Relazione mini challenge

BIOS, UEFI e Full Disk Encryption

Marco Lo Bello
100016159
DIPARTIMENTO DI MATEMATICA INFORMATICA
UNICT

Obiettivo della mini challenge

Lo scopo della mini challenge era quello di documentarci sugli aspetti di sicurezza del BIOS e del UEFI, in particolare rispondendo alle seguenti domande:

- Cosa sono BIOS e UEFI?
- Quali sono le differenze tra BIOS e UEFI?
- A cosa servono le password del BIOS e del UEFI?
- Queste password si possono aggirare?
- Cos'è il TPM?
- Cos'è la full disk encryption?
- Quante password occorrono per rendere sicura una macchina?

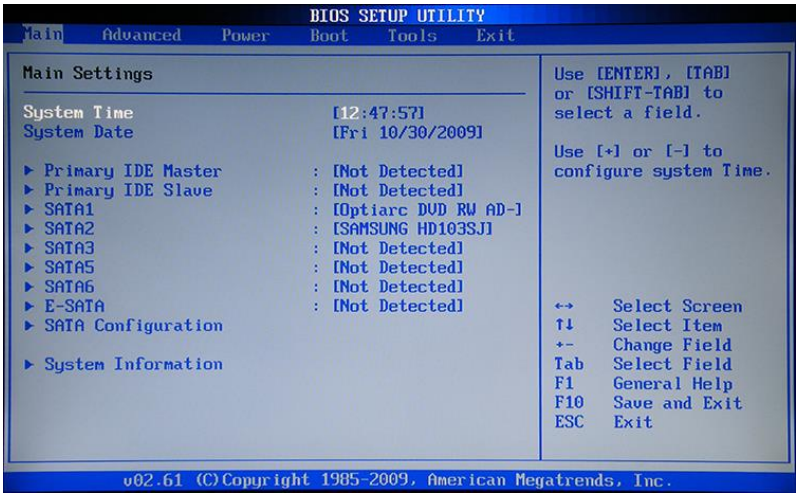
Svolgimento

Cos'è il BIOS?

Il BIOS è un programma che viene eseguito all'avvio di una macchina e il suo compito è quello innanzitutto di fare un controllo delle periferiche del computer e riportare eventuali malfunzionamenti. Successivamente il suo compito è quello di caricare il sistema operativo per poterlo utilizzare.

Noi possiamo accedere al BIOS e una volta entranti nel menù, ci accorgiamo che sono presenti diverse funzioni. In particolare, ci accorgiamo che possiamo:

- Modificare alcune informazioni come la data e l'ora
- Visualizzare informazioni riguardo i componenti
- Cambiare la periferica di avvio, ovvero scegliere da quale dispositivo prendere il sistema operativo da caricare.
- Impostare una password utente e una password amministratore
- Modificare alcune prestazioni dei componenti come CPU, RAM, ecc.



Cos’è il UEFI e quali sono le differenze con il BIOS?

UEFI è l’evoluzione del BIOS, il compito per tanto è lo stesso e di conseguenza si possono svolgere le stesse operazioni del BIOS. Ma oltre alle operazioni del BIOS possiede delle differenze soprattutto nell’ambito della sicurezza. Le principali differenze del UEFI sono:

- Possiede un’interfaccia grafica che lo rende più intuitivo e più facile da usare
- Supporta l’avvio su dischi rigidi con capienza maggiore di 2 TB
- Supporta le funzionalità di rete
- Supporta il secure boot (avvio sicuro)

Il secure boot è un’importante aggiunta per quanto riguarda la sicurezza, perché il suo compito è quello di evitare che venga caricato un software malevolo all’avvio del PC.

Scenario d’esempio: Un attaccante che trova una macchina incustodita potrebbe tranquillamente entrare nel menù del BIOS se necessario modificare il boot order delle periferiche e far sì che riavviando il pc venga eseguito del software malevolo caricato in una chiavetta. Questo fortunatamente non sarebbe possibile se la macchina fosse dotata di secure boot perché andrebbe a controllare la “firma” del software e successivamente decidere se far partire il programma oppure no.

A cosa servono le password del BIOS e del UEFI?

Normalmente per accedere al BIOS non è richiesta nessuna password, però all'interno del menù del BIOS è possibile impostare una password utente e una password amministratore.

Queste password servono a proteggere l'accesso al BIOS, come abbiamo visto nell'esempio precedente chiunque potrebbe facilmente entrare nel BIOS e modificare per esempio il boot order in modo tale da far partire del SW malevolo, quello che non è stato detto prima è che dal UEFI si può disattivare il secure boot. Quindi l'attaccante non solo cambierà il boot order ma disattiverà il secure boot facendo partire sicuramente il software malevolo.

Di conseguenza l'utilizzo di queste password è indispensabile per limitare accessi non autorizzati al BIOS.

- Password utente: se si accede con questa password al BIOS, le funzionalità saranno veramente ridotte di fatto non si potrà fare nulla se non guardare le informazioni della macchina e modificare la data e l'ora.
- Password amministratore: se si accede con questa password invece sarà possibile utilizzare tutte le funzionalità del BIOS.

Queste password si possono aggirare?

Esistono delle tecniche per aggirare le password del BIOS, il primo metodo che però funziona con computer molto vecchi è quello di rimuovere la batteria CMOS in modo tale da resettare le impostazioni a quelle di default e quindi eliminare la password. Ma ormai questa tecnica è obsoleta perché con le nuove architetture è difficile rimuovere queste batterie perché saldate.

Un altro metodo un po' più efficiente ma su vecchie versioni di BIOS è quello dell'utilizzo delle master password, non sono altro che password impostate dal produttore della scheda madre che permettono di resettare la password e quindi di poter accedere al BIOS. Generalmente quando si prova ad inserire una password dopo tre tentativi errati viene generato un codice di errore e grazie a questo è possibile risalire alla master password.

Per quanto riguarda il UEFI apparentemente non sembra esserci un modo immediato per aggirare le password.

Cos’è il TPM?

Il TPM (Trusted Platform Module) è un chip che le macchine moderne possiedono e si trova montato sulla scheda madre. Il suo compito è quello di aumentare la sicurezza della macchina perché genera una chiave cifrata mediante l’algoritmo RSA e ogni volta che viene eseguito un programma il TPM effettua un controllo per vedere se quel SW è autorizzato a compiere determinate operazioni. Inoltre, tutte le operazioni vengono effettuate dentro il TPM questo evita che i dati possano finire in RAM o salvate nell’HDD e che quindi possano essere reperiti in altro modo. Un altro vantaggio del TPM è quello di riconoscere lo stato della macchina, questo vuol dire che se qualcuno dovesse smontare il TPM e montarlo su un’altra macchina questo comunque non funzionerà e quindi non permetterà di risalire alle chiavi.

Cos’è la full disk encryption?

Utilizzare le password per accedere al UEFI è una buona misura di sicurezza ma può essere l’unica? La risposta è no.

Le password evitano che qualcuno possa accedere al BIOS e di conseguenza al pc, ma cosa succede se qualcuno smontasse l’hard disk e lo montasse in un altro computer? In quel caso si avrebbe accesso a tutti i dati perché dal secondo pc si potrebbe vedere il contenuto dell’intero hard disk.

Per evitare che questo accada bisogna utilizzare la full disk encryption, consiste nell’utilizzare dei software specifici che vanno a criptare gli hard disk in modo tale che sia possibile accedervi solo dopo aver inserito una password, così facendo solo il vero proprietario di quell’hard disk può accedere ai dati anche se viene montato su un altro PC.

Quante password occorrono per rendere sicura una macchina?

Questo ci porta a chiederci quindi il numero di password necessarie per rendere sicura una macchina, in particolare uno spazio utente. Per i ragionamenti fatti emerge che dovrebbero essere impostate almeno tre password per rendere la macchina sicura.

Le tre password che vanno sicuramente impostate sono:

1. Password Amministratore: è la password del BIOS che permette di accedere alle funzioni critiche come il boot order e il secure boot
2. Password Utente: è la password che viene richiesta quando il sistema operativo si avvia, molto semplicemente serve ad evitare che chiunque possa sbloccare la macchina
3. Password della FDE: è la password che bisogna usare per "montare" l'hard disk e far sì che si possano utilizzare l'hard disk.

Conclusioni

Per concludere posso dire che la mini challenge si è rilevata molto utile, dandomi modo di conoscere questi aspetti di sicurezza ma più precisamente di sapere cosa si rischia nel caso in cui queste protezioni non vengano utilizzate.