Dark side of XBOX

Giuseppe Augiero

Disclaimer

- Ogni marchio appartiene al rispettivo proprietario.
- Le prove effettuate sono da ritenersi da “Laboratorio”, qualsiasi test effettuato potrebbe danneggiare irreparabilmente la console.
- L’apertura della Xbox annulla la garanzia ufficiale.
- Lo scopo delle slide e’ puramente didattico.

Xbox

- Console giochi di Microsoft.
- Prestazioni superiori rispetto alle altre console grazie alla sua potenza di calcolo.
- All'interno della Xbox troviamo un comune Pc x86.
- Costo 99 euro.

Xbox Hardware: CPU

- Pentium III Celeron (core Coppermine) - 0.18 µ
- 128 kb di cache di L2
- Architettura 32 bit
- FSB a 133 Mhz
- Non è supportato il set di istruzioni SSE2
- Saldato direttamente su scheda madre

Xbox Hardware: GPU

- Derivato dal chipset nForce 420-D
- Nella versione per pc l'IGP ha il core di una GeForce2 MX, qui è presente una versione custom
- Si tratta di una “specie” di GeForce3, con qualche piccola miglioria
- È da considerarsi il North Bridge del sistema

Xbox Hardware: Memorie

- Ram: 64 Mb (sdram 133 Mhz) upgradabile.
- HDD: 8 Gb o 10 Gb.
- DVD-Rom Drive (Philips, Thomson, Samsung)

- I lettori Dvd non leggono tutti i formati e tipi di cdrom/dvdrom

Xbox Hardware

- Supporto Dolby Digital 5.1
- Scheda di rete 10/ 100
- 4 porte USB mascherate da porte proprietarie.

Software

- Il sistema operativo utilizzato e' una versione "modificata" di Windows 2000.
- Il file system adoperato dalla Xbox e' Xfat.
- Il Bios e' stato scritto direttamente da Microsoft.
- La Dashboard (interfaccia grafica) e' proprietaria.
- Librerie XDK.

Software

- **E’ impossibile eseguire codice non Microsoft.**

Protezioni

- Il kernel è cifrato (la chiave è simmetrica e contenuta nel boot loader).
- All'avvio il BIOS deve rispondere ad un challenge del controllore di interruzione (PIC), pena il reset della CPU.
- Il boot loader calcola e verifica un hash dell'immagine del kernel e di altri dati prima di avviarlo.
- Le applicazioni sono firmate digitalmente (RSA con chiave a 2048 bit) e non vengono eseguite dal kernel se la verifica fallisce.

Trusted Computing

- Xbox utilizza sistemi di trusted computing.
- La console rappresenta una prima soluzione “non completa” del progetto Palladium.
- E’ possibile regolamentare la fruizione di contenuti multimediali (DRM).
- La modifica o disabilitazione di sistemi TC portano alla perdita delle funzionalità e dei contenuti fidati.

Debolezza

- Il modello di protezione di XBox è a stadi.
- Ogni stadio verifica il successivo. Se questo è integro e fidato, lo esegue.
- **Su XBox il *primo* stadio è debole**.
- Anche se possono essere eseguite solo applicazioni certificate, eventuali vulnerabilità di queste permettono di prendere il controllo del sistema anche quando questo è in stato “fidato”.

Installare Linux

Hardware o software ?

- Per installare Linux su una Xbox occorre effettuare una modifica Hw o Sw alla console.

- L'apertura della console per la modifica hardware annulla la garanzia ufficiale.
- Richiede minime conoscenze di elettronica e una attrezzatura tecnica per effettuare l'installazione del chip.
- In alcuni casi la modifica è irreversibile.
- Consente la sostituzione dell'hw.

Modifica software

Pro:

- Non si deve aprire la console.
- È reversibile.
- Non richiede conoscenze specifiche (saldatura,...).
- Consente il Dual-Boot.

Contro:

- Non consente la sostituzione dell'hardware.
- Alcune distro non possono essere installate.
- Alcuni fastidiosi bug (es: “*the clock loop*”).

Due metodi software

007/Mech Assault save game exploit:

- Usando un save game costruito ad-hoc è possibile caricare linux. Per avviarlo si deve lanciare il gioco e caricare il save game, nel frattempo il cd deve restare nel lettore.

Dashboard exploit:

- Si sfutta ancora il bug di 007/Mech Assault per modificare la dashboard. In questo modo non è più necessario il cd del gioco.

Xebian

- Bootare usando il cd della Xebian
- Lanciare la procedura di installazione:
- Segliere la partizione in cui installare linux, scelta tra “*Game Partition*” e “*Unused Space*”
- Dare le dimensioni della Swap (256 Mb)
- Avere un po' di pazienza (la procedura dura circa 4~5 minuti)
- Configurare le opzioni di rete: IP, gateway
- Riavviare.

Utilizzi

E’ possibile utilizzare la console come:

- un vero e proprio personal computer, con tutte le funzionalità di un vero pc di casa.
- una stazione multimediale, un grande jukebox collegato alla tua televisione o al tuo home theater per vedere film e ascoltare musica.
- un piccolo server di qualunque tipo (http,ftp,smb,nfs etc).
- un router / firewall / gateway.

Cluster

E’ possibile collegare fino a quattro Xbox in modo da creare un cluster Open Mosix.

Fate attenzione!

- Non e’ possibile eseguire codice non Microsoft se:
- La versione della console e’ 1.6
- Avete usufruito dei servizi di Xbox-Live.

Domande?

Per ulteriori informazioni:

Giuseppe Augiero –
giuseppe@augiero.it