



Valutazione del rischio tramite la logica fuzzy

Antonio Parata
Emaze Networks

antonio.parata@emaze.net

OWASP

SMAU E-Accademy
20 Ottobre 2007

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org>

Agenda

- Chi sono
- Introduzione alla valutazione del rischio
- Modelli di valutazione
- Introduzione alla logica fuzzy
- Logica fuzzy e valutazione del rischio
- FREACS il tool
- FREACS demo
- Conclusioni

Agenda

- Chi sono
- Introduzione alla valutazione del rischio
- Modelli di valutazione
- Introduzione alla logica fuzzy
- Logica fuzzy e valutazione del rischio
- FREACS il tool
- FREACS demo
- Conclusioni

Chi sono

- Laureato in ingegneria informatica al Politecnico di Milano
- Security Consultant presso Emaze Networks
- Collaboratore Owasp Italy
- Co-autore della OWASP Testing Guide v. 2.0
- Mi occupo di sicurezza dal 2002
- Appassionato di tutto ciò che riguarda la software security

Agenda

- Chi sono
- **Introduzione alla valutazione del rischio**
- Modelli di valutazione
- Introduzione alla logica fuzzy
- Logica fuzzy e valutazione del rischio
- FREACS il tool
- FREACS demo
- Conclusioni

Introduzione alla valutazione del rischio

- Terminologia -

- **Minaccia:** raggiungimento di uno scopo da parte di un attaccante.
 - ▶ Esistono varie definizioni, noi ci riferiamo a questa.
- **Vulnerabilità:** difetto software che permette alla minaccia di realizzarsi.
- **Rischio:** concetto strettamente legato a quello di vulnerabilità. È la caratterizzazione di una vulnerabilità.

Introduzione alla valutazione del rischio

- Perché valutarlo? -

- Per classificare le minacce che necessitano di un'urgente azione di mitigazione.
 - ▶ In questo modo si può porre rimedio già dalle prime fasi del ciclo di sviluppo software.
- Per produrre software più sicuro e di conseguenza di ridurre le spese di *patching*.
 - ▶ Valutazione del rischio durante il ciclo di sviluppo
- Se non lo fate voi lo farà qualcun altro
 - ▶ Può sminuire il vostro lavoro

Introduzione alla valutazione del rischio

- Come valutarlo? -

■ Qualitativamente

- ▶ Fornisce una stima più che una valutazione
- ▶ Non molto gradito dai puristi

■ Quantitativamente

- ▶ Fornisce una "stima precisa" del rischio
- ▶ Valutazione generalmente non unanimemente accettata

Agenda

- Chi sono
- Introduzione alla valutazione del rischio
- **Modelli di valutazione**
- Introduzione alla logica fuzzy
- Logica fuzzy e valutazione del rischio
- FREACS il tool
- FREACS demo
- Conclusioni

Modelli di valutazione del rischio

- **DREAD**
- **New DREAD**
- **OWASP Testing Model**
- **CVSSv2**

Modelli di valutazione del rischio

- DREAD -

- **Realizzato da Michael Howard e David LeBlanc di Microsoft.**
- **Si basa su 5 fattori**
 - ▶ Damage Potential
 - ▶ Reproducibility
 - ▶ Exploitability
 - ▶ Affected users
 - ▶ Discoverability
- **Ad ogni termine si assegna un numero da 1 a 10. Il rischio è la media dei valori.**

Modelli di valutazione del rischio

- New DREAD -

- **Modello di valutazione identico al DREAD.**
- **Invece che da 1 a 10, si assegnano dei valori da 1 a 3.**
- **La valutazione del rischio viene effettuata come sempre mediando i valori dei vari fattori.**

Modelli di valutazione del rischio

- OWASP Model -

- **Realizzato con la OWASP Testing Guide v. 2.0.**
- **Modello decisamente più articolato, costruito aggregando varie fasi.**
- **Prende in esame non solo i fattori relativi alla minaccia, ma anche il contesto aziendale.**
- **Si basa su valutazioni sia qualitative che quantitative.**

Modelli di valutazione del rischio

- CVSSv2 (1)-

- **Modello creato dal FIRST e CVSS-SIG team.**
- **È stata appena rilasciata (giugno 07) la versione 2.0.**
- **Modello decisamente complesso e articolato.**
- **Caratterizzato da vari fattori, è basato su formule prestabilite per il calcolo del rischio.**

Modelli di valutazione del rischio

- CVSSv2 (2)-

- Il modello è stato pensato per la valutazione delle vulnerabilità e non per la valutazione del rischio delle minacce.
- CVSSv2 **NON** si presta bene alla valutazione tramite logica fuzzy.
 - ▶ Si basa sull'assegnazione di **valori fissi**.
- La valutazione viene fatta mediante oscure (non se ne capisce la provenienza) formule matematiche.

Modelli di valutazione del rischio

- CVSSv2 (3)-

DRAFT CVSS v2.10 Equations (last revised 3-20-07)

CVSS Base Score Equation

$$\text{BaseScore} = (.6 * \text{Impact} + .4 * \text{Exploitability} - 1.5) * f(\text{Impact})$$

$$\text{Impact} = 10.41 * (1 - (1 - \text{ConfImpact})(1 - \text{IntegImpact})(1 - \text{AvailImpact}))$$

$$\text{Exploitability} = 20 * \text{AccessComplexity} * \text{Authentication} * \text{AccessVector}$$

$$f(\text{Impact}) = 0 \text{ if } \text{Impact} = 0; 1.176 \text{ otherwise}$$

AccessComplexity = case AccessComplexity of

high:	0.35
medium:	0.61
low:	0.71

Authentication = case Authentication of

Requires no authentication:	0.704
Requires single instance of authentication:	0.56
Requires multiple instances of authentication:	0.45

AccessVector = case AccessVector of

Requires local access:	.395
Local Network accessible:	.646
Network accessible:	1

ConfImpact = case ConfidentialityImpact of

none:	0
partial:	0.275
complete:	0.660

IntegImpact = case IntegrityImpact of

none:	0
partial:	0.275
complete:	0.660

AvailImpact = case AvailabilityImpact of

none:	0
partial:	0.275
complete:	0.660

CVSS Temporal Equation

$$\text{TemporalScore} = \text{BaseScore} * \text{Exploitability} * \text{RemediationLevel} * \text{ReportConfidence}$$

Exploitability = case Exploitability of

unproven:	0.85
proof-of-concept:	0.9
functional:	0.95
high:	1.00
not defined:	1.00

RemediationLevel = case RemediationLevel of

official-fix:	0.87
temporary-fix:	0.90
workaround:	0.95
unavailable:	1.00
not defined:	1.00

ReportConfidence = case ReportConfidence of

unconfirmed:	0.90
uncorroborated:	0.95
confirmed:	1.00
not defined:	1.00

CVSS Environmental Equation

$$\text{EnvironmentalScore} = (\text{AdjustedTemporal} + (10 - \text{AdjustedTemporal}) * \text{CollateralDamagePotential}) * \text{TargetDistribution}$$

AdjustedTemporal = TemporalScore recomputed with the Impact sub-equation replaced with the following AdjustedImpact equation.

$$\text{AdjustedImpact} = \text{Min}(10, 10.41 * (1 - (1 - \text{ConfImpact} * \text{ConfReq}) * (1 - \text{IntegImpact} * \text{IntegReq}) * (1 - \text{AvailImpact} * \text{AvailReq})))$$

CollateralDamagePotential = case CollateralDamagePotential of

none:	0
low:	0.1
low-medium:	0.3
medium-high:	0.4
high:	0.5
not defined:	0

TargetDistribution = case TargetDistribution of

none:	0
low:	0.25
medium:	0.75
high:	1.00
not defined:	1.00

ConfReq = case ConfidentialityImpact of

Low:	0.5
Medium:	1
High:	1.51
Not defined:	1

IntegReq = case IntegrityImpact of

Low:	0.5
Medium:	1
High:	1.51
Not defined:	1



Agenda

- Chi sono
- Introduzione alla valutazione del rischio
- Modelli di valutazione
- **Introduzione alla logica fuzzy**
- Logica fuzzy e valutazione del rischio
- FREACS il tool
- FREACS demo
- Conclusioni

Introduzione alla logica fuzzy

- Cenni di logica fuzzy -

- **Logica basata su gradi di verità (spesso confusi con probabilità).**
- **Esprime quanto un fatto sia vero e non quale è la probabilità che avvenga.**
- **Le variabili in gioco vengono espresse attraverso dei "fuzzy sets".**
- **Esse vengono combinate attraverso delle regole IF/THEN.**



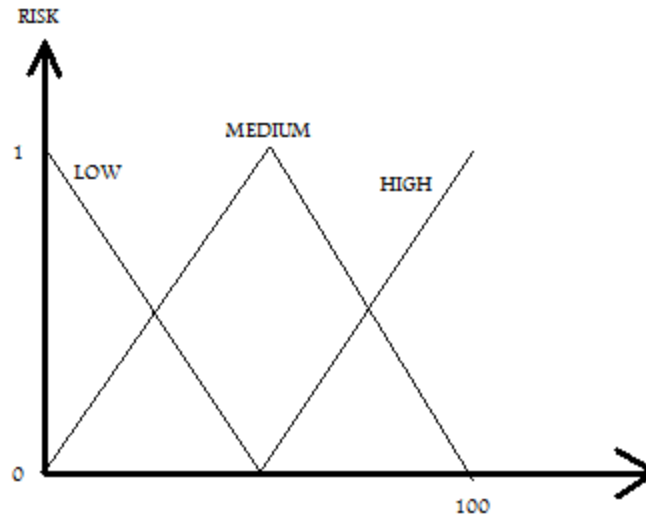
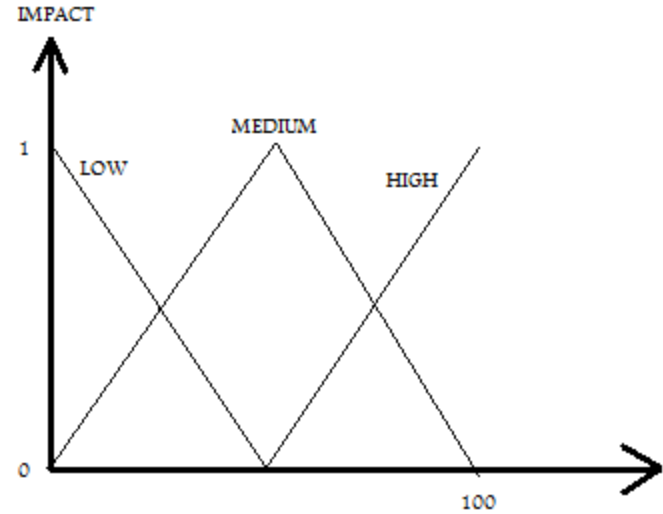
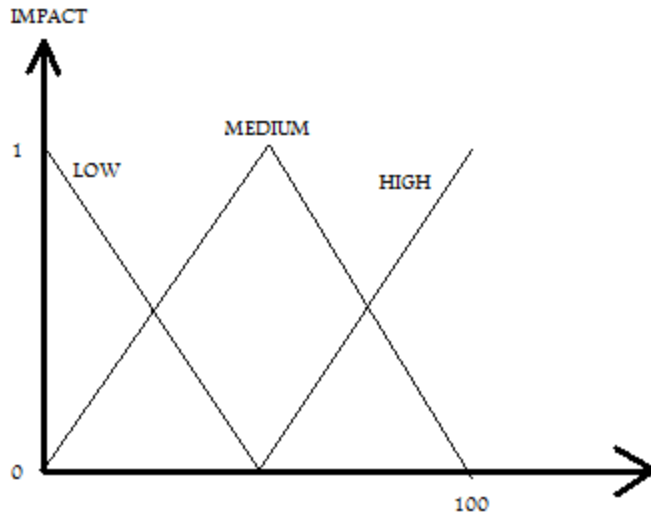
Introduzione alla logica fuzzy

- Definizione delle variabili in gioco -

- **2 Variabili: impact e likelihood.**
- **Ogni variabile ha 3 possibili valori low, medium, high.**
- **Ci sono 9 regole:**
 - ▶ **IF impact IS Low AND likelihood IS Low THEN Risk is Low**
 - ▶ ...
 - ▶ **IF impact IS HIGH AND likelihood IS High THEN Risk is High**

Introduzione alla logica fuzzy

- Definizione fuzzy sets -



Agenda

- Chi sono
- Introduzione alla valutazione del rischio
- Modelli di valutazione
- Introduzione alla logica fuzzy
- **Logica fuzzy e valutazione del rischio**
- FREACS il tool
- FREACS demo
- Conclusioni

Logica fuzzy e valutazione del rischio

- Possiamo utilizzare la logica fuzzy per ottenere dei valori qualitativi del rischio.
- È possibile adattare i modelli presentati alla logica fuzzy, ottenendo una valutazione di tipo qualitativo/quantitativo.
- Ciò che a noi interessa sapere è una stima del rischio, e solo in rari casi avere una valutazione di tipo numerico.

Logica fuzzy e valutazione del rischio (1)

■ Problema: come modellare?

- ▶ Fuzzy sets?
- ▶ Regole di computazione?
- ▶ Altri aspetti relativi alla logica fuzzy?
 - Operatore di defuzzyficazione
 - Peso delle regole
 - Operatore di aggregazione

Logica fuzzy e valutazione del rischio (2)

■ Proposta:

- ▶ **Fuzzy sets di tipo triangolare o quadrilateri.**
- ▶ **Le regole sono state create prendendo in esame tutte le possibili combinazioni.**
- ▶ **L'operatore di defuzzyficazione viene consigliato dall'engine selezionato.**
 - **È comunque possibile impostarlo a proprio piacere scegliendo tra quelli più comunemente utilizzati**
- ▶ **Attualmente ogni regola ha peso 1.**
- ▶ **L'operatore di aggregazione è l'unione dei fuzzy sets.**

Agenda

- Chi sono
- Introduzione alla valutazione del rischio
- Modelli di valutazione
- Introduzione alla logica fuzzy
- Logica fuzzy e valutazione del rischio
- **FREACS il tool**
- FREACS demo
- Conclusioni

FREACS il tool

- Caratteristiche -

- **Utilizzato per il calcolo del rischio tramite logica fuzzy.**
- **I modelli vengono definiti attraverso dei file xml.**
- **Ogni modello può essere tarato a seconda delle proprie esigenze modificando il file descrittore del modello.**
- **Scritto in java :)**

Agenda

- Chi sono
- Introduzione alla valutazione del rischio
- Modelli di valutazione
- Introduzione alla logica fuzzy
- Logica fuzzy e valutazione del rischio
- FREACS il tool
- **FREACS demo**
- Conclusioni

FREACS demo

Agenda

- Chi sono
- Introduzione alla valutazione del rischio
- Modelli di valutazione
- Introduzione alla logica fuzzy
- Logica fuzzy e valutazione del rischio
- FREACS il tool
- FREACS demo
- **Conclusioni**

CONCLUSIONI

- **Requisito: privilegiare la valutazione del rischio in modo qualitativo piuttosto che quantitativo.**
- **La logica fuzzy è un utile strumento per avere analisi di tipo qualitativo.**
 - ▶ **Permette inoltre di avere una valutazione di tipo quantitativa.**
- **La logica fuzzy permette di modellare la maggior parte dei modelli presentati all'inizio.**
- **FREACS il tool – <http://www.ictsc.it>**



**GRAZIE DELL'ATTENZIONE.
DOMANDE ?**