La storia del DRM

Un viaggio nel passato delle tecnologie anti-pirateria

Leonardo 'scudo' Rossi
Pietro 'neonsn0w' Prase

End Summer Camp 21, 6 settembre 2025

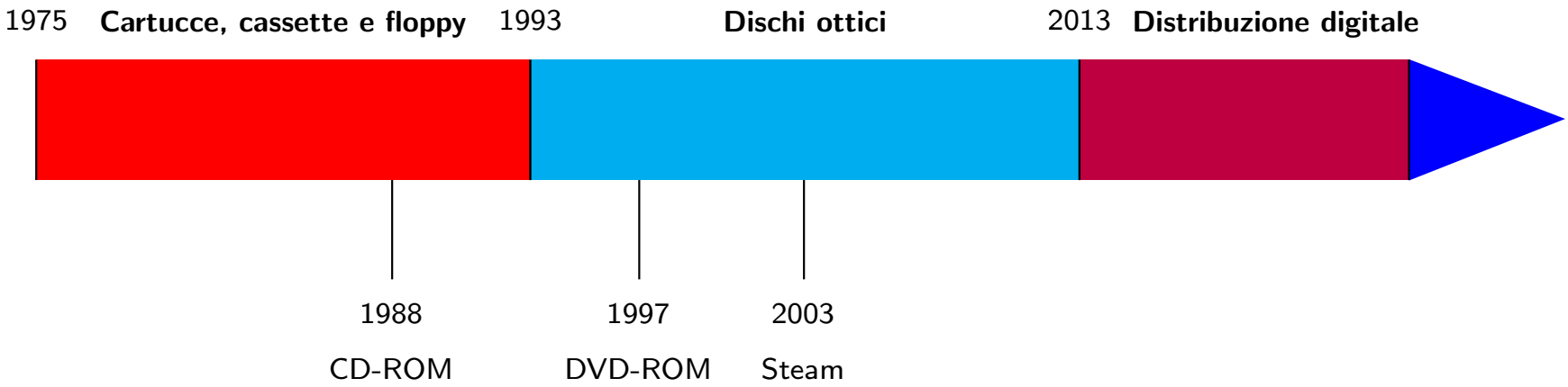
Introduzione

Digital Rights Management:

- Set di tecnologie hardware e software
- Impedire o rilevare copia non autorizzata di informazioni (software, musica, film...)
- Tratteremo solo il software

Timeline

Periodi di dominanza dei vari canali di distribuzione del software:



Cartucce

Caratteristiche:

- Comuni fra le console (ma presenti su alcuni computer)
- Memoria ROM o flash
- Possibilità di aggiungere hardware specializzato (es. CIC)
- Iniziale importanza di fermare software non approvato

Cartucce

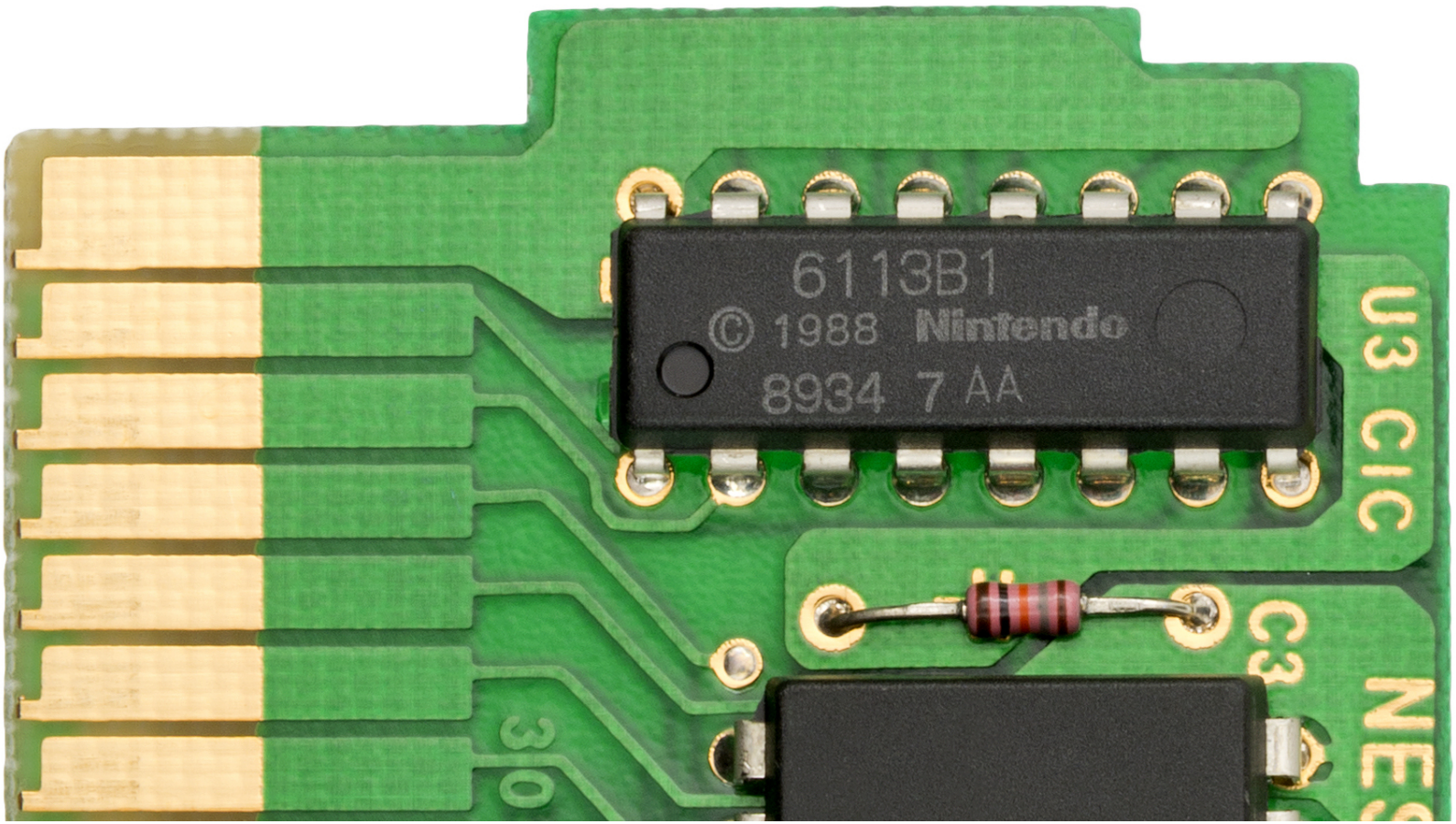
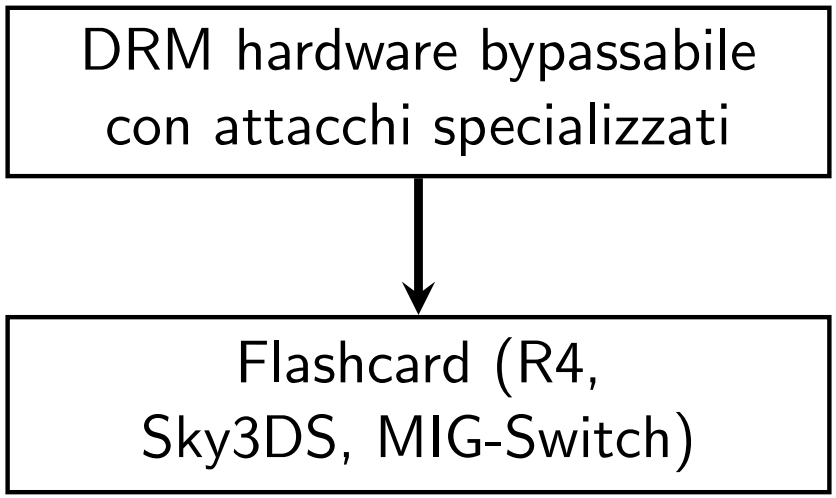


Figura: Un chip CIC usato nel Nintendo Entertainment System.

Cartucce

Problemi delle cartucce:



- Meglio usare tecniche crittografiche (firmare e criptare il software)
- Formato generalmente in disuso (alti costi di produzione)

Floppy disk

Caratteristiche:

- Comuni nei computer (ma presenti su alcune console)
- Disco magnetizzato rotante
- Inizialmente più formati, che convergono $\rightarrow$ rampante pirateria

Floppy disk

È possibile identificare alcune tecniche comuni:

- Settori allocati in modo non standard (rimappati)
- Disco formattato in modo non standard (custom fs: più dati)
- Uso di *fuzzy bits* (informazioni magnetiche con stato non definito)

In genere si cercano caratteristiche che può avere solo un floppy originale.

Altri tipi di protezione

Altre tecniche meno comuni cadute in disuso sono:

- *Codewheel*
- Protezioni basate sul manuale (ricerca di parole)
- *Dongle* di vario tipo

Quindi oggetti fisici venduti assieme al gioco.

Altri tipi di protezione

Figura: Un *codewheel*.

Optical media good

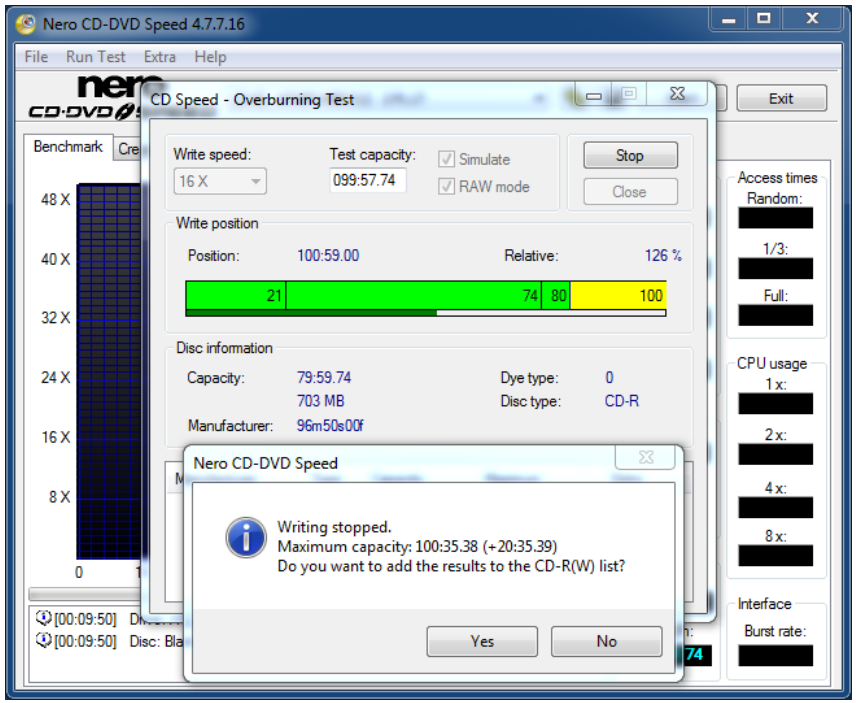
Nei primi anni del CD-ROM, **non si pose il problema della copia pirata**.

- I masterizzatori erano ancora molto costosi (>20.000$!)
- Tecniche anti-copia rudimentali:
  - Fake TOC (Table of Contents)
  - CD-ROM più capienti del normale

CD-ROM più capienti

CD "pressati" con capacità più ampia di un CD-R → impedire la copia.
Approccio fallato:

- Spesso c'era molto "filler" rimovibile
- **Overburning**



SecuROM

SecuROM era uno dei primi DRM sofisticati per CD

- Creato da **Sony**
- **Chiave univoca** per ogni CD, non copiabile da un drive
- **Parti dell'eseguibile criptate**, decriptate all'esecuzione con la chiave univoca e un driver kernel
- **Il disco doveva essere nel PC per eseguire il software**

SecuNOT

SecuROM fallì nel suo intento:

- Era possibile **leggere l'eseguibile decriptato** con un debugger
- Nacquero le crack "*NoCD*"

In compenso, **anche chi possedeva la copia originale del disco riscontrava problemi...**

- A volte il disco non veniva rilevato
- Problemi su Windows Vista
- SecuROM **non funzionava** con certi drive

SecuROM + Attivazione Online

Con l'uscita di Spore, EA aggiunse a SecuROM un sistema di **attivazione online**. Questo approccio era **un inferno**:

- Connessione a internet obbligatoria
- Numero di attivazioni limitato
- Ogni modifica hardware rendeva necessaria un'ulteriore attivazione

EA fu costretta a rimuovere SecuROM da Spore in seguito ad un'azione legale

Figura: Spore (2008)

StarForce

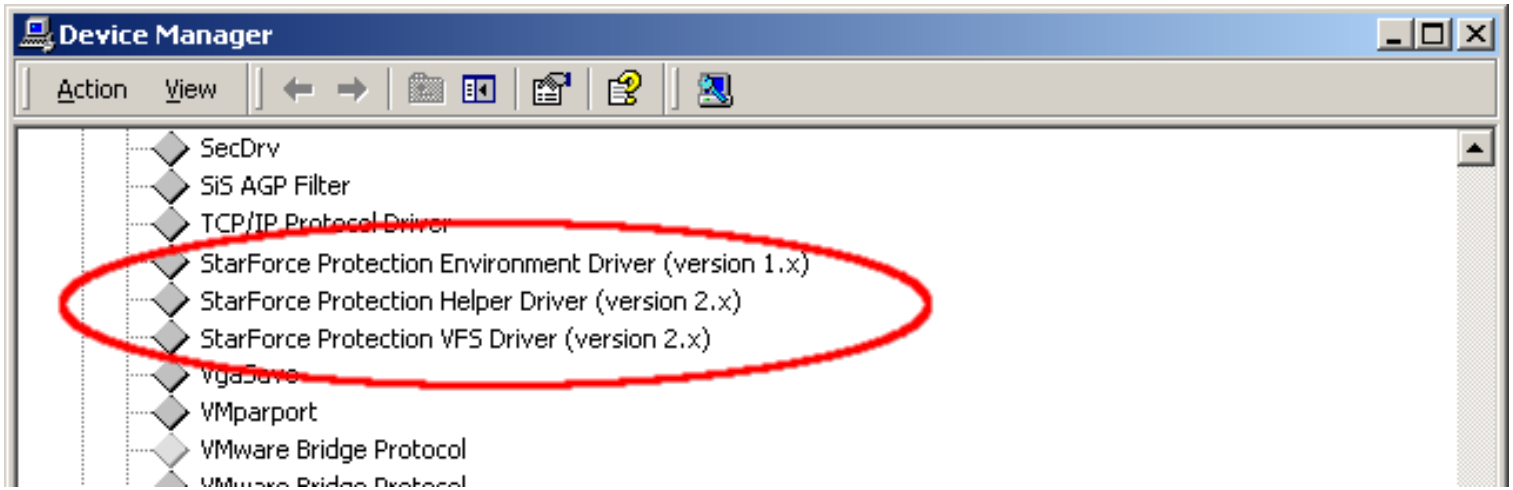
DRM **molto sofisticato**.

- Sviluppato da **Protection Technology**
- Approccio multi-tier
- Moltissimi file nel disco erano criptati
- Ogni disco aveva dei parametri univoci

Assomiglia a SecuROM, ma ci sono delle differenze fondamentali

StarForce

StarForce installa driver **Ring 0 (kernel)**, che gestiscono il drive.

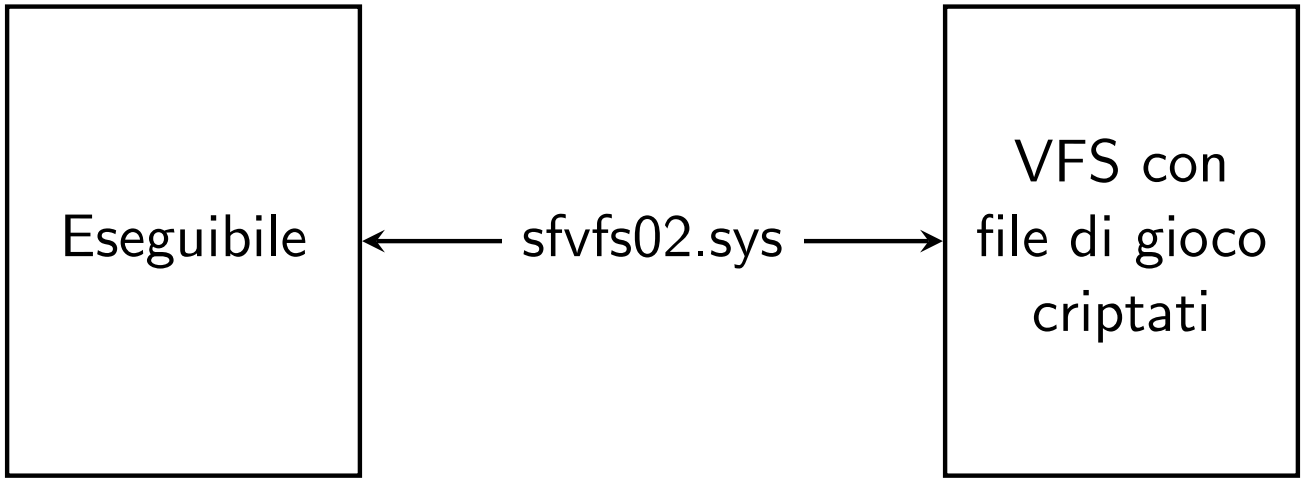


Il driver VFS gestisce il *virtual filesystem*

StarForce VFS

Il VFS è composto da:

- dei file "container" che contengono i dati di gioco
- il driver usato per accedere ai dati di gioco (sfvfs02.sys)



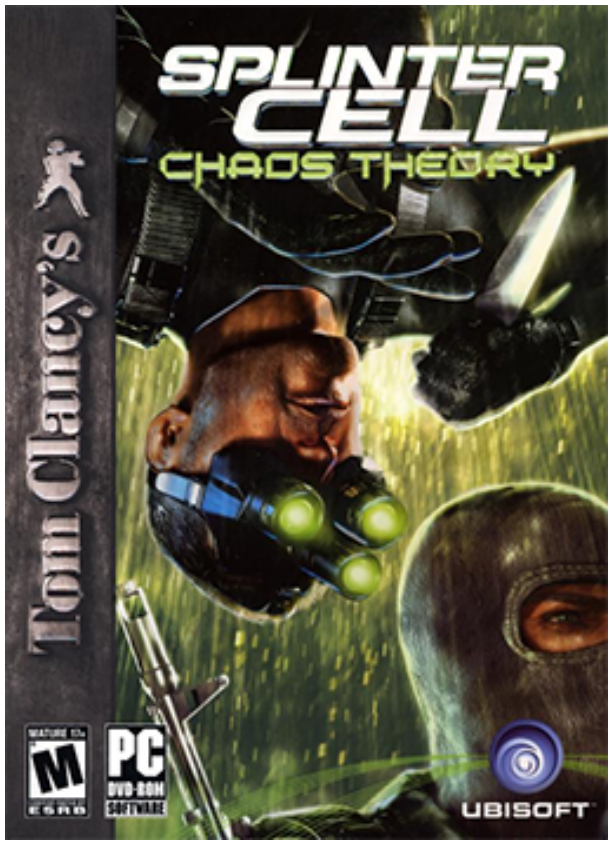
Il VFS viene quindi usato per nascondere i file di gioco.

StarForce

StarForce fu molto efficace.

Splinter Cell: Chaos Theory fu craccato solo dopo **422 giorni**.

Tuttavia, i problemi non mancavano...



Uh oh...

- Incompatibilità con Vista e successivi
- Instabilità anche su XP
- StarForce non era menzionato nell'EULA
- Driver Ring 0 installati senza avvisare l'utente
  - Rimanevano dopo la rimozione del gioco
  - StarForce Removal Tool non sempre funzionava
- Non era possibile avere più di un drive
- DMA disabilitato
- Problemi con dischi non StarForce
- **Danneggiamento del drive**

Windows 10

Nel 2015, con l'uscita di Windows 10, Microsoft annunciò che i vecchi giochi che usavano dei DRM che agivano sul kernel (SecuROM, StarForce, SafeDisc, ecc.) non avrebbero più funzionato per motivi di sicurezza.

Distribuzione digitale

Caratteristiche:

- Vendita e distribuzione via Internet direttamente al cliente
- Rimozione dei costi di produzione (supporto fisico usato come token)
- Invio di patch in tempo reale (niente richiami di prodotto)
- Inizialmente solo su PC, poi anche su console
- Forte spinta dopo il successo di Steam

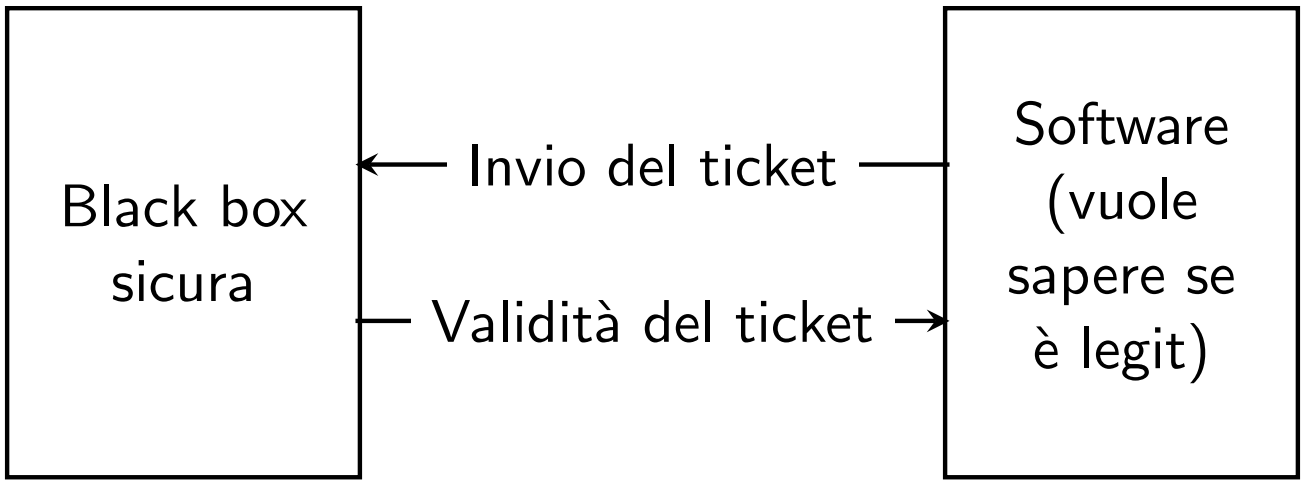
Distribuzione digitale

Varie tecnologie:

- Collegamenti con account online proprietari
- Sistemi DRM always-online
- Uso di virtualizzazione e offuscamento

Distribuzione digitale - Ticket

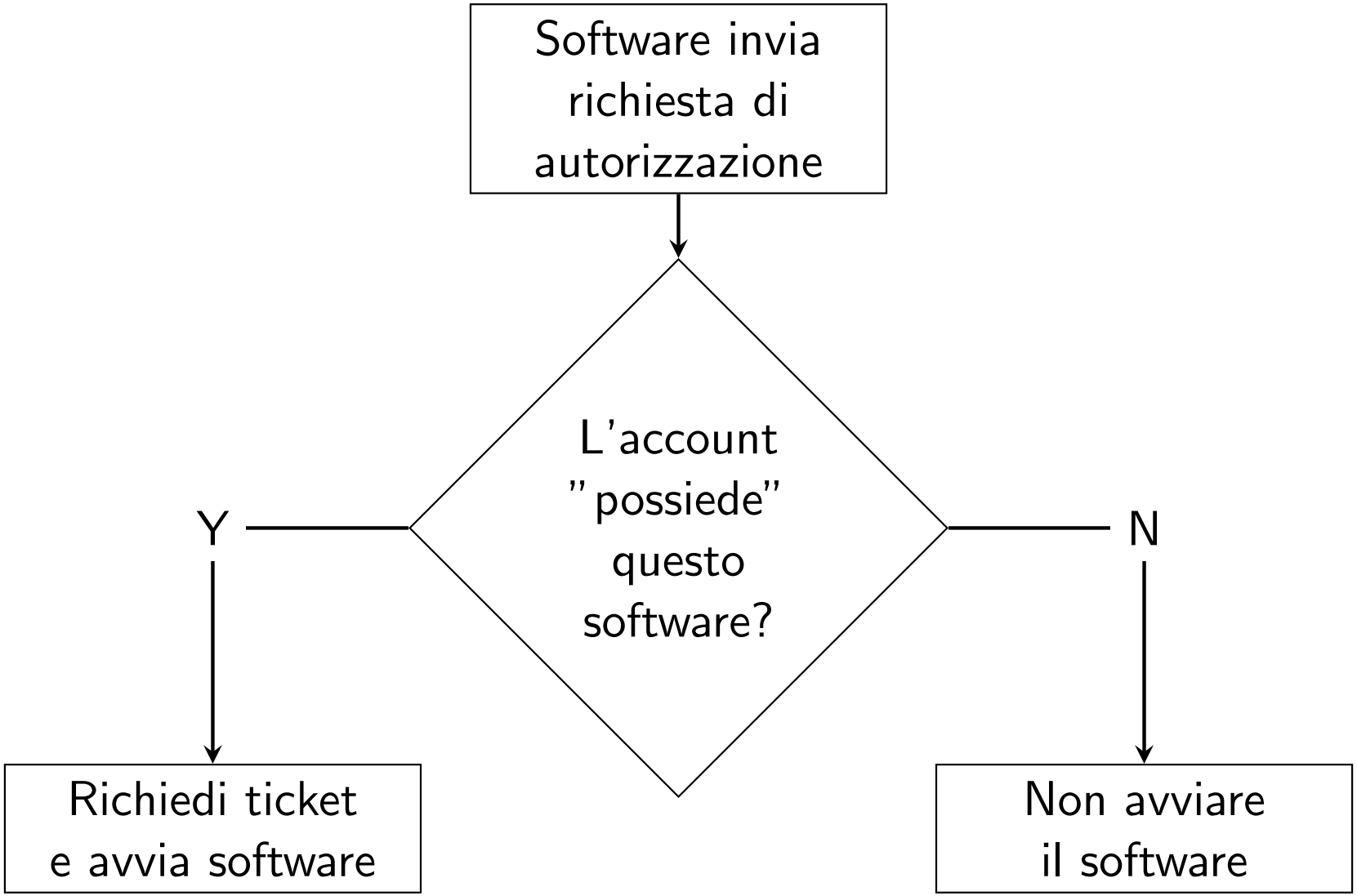
Ticket: piccoli file che contengono una "autorizzazione" firmata crittograficamente che certifica che chi ne è in possesso puó utilizzare quel software.



Es.

- IOS (Wii)

Distribuzione digitale - Account online



Distribuzione digitale - Sistemi *always-online*

Funzionamento:

- Controllo account all'avvio
- Controllo ticket periodico con il server
- Errore di connessione/verifica fallita $\rightarrow$ chiusura software
- Spesso collegato con anticheat

Distribuzione digitale - Virtualizzazione e offuscamento

Funzionamento:

- Sezioni dell'eseguibile criptate e/o offuscate
- Decriptazione/deoffuscamento grazie al ticket
- Ticket collegato ad autenticazione con server DRM
- Uso di VM proprietarie (VMProtect, Denuvo)

Crediti e ringraziamenti

Domande?