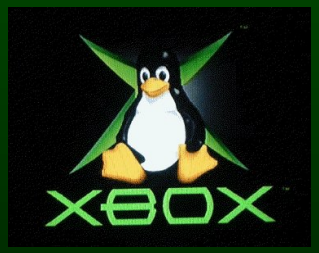
Il progetto PBox
“Vogliamo scatole, non programmi”

Gianni Bianchini
giannibi@firenze.linux.it



E-Privacy 2005
Firenze, 27-28 Maggio 2005

©2005 Gianni Bianchini
Sono consentiti l’uso, la copia, la modifica e la redistribuzione di questo documento nei termini della GNU General Public License (http://www.gnu.org/licenses/gpl.html). Per ottenere i sorgenti modificabili LaTeXcontattare l’autore.

Sommario

- Perché una Privacy-Box
- Il progetto PBox del PWS
- Da XBox a PBox
  - (X)Scatola chiusa? No, grazie!
  - XBox: prove generali di trusted computing
  - Uscire dalla gabbia
- La PBox tipo I: pan per focaccia al Grande Fratello
  - Software
  - Servizi generici
  - Servizi per la e-privacy
- L'evoluzione: PBox tipo II e tipo III

Perché una Privacy-Box

- In rete, in assenza di opportuni accorgimenti, non c'è privacy
- Gli strumenti di tutela della riservatezza esistono
  - ⋆ Tecniche per la navigazione web sicura, riservata, anonima
  - ⋆ Reti di pubblicazione anonima (Freenet)
  - ⋆ Anonymous remailer
- Questi sistemi, oltre che poco conosciuti, spesso non sono alla portata dell'utente medio della rete anche nella loro semplice fruizione
- Nel caso della PBox modello I, lo ammettiamo, c'è anche l'incontenibile piacere di riconvertire ad uno scopo un dispositivo concepito per realizzare essenzialmente lo scopo contrario, ma questo è un problema diverso e che fortunatamente riguarda un insieme piuttosto ristretto di individui : -)

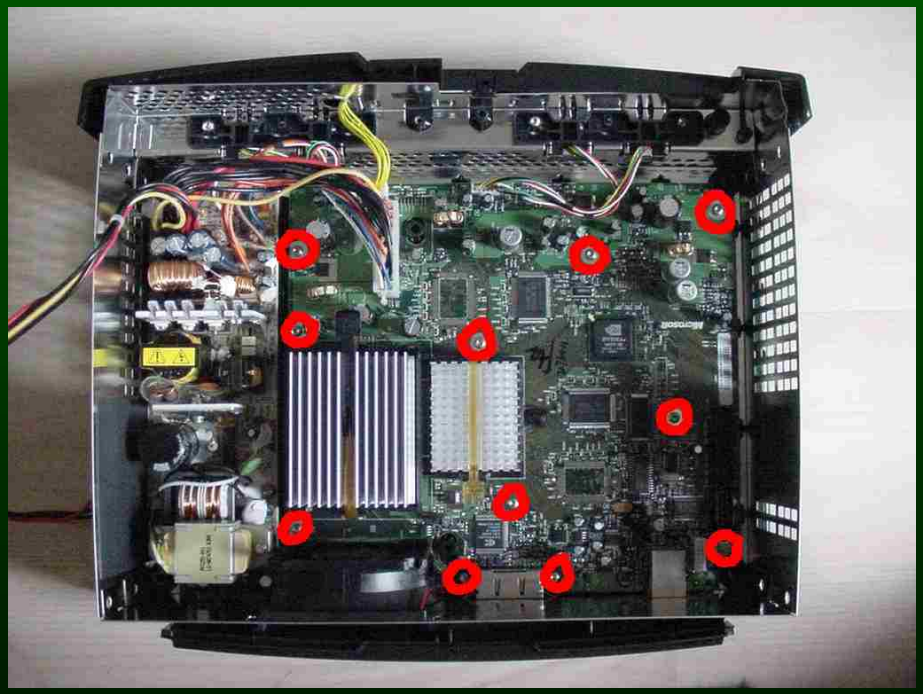
Il progetto PBox

- Realizzazione di appliance per comunicazione riservata ed anonima in rete
- Produzione di documentazione
- Realizzazione di distribuzioni GNU/Linux privacy-oriented
- Supporto
- Creazione di gruppi di discussione

- Scatole sì, ma...
  - ⋆ È comunque fondamentale una corretta educazione ai problemi legati alla privacy

(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 meno della 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: Proprietario Microsoft(R) su flash ROM
- Sistema operativo: versione ridotta ed adattata del kernel di Microsoft Windows(TM) 2000 (su flash ROM)
- Interfaccia grafica proprietaria (Dashboard)
- Librerie di programmazione (XDK)
  - ⋆ Proprietarie e non ufficialmente disponibili

XBox: prove generali di trusted computing

- XBox impiega tecniche simili a quelle presenti nelle piattaforme di *trusted computing*

  1. Verifica all'avvio, mediante metodi crittografici realizzati in hardware, della fidatezza 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: prove generali di trusted computing

- 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: prove generali di trusted computing

- 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 possono permettere 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, 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 avviare il kernel linux. Poi, è possibile modificare il comportamento della Dashboard per avviare linux da HDD mediante exploit analogo (font exploit)
- Il servizio XBox-live aggiorna senza avviso il software di sistema per evitare gli exploit, esamina il disco e cancella eventuali file “impropri”
  - ⋆ Questo “aggiornamento”, oltre a violare la privacy dell’utente, si configura come illegale (almeno nella UE): la XBox è un prodotto, non alterabile senza il consenso del proprietario, nonché un sistema informatico 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
- Installazione di un mod-chip riprogrammabile conenente un BIOS alternativo
- Cromwell BIOS. È libero, non contiene codice Microsoft XDK, permette l'avvio del kernel linux ma non l'esecuzione di copie di programmi

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

PBox tipo I

- La scoperta dell'acqua calda: con la X-Box si può realizzare un sistema GNU/Linux con un gran numero di funzionalità
  - ⋆ Compatto, silenzioso, consuma poco
- Sistema GNU/Linux, distribuzione Xebian
- Macchine virtuali User Mode Linux (UML) e loopback devices
  - ⋆ Isolamento dei servizi critici
  - ⋆ Non si altera la struttura originale del disco
- Servizi generici
  - ⋆ Mantenimento e condivisione in rete locale della connessione a Internet con modem USB o ethernet
  - ⋆ Router-firewall, gateway VPN
  - ⋆ Piccolo server di rete (WWW, posta elettronica)

PBox tipo I: servizi per la privacy

- Nodo di reti di anonymous remailing
  - Mixmaster
  - Mixminion
- Pseudonym server
- Nodo di reti anonime a bassa latenza
  - Tor
- Proxy per navigazione sicura / anonima
  - Privoxy + Tor
- PBox anywhere(TM)
  - Accesso da qualunque nodo Internet mediante tunnel OpenVPN
  - Gateway HTTP/SSL verso i servizi

Eccola!

PBox tipo II

- PC embedded Soekris 4501
  - CPU AMD Elan
  - 64 Mb RAM
  - Compact Flash 512 Mb
  - Seriale
  - 3 Ethernet
  - No HDD

- Fornisce i servizi del tipo I

PBox tipo III

- Caratteristiche simili a PBox II, più
  - HDD 2.5”
  - Access point Wi-Fi
- Fornisce i servizi dei tipi I e II, più
  - Nodo Freenet
  - Servizi wireless
  - File server

Il progetto PBox

http://www.winstonsmith.info/pbox/index.html

- Realizzazione di appliance per comunicazione riservata ed anonima in rete
- Produzione di documentazione
- Realizzazione di distribuzioni GNU/Linux privacy-oriented
- Mailing list di discussione

https://lists.firenze.linux.it/mailman/listinfo/p-box

- “Help desk”

pbox-info@winstonsmith.info

- Forum

Il progetto PBox

- Niente di particolarmente complicato: si tratta di assemblare tecnologie note, seppure innovative
- Ciò che abbiamo presentato è in larga parte ancora da realizzare

⇓

Collaborate!

Fine

Grazie per l’attenzione!

/giannibi

Riferimenti

- Il Progetto PBox,
  http://www.winstonsmith.info/pbox/index.html
- Progetto Winston Smith,
  http://www.winstonsmith.info
- 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