La tutela tecnica del software

Tutela della proprietà intellettuale del software a livello nazionale ed internazionale: aspetti giuridici e tecnici

Pisa, 10 dicembre 2008

Claudio Telmon – CLUSIT

ctelmon@clusit.it

Cosa vogliamo proteggere?

- Il software inteso come codice e algoritmi
  - Lo scopo è evitare l'accesso al codice e il reverse engineering
  - Particolarmente interessante per linguaggi di scripting
- La copiatura del software
- L'esecuzione del software
  - Numero di installazioni, esecuzioni...
- Tracciatura
  - Volgiamo rilevare quale copia è stata diffusa

Open Source

- Si appoggia alla normativa vigente, ma ha esigenze diverse da quelle delle licenze chiuse
- La principale esigenza è evitare la distribuzione di copie o di prodotti derivati sotto licenze chiuse
- Esempi tipici: apparati di rete con Linux embedded (es. modem/router ADSL)
- Riconoscimento mediante fingerprinting o reverse engineering

Il contesto

- Differenti tipologie di hardware
  - Apparati dedicati, cellulari, console, PC
- Differenti tipologie di software
  - Economico ad ampia diffusione
    - Sistemi operativi, pacchetti per ufficio, giochi...
  - Costoso (potenzialmente) ad ampia diffusione
    - CAD...
  - Sviluppato su misura
    - Protezione del codice

Il problema etico

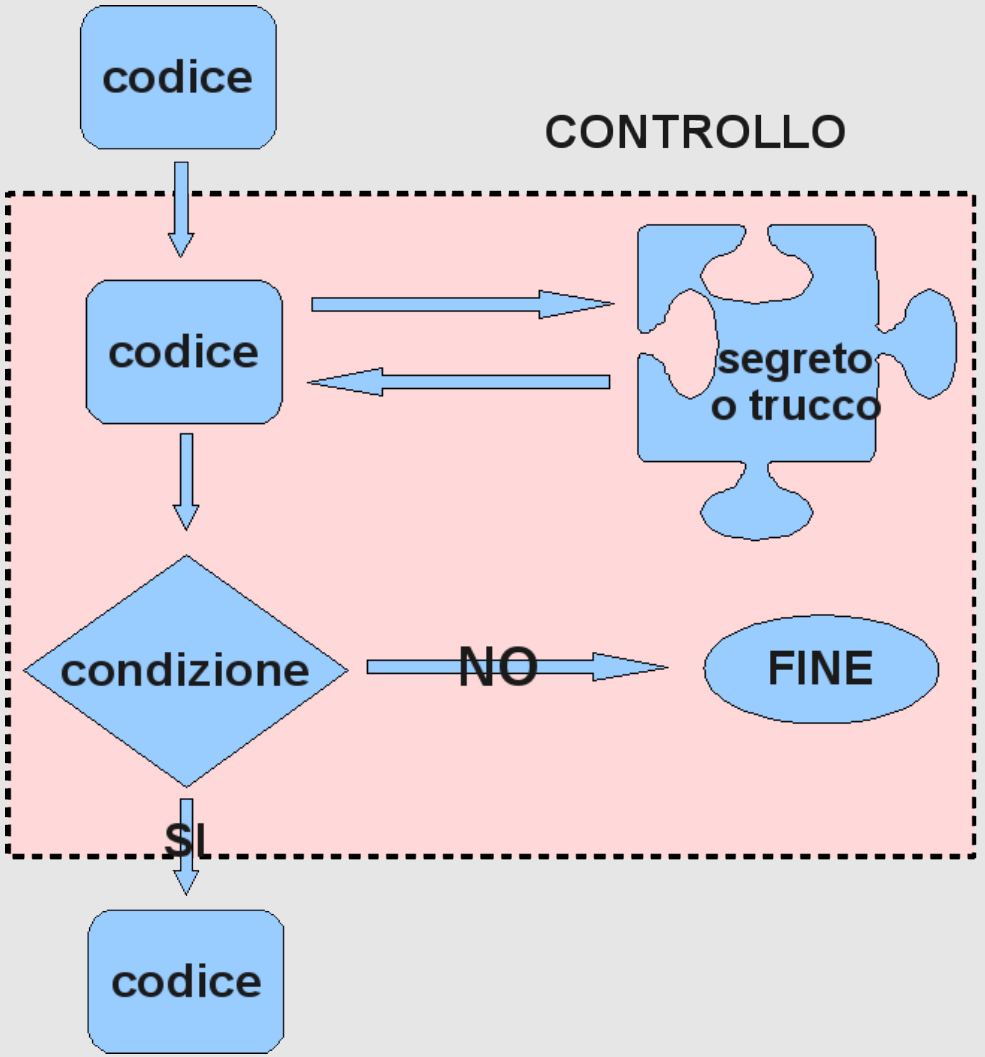
- Le tecniche di protezione devono contrastare i comportamenti di chi è legittimamente in possesso del software
- La riprovazione per l'illecito è generalmente molto bassa
  - Può addirittura essere visto positivamente
  - Interessante il caso delle pay-TV
- È una peculiarità di questo tipo di protezioni
- Vale anche per l'open source...

La copia delle informazioni

- Una volta avuto accesso alle informazioni (codice) questo può essere copiato un numero illimitato di volte:
  - Senza errore
  - Trasferibile con diversi mezzi, compreso il P2P
- In questo contesto non vale il concetto che la qualità dell'originale è migliore
  - Solo per fattori collaterali come la confezione
  - Rischio di virus ecc. a seconda del canale di distribuzione

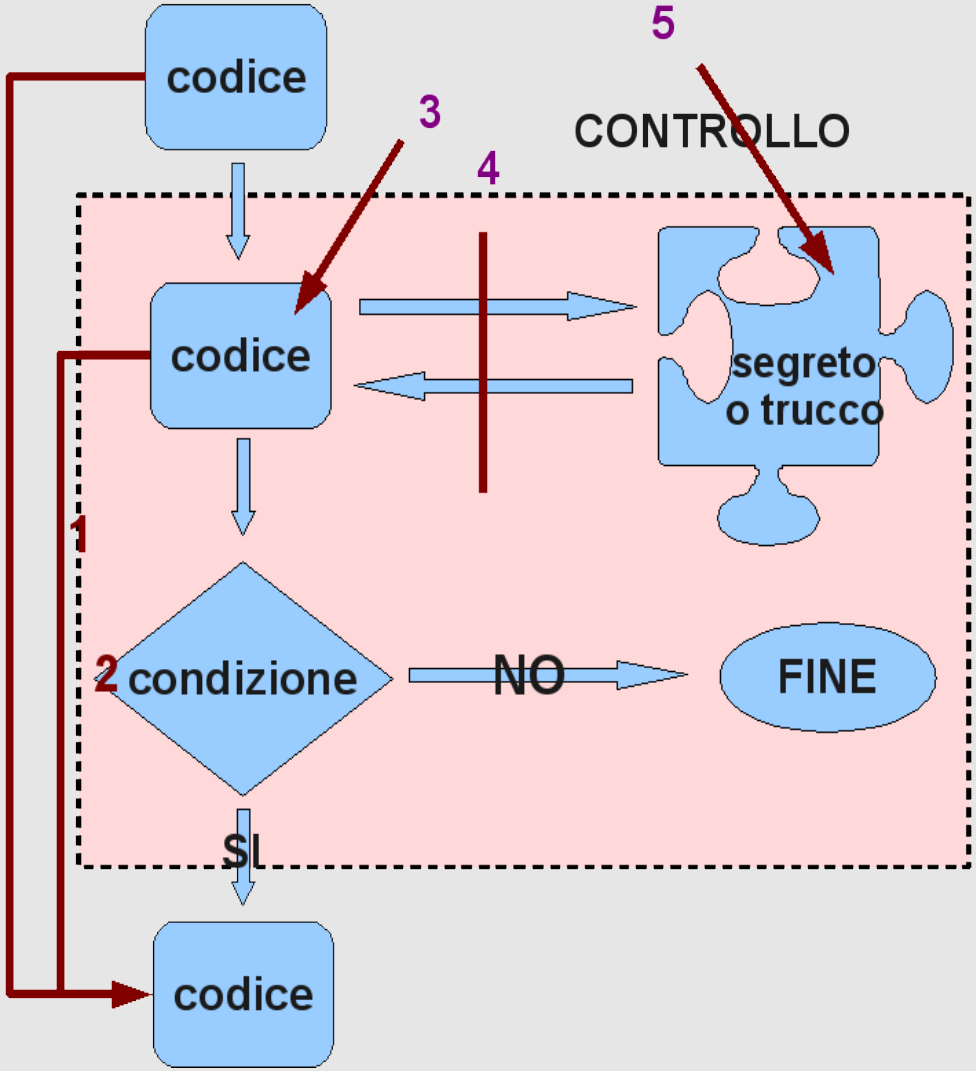
“Crackare il software”

- Aggirare i meccanismi di protezione analizzando il codice
- All'interno del codice, i meccanismi di protezione sono essenzialmente delle condizioni:
  - Si, vai avanti
  - No, esci



“Crackare il software”

1. Aggirare il controllo
2. Aggirare il salto
3. Rendere sempre vera la condizione
4. Fornire dei valori noti escludendo il componente esterno
5. Sostituire/manipolare il componente esterno



“Soluzione”

- Distribuire i controlli all'interno del software
  - Rende costoso il cracking: diventa interessante solo a scopi commerciali e per prodotti costosi
  - Efficacia limitata
- Utilizzare componenti esterni difficili da escludere
  - Difficile per il software, più adatto ad altri tipi di prodotti
- Rendere più difficile l'accesso al codice

Chiavi di licenza

- Poco efficace, a meno di interazioni online
- In generale, si possono scambiare e replicare illimitatamente
  - es. chiavi per Windows
- Difficile tracciare la fonte per prodotti Common Of The Shelf (COTS, prodotti da scaffale)
- Generatori di chiavi:
  - È possibile impedirlo in generale usando tecniche crittografiche, ma conta la lunghezza
  - Non se “sfugge” l'algoritmo (è informazione anche quello)

“Dongle”

- Componenti hardware da connettere al PC per poter usare il software

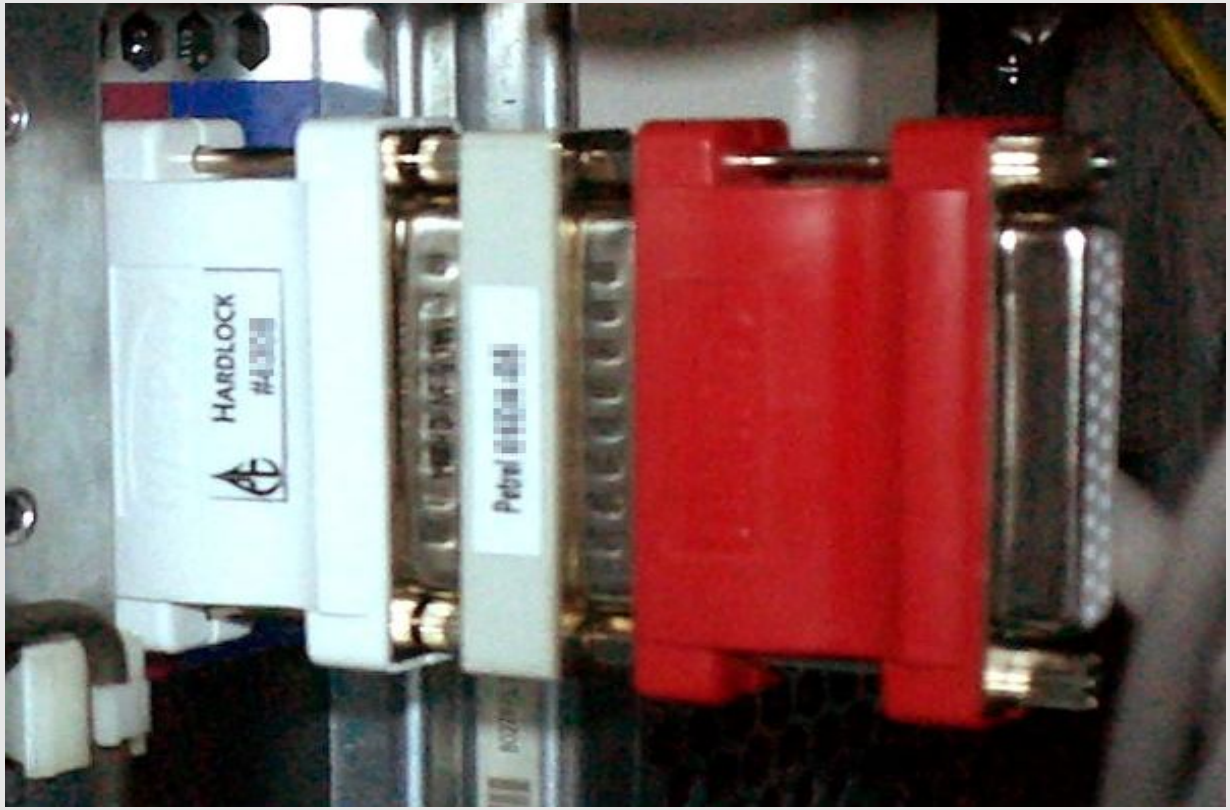


Photo by David Gerard, GNU Free Documentation License, Version 1.2

“Dongle”

- Originariamente su porta seriale/parallela, ora USB; simili a smart card
- Costosi, adatti a software costoso e non troppo diffuso
- È possibile in generale escluderli crackando il software
  - Efficaci contro la copia non commerciale
  - Nelle versioni più moderne, parti fondamentali del codice possono essere eseguite sul dongle
  - Il programma crackato è più facile da usare e può essere più veloce

CD/DVD con masterizzazione non standard

- In origine, floppy con formattazione proprietaria
- Il software richiede che il CD/DVD sia inserito
- Vantaggi: controlla il numero di installazioni e impedisce la copia
- Di fatto, si tratta di “errori” sul disco
- Efficace solo contro la copia occasionale
- Disponibili programmi molto efficaci (es. Alcohol 120%, Daemon tools...)
- Tipica dei giochi, inadatta a installazioni multiple

Watermarking

- Watermark = filigrana
- Introduzione di dati crittografici “nascosti” contenenti un'informazione relativa al copyright
- I dati sono difficili da rimuovere anche da piccole porzioni dei dati e modificandoli
- Più comune per immagini, possibile anche per il codice
- Utile per dimostrare l'origine
- Come tracciatura, ma richiede watermark diversi per ogni copia

Code obfuscation

- Rende “illeggibile” il codice per renderne difficile la manipolazione o il reverse engineering
- Non previene la copia, ma rende più difficile la modifica
- Più usato per linguaggi in cui il sorgente o un codice intermedio sono distribuiti (es. java)
- È un “palliativo”, più o meno efficace a seconda del contesto

Esempio

- Stampa i numeri primi fino a 100 (linguaggio C)

```
_(__,___,____){___/__<=1?_(__,___+1,____):!
(___%__)?_(__,___+1,0):___%__==___/
__&&!____?
(printf("%d\t",___/__),_(__,___+1,0)):___
%__>1&&___%__<___/__?_(__,1+
___,____+!(___/__%(___%__))):___<__*__?
_(__,___+1,____):0;}main(){_(100,0,0);}
```

- Traduttori che preservano la semantica

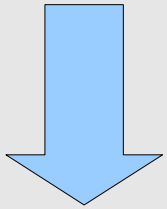
Il problema del “Trusted Client”

- Avere un client che sia “fidato” per chi fornisce il software/i contenuti a prescindere dalla volontà dell'utente
- I dati (es. software) vengono forniti cifrati al trusted client
- Il trusted client li decifra e utilizza solo se è in una condizione “sicura”
  - Deve avere accesso alla chiave di decifratura
- Questo comporta meccanismi di tamper resistance e soprattutto tamper detection

Le chiavi di decifratura

- Le chiavi sono nel trusted client, se ne escono l'intero meccanismo fallisce (es. decifratura e riproduzione in chiaro dei dati protetti)
- Si era provato con la cifratura dei DVD (CSS)

TROPPI ATTORI POCO MOTIVATI



FALLIMENTO

Le console per giochi

- Hardware dedicato, unico produttore molto motivato
- L'intera architettura è progettata per tenere conto delle esigenze di protezione
- Poca “flessibilità”: la console fa quello che vuole il produttore
- Modding: modifica dell'hardware/software per, ad esempio, poter utilizzare altro software o CD copiati
- Possibile sfruttando difetti dell'architettura

E il PC?

- “Soluzioni” software: il caso Sony BMG
- Installato all'insaputa dell'utente un componente software per impedire la copiatura dei CD Sony
- Scoperto (ovviamente), si è visto che:
  - Apriva una falla nella sicurezza di Windows; la falla è stata poi sfruttata da malware per attaccare i PC con il componente installato
  - Interferiva con l'uso legittimo del PC
  - Pare sia stato realizzato utilizzando anche software con licenza open source (LAME)

Il Trusted Computing

- Concetti fondamentali:
  - Componente hardware sicuro (Trusted protection Module, TPM), con capacità crittografiche e memoria protetta
  - Endorsement Key: chiave generata nel TPM e “certificata” solo per l'hardware conforme
    - Meccanismo di Terze Parti Fidate (Certification Authorities) per la gestione delle chiavi
    - Non sono chiavi di sola autenticazione, ma anche di conformità ai desiderata di chi le certifica

Trusted Computing - semplificato

- Il processo di boot:
  - Tutti i componenti, a partire dal BIOS, sono firmati e Trusted:
    - BIOS -> Sistema Operativo -> Applicazione
- Remote attestation: Il TPM, usando l'endorsement key, dichiara che il PC è in uno stato sicuro; gli viene fornita una chiave per accedere alle informazioni (es. contenuti multimediali, sofgtware...)
- I dati sul disco sono cifrati: acceduti tramite il TPM solo se il sistema è “sicuro”

Effetti del TC

- Solo software trusted può essere in esecuzione mentre sono acceduti contenuti protetti
  - Evita che sw non fidato possa accedere ai dati protetti e farne copie non cifrate o trasferirli
  - Solo software trusted in generale, chi vuole riavviare il pc per accedere a dei dati?
- Lato positivo: difficoltà nell'installazione di virus

Rischi

- Lock-in: i grossi player del mercato del software saranno trusted e certificati, che interesse hanno i fornitori di contenuti nel certificare una start-up?
  - Ruolo dei produttori di sw minori?
  - Non servono accordi di cartello
- Perdita di controllo del PC da parte dell'utente: la possibilità di installare software arbitrario diventa limitata
  - Il modello è più quello della console di intrattenimento che quella del PC

Digital Restrictions Management

- La soluzione tecnica impone dei vincoli, non il rispetto di diritti
  - Che i diritti corrispondano è possibile ma non necessario
  - Comunque secondo un certo insieme di norme
  - Indebolire il meccanismo per rispettare le norme di diversi paesi?
  - Inefficacia sostanziale delle norme?
    - Macrovision...

Riferimenti

- Xbox 360 modding
  - http://www.360mods.net/index.php?name=News&catid=1
- Il caso Sony BMG:
  - http://en.wikipedia.org/wiki/2005_Sony_BMG_CD_copy_protection_scandal
- Il Trusted Computing Group:
  - https://www.trustedcomputinggroup.org/home
- I rischi del Trusted Computing
  - http://www.clusit.it/download/index.htm