TPM, chi e' costui?

Emanuele Zamprogno
aka Pinguozz

[pinguozz@netsons.org]

TPM, chi e' costui?

- Il TPM o Trusted Platform Modules e' un integrato e che voi lo sappiate o no, e' un requisito per essere Windows Vista Ready

Ma voi vi domanderete.....

Perche'?

TPM, chi e' costui?

Il TPM e' un chip di crittografia in hardware la cui funzione ufficiale e' generare chiavi di autenticazione per i file che un utente produce.....

Unico Problema....

Lui autentifica anche il programma e il sistema in cui questi file vengono prodotti.

TPM, chi e' costui?

Diciamo di piu'....

Una scheda di crittografia in hardware costa parecchi marenghi....

Improvissamente invece iniziano a regalarmene come nocciole in tutti i pc che compro.....uhmm...

Perche'?

TPM, chi e' costui?

Il tpm e' quindi un chip integrato in tutte le nuove schede madri di tutti i pc e laptop che vengono venduti e integrandosi con il sistema operativo mette a disposizione una serie di funzioni di crittografia e autenticazione avanzate.

Esso pero' nel caso che il sistema operativo sia Window Vista con il Driver a lui dedicato, che prende il piacevole nome di Nexus, inizia a tenere sotto controllo tutti i programmi che vengono eseguiti, impedendo a tutti quelli che Windows riterra' pericolosi di essere eseguiti.

Questa protezione non e' un software che poi potra' essere craccato, il tpm impedisce a livello fisico che il programma venga eseguito e che possa produrre file di alcun tipo.

TPM, chi e' costui?

Ma perche' non fare qualche esempio pratico ???

Se la autenticazione per l'esecuzione dei programmi venisse data da una joint venture delle principali marche del settore informatico secondo voi l'autenticazione per la sicurezza in ambiente Windows Vista sarebbe proponibile:

- A programmi di peer to peer come **Emule**??
- A programmi per lo scaricamento di **mp3**?? (tranne forse **itunes**?)

Se poi l'autenticazione fosse conseguita dopo pagamento di costose royalties progetti come:

- ***Firefox o Thunderbird***
- ***Openoffice.org***

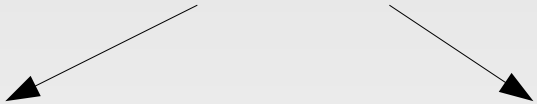
potrebbero permetterselo?????

TPM, chi e' costui?

Sotto Vista abbiamo capito che non ci resta che piangere.....

PERCIO'

Iniziamo a pensare delle alternative....



Mac OS X ????

Peggio che andare di notte, dato che il tpm lo ha inserito oltre che nei suoi macbook e prevede di metterne una versione dedicata nei nuovi ipod video

GNU/Linux o altri sistemi liberi????

Diciamo che s'inizia a ragionare

TPM, chi e' costui?

Come va la storia con il pinguino???

il modello open permette di sfruttare in maniera interessante questa tecnologia messa a disposizione.

In Linux e' implemetata la compatibilita' con i chip di tipo tpm e grazie ad un progetto di ***IBM*** e' disponibile una libreria per la gestione dell'integrato, con la possibilita' di usare le capacita' crittografiche del integrato per crittare in real time parti del sistema od interi filesystem

Particolarmente rispetto a quest'utlimo punto e' il progetto **encryptfs** che prevede di essere inserito nella mainstream del kernel entro la versione 2.6.20 e ha al suo interno gia' dei toolkit completi per l'uso in ambito produttivon

TPM, chi e' costui?

Concludendo: sto' chippone e' il male oppure no?

La risposta e' ..... **NI!!!**

La sicurezza non viene mai garantita da un componente hardware, ma dall'attenzione e dal buon senso degli utenti di un sistema.....Insieme ovviamente ad un sistema che sia stato fatto con buon senso e qui non c'e' il dubbio

che i sistemi liberi siano una VERA garanzia!!!

TPM, chi e' costui?

Grazie a tutti per l'attenzione

e

Buona Serata a tutti!