

Protezione di una rete di macchine LINUX con

TRIPWIRE


A cura di:
Francesco Casertano e
Attilio Stanziale

prof. Alfredo De Santis
Anno Accademico 2003-04

INDICE

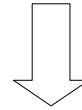
1. Introduzione
2. Panoramica su Tripwire
3. Utilizzo di Tripwire
4. Installazione e personalizzazione
5. Inizializzazione del Database
6. Controllo d'integrità
7. Analisi dei report
8. Aggiornamento del database e del policy file
9. Comandi usati da Tripwire
10. Algoritmi utilizzati
11. File & Directory usate da Tripwire
12. Bibliografia

INDICE

1. Introduzione 
2. Panoramica su Tripwire
3. Utilizzo di Tripwire
4. Installazione e personalizzazione
5. Inizializzazione del Database
6. Controllo d'integrità
7. Analisi dei report
8. Aggiornamento del database e del policy file
9. Comandi usati da Tripwire
10. Algoritmi utilizzati
11. File & Directory usate da Tripwire
12. Bibliografia

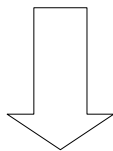
INTRODUZIONE

I meccanismi che scoprono cambiamenti nel file system fanno parte di una strategia di sicurezza.



Permettono di scovare Trojan, creazione di backdoors e modifica di file di configurazione.


Analizziamo uno dei più conosciuti strumenti di verifica dell'integrità del file system.



TRIPWIRE

versione 2.3-47 per sistemi operativi Linux.

INDICE

1. Introduzione
2. Panoramica su Tripwire 
3. Utilizzo di Tripwire
4. Installazione e personalizzazione
5. Inizializzazione del Database
6. Controllo d'integrità
7. Analisi dei report
8. Aggiornamento del database e del policy file
9. Comandi usati da Tripwire
10. Algoritmi utilizzati
11. File & Directory usate da Tripwire
12. Bibliografia

CENNI STORICI

Tripwire è stato sviluppato:

- negli anni 90 da Gene Kim ed Eugene Spafford
- per sistemi operativi Linux
- successivamente è stato sviluppato anche per altre piattaforme.

Lo scopo di Tripwire

Lo scopo di Tripwire è quello di garantire l'integrità dei dati.



Aiuta ad individuare problemi causati da un uso improprio del sistema oppure dall'azione di un virus.

Come Agisce

Tripwire individua e mostra i cambiamenti che avvengono nel file system.

Come Agisce

Quando il sistema è in uno stato sicuro



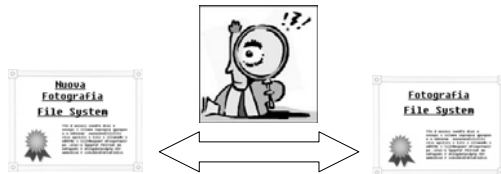
Tripwire ne calcola la fotografia



la conserva in un database firmato con chiave cifrata da passphrases

Come Agisce

Quando l'utente vuole verificare se ci sono state intrusioni, Tripwire effettua una nuova fotografia del sistema



e la confronta con quella precedente: cerca quindi le eventuali differenze tra lo stato attuale del file system e le informazioni contenute nel database

Passphrases

Ma a cosa servono?

La site passphrase serve a generare la chiave che protegge il file di configurazione ed il policy file.

+

La local passphrase serve a generare la chiave che protegge il file del database ed il file dei reports.

=

Cifrando queste chiavi, Tripwire impedisce a chiunque non sia in possesso delle passphrases di visualizzare i files e quindi di modificarli.

Sicurezza di Tripwire

La sicurezza di Tripwire si basa essenzialmente su tre primitive:

firma digitale
cifratura simmetrica
funzione hash

Scopo della Firma Digitale

La firma digitale, garantisce l'autenticità delle istantanee conservate nel database.

Un utente malizioso nel momento in cui modifica un oggetto del sistema, causa una differenza tra l'istananea conservata nel database e quella creata da Tripwire quando effettua una verifica, e di conseguenza la firma digitale non è più consistente .

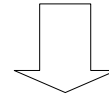
Scopo della Cifratura Simmetrica

La cifratura simmetrica applicata ai files che contengono le chiavi, fa in modo che un attaccante, non potendo accedere alla chiave privata, non può riprodurre la stessa firma di Tripwire su files modificati.

Scopo della Funzione Hash

La funzione hash garantisce l'unicità dell'istananea.

Ogni modifica di oggetti del sistema da luogo ad un valore hash diverso che produce un'istananea diversa.



Ogni cambiamento da parte di persone maliziose viene facilmente rilevato.

Tripwire è composto da:

1. Un database per il controllo dei file (firmato);
2. Programmi per effettuare dei report dal database o per aggiornare il database.
3. Regole contenute in un policy file che stabiliscono quali oggetti devono essere controllati ed in che modo.

Violazioni del file system

Se Tripwire riporta delle violazioni del file system, la causa può essere:

1. Attività inusuali su file che violano le politiche.
Soluzione: Aggiornare il database.
2. Una ristretta politica di gestione dei file che considera attività normali come delle violazioni.
Soluzione: Aggiornare il policy file.

Violazioni del file system

3. Una violazione della sicurezza.
Soluzione: Effettuare riparazioni e rimozione dei file compromessi ed effettuare attività investigative su un potenziale crack.

INDICE

1. Introduzione
2. Panoramica su Tripwire
3. Utilizzo di Tripwire
4. Installazione e personalizzazione
5. Inizializzazione del Database
6. Controllo d'integrità
7. Analisi dei report
8. Aggiornamento del database e del policy file
9. Comandi usati da Tripwire
10. Algoritmi utilizzati
11. File & Directory usate da Tripwire
12. Bibliografia

L'utilizzo di Tripwire può essere riassunto da questo diagramma:



INDICE

1. Introduzione
2. Panoramica su Tripwire
3. Utilizzo di Tripwire
4. Installazione e personalizzazione
5. Inizializzazione del Database
6. Controllo d'integrità
7. Analisi dei report
8. Aggiornamento del database e del policy file
9. Comandi usati da Tripwire
10. Algoritmi utilizzati
11. File & Directory usate da Tripwire
12. Bibliografia

Distribuzioni

Il pacchetto di Tripwire è distribuito in tre versioni:

1. Un RPM 3.0 per Red Hat dalla 5.x alla 6.2.x.
2. Un RPM 4.0 per Red Hat dalla 7.x.
3. Un tarball per tutte le altre distribuzioni di Linux.

Installazione

Per installare le versioni RPM bisogna usare il comando:

```
rpm -Uhv /path/tripwire2.3-47.i386.rpm
```

Per installare la versione tarball bisogna usare il comando:

```
tar xvfz /path/tripwire2.3-47.bin.tar.gz
```

Installazione

Con l'installazione viene creata la directory:

`/etc/tripwire/`

che conterrà:

`twcfg.txt`: versione non crittografata e non firmata del file di configurazione (`tw.cfg`)

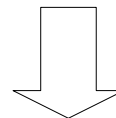
`twpol.txt`: versione non crittografata e non firmata del policy file (`tw.pol`)

`install.sh`: script per la configurazione e l'inizializzazione di Tripwire

Personalizzazione del File di Configurazione

E' possibile cambiare le impostazioni di configurazione

Ad esempio per cambiare impostazioni di e-mail o dei report



Per modificare il file di configurazione si può partire dal file in chiaro `twcfg.txt`.

Il File di Configurazione

Il file di configurazione di Tripwire è strutturato come una lista di coppie Keyword/Valore, e può inoltre contenere commenti e definizioni di variabili.

Sintassi

Le linee che cominciano con '#' sono commenti:

`#questo è un commento`

La definizione di una variabile è:

`keyword = value` \longleftrightarrow `EDITOR=/usr/local/sbin/emacs`

Per usare il valore di una variabile:

`$(Varname)` \longleftrightarrow `DBFILE=$(Root)/db/$(Hostname).db`

Variabili predefinite

Alcune variabili sono predefinite e non possono essere cambiate:

Variabile	Significato
HOSTNAME	Nome dell'host sul quale gira Tripwire.
DATE	Stringa che rappresenta la data e l'ora.

Variabili obbligatorie

Se le seguenti variabili non sono settate prendono il valore di default:

Variabile	Descrizione
POLFILE	Policy file (<code>/etc/tripwire/tw.pol</code>)
DBFILE	File del database (<code>/var/lib/tripwire/\$(HOSTNAME).twd</code>)
REPORT FILE	Nome dei report (<code>/var/lib/tripwire/report/\$(HOSTNAME)-\$(DATE).twr</code>)
SITEKEY FILE	Site key file (<code>/etc/tripwire/site.key</code>)
LOCALKEY FILE	Local key file (<code>/etc/tripwire/\$(HOSTNAME)-local.key</code>)

Variabili opzionali

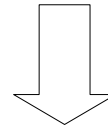
Le seguenti variabili sono opzionali, ma alcune funzionalità del programma sarebbero perse senza la loro dichiarazione:

- EDITOR
- MAILPROGRAM
- LATEPROMPTING
- LOOSEDIRECTORYCHECKING

Creazione del File di Configurazione

Per rendere di default, il file di configurazione creato usiamo il comando:

```
twadmin --create-cfgfile --site-keyfile ./key/site.key configfile.txt
```



In questo modo il file di configurazione viene cifrato, firmato e salvato.

Personalizzazione del Policy File

Lo scopo del policy file di Tripwire è di assegnare gli attributi da controllare per i vari files, directories e devices.

Per modificare il policy file si può partire dal file in chiaro twpol.txt.

Il file twpol.txt potrebbe contenere dei file che non esistono nel sistema, generando degli errori nei report di Tripwire.

Sintassi

Supponiamo di voler controllare per il file /etc/fstab la grandezza, la data di modifica, il tipo di file. La regola nel file twpol.txt potrebbe essere:

```
/etc/fstab -> smt;
```

Questo tipo di assegnamento è detto "normal rule" e la sintassi generale è :

```
object_name -> property_mask;
```

Terminologia di Tripwire

Nella terminologia di Tripwire, files, directories e devices sono chiamati objects, mentre la lista di attributi da controllare è detta property mask.

Le property masks rappresentano un insieme di proprietà individuali da controllare, ognuna rappresentata da un carattere.

Property Masks

Car.	Attributo da controllare	Car.	Attributo da controllare
a	Access timestamp	p	Permissions and file mode bits
b	Number of blocks allocated	r	ID of device pointed to by inode (valid only for device objects)
c	I-node timestamp (create/modify)	s	File size
d	ID of device on which i-node resides	t	File type
g	File owner's group ID	u	File owner's user ID
i	I-node number	C	CRC-32 hash value
l	File is increasing in size (a "growing file")	H	Haval hash value
m	Modification timestamp	M	MD5 hash value
n	Number of links (i-node reference count)	S	SHA hash value

Variabili

Spesso le property masks sono rappresentate da variabili:

```
SEC_INVARIANT = tpug;
```

Controlliamo:
•Il tipo di file
•I permessi sul file
•User Id del proprietario del file
•Group Id del proprietario del file

La variabile può essere usata con questa sintassi:

```
/etc -> $(SEC_INVARIANT);
```

Variabili predefinite

Tripwire ha alcune variabili predefinite che non possono essere eliminate:

Variable	Property Mask	Description
\$(ReadOnly)	+pinugtsdbmCM-rlacSH	file da aprire in sola lettura
\$(Dynamic)	+pinugtdl-srlbancCMSH	file dinamici
\$(Growing)	+pinugtdl-srbancCMSH	file che possono solo aumentare in grandezza
\$(Device)	+pugsdr-intlbancCMSH	tipi di file che non deve aprire
\$(IgnoreAll)	-pinugtsdrilbancCMS	controllare la presenza di file
\$(IgnoreNone)	+pinugtsdrbancCMSH-I	controllare tutte le proprietà

Recurse

Le normal rules possono essere associate ad una coppia (attributo=valore).

Ad esempio:

```
/home -> $(SEC_INVARIANT) (recurse = 0);
```

(recurse = 0) è una "rule attribute" che specifica di applicare la regola Sec_Invariant alla directory /home, ma di non applicarla ricorsivamente.

Stop Point

Per evitare il controllo su oggetti contenuti in una directory controllata da Tripwire, è possibile usare gli "stop point".

La sintassi di uno stop point è: `object_name;`

Un esempio di utilizzo è:

```
/boot -> $(SEC_CRIT);  
!/boot/System.map;  
!/boot/module-info;
```

Controlliamo tutta la directory /boot tranne i files: system.map e module-info

Direttive/1

Le direttive permettono interpretazioni condizionali di alcune operazioni. Il loro uso principale è permettere a diverse parti di condividere un singolo policy file. La sintassi di una direttiva è :

```
@@ directive_name [arguments]
```

Direttive/2

Tripwire supporta le seguenti direttive:

`@@aasection` designa una sezione del policy file.
`@@ifhost` permette un'interpretazione condizionale.
`@@else` un'alternativa valutazione di `@@ifhost`.
`@@endif` la fine di un `@@ifhost`.
`@@print` stampa un messaggio sullo standard output.
`@@errore` stampa un messaggio di errore sullo standard output ed esce.
`@@end` marca l'end-of-file logico.

Editare il Policy File

Per editare il policy file in chiaro si usa il comando:

```
twadmin --print-polfile |less /*(>file.txt)*/
```

Attenzione!!! La sicurezza di Tripwire dipende tutta dal policy file, quindi è molto importante eliminare dal sistema la versione in chiaro.

Creazione del Policy File

Per rendere il nostro file il nuovo policy file usiamo due comandi:

```
twadmin --create-polfile file_policy.txt
```

Crea un policy file
ex-novo

```
tripwire --update-policy file_policy.txt
```

Modifica un database
esistente

install.sh

Dopo aver modificato il policy file ed il file di configurazione, possiamo lanciare come "root" lo script install.sh.

Se non specificate, lo script richiede la local e la site passphrase per generare le chiavi che proteggono i file di Tripwire.


In seguito lo script crea i file \$(Hostname)-local.key e site.key, che contengono le chiavi, e li firma.

Passphrases

La local e la site passphrase devono rispettare le seguenti regole:

- 1) Lunghezza compresa tra 8 e 1023 caratteri alfanumerici e simbolici.
- 2) Non utilizzare virgolette ("").
- 3) Differenti dalla password di root o da qualunque altra password presente nel sistema.
- 4) Differenti tra loro.

INDICE

1. Introduzione
2. Panoramica su Tripwire
3. Utilizzo di Tripwire
4. Installazione e personalizzazione
5. Inizializzazione del Database 
6. Controllo d'integrità
7. Analisi dei report
8. Aggiornamento del database e del policy file
9. Comandi usati da Tripwire
10. Algoritmi utilizzati
11. File & Directory usate da Tripwire
12. Bibliografia

Il Database

Dopo aver configurato i file "tw.cfg" e "tw.pol" è possibile generare il database.

Questo file è la copia autorevole alla quale Tripwire fa riferimento quando controlla l'integrità del file system.



Inizializzazione

Durante l'inizializzazione del database, Tripwire inserisce (nel database) una serie di oggetti del file system basati sulle regole contenute nel policy file.

Il comando da usare per inizializzare il database è:

```
tripwire --init
```

Inizializzazione


Il database cifrato sarà contenuto in:

```
$(DBFILE)/$(HOSTNAME).twd
```

DBFILE è la variabile dichiarata nel file di configurazione di Tripwire (tw.cfg)

Per rendere il sistema più sicuro è consigliabile salvare il database su periferiche esterne e caricarlo solo quando è necessario.

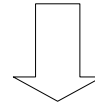
INDICE

1. Introduzione
2. Panoramica su Tripwire
3. Utilizzo di Tripwire
4. Installazione e personalizzazione
5. Inizializzazione del Database
6. Controllo d'integrità 
7. Analisi dei report
8. Aggiornamento del database e del policy file
9. Comandi usati da Tripwire
10. Algoritmi utilizzati
11. File & Directory usate da Tripwire
12. Bibliografia

Check

Dopo aver creato il database, è possibile lanciare il check di Tripwire attraverso il comando:

```
tripwire --check
```



esegue un controllo di integrità per scoprire quale file è stato aggiunto, eliminato o modificato, mettendo a confronto lo stato attuale del file system con quello contenuto nel database.

Report


Una volta effettuato il check, viene stampato un report a video ed un altro report più approfondito viene salvato nella directory assegnata alla variabile REPORTFILE del file di configurazione.

```
/var/lib/tripwire/report/
```

Automatizzare il Check

Per default il processo di installazione di Tripwire aggiunge alla directory /etc/cron.daily/ uno script della shell chiamato tripwire-check che avvierà quotidianamente un controllo di integrità.

INDICE

1. Introduzione
2. Panoramica su Tripwire
3. Utilizzo di Tripwire
4. Installazione e personalizzazione
5. Inizializzazione del Database
6. Controllo d'integrità
7. Analisi dei report 
8. Aggiornamento del database e del policy file
9. Comandi usati da Tripwire
10. Algoritmi utilizzati
11. File & Directory usate da Tripwire
12. Bibliografia

Report

Se durante il checking, Tripwire ha trovato delle variazioni rispetto al database, bisogna esaminare il report per capire se si sono verificate delle violazioni.

Per visualizzare in chiaro i reports ed il database cifrati è possibile utilizzare il comando 'twprint':

```
twprint -m r --twrfile /REPORTFILE/nomereport.twr
```

Report

Il report è formato da quattro parti, ognuna della quali ha una o più sezioni:

1. Un'intestazione che contiene il nome dell'utente che ha generato il report (generalmente root), la data di creazione del report e la data dell'ultimo aggiornamento del database.
2. Una parte che contiene un riassunto delle violazioni, che aiuta a capire velocemente ogni problema.

Report


3. Una parte che contiene le specifiche delle violazioni riportate nel sommario. Questo serve a capire se una violazione è dovuta ad attività normali o ad un possibile crack.
4. Una parte che elenca tutti i tipi di errore riscontrati.

twprint


Twprint può essere usato anche per visualizzare l'intero database o informazioni specifiche su un file.

I comandi da utilizzare sono:

Per visualizzare il database completo  `/usr/sbin/twprint -m d --print-dbfile | less`

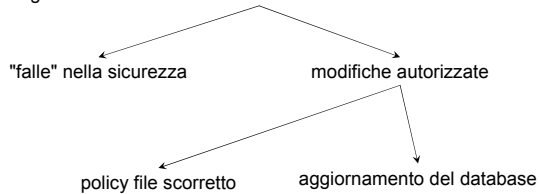
Per visualizzare le informazioni relative a un file  `/usr/sbin/twprint -m d --print-dbfile file`

INDICE

1. Introduzione
2. Panoramica su Tripwire
3. Utilizzo di Tripwire
4. Installazione e personalizzazione
5. Inizializzazione del Database
6. Controllo d'integrità
7. Analisi dei report
8. Aggiornamento del database e del policy file 
9. Comandi usati da Tripwire
10. Algoritmi utilizzati
11. File & Directory usate da Tripwire
12. Bibliografia

Modifiche autorizzate

Se il controllo dell'integrità ha riscontrato delle violazioni, bisogna determinare se:



Aggiornare il Database

Problema

Se di recente è stato installata un'applicazione o sono stati modificati dei file di sistema importanti, Tripwire segnalerà tutte le operazioni che sono state eseguite come violazioni dell'integrità del sistema.



Aggiornare il Database

Per aggiornare il database in modo che accetti le violazioni, Tripwire crea un file report a riferimenti incrociati per il database e poi integra al suo interno le violazioni estrapolate dal file report.

Per aggiornare il database si può usare il comando:

```
tripwire --update --twrfile /var/lib/tripwire/report/name.twr
```

Aggiornare il Database

Tripwire visualizza il file di report utilizzando l'editor di testo predefinito che è stato specificato nel file di configurazione (se non è stato cambiato è vi).

È importante modificare solo le violazioni dell'integrità autorizzate.

Tutti gli aggiornamenti proposti hanno una [x] che precede il nome del file: se si vuole escludere una violazione valida dal database basta rimuovere la [x].

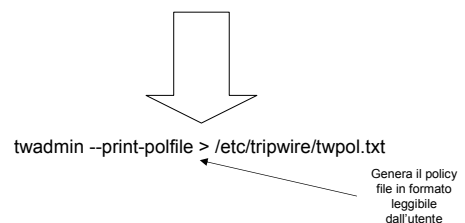
Aggiornare il Database

Dopo aver chiuso l'editor, viene chiesta la local passphrase ed il database verrà ricostruito e firmato.

A questo punto, tutte le violazioni autorizzate non verranno più segnalate al controllo di integrità successivo.

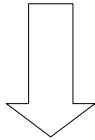
Aggiornare il Policy File

Se le violazioni sono dovute ad una politica ristretta attuata sui file, bisogna modificare il policy file.



Aggiornare il Policy File

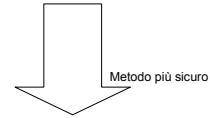
Bisogna indicare a Tripwire di creare un nuovo policy file firmato e di generare un file del database aggiornato in base alle nuove informazioni di policy.



```
twadmin --create-polfile -S site.key file_chiario
```

Aggiornare il Policy File

Una volta creato il policy file bisogna aggiornare il database.



1. Rimuovere il vecchio database.
`rm /var/lib/tripwire/$(HOSTNAME).twd`
2. Creare un nuovo database.
`tripwire --init`

INDICE

1. Introduzione
2. Panoramica su Tripwire
3. Utilizzo di Tripwire
4. Installazione e personalizzazione
5. Inizializzazione del Database
6. Controllo d'integrità
7. Analisi dei report
8. Aggiornamento del database e del policy file
9. Comandi usati da Tripwire
10. Algoritmi utilizzati
11. File & Directory usate da Tripwire
12. Bibliografia

I Comandi di Tripwire

tripwire

- inializza il database;
- esegue il controllo dell'integrità;
- aggiorna il database;
- aggiorna il policy file;

I Comandi di Tripwire

siggen

- calcola i valori delle firme crittografiche dei file;

I Comandi di Tripwire

twadmin


- crea e stampa il file di configurazione ed il policy file;
- appone o rimuove una firma da un file;
- valuta lo stato della firma di un file;
- genera le chiavi.

I Comandi di Tripwire

twprint

- stampa il file del database;
- stampa il file del report;

INDICE

1. Introduzione
2. Panoramica su Tripwire
3. Utilizzo di Tripwire
4. Installazione e personalizzazione
5. Inizializzazione del Database
6. Controllo d'integrità
7. Analisi dei report
8. Aggiornamento del database e del policy file
9. Comandi usati da Tripwire
10. Algoritmi utilizzati 
11. Files & Directory usati da Tripwire
12. Bibliografia

Algoritmi usati da Tripwire

Normalmente, un solo controllo per file è sufficiente per individuare delle violazioni, e per motivi di velocità, un controllo facile da effettuare sarebbe preferito.

Firme facili da
calcolare



Firme facili da
rompere

Algoritmi usati da Tripwire

Tripwire include diversi algoritmi di firma difficili da forzare, oltre a due routines CRC convenzionali.

Di default per ogni entry del database sono memorizzate due firme (MD-5 e Snefru) che assicurano che un file non sia modificato.

PROBLEMA

Lanciare MD-5 e Snefru per ogni file è computazionalmente costoso.

SOLUZIONE

Per bilanciare l'equazione tra sicurezza e velocità usare MD-5 e Snefru per controllare i file più critici e solo MD-5 per controllare tutti gli altri files.

Algoritmi

Tra gli algoritmi più usati da Tripwire troviamo:

1. MD-5;
2. MD-4;
3. SNEFRU;
4. CRC-32;
5. CRC-16.

MD-5

Progettato nel 1995 da Ron Rivest.

Prende il suo nome da "Message Digest".

MD-5 permette di effettuare operazioni efficienti su architetture a 32 bit little endian.

L'algoritmo prende in input una sequenza di bit casuale ($\leq 2^{64}$ bit) e restituisce in output una sequenza di 128 bit.

MD-5 esegue 4 round ognuno di 16 operazioni, per assicurare un output pseudorandomico.

MD-4

MD-4 è il predecessore di MD-5 e si distingue per i seguenti motivi:

- 1) MD-5 ha quattro round ognuno con sedici operazioni, mentre MD-4 ne ha tre con sedici operazioni;
- 2) MD-5 usa quattro funzioni logiche mentre MD-4 ne usa tre;
- 3) MD-5 ha 64 costanti additive mentre MD-4 ne ha due.

SNEFRU

Snefru, della Xerox Secure Hash Function, prende il nome da un antico faraone egiziano.

Al momento è consigliabile usare la versione a 4 passi di Snefru. L'ultima versione disponibile di Snefru è la 2.5, già inclusa in Tripwire.

In generale Snefru è un algoritmo one-way hash che fornisce autenticazione ma non segretezza.

L'algoritmo prende in input una sequenza di bit di qualsiasi grandezza e ne da in output una di 128.

CRC-32

CRC-32 può essere visto come un efficiente alternativa ai lenti algoritmi Message-Digest.

Gli algoritmi appartenenti alla famiglia "Cyclic Redundance Checks" sono stati per lungo tempo gli standard per la verifica di errori nei dati.


Questi algoritmi sono veloci, robusti e forniscono una affidabile verifica degli errori che avvengono nella trasmissione dei dati.

CRC-16

CRC-16 è il predecessore di CRC-32, ed usa soltanto 16 bit per memorizzare i dati.

Generalmente CRC-16 fa parte dei programmi hardware (ROM) ed è usato per verificare gli errori a livello di trasmissione.

INDICE

1. Introduzione
2. Panoramica su Tripwire
3. Utilizzo di Tripwire
4. Installazione e personalizzazione
5. Inizializzazione del Database
6. Controllo d'integrità
7. Analisi dei report
8. Aggiornamento del database e del policy file
9. Comandi usati da Tripwire
10. Algoritmi utilizzati
11. File & Directory usate da Tripwire 
12. Bibliografia

File & Directory/1

```
/usr
  /sbin
    tripwire      eseguibili
    twadmin
    twprint
    siggen
  /share
    /man          manuali
```


File & Directory/2

```
/etc
  /tripwire
    install.sh    script d'installazione
    tw.cfg        file di configurazione
    twcfg.txt     " in chiaro
    tw.pol        policy file
    twpol.txt     " in chiaro
    site.key      chiavi
    $(HOSTNAME)-local.key
```

File & Directory/3

```
/var
  /lib
    /tripwire
      $(HOSTNAME).twd    database
    /report
      host_name-data-ora.twr report
```

INDICE

1. Introduzione
2. Panoramica su Tripwire
3. Utilizzo di Tripwire
4. Installazione e personalizzazione
5. Inizializzazione del Database
6. Controllo d'integrità
7. Analisi dei report
8. Aggiornamento del database e del policy file
9. Comandi usati da Tripwire
10. Algoritmi utilizzati
11. File & Directory usate da Tripwire
12. Bibliografia 

Siti per il download

www.tripwire.org versione freeware di tripwire
www.tripwire.com versione commerciale di Tripwire
www.tripwiresecurity.com versione commerciale di Tripwire

Manuali e libri

1. Tripwire Security Systems, Inc.; Tripwire for Unix User's Guide.
2. Gene H. Kim and Eugene H. Spafford.
The design and implementation of Tripwire: A file system integrity checker.
Technical Report CSD-TR-93-071, Purdue University, Novembre 1993.
3. Gene H. Kim and Eugene H. Spafford.
Experiences with Tripwire: using integrity checkers for intrusion detection. In *Systems Administration, Networking and Security Conference III*. The USENIX Association, Aprile 1994.