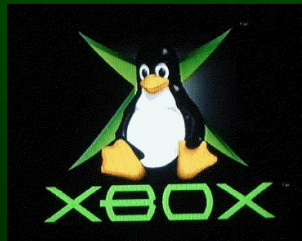


GNU/Linux su XBox

Gianni Bianchini

`giannibi@firenze.linux.it`



Linux Day 04
Siena, Novembre 2004

©2004 Gianni Bianchini

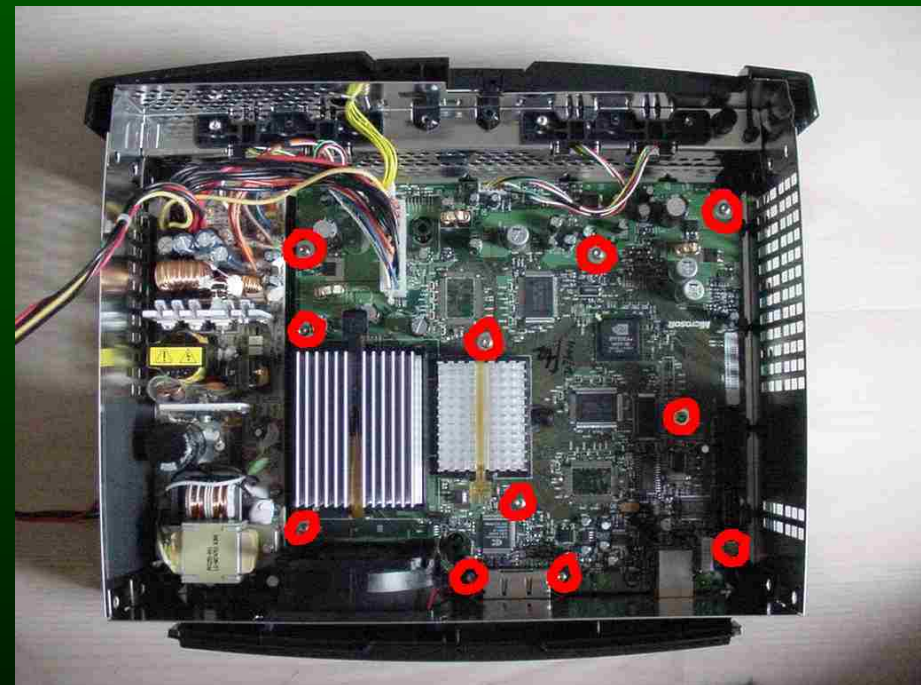
Sono consentite la copia e la redistribuzione in forma integrale di questo documento a condizione che questa nota sia preservata
Per ottenere la versione con sorgenti L^AT_EX sotto licenza libera contattare l'autore.

Sommario

- (X)Scatola chiusa? No, grazie!
 - ★ XBox: Hardware
 - ★ XBox: Software
- Di chi è il mio computer (o la mia console)?
 - ★ Meccanismi di protezione
 - ★ XBox e trusted computing
- Uscire dalla gabbia
- Il progetto XBox-Linux
- Alcuni impieghi creativi

(X)Scatola chiusa? No, grazie!

- Microsoft(R) Xbox è un comune PC *legacy-free*, salvo alcuni (abili?) accorgimenti per mascherare l'hardware da console per videogiochi ed impedire l'esecuzione di software non approvato



- Xbox costa circa la metà di un PC di fascia bassa

XBox: Hardware

- CPU: Intel Celeron(R) 733 MHz
- RAM: 64Mb DDR
- Motherboard/chipset: nVidia nForce-like
 - ★ Audio
 - ★ Controller IDE
 - ★ Controller USB OHCI
 - ★ Controller Ethernet 10/100
- Controller video: Geforce3 con encoder TV
- IDE HDD 8/10 Gb, DVD-ROM
- Mancano porte seriali, parallela, floppy, PS/2 (*legacy-free*)
- Porte USB mascherate da connettori proprietari per joypad

XBox: Software

- BIOS: Microsoft proprietario su flash ROM
- Sistema operativo: versione ridotta ed adattata del kernel di Microsoft Windows 2000 (su flash ROM)
- Interfaccia grafica proprietaria (Dashboard)
- Librerie di programmazione (XDK)
 - ★ Proprietarie e non ufficialmente disponibili

XBox: Sistemi di protezione

- Il codice di inizializzazione della macchina è cablato all'interno del chip di gestione I/O (MCPX), non nella flash ROM che ha un codice di boot fasullo
 - ★ Il codice di boot ricerca una stringa (1.0), o effettua un hash (1.1) della ROM prima di eseguirne il codice (caricatore del sistema operativo) per controllare che sia originale
- 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
- Il kernel è cifrato (la chiave è simmetrica e contenuta nel boot loader)
- Le applicazioni sono firmate digitalmente (RSA con chiave a 2048 bit (!)) e non vengono eseguite dal kernel se la verifica fallisce

XBox e trusted computing: di chi è il mio computer (o la mia console)?

- Xbox impiega tecniche simili a quelle presenti nelle piattaforme di *trusted computing*
 1. Verifica all'avvio, mediante metodi crittografici realizzati in hardware, della fidezza del sistema
 2. Esecuzione sul sistema fidato di software operativo che realizza funzioni di autenticazione in accordo con una data politica
- Regolamentazione della fruizione di contenuti multimediali (DRM)
- Esecuzione di solo software certificato e con modalità preifssate
- I sistemi di TC non sono concepiti per resistere alla disabilitazione, anzi la consentono (con perdita delle funzionalità e dei contenuti fidati). La Xbox forse lo era.

XBox: sicurezza

- 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
 - ★ Rilevazione della stringa di autenticazione in ROM letta dal MCPX, mediante sniffing del bus interno (1.0)
 - ★ Modifica del boot loader senza alterare l'hash della ROM per debolezza dell'algoritmo usato (1.1)
- 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"

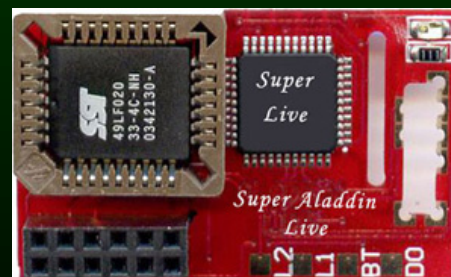
Uscire dalla gabbia: exploit software

- Una volta che il BIOS ed il kernel sono partiti ed eventuali applicazioni sono state autenticate, se queste offrono la possibilità di deviare il flusso della loro esecuzione, abbiamo in mano la macchina : –)
- Alcuni giochi (ad es. *MechAssault*), grazie a bug di tipo *buffer overflow*, permettono di eseguire codice arbitrario memorizzato in un file di salvataggio della partita (*savegame*)
- È sufficiente copiare e caricare un *savegame* forgiato per effettuare il boot del kernel linux. Poi, è possibile modificare il comportamento della Dashboard per avviare linux da HDD mediante exploit analogo (font exploit)
- **Attenzione!** Il servizio XBox-live di Microsoft aggiorna senza permesso il software di sistema per evitare gli exploit e cancella eventuali file “impropri”
 - ★ Questo “aggiornamento” è illegale (almeno nella UE) poiché la XBox è un prodotto, non alterabile senza il consenso del proprietario, ed un sistema a cui non è consentito accedere abusivamente

Uscire dalla gabbia: sostituzione del BIOS

Rimpiazzo del BIOS originale con uno alternativo che permetta l'avvio del kernel linux e la modifica dell'hardware (HDD, DVD-ROM, ecc.)

- Riprogrammazione della flash memory interna
 1. Abilitazione della scrittura della flash mediante ponte di saldatura
 2. Installazione ed avvio del programma di flashing da linux mediante exploit software
- ★ Le Xbox recenti (versione 1.6) non sono riprogrammabili
- Installazione di un mod-chip riprogrammabile contenente un BIOS alternativo



Uscire dalla gabbia: sostituzione del BIOS

- Alcuni BIOS, che contengono codice Microsoft XDK senza licenza, consentono di effettuare copie di programmi originali ed eseguire codice non firmato o di importazione
 - ★ La legalità di questi BIOS è dubbia.
Oltre alla violazione del diritto d'autore su XDK, direttive quali la EUCD (UE) o il DMCA (USA) proibiscono l'uso di misure di aggiramento di protezioni a tutela di materiale protetto da diritto d'autore, indipendentemente dall'effettiva violazione
- Cromwell BIOS. È libero, non contiene codice Microsoft XDK, permette l'avvio del kernel linux ma non l'esecuzione di copie di programmi
 - ★ L'installazione e l'uso di Cromwell sono perfettamente legali

Il progetto XBox-Linux

- Cromwell BIOS
- Drivers per il kernel linux
- Distribuzioni ad-hoc
 - ★ Xebian (Ed's Debian)
 - ★ GentooX
- Utilities
 - ★ Raincoat BIOS flashing utility
 - ★ Mechinstaller
- Documentazione



<http://www.xbox-linux.org>

Alcuni impieghi creativi

- PC desktop, con tastiera e mouse USB. Piccolo, silenzioso, consuma poco
- Lettore di contenuti multimediali (Freevo).
- Router-firewall, condivisione della connessione a Internet, gateway VPN
- Server di rete / web / posta



Alcuni impieghi creativi

- Cluster!



- Appliance dedicato
- Impiego di user-mode linux e loopback devices sui filesystem nativi

Un esempio: il progetto PBox (Privacy Box)

- Creazione di un appliance basato su hardware XBox per applicazioni di tutela della privacy in rete
- Proxy per navigazione sicura / anonima
- Nodo di sistemi di remailing Mixminion e Mixmaster
- Nodo Freenet
- Nodo di reti a bassa latenza (Tor)
- Sistema di storage cifrato

Fine

Grazie per l'attenzione!

/giannibi

Riferimenti

- Xbox Linux Project,
<http://www.xbox-linux.org>
- Xbox Scene,
<http://www.xbox-scene.org>
- Bunnie's adventures hacking the Xbox,
<http://www.xenatera.com/bunnie/proj/anatak/xboxmod.htm>
- Xbox Debian (Ita),
<http://www.xboxdebian.org>
- Progetto Winston Smith,
<http://www.winstonsmith.info>