



Sicurezza delle reti

Monga

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Sicurezza delle reti¹

Mattia Monga

Dip. di Informatica e Comunicazione
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2010/11

¹ © 2011 M. Monga. Creative Commons Attribuzione-Condividi allo stesso modo 2.5 Italia License. <http://creativecommons.org/licenses/by-sa/2.5/it/>. Materiale derivato da © 2010 M. Cremonini.



Sicurezza delle reti

Monga

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Lezione XI: Rilevamento delle intrusioni



Sicurezza delle reti

Monga

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Intrusion detection system (IDS)

IDS

È un sistema di monitoraggio (generalmente del tutto passivo) che genera **allarmi**

Saranno necessarie tre fasi:

- 1 Raccolta dati
- 2 Analisi dei dati
- 3 Generazione degli allarmi

Agli allarmi deve poi seguire una risposta dell'amministratore del sistema: come vedremo non è facile automatizzare questa ultima fase.



Sicurezza delle reti

Monga

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Perché usare un IDS?

In generale i sistemi di monitoraggio sono utili perché:

- le tecnologie di prevenzione degli eventi indesiderati o pericolosi possono fallire
- è utile avere un un meccanismo di segnalazione che permetta di attivare procedure di correzione o di emergenza
- l'uso di strumenti che permettano di monitorare lo stato corrente di un sistema, sia esso un componente che una rete, per accumulare conoscenza statistica sulle modalità d'uso



Sicurezza delle reti
 Monga
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi

Gli IDS possono essere classificati in base al punto in cui avviene la raccolta dati

HIDS (Host-based Intrusion Detection System) sistemi che analizzano informazioni relative all'attività locale di un singolo host (log di sistema, accesso a file critici, ...)

NIDS (Network Intrusion Detection System) sistemi che utilizzano le informazioni raccolte da analizzatori di traffico di rete.



Sicurezza delle reti
 Monga
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi

L'analisi dei dati raccolti per **rilevare** una situazione d'allarme può essere fatta secondo due approcci fondamentali

Misuse detection Si caratterizza l'**abuso**: si rilevano le situazioni che ricadono nella descrizione di un attacco (sono detti anche **signature based**)

Anomaly detection Si caratterizza l'**uso normale**: si rilevano le situazioni che si scostano dal "normale" funzionamento in modo da poter rilevare anche attacchi ancora sconosciuti



Sicurezza delle reti
 Monga
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi

Occorre elencare le situazioni che riteniamo pericolose:

Signature Detection
 L'amministratore definisce pattern (**signature**) predefiniti di usi non conformi e il sistema analizza gli eventi monitorati (di rete, di sistema, nei log) rispetto all'elenco di pattern

È la tecnica che si è affermata e diffusa nella maggior parte dei sistemi in produzione



Sicurezza delle reti
 Monga
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi

I misuse detection rilevano solo attacchi che corrispondono a schemi noti

- Regole rigide non rilevano attacchi non noti e varianti (a volte l'IDS è così rigido che basta cambiare un bit per evadere la rilevazione)
- Più le regole sono flessibili e più aumenta la complessità di gestione/configurazione
- l'elenco di firme deve essere adattato alle specificità della rete monitorata

Anomaly detection



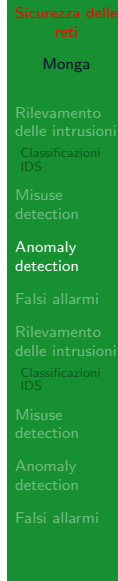
Le anomalie possono essere rispetto

- ad eventi singoli: esempio azioni “anomale” di un utente rispetto un profilo d'uso predefinito
es: `http://example.com/##&<>623??%`
- a dati aggregati: tipicamente, deviazioni rispetto a parametri statistici
es: il traffico con sorgente 123.45.67.88 è di 5GB al minuto

Vantaggi

- + Non dipende dalla conoscenza puntuale di tutte le modalità di intrusione
- Molto complesso da realizzare (come fare il modello dell'uso “normale”?) e oneroso da gestire
- Non forniscono informazioni su quale vulnerabilità l'attaccante intende colpire

123



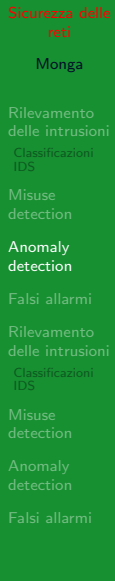
Modelli di uso normale



Il sistema viene monitorato durante gli usi normali per raccogliere i parametri che caratterizzano i profili d'uso non anomali.

- L'ipotesi di assenza di compromissione e normalità non è facile da verificare: gli usi in fase di test rischiano di essere anomali rispetto all'uso realistico sul campo
- Impiego di tecniche come data mining, sistemi esperti, data fusion, analisi bayesiana, ecc...
- È molto complesso tenere il passo con l'evoluzione del sistema
- il monitoraggio introduce in generale inefficienze maggiori rispetto ai misuse

124



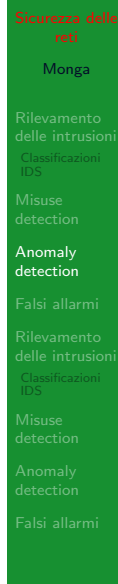
Usi consolidati dell'anomaly detection



Ci sono casi in cui l'anomaly detection funziona bene e il loro uso è ormai standard

- hashing dei file (HIDS): l'integrità dei file del sistema viene controllata calcolando gli hash (MD5, SHA1, ...) dei file di sistema presi da una distribuzione originale e li si confronta periodicamente con gli hash del sistema da monitorare. (es. Tripwire)
- Protocol Anomaly Detection (NIDS): viene analizzato il traffico di rete rispetto alle specifiche del protocollo applicativo (vedi lezione sui proxy applicativi: monitoraggio anziché filtraggio)

125



Falsi allarmi



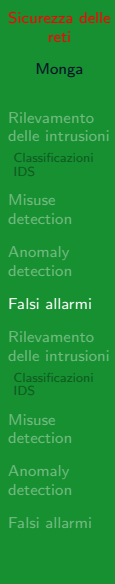
In generale in tutti gli IDS (misuse e anomaly) occorre bilanciare

falsi negativi attacchi non rilevati

falsi positivi attacchi rilevati corrispondenti a situazioni normali

- Quanto più la rilevazione è **specificata** (ad esempio firme molto dettagliate) tanto più aumenta il carico computazionale e la rilevazione diventa sensibile a variazioni o mutazioni dell'evento analizzato
- Quanto più la rilevazione si fa **lasca** (ad esempio firme generiche) tanto più il carico computazionale cala, la rilevazione dell'evento analizzato risulta poco influenzata da varianti e mutazioni ma tanto più eventi simili ma non analoghi all'evento analizzato possono essere erroneamente rilevati

126



Relazione fra FP e FN



Le due grandezze FP e FN risultano correlate inversamente: agendo per diminuire l'una, tipicamente l'altra aumenta. Il problema si ripropone in moltissime discipline (information retrieval, farmacologia, ...): ogni volta che si ha una decisione binaria (test) basata su considerazioni statistiche.

	positivo	negativo
attacco	TP	TN
non attacco	FP	FN

$$TP + TN + FP + FN = totale$$

FP Type I error, falso allarme

FN Type II error, miss

sensibilità del test, recall, hit rate $\frac{TP}{TP+FN}$

specificità del test $\frac{TN}{TN+FP}$

accuratezza del test $\frac{TP+TN}{totale}$

precisione del test $\frac{TP}{TP+FP}$

Sicurezza delle reti
Monga
Rilevamento delle intrusioni
Classificazioni IDS
Misuse detection
Anomaly detection
Falsi allarmi
Rilevamento delle intrusioni
Classificazioni IDS
Misuse detection
Anomaly detection
Falsi allarmi

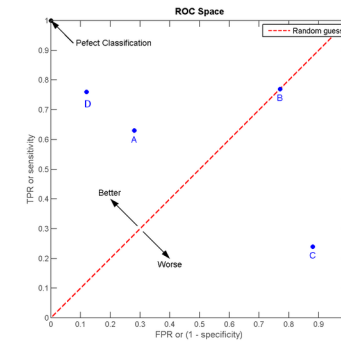
Esempio



Quali regole di IDS hanno lavorato meglio?

receiver operating characteristic (ROC): sensibilità vs. tasso dei falsi positivi

A (0.28,0.63)	allarme	¬allarme
attacco	TP=63	FN=37
¬attacco	FP=28	TN=72
B (0.77,0.77)	allarme	¬allarme
attacco	TP=77	FN=23
¬attacco	FP=77	TN=23
C (0.88,0.24)	allarme	¬allarme
attacco	TP=24	FN=76
¬attacco	FP=88	TN=12
D (0.12,0.76)	allarme	¬allarme
attacco	TP=76	FN=24
¬attacco	FP=12	TN=88

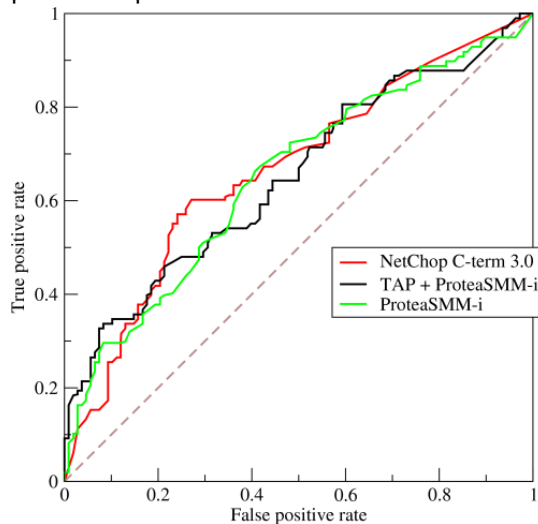


Sicurezza delle reti
Monga
Rilevamento delle intrusioni
Classificazioni IDS
Misuse detection
Anomaly detection
Falsi allarmi
Rilevamento delle intrusioni
Classificazioni IDS
Misuse detection
Anomaly detection
Falsi allarmi

E un insieme di regole?



E come valutare l'efficacia di un insieme di regole per tutti i parametri possibili? A volte si usa l'Area under curve.



Sicurezza delle reti
Monga
Rilevamento delle intrusioni
Classificazioni IDS
Misuse detection
Anomaly detection
Falsi allarmi
Rilevamento delle intrusioni
Classificazioni IDS
Misuse detection
Anomaly detection
Falsi allarmi

Lezione XIII: Rilevamento delle intrusioni



Sicurezza delle reti
Monga
Rilevamento delle intrusioni
Classificazioni IDS
Misuse detection
Anomaly detection
Falsi allarmi
Rilevamento delle intrusioni
Classificazioni IDS
Misuse detection
Anomaly detection
Falsi allarmi

Intrusion detection system (IDS)



Sicurezza delle reti

Monga

Rilevamento delle intrusioni
Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Rilevamento delle intrusioni
Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

IDS

È un sistema di monitoraggio (generalmente del tutto passivo) che genera **allarmi**

Saranno necessarie tre fasi:

- 1 Raccolta dati
- 2 Analisi dei dati
- 3 Generazione degli allarmi

Agli allarmi deve poi seguire una risposta dell'amministratore del sistema: come vedremo non è facile automatizzare questa ultima fase.

138

Perché usare un IDS?



Sicurezza delle reti

Monga

Rilevamento delle intrusioni
Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Rilevamento delle intrusioni
Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

In generale i sistemi di monitoraggio sono utili perché:

- le tecnologie di prevenzione degli eventi indesiderati o pericolosi possono fallire
- è utile avere un meccanismo di segnalazione che permetta di attivare procedure di correzione o di emergenza
- l'uso di strumenti che permettano di monitorare lo stato corrente di un sistema, sia esso un componente che una rete, per accumulare conoscenza statistica sulle modalità d'uso

139

HIDS e NIDS



Sicurezza delle reti

Monga

Rilevamento delle intrusioni
Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Rilevamento delle intrusioni
Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Gli IDS possono essere classificati in base al punto in cui avviene la raccolta dati

HIDS (Host-based Intrusion Detection System) sistemi che analizzano informazioni relative all'attività locale di un singolo host (log di sistema, accesso a file critici, ...)

NIDS (Network Intrusion Detection System) sistemi che utilizzano le informazioni raccolte da analizzatori di traffico di rete.

140

Rilevazione di eventi critici



Sicurezza delle reti

Monga

Rilevamento delle intrusioni
Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Rilevamento delle intrusioni
Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

L'analisi dei dati raccolti per **rilevare** una situazione d'allarme può essere fatta secondo due approcci fondamentali

Misuse detection Si caratterizza l'**abuso**: si rilevano le situazioni che ricadono nella descrizione di un attacco (sono detti anche **signature based**)

Anomaly detection Si caratterizza l'**uso normale**: si rilevano le situazioni che si scostano dal "normale" funzionamento in modo da poter rilevare anche attacchi ancora sconosciuti

141

Misuse detection



Sicurezza delle reti

Monga

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Occorre elencare le situazioni che riteniamo pericolose:

Signature Detection

L'amministratore definisce pattern (*signature*) predefiniti di usi non conformi e il sistema analizza gli eventi monitorati (di rete, di sistema, nei log) rispetto all'elenco di pattern

È la tecnica che si è affermata e diffusa nella maggior parte dei sistemi in produzione

142

Problemi



Sicurezza delle reti

Monga

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

I misuse detection rilevano solo attacchi che corrispondono a schemi noti

- Regole rigide non rilevano attacchi non noti e varianti (a volte l'IDS è così rigido che basta cambiare un bit per evadere la rilevazione)
- Più le regole sono flessibili e più aumenta la complessità di gestione/configurazione
- l'elenco di firme deve essere adattato alle specificità della rete monitorata

143

Anomaly detection



Sicurezza delle reti

Monga

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Le anomalie possono essere rispetto

- ad eventi singoli: esempio azioni "anomale" di un utente rispetto un profilo d'uso predefinito
es: <http://example.com/##&<623??%>
- a dati aggregati: tipicamente, deviazioni rispetto a parametri statistici
es: il traffico con sorgente 123.45.67.88 è di 5GB al minuto

Vantaggi

- + Non dipende dalla conoscenza puntuale di tutte le modalità di intrusione
- Molto complesso da realizzare (come fare il modello dell'uso "normale"?) e oneroso da gestire
- Non forniscono informazioni su quale vulnerabilità l'attaccante intende colpire

144

Modelli di uso normale



Sicurezza delle reti

Monga

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Il sistema viene monitorato durante gli usi normali per raccogliere i parametri che caratterizzano i profili d'uso non anomali.

- L'ipotesi di assenza di compromissione e normalità non è facile da verificare: gli usi in fase di test rischiano di essere anomali rispetto all'uso realistico sul campo
- Impiego di tecniche come data mining, sistemi esperti, data fusion, analisi bayesiana, ecc...
- È molto complesso tenere il passo con l'evoluzione del sistema
- il monitoraggio introduce in generale inefficienze maggiori rispetto ai misuse

145

Usi consolidati dell'anomaly detection



Sicurezza delle reti
 Monga
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi

Ci sono casi in cui l'anomaly detection funziona bene e il loro uso è ormai standard

- hashing dei file (HIDS): l'integrità dei file del sistema viene controllata calcolando gli hash (MD5, SHA1, ...) dei file di sistema presi da una distribuzione originale e li si confronta periodicamente con gli hash del sistema da monitorare. (es. Tripwire)
- Protocol Anomaly Detection (NIDS): viene analizzato il traffico di rete rispetto alle specifiche del protocollo applicativo (vedi lezione sui proxy applicativi: monitoraggio anziché filtraggio)

146

Falsi allarmi



Sicurezza delle reti
 Monga
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi

In generale in tutti gli IDS (misuse e anomaly) occorre bilanciare

falsi negativi attacchi non rilevati

falsi positivi attacchi rilevati corrispondenti a situazioni normali

- Quanto più la rilevazione è **specifica** (ad esempio firme molto dettagliate) tanto più aumenta il carico computazionale e la rilevazione diventa sensibile a variazioni o mutazioni dell'evento analizzato
- Quanto più la rilevazione si fa **lasca** (ad esempio firme generiche) tanto più il carico computazionale cala, la rilevazione dell'evento analizzato risulta poco influenzata da varianti e mutazioni ma tanto più eventi simili ma non analoghi all'evento analizzato possono essere erroneamente rilevati

147

Relazione fra FP e FN



Sicurezza delle reti
 Monga
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi

Le due grandezze FP e FN risultano correlate inversamente: agendo per diminuire l'una, tipicamente l'altra aumenta. Il problema si ripropone in moltissime discipline (information retrieval, farmacologia, ...): ogni volta che si ha una decisione binaria (test) basata su considerazioni statistiche.

	positivo	negativo
attacco	TP	TN
non attacco	FP	FN

$$TP + TN + FP + FN = \text{totale}$$

FP Type I error, falso allarme

FN Type II error, miss

sensibilità del test, recall, hit rate $\frac{TP}{TP+FN}$

specificità del test $\frac{TN}{TN+FP}$

accuratezza del test $\frac{TP+TN}{\text{totale}}$

precisione del test $\frac{TP}{TP+FP}$

148

Esempio

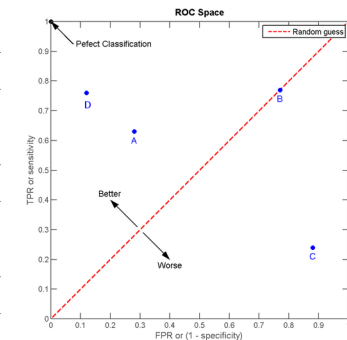


Sicurezza delle reti
 Monga
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi
 Rilevamento delle intrusioni
 Classificazioni IDS
 Misuse detection
 Anomaly detection
 Falsi allarmi

Quali regole di IDS hanno lavorato meglio?

receiver operating characteristic (ROC): sensibilità vs. tasso dei falsi positivi

	positivo	negativo
A (0.28,0.63)	TP=63	TN=72
non attacco	FP=28	FN=37
B (0.77,0.77)	TP=77	TN=23
non attacco	FP=77	FN=23
C (0.88,0.24)	TP=24	TN=12
non attacco	FP=88	FN=76
D (0.12,0.76)	TP=76	TN=88
non attacco	FP=12	FN=24

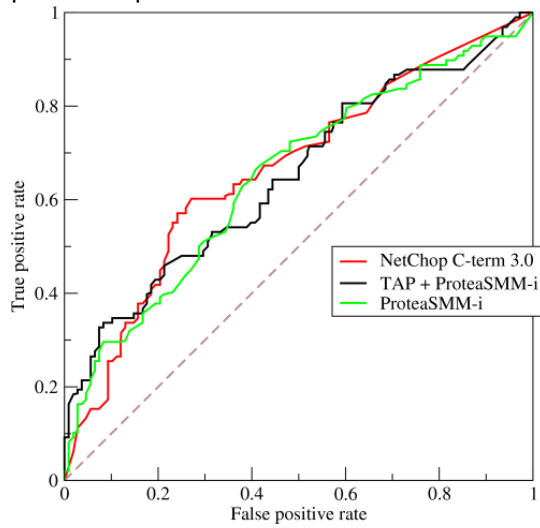


149

E un insieme di regole?



E come valutare l'efficacia di un insieme di regole per tutti i parametri possibili? A volte si usa l'Area under curve.



150

Scurezza delle reti

Monga

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi

Rilevamento delle intrusioni

Classificazioni IDS

Misuse detection

Anomaly detection

Falsi allarmi