] Current files	[4]	[4]	[6]	[7]	[5]	[6]	[5]
[SI] Internal services							
[email] E-mail	[4]			[7]		[6]	
[archivo] Central historical archive	[5]	[4]	[5]	[7]	[5]	[6]	[5]
[E] Equipment							
[SW_exp] Processing of files	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[PC] Working positions	[5]	[2]	[5]	[6]	[2]	[6]	[5]
[SRV] Server	[5]	[2]	[5]	[6]	[2]	[6]	[5]
[firewall] Firewall	[5]	[2]	[5]	[6]	[2]	[6]	[5]
[LAN] Local network	[5]	[2]	[6]	[7]	[5]	[6]	[5]
[ADSL] Internet connection	[2]	[2]	[5]	[7]	[5]	[6]	[5]

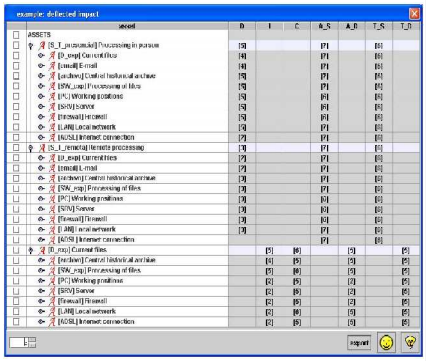
3 export

31

MAGERIT: esempio 2

fonte: MAGERIT v2,
metodo (eng version), pp 131

- **calcolo l'impatto riflesso**
- **considera:**
  - degrado per minaccia
  - dipendenze per asset



32

Esempio: MAGERIT

cfr MAGERIT v2,
tecniche (eng version), pp 10

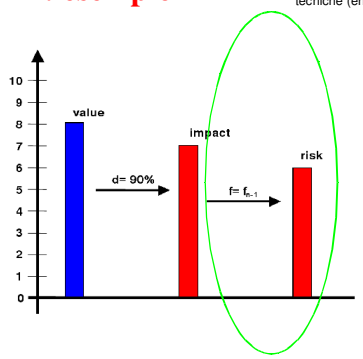
- **calcolo del rischio:**

	qualitativa	quantitativa
frequenza minacce	scala di valori simbolici: F = { ..., f0, f1, ..., fi, … } neglegibile quando =< f0, fn = frequenza di normalizzazione", es, 1/anno	reali positivi: f in {R+} neglegibile quando =< f0
rischi	risk = ℜ(impact, frequency) con ℜ una funzione crescente in vi e fi, e ℜ(v0, fn) = v0 esempio di funzione adatta: ℜ(vi, fj) = vi+j-n	risk = impact × frequency neglegibile quando =< r0 = v0
rischi accumulati (accumulated risk)	come per i rischi ma si usa l'impatto accumulato	
rischi riflessi (deflected risk)	come per i rischi ma si usa l'impatto riflesso	

33

MAGERIT: esempio 2

cfr MAGERIT v2,
tecniche (eng version), pp 8-9

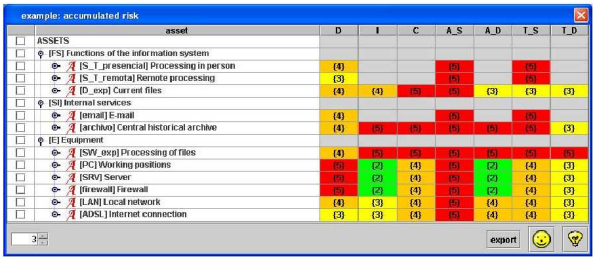


34

MAGERIT: esempio 2

fonte: MAGERIT v2,
metodo (eng version), pp 130

- **calcolo il rischio accumulato:**

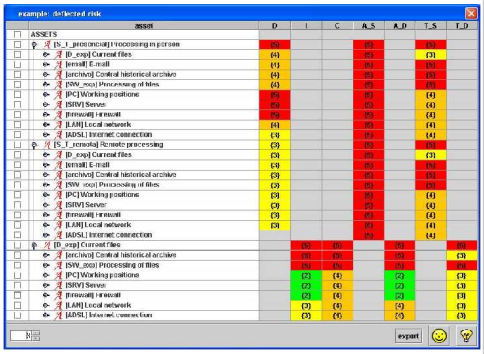


35

MAGERIT: esempio 2

fonte: MAGERIT v2,
metodo (eng version), pp 130

- **calcolo il rischio riflesso:**



36

MAGERIT: esempio 2

- **esempio di analisi qualitativa:**

- se il bene A con valore 'v5' dipende dal bene B con valore v8

- e se la minaccia M degrada B del 90% con frequenza stimata 'f2'
(e 'f3' è la frequenza di normalizzazione)

- e se i controlli scelti riducono l'impatto del 50% e la frequenza del 50%.

- allora, il metodo calcola:

per A:	**per B:**
valore accumulato = v5	**valore accumulato = v5 + v8 = v8**
impatto riflesso = v4	**impatto accumulato = v7**
rischio riflesso = v3	**rischio accumulato = v6**
danno residuo = 45%	**danno residuo = 45%**
impatto residuo = v2	**impatto residuo = v3**
frequenza residua = f1	**frequenza residua = f1**
rischio residuo = v0	**rischio residuo = v1**

37

MAGERIT: esempio 2

- **esempio di analisi quantitativa:**

- se il bene A con valore '10000' dipende per il 30% dal bene B con valore '1000'
- e se la minaccia M degrada B del 90% con frequenza stimata '0.1'
- e se i controlli scelti riducono l'impact del 90% e la frequenza del 50%
- allora, il metodo calcola:

per B:
impatto = 1000 x 90% = 900
rischio = 900 x 0.1 = 90
impatto residuo = 900 x (1-0.9) = 90
frequenza residua = 0.1 x (1-0.5) = 0.05
rischio residuo = 90 x 0.05 = 4,5
efficienza controlli =
1 – (1–90%) x (1–50%) = 95%

per A:
impatto riflesso =
10000 x 90% x 30% = 2700

38

EBIOS: esempio

fonte: EBIOS, tecniche (eng version), pp 19

- **matrice delle dipendenze tra informazioni/servizi e dispositivi:**

Entities / Essential elements	HARDWARE				SOFTWARE				NETWORKS				PERSONNEL					SITES			ORGA.		
	M1	M2	M3	M4	L1	L2	L3	L4	R1	R2	R3	R4	P1	P2	P3	P4	P5	S1	S2	S4	O1	O2	O3
Function 1	I					I		I					I	I	I	I						I	I
...	+					+	+	+					+	+	+	+	+	+	+		+		+
Function N	+	+			+	+		+	+			+		+	+	+	+	+	+			+	+
Information 1	+		+		+	+		+		+		+		+	+	+	+	+	+			+	+
...	+			+	+	+		+			+	+		+	+	+	+	+	+			+	+
...	+					+	+	+					+	+	+	+			+	+	+	+	+
Information N	+					+	+	+					+	+	+	+	+	+	+	+			+

39

EBIOS: esempio

fonte: EBIOS, tecniche (eng version), pp 19

- **scleata di:**
  - criteri di sicurezza
  - scala dei valori

Security needs	Availability	Integrity	Confidentiality
0	No availability need	No integrity need	Public
1	Long term (specify)	[value not used]	Restricted
2	Medium term (specify)	Medium integrity need	Confidential (partners)
3	Short term (specify)	[value not used]	Confidential (internal)
4	Very short term (specify)	Total integrity	Secret

40

EBIOS: esempio

fonte: EBIOS, tecniche (eng version), pp 22

- **definizione del valore degli impatti per ogni bene:**

Name of the sensitive element	Damage	Impact 1	...	Impact n	Security needs	Comments
Security criterion i	Damage i	Bi1 i	...	Bi1n	f(Bi1 i...Bimi)	
Security criterion j	...	...	...	...		
Security criterion l	Damage n	Bl1n1	...	Bl1nn		
...	...	...	...	...	...	
Security criterion m	Damage 1	Bm1 1	...	Bm1n	f(Bm1 1...Bmnn)	
Security criterion m	...	...	...	...		
Security criterion m	Damage n	Bmn1	...	Bmnn		

- **riassunta in:**

List of essential elements	Summary of security needs		
	Confidentiality	Integrity	Availability
Function 1	0	3	3
Function 2	1	3	2
...	...	...	...
Function n	0	4	2
Information 1	2	1	1
...	...	...	...
Information n	4	3	0

41

EBIOS: esempio

fonte: EBIOS, tecniche (eng version), pp 26

- **caratterizzare le minacce assegnando la potenzialità:**
  - 1 (accidental and random)
  - 2 (limited opportunities or resources)
  - 3 (high level of expertise, opportunity and resources)

	Attack methods	Threat elements: Type: Natural	Type: Human.	Type: Environmental	Cause: Accidental	Cause: Deliberate	Attack potential	Security criteria affected: Availability	Integrity	Confidentiality
1	Fire	+	+	+	+	+	2	+	+	
13	Loss of means of telecommunication			+	+	+	1	+		
19	Eavesdropping		+	+		+	2			+
20	Theft of media or documents			+		+	2			+
21	Theft of equipment			+		+	1	+		+
23	Divulgation		+	+	+	+	1			+
26	Tampering with software			+		+	1	+	+	+
42	Attack on availability of personnel	+	+	+	+	+	1	+		

42

EBIOS: esempio

fonte: EBIOS, tecniche (eng version), pp 26

- **stimare il livello di vulnerabilità per minaccia:**
  - da 0 (totally improbable or unfeasible) ... a 4 (certain or possible for anyone)

Attack methods		Vulnerabilities	Hardware and software	Internal networks	External networks	Site	Personnel	Organisation
1	Fire	Fire prevention measures not consistent with the information system				2		
		No instructions (warning, prevention, training, etc.)						2
		No organisation of fire safety						3
13	Loss of means of telecommunication	Operating faults on the internal telephone network				1		
		Malfunction of external networks (PSTN)			1			
		Malfunction of external networks (network services)			1			
...	...	...	...	...	...	...	...	...

43

EBIOS: esempio

fonte: EBIOS, tecniche (eng version), pp 26

- **formalizzare le minacce e stimare l'opportunità in base alle vulnerabilità presenti:**

Threats		Attack method	Attack potential	D	I	C	Opportunity
M.INCENDIE	Consequences of a fire aggravated because the fire prevention measures are inconsistent with the information system (site of the office), or there are no fire safety instructions or arrangements (organisation of the office)	1	2	+			2
M.TELECOM	Loss of means of telecommunication because of a malfunction of external networks (Internet)	12	1	+			1
M.VOL-DOC	Theft of media or documents by a visitor or cleaning personnel because the premises are easy to enter during working hours (site of the office)	19	2			+	3
…	…	…	…	…	…	…	…

44

EBIOS: esempio

fonte: EBIOS, tecniche (eng version), pp 26

- **caratterizzare il rischio in termini di requisiti di sicurezza:**

Risk summary				Element 1			…			Element N		
				D	I	C	D	I	C	D	I	C
				3	2	0	…	…	…	0	1	0
				Security needs concerned								
Attack methods	D	I	C	D	I	C	D	I	C	D	I	C
Eavesdropping			X	0	0	0	…	…	…	0	0	0
Theft of equipment	X		X	3	0	0	…	…	…	0	0	0
…	…	…	…	…	…	…	…	…	…	…	…	…

Risks		Maximum of the security needs concerned	The threat opportunity	Attack potential
R.PILOTAGE	An intruder tampers with the software by modifying the system commands, installing pirated programmes, modifying an application (hardware, software and Internet) or acting on the system resource software (via Internet), thereby breaching the confidentiality of sensitive information (estimates, contentious issues file, etc.) and the integrity of essential elements (calculate the structures, estimates, technical plan, technical parameters, litigation file, etc.)	4	3	1
R.VOL_VISITEUR	Because of easy access to the premises (site of the office), a visitor or cleaner steals equipment known to be especially tempting (backup/technological value of most of the equipment, software and network elements) thereby breaching the availability of several essential elements and the confidentiality of sensitive information (estimates, litigation file, etc.)	2	1	1
…	…	…	…	…

45

EBIOS: esempio

fonte: EBIOS, tecniche (eng version), pp 31

- **determinare i requisiti di sicurezza in gioco:**

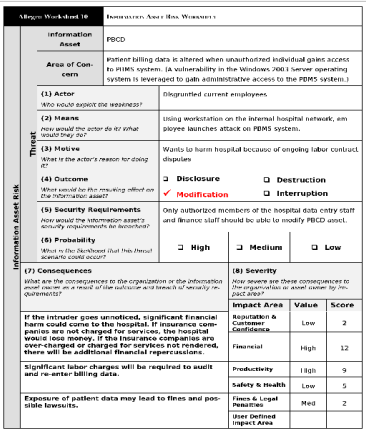
Risk summary				Element 1			…			Element N		
				D	I	C	D	I	C	D	I	C
				3	2	0	…	…	…	0	1	0
				Security needs concerned								
Attack methods	D	I	C	D	I	C	D	I	C	D	I	C
Eavesdropping			X	0	0	0	…	…	…	0	0	0
Theft of equipment	X		X	3	0	0	…	…	…	0	0	0
…	…	…	…	…	…	…	…	…	…	…	…	…

- **e caratterizzare i rischi:**

Risks		Maximum of the security needs concerned	The threat opportunity	Attack potential
R.PILOTAGE	An intruder tampers with the software by modifying the system commands, installing pirated programmes, modifying an application (hardware, software and Internet) or acting on the system resource software (via Internet), thereby breaching the confidentiality of sensitive information (estimates, contentious issues file, etc.) and the integrity of essential elements (calculate the structures, estimates, technical plan, technical parameters, litigation file, etc.)	4	3	1
R.VOL_VISITEUR	Because of easy access to the premises (site of the office), a visitor or cleaner steals equipment known to be especially tempting (backup/technological value of most of the equipment, software and network elements) thereby breaching the availability of several essential elements and the confidentiality of sensitive information (estimates, litigation file, etc.)	2	1	1
…	…	…	…	…

46

OCTAVE: esempio



Allegro Worksheet 10	Information Asset Risk Worksheet	
Information Asset Risk	Information Asset	PBCD
	Area of Concern	Patient billing data is altered when unauthorized individual gains access to PBMS system. (A vulnerability in the Windows 2003 Server operating system is leveraged to gain administrative access to the PBMS system.)
Threat	(1) Actor *Who would exploit the weakness?*	Disgruntled current employees
	(2) Means *How would the actor do it? What would they do?*	Using workstation on the internal hospital network, employee launches attack on PBMS system.
	(3) Motive *What is the actor's reason for doing it?*	Wants to harm hospital because of ongoing labor contract disputes
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ Disclosure ❑ Destruction ✓ Modification ❑ Interruption
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Only authorized members of the hospital data entry staff and finance staff should be able to modify PBCD asset.
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ High ❑ Medium ❑ Low
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*

Impact Area	Value	Score
Reputation & Customer Confidence	Low	2
Financial	High	12
Productivity	High	9
Safety & Health	Low	5
Fines & Legal Penalties	Med	2
User Defined Impact Area		

If the intruder goes unnoticed, significant financial harm could come to the hospital. If insurance companies are not charged for services, the hospital would lose money. If the insurance companies are over-charged or charged for services not rendered, there will be additional financial repercussions.

Significant labor charges will be required to audit and re-enter billing data.

Exposure of patient data may lead to fines and possible lawsuits.

fonte: OCTAVE Allegro Guidebook, pp 98

47

STRIDE

- **si parte da un modello DFD che identifica i beni**
- **e dalle relazione tra le categorie STRIDE e gli elementi di un modello DFD:**

categorie STRIDE / elementi DFD	S	T	R	I	D	E
agenti esterni	X		X			
flusso di dati		X		X	X	
archivi		X	X*	X	X	
processi	X	X	X	X	X	X

cfr. M.Howard, S.Lipner, The Security Development Lifecycle, Microsoft Press, pp. 119

* se l'archivio contiene dati di audit o di logging, un attaccante potrebbe manipolarli per nascondere le sue tracce

48

STRIDE: identificazione delle minacce

- **per il modello DFD di uno specifico sistema:**
  - si identificano univocamnte tutti gli oggetti presenti nel diagramma
    - agenti esterni, archivi, processi
    - i flussi dati risultano univocamente identificati dalla tripla *{dato,oggetto di partenza,oggetto d'arrivo}*
  - si costruisce una tabella che associa le appropriate categorie di minacce ad ogni oggetto nel DFD
  - per ogni coppia oggetto-categoria si identificano le eventuali minacce di quel tipo effettivamente presenti nel sistema

18/05/09

49

Identificazione delle minacce

cfr. M.Howard, S.Lipner, The Security Development Lifecycle, Microsoft Press, pp. 119

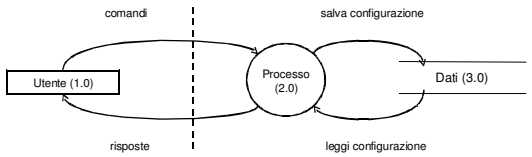
- **associazione oggetti DFD e minacce STRIDE:**

categorie STRIDE	identificativo oggetto DFD (esempi)
Spoofing	Agenti esterni: (ID1.0), (ID2.0), ... Processi: (ID4.2), (ID4.5), ...
Tampering	Processi: (ID4.2), (ID4.5), ... Archivi: (ID4.1), (ID4.3), ... Flussi dati: (4.1->4.2), (2.0->4.2->2.0), (1.0->4.2->1.0), ...
Repudiation	Agenti esterni: (ID1.0), (ID2.0), ... Processi: (ID4.7.10), ...
Information disclosure	Processi: (ID4.2), (ID4.7.1), ... Archivi: (ID4.1), (ID4.8), ... Flussi dati: (4.1->4.2), (1.0->4.2->1.0), ...
DoS	Processi: (ID4.2), (ID4.7.1), ... Archivi: (ID4.1), (ID4.8), ... Flussi dati: (4.1->4.2), (2.0->4.2->2.0), ...
EoP	Processi: (ID4.2), (ID4.6), ...

50

STRIDE: esempio

- **l'utente è un agente esterno che interagisce con il sistema**
- **i dati inviati dall'utente e quelli generati dal processo non hanno lo stesso grado di affidabilità:**
  - è necessario specificare questa condizione usando un Trust Boundary



18/05/09 51

STRIDE: esempio

- **tabella degli identificativi degli oggetti DFD:**

Categorie Elementi DFD	STRIDE	Identificativo Elemento DFD
Agenti esterni	S; R	(1.0)
Processi	S; T; R; I; D; E	(2.0)
Archivi	T; (R*); I; D	(3.0)
Flusso di dati	T; I; D	(1.0→2.0→1.0); (2.0→3.0→2.0)

18/05/09 52

STRIDE: esempio

- **taabella dell'identificazione delle minacce:**

Categorie Minacce (STRIDE)	Identificativo Elemento DFD
Spoofing	Agenti esterni: (1.0) Processi: (2.0)
Tampering	Processi: (2.0) Archivi: (3.0) Flusso di dati: (1.0→2.0→1.0); (2.0→3.0→2.0)
Repudiation	Agenti esterni: (1.0) Flusso di dati: (1.0→2.0→1.0); (2.0→3.0→2.0)
Information Disclosure	Processi: (2.0) Archivi: (3.0) Flusso di dati: (1.0→2.0→1.0); (2.0→3.0→2.0)
DoS	Processi: (2.0) Archivi: (3.0) Flusso di dati: (1.0→2.0→1.0); (2.0→3.0→2.0)
EoP	Processi: (2.0)

18/05/09 53

DREAD

- **metodo proposto da Microsoft per l'uso in associazione a STRIDE**
- **per quantificare, confrontare e prioritizzare i rischi**
- **un acronimo che identifica 5 categorie**
- **rischio = (Damage + Reproducibility + Exploitability + Affected Users + Discoverability) / 5**
- **ogni fattore è valorizzato tra 0 e 10**

54

DREAD

- **critiche:**
  - distante dal classico approccio (impatto x probabilità)
    - Damage Potential + Affected Users ~ Impact
    - Reproducibility + Exploitability + Discoverability ~ Probability
    - non hanno peso uguale
- **pro:**
  - tentativo di costruire un modello più predittivo, ma rivelatosi troppo semplice

55

DREAD

- **poco usato**
- **sostituito internamente in Microsoft da un metodo basuto su livelli di severità:**
  - SDL Privacy Bug Bar:
    - http://msdn.microsoft.com/en-us/library/cc307403.aspx
  - SDL Security Bug Bar
    - http://msdn.microsoft.com/en-us/library/cc307404.aspx
  - non pienamente documentato

56

Bug Bar

- **livelli di criticità:**
  - **SEV 1** – *A security vulnerability that would be rated as having the highest potential for damage.*
  - **SEV 2** – *A security vulnerability that would be rated as having significant potential for damage, but less than SEV 1.*
  - **SEV 3** – *A security vulnerability that would be rated as having moderate potential for damage, but less than SEV 2.*
  - **SEV 4** – *A security vulnerability that would be rated as low potential for damage.*

57

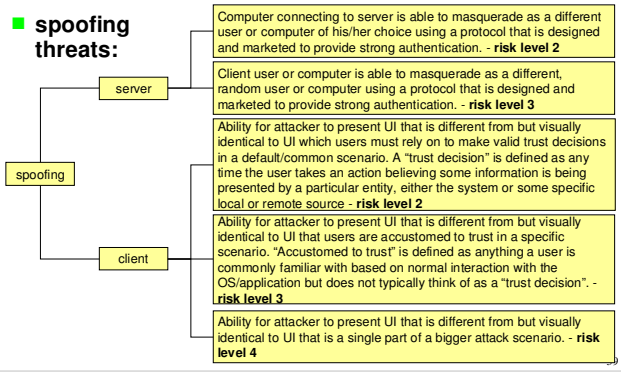
Bug Bar

- **le caratterische della minaccia considerate per la classificazione sono:**
  - interessa un'applicazione server vs client
  - richiede accesso locale vs remoto
  - richiede accesso da parte di utenti anonimi vs autenticati vs amministratori
  - vulnerabilità attiva vs disattiva di default
  - grado di interazione utente rischiesto
  - per disclosure, se interessa informazioni personali o dati sensibili
  - per DoS, se l'applicazione continua a non funzionare anche dopo il termine dell'attacco

58

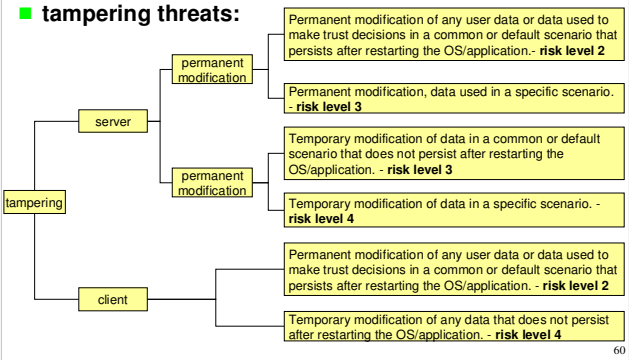
Bug Bar: esempi

- **spoofing threats:**



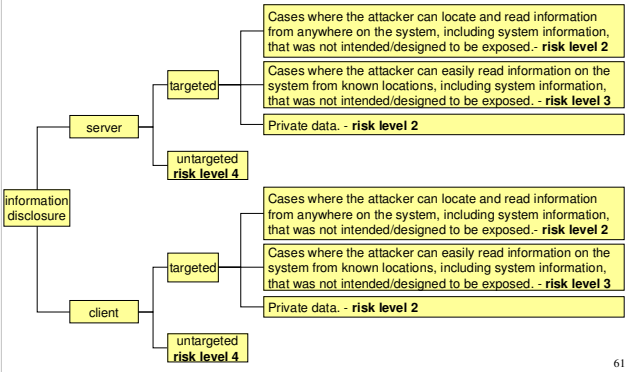
Bug Bar: esempi

- **tampering threats:**



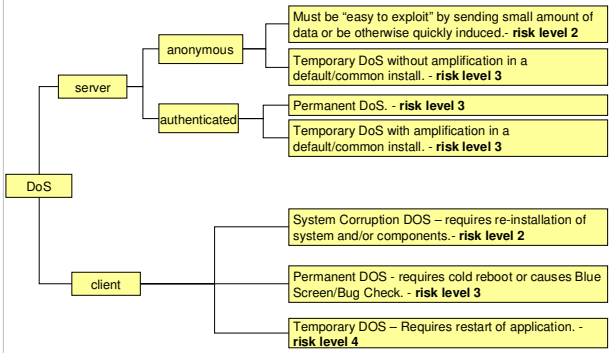
60

Bug Bar: esempi



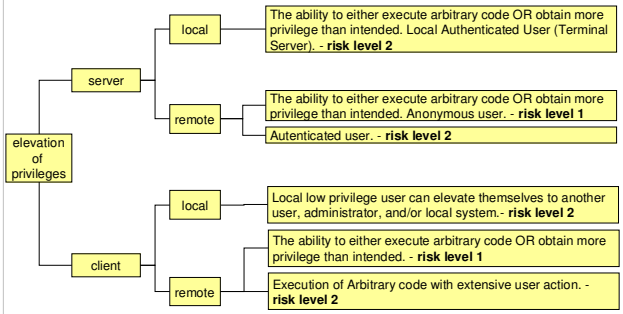
61

Bug Bar: esempi



62

Bug Bar: esempi



63

OWASP Risk Rating

- **parte della OWASP Testing Guide (pp 329-330)**
- **riscio = impatto x probabilità**
- **scala di valori:**

Likelihood and Impact Levels	
0 to <3	HIGH
3 to <6	MEDIUM
6 to 9	LOW

67

OWASP Risk Rating

- **probabilità:**

Threat agent factors				Vulnerability factors			
Skill level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1	3	6	9	2
Overall likelihood=4.375 (MEDIUM)							

- **impatto:**

Technical Impact				Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability	Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8	1	2	1	5
Overall technical impact=7.25 (HIGH)				Overall business impact=2.25 (LOW)			

OWASP Risk Rating

- **rischio:**

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

69

CVSS

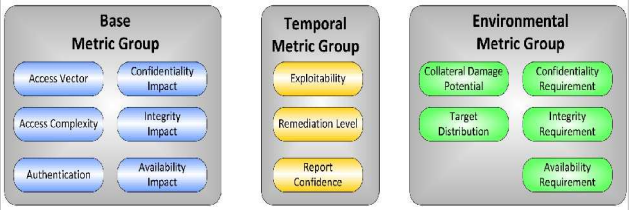
- **Common Vulnerability Scoring System**
- **sviluppato da NIST per prioritizzare le vulnerabilità contenute in NVD**
  - www.first.org/cvss/

70

CVSS: metriche

fonte: CVSS guide

- **tre gruppi di fattori (o metriche):**
  - base: costanti nel tempo e per tutti i sistemi
  - temporali: variano nel tempo
  - ambientali: variano in base al sistema

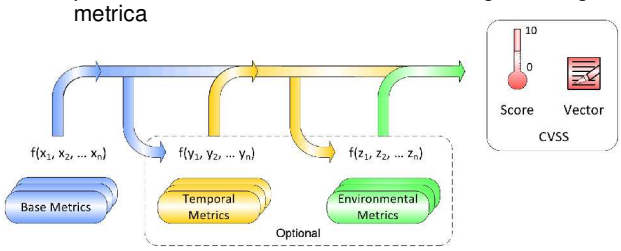


71

CVSS: equazioni

fonte: CVSS guide

- **le metriche sono combinate in:**
  - un punteggio (score) globale tra 0 e 10
  - più un vettore che contiene il valore assegnato a ogni metrica



72

CVSS: metriche base

- **Access Vector (AV)**
  - come la vulnerabilità può essere sfruttata
    - Local (L): richiede accesso locale, fisico o shell locale
    - Adjacent Network (A): richiede accesso alla rete locale (subnet IP, WiFi, Bluetooth)
    - Network (N): accesso remoto è sufficiente
  - più remoto un attaccante può essere più alto lo score

73

CVSS: metriche base

- **Access Complexity (AC)**
  - difficoltà nello sfruttare la vulnerabilità
    - High (H): richiede condizioni di accesso specifiche (privilegi elevati, azioni molto sospette, configurazione usata di raro, race condition con finestra stretta)
    - Medium (M): le condizioni di accessso ono ristrette (gruppo limitato di utenti, richiede previa raccolta di informazioni, configurazione non di default, richiede social engineering limitato)
    - Low (L): (sistema esposto a molti utenti, configurazione di default o diffusa, attacco manuale e con poco skill)

74

CVSS: metriche base

- **Autentication (Au)**
  - quante volte l'attaccante deve autenticarsi per sfruttare la vulnrabilità
    - Multiple (M): 2 o più volte, anche con la stessa credenziale
    - Single (S): un'istanza è sufficiente
    - None (N): accesso anonimo

75

CVSS: metriche base

- **Confidentiality Impact (C)**
  - misura l'impatto sulla segretezza
    - None (N): nessuno
    - Partial (P): l'attaccante non ha il controllo di ciò che ottiene o la perdita è contenuta
    - Complete (C): l'attaccante è in grado di leggere tutti i dati del sistema (memory, files, etc.)

76

CVSS: metriche base

- **Integrity Impact (I)**
  - misura l'impatto sull'integrità
    - None (N): nessuno
    - Partial (P): l'attaccante non ha il controllo di ciò che viene modificato o la modifica è contenuta
    - Complete (C): l'attaccante è in grado di modificare tutti i dati del sistema

77

CVSS: metriche base

- **Availability Impact (A)**
  - misura l'impatto sull'integrità
    - None (N): nessuno
    - Partial (P): performance ridotte o interruzione nella disponibilità della risorsa
    - Complete (C): risorsa completamente non disponibile

78

CVSS: metriche temporali

- **Exploitability (E)**
  - misura la disponibilità corrente di tecniche e codice per sfruttare la vulnerabilità
    - Unproven (U): nessuno o teorico
    - Proof-of-Concept (POC): tecnica/codice esistente, ma non sempre funzionante e richiede un'elaborazione sostanziale da parte di un attaccante esperto
    - Functional (F): codice disponibile e funzionante
    - High (H): disponibile del codice mobile autonomo, o non è richiesto un exploit (manuale e dettagli)
    - Not Defined (N): valore che non influenza lo score

79

CVSS: metriche temporali

- **Remediation Level (RL)**
  - disponibilità di rimedi
    - Official Fix (OF): patch o upgrade ufficiali
    - Tmporary Fix (TF): hotfix, tool o workaround temporaneo pubblicato dal produttore
    - Workaround (W): soluzione non ufficiale
    - Unavailable (U): non disponibile
    - Not Defined (N): valore che non influenza lo score

80

CVSS: metriche temporali

- **Report Confidence (RC)**
  - grado di convinzione nell'esistenza della vulnerabilità e credibilità dei dettagli tecnici associati
    - Unconfirmed (UC): singola sorgente o informazioni contrastanti
    - Uncorroborated (UR): sorgenti non ufficiali multiple, dettagli tecnici conflittuali
    - Confirmed (C): ufficiale
    - Not Defined (N): valore che non influenza lo score

81

CVSS: metriche ambientali

- **Collateral Damage Potential (CDP)**
  - potenziale perdita di beni materiali, perdita economica o di produttività
    - None (N): nessuna
    - Low (L): lieve perdita materiale/economica
    - Low-Medium (LM): moderata perdita materiale/economica
    - Medium-High (MH): significativa perdita materiale/economica
    - High (H): catastrofica perdita materiale/economica
    - Not Defined (N): valore che non influenza lo score

82

CVSS: metriche ambientali

- **Target Distribution (TD)**
  - proporzione di sistemi vulnerabili
    - None (N): nessuna
    - Low (L): l'ambiente target è affetto ma su scala ridotta (1%-25% del sistema)
    - Medium (M): 26%-75% del sistema è affetto
    - High (H): 76%-100%
    - Not Defined (N): valore che non influenza lo score

83

CVSS: metriche ambientali

- **Security Requirements (CR, IR, AR)**
  - permetto di personalizzare l'impatto sulle dimensioni CIA per uno specifico ambiente
    - Low (L)
    - Medium (M)
    - High (H)
    - Not Defined (N): valore che non influenza lo score

84

CVSS: vettori

fonte: CVSS guide

- **le metriche possono essere rappresentate in modo compatto in un formato vettoriale:**
  - nome_metrica : sigla_valore / ...

Metric Group	Vector
Base	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
Temporal	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
Environmental	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND]

85

CVSS: equazioni

fonte: CVSS guide

- **equazioni base:**

BaseScore =	round(((0.6 x Impact)+(0.4 x Exploitability)–1.5) x f(Impact))
Impact =	10.41 x (1-(1-ConfImpact) x (1-IntegImpact) x (1-AvailImpact))
Exploitability =	20 x AccessVector x AccessComplexity x Authentication
f(impact) =	0 if Impact=0, 1.176 otherwise
AccessVector =	[0.395 (L) , 0.646 (A) , 1.0 (N)]
AccessComplexity =	[0.35 (H) , 0.61 (M) , 0.71 (L)]
Authentication =	[0.45 (M) , 0.56 (S) , 0.704 (N)]
ConfImpact =	[0.0 (N) , 0.275 (P) , 0.660 (C)]
IntegImpact =	[0.0 (N) , 0.275 (P) , 0.660 (C)]
AvailImpact =	[0.0 (N) , 0.275 (P) , 0.660 (C)]

86

CVSS: equazioni

fonte: CVSS guide

- **equazioni temporali:**
  - aggiornano il base score, producendo un nuovo score nel range [67% base score, base score]

TemporalScore =	round(BaseScore x Exploitability x RemediationLevel x ReportConfidence)
Exploitability =	[0.85 (U) , 0.9 (POC) , 0.95 (F), 1.0 (H), 1.0 (ND)]
RemediationLevel =	[0.87 (OF) , 0.9 (TF) , 0.95 (W), 1.0 (U), 1.0 (ND)]
ReportConfidence =	[0.9 (UC) , 0.95 (UR) , 1.0 (C), 1.0 (ND)]

87

CVSS: equazioni

fonte: CVSS guide

- **equazioni ambientali:**
  - aggiorna con un nuovo score nel range [0,temporal score]

EnvironmentalScore =	round((AdjustedTemporal + (10-AdjustedTemporal) x CollateralDamagePotential) x TargetDistribution)
AdjustedTemporal =	TemporalScore recomputed with the BaseScore's Impact equation replaced with the AdjustedImpact equation
AdjustedImpact =	min(10 , 10.41 x (1-(1-ConfImpact x ConfReq) x (1-IntegImpact x IntegReq) x (1-AvailImpact x AvailReq)))
CollateralDamagePotential =	[0 (N) , 0.1 (L) , 0.3 (LM), 0.4 (MH), 0.5 (H), 0 (ND)]
TargetDistribution =	[0 (N) , 0.25 (L) , 0.75 (M), 1.0 (H), 1.0 (ND)]
ConfReq =	[0.5 (L) , 1.0 (M) , 1.51 (H), 1.0 (ND)]
IntegReq =	[0.5 (L) , 1.0 (M) , 1.51 (H), 1.0 (ND)]
AvailReq =	[0.5 (L) , 1.0 (M) , 1.51 (H), 1.0 (ND)]

88

CVSS: esempio

fonte: CVSS guide

BASE METRIC	EVALUATION	SCORE
Access Vector	[Network]	(1.00)
Access Complexity	[Low]	(0.71)
Authentication	[None]	(0.704)
Confidentiality Impact	[None]	(0.00)
Integrity Impact	[None]	(0.00)
Availability Impact	[Complete]	(0.66)

BASE FORMULA	BASE SCORE

```
Impact = 10.41*(1-(1)*(1)*(0.34)) == 6.9
Exploitability = 20*0.71*0.704*1 == 10.0
f(Impact) = 1.176
BaseScore = (0.6*6.9 + 0.4*10.0 - 1.5)*1.176
                                    == (7.8)
```

TEMPORAL METRIC	EVALUATION	SCORE
Exploitability	[Functional]	(0.95)
Remediation Level	[Official-Fix]	(0.87)
Report Confidence	[Confirmed]	(1.00)

TEMPORAL FORMULA	TEMPORAL SCORE
round(7.8 * 0.95 * 0.87 * 1.00)	== (6.4)

ENVIRONMENTAL METRIC	EVALUATION	SCORE
Collateral Damage Potential	[None - High]	(0 - 0.5)
Target Distribution	[None - High]	(0 - 1.0)
Confidentiality Req.	[Medium]	(1.0)
Integrity Req.	[Medium]	(1.0)
Availability Req.	[High]	(1.51)

ENVIRONMENTAL FORMULA	ENVIRONMENTAL SCORE

```
AdjustedImpact = min(10,10.41*(1-(1-0*1)*(1-0*1)
         *(1-0.66*1.51))                  == (10.0)
AdjustedBase =((0.6*10)+(0.4*10.0)-1.5)*1.176
                                          == (10.0)
AdjustedTemporal == (10*0.95*0.87*1.0)    == (8.3)
EnvScore = round((8.3+(10-8.3)*(0-0.5))*(0-1))
                                          == (0.00 - 9.2)
```

89

Osservazioni

- **a prescindere dalla specifica tecnica:**
  - è difficile assegnare i valori iniziali
  - per sistemi grandi è difficile interpretare i risultati
- **è necessario affinare la stima attraverso iterazioni successive**
  - confrontando i risultati ottenuti a partire da insiemi di valori iniziali diversi
- **è fondamentale tener traccia dei valori inizialiche hanno contribuito a un risultato**
- **i tool dovrebbero fornire funzioni automatiche per l'analisi della sensitività dei risultati ai vari parametri stimati**

18/05/09 90