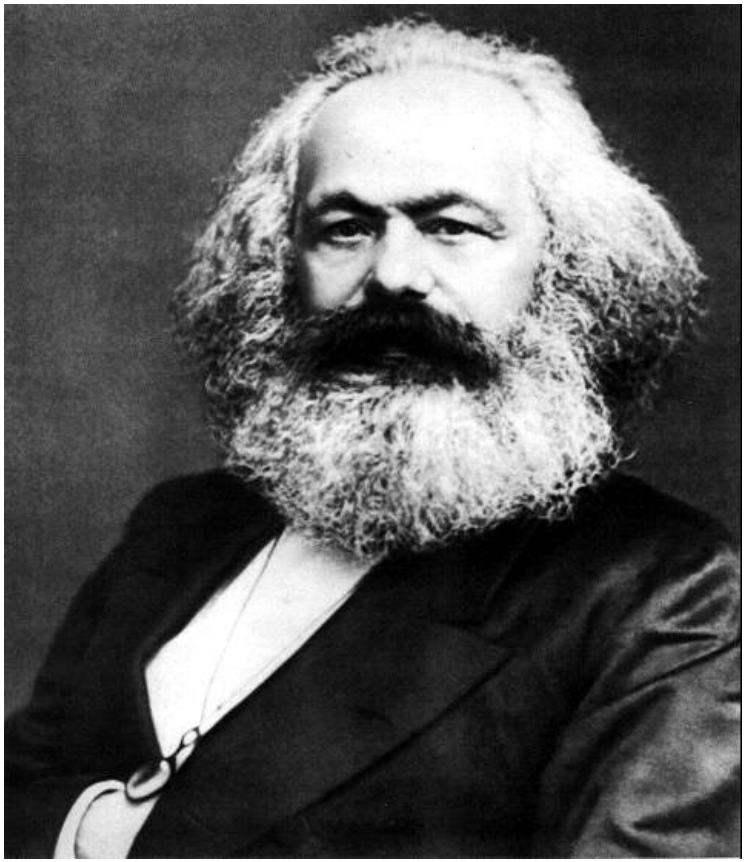
Úvod do Copy Protection

Politický úvod

Realita vs. digitálny svet:

- Vlastníctvo
- Ponuka
- Dopyt
- Krádež



Vlastníctvo v IT

- Legislatívne vychádza z predtým existujúcej legislatívy, nie z technického charakteru veci
- Programátor (zamestnanec) má *osobnostné právo* (reálne nič)
- Firma (zamestnávateľ) má *majetkové právo*
- Po/užívateľ má *licenciu* tj. zmluvnú dohodu na rôzne obmedzené využívanie softvéru

Kradnutie v IT

Z legislatívneho hľadiska

- Kopírovanie je porušením licenčnej zmluvy
- Používanie bez licencie je porušením majetkového práva

Z technického hľadiska

- Náklady len na vývoj
- Neobmedzené kopírovanie bez nákladov
- Nikto nemá priamu stratu

Licencia

- Poskytuje obmedzené právo používať softvér
- Bežné obmedzenia:
  - Obmedzenie počtu užívateľov a inštalácii
  - Obmedzenie funkcionality
  - Časové obmedzenie
  - Obmedzený počet použití
  - Mnoho ďalších obmedzení, ktoré nás nezaujímajú (účelu použitia, odvodených prác, …)

Open Source Alternatíva?

- Financovanie vývoja:
  - Dobrovoľné príspevky
  - Postranné aktivity (napr. support)
  - Predaj odvodených produktov
  - Ďalšie? (štátne financovanie, ...)
- Rozvíja sa veľmi sľubne
- Komerčnú sféru však nenahradzuje, ani v skorom čase nenahradí

Úlohou Copy Protection je technologicky zabezpečiť dodržiavanie licenčných podmienok

Technická implementácia licencovania

Obmedzenie počtu inštalácii

- Pamätať si počet inštalácii na serveri
  - Vyžaduje pripojenie k internetu
  - Komunikáciu možno podvrhnúť
  - Reinštalácia?
- Previazať program na konkrétny HW
  - Previazať priamo je technicky náročné
  - Preto býva previazaný licenčnom súbore
  - Ktorý HW testovať?
  - Čo robiť pri výmene HW?

Obmedzenie funkčnosti

- Dodať program, ktorý vie len to, za čo zákazník zaplatil
  - Často technicky príliš náročné
- Implementovať funkčnosť pomocou pluginov
  - Ako zabrániť ich kopírovaniu medzi legálnymi užívateľmi programu?
- Overovať licenčný súbor
  - Šifrovať kritické časti programu, dešifrovať kľúčmi z licencie

Časové obmedzenie

- Uložiť čas inštalácie na užívateľovom počítači a porovnať
  - Užívateľ môže vyhľadať a vymazať miesta kde je pôvodný čas uložený, prípadne inak obnoviť systém
  - Užívateľ môže preinštalovať operačný systém
  - Užívateľ môže meniť systémový čas
- Nastaviť pevný „deadline“ už pri distribúcii
  - Pohodlnejšie v licenčnom súbore
  - Užívateľ môže podvrhnúť systémový čas
- Overovať u dodávateľa cez internet

Obmedzenia natvrdo v programe

- Technicky náročné
- Výrobca musí komunikovať priamo so zákazníkom
- Prakticky možné len pri „home-made“ programoch s malou klientelou

Licenčný súbor

- Obsahuje informácie o konkrétnej licencii
  - Dátum konca platnosti licencie
  - Povolená / zakázaná funkcionalita
  - Informácie o HW počítača kde program môže bežať
- Nevyžaduje pripojenie k internetu
- Jednoduchá distribúcia
- Nebezpečenstvo KeyGen-ov

Licenčný server

- Nutnosť stáleho pripojenia k internetu
- Dočasná nefunkčnosť programu pri výpadku serveru
- Trvalá nefunkčnosť programu pri krachu autorskej firmy
- Možnosť podvrhnúť údaje pre server

Zabezpečenie licenčného kódu

Prečo sa nedá zabezpečiť

- Softvér beží na počítači užívateľa
- Užívateľ má nad svojim počítačom plnú kontrolu
- Užívateľ môže program meniť a/lebo mu dodávať nepravdivé údaje

Problém:
Užívateľ má plnú kontrolu

- Špinavé riešenie: ovládač
  - Užívateľ má svoje ovládače, boj „kto z koho“
- Čistejšie riešenie: OS implementujúci DRM
  - Užívateľ dokáže prebrať kontrolu ešte pred štartom OS
- Čisté riešenie: Trusted Computing
  - Aj „trusted“ software obsahuje chyby
  - Užívateľ dokáže manipulovať hardware
  - Príliš nepohodlný pre „konzumentov“

Problém:
Program beží na počítači užívateľa

- Presunúť časť kódu do „trusted“ externého zariadenia (Dongle)
- Presunúť časť kódu na externý server

Dongle

- Pripája sa cez USB alebo LPT port
- Musí byť fyzicky dodaný zákazníkovi
- S kvalitou rapídne stúpa cena za každý kus

Externý server

- Vyžaduje od užívateľa nepretržité pripojenie na internet
- Server nevie spoľahlivo autentifikovať užívateľa
- Komunikácia je časovo náročná
- Pri väčšom počte užívateľov je to náročné na HW
- Program prestane fungovať, ak firma prestane prevádzkovať server.

Problém:
Užívateľ môže program meniť

Čo znamená „meniť program“

Pôvodný program:

```
if ( LicenseOkay() )
{
   ...
}
```

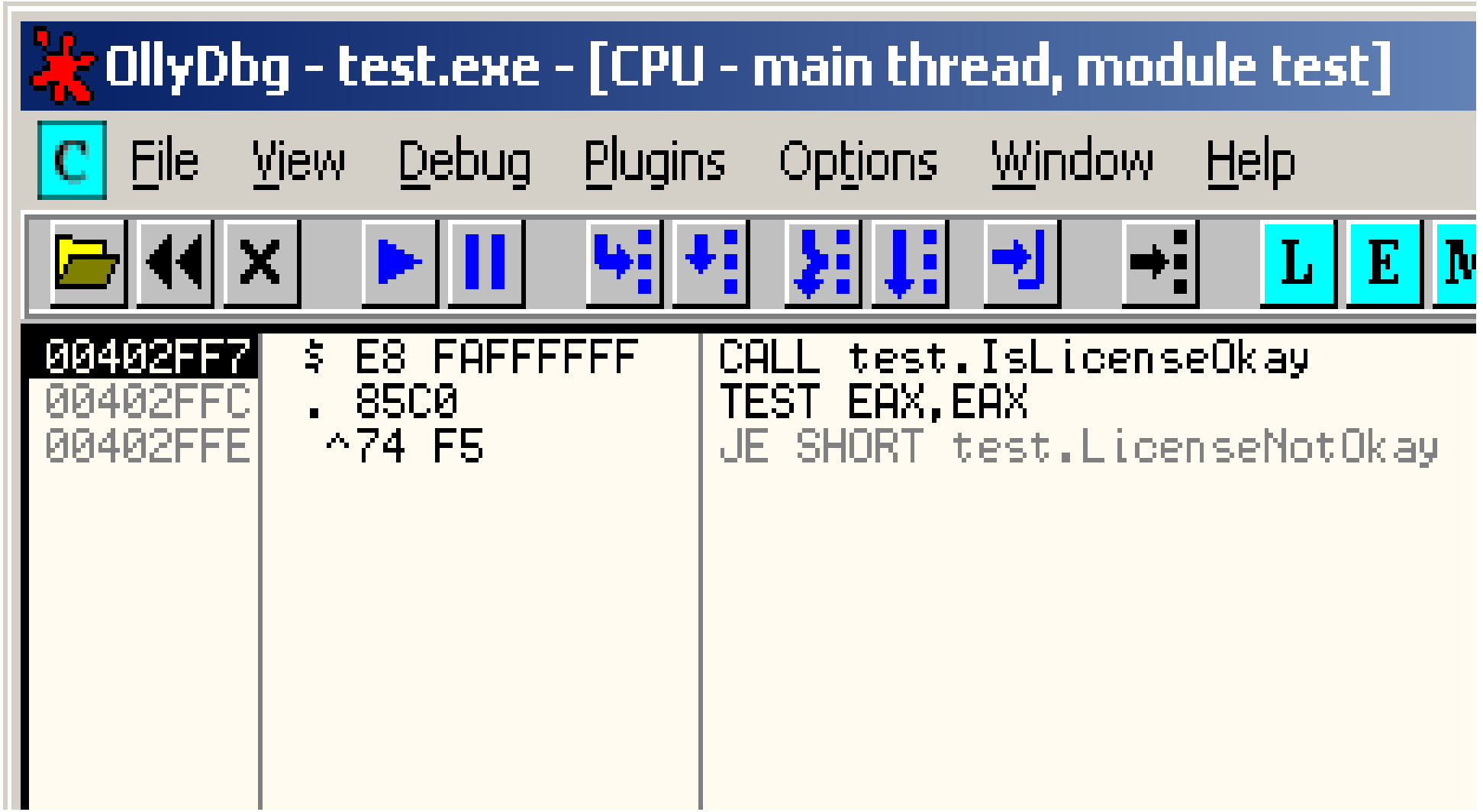
Skompilovaný:

```
E8 XX    call IsLicenseOkay
85 C0    test return value
74 XX    jump if zero
```

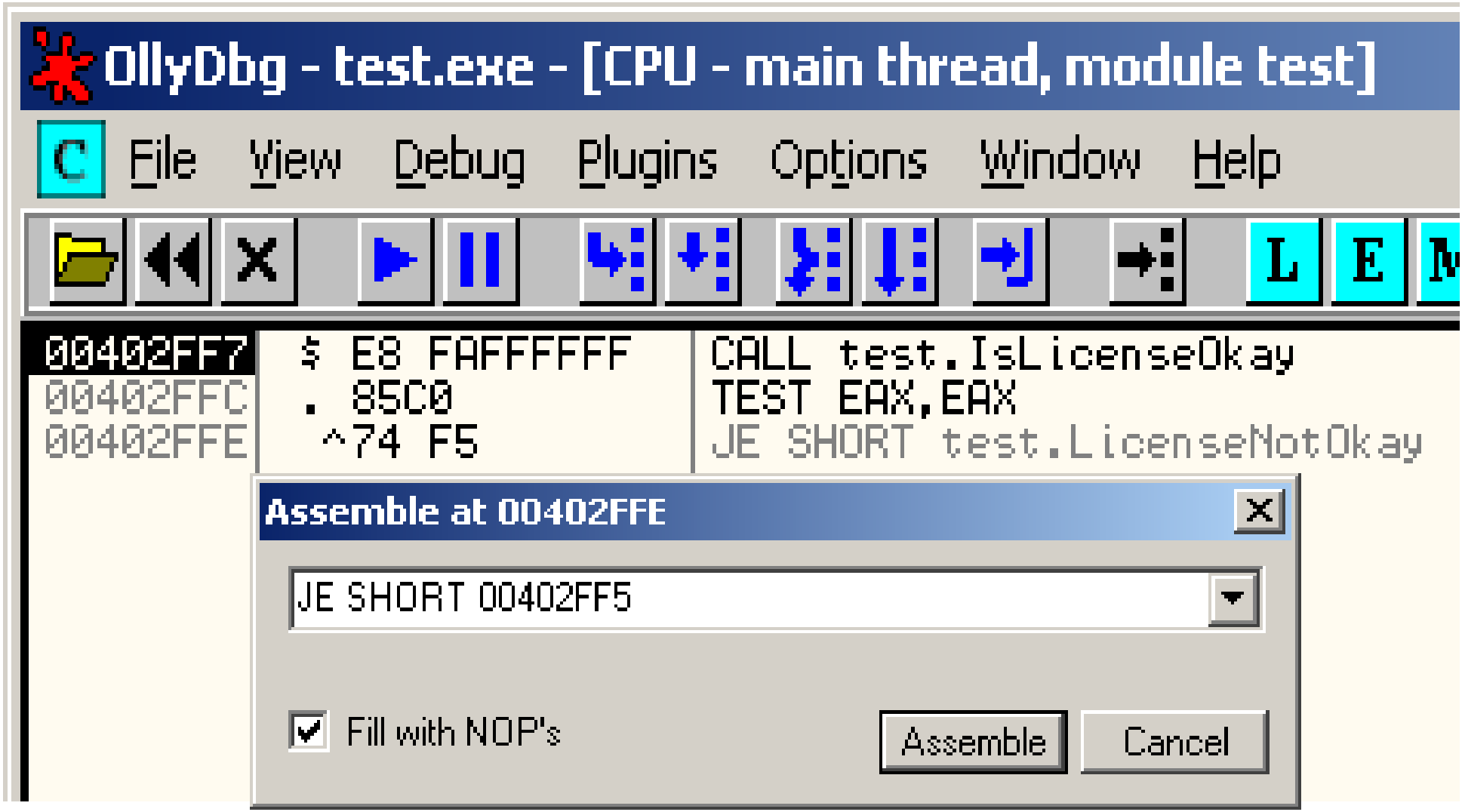
Cracknutý:

```
E8 XX    call IsLicenseOkay
85 C0    test return value
75 XX    jump if not zero
```

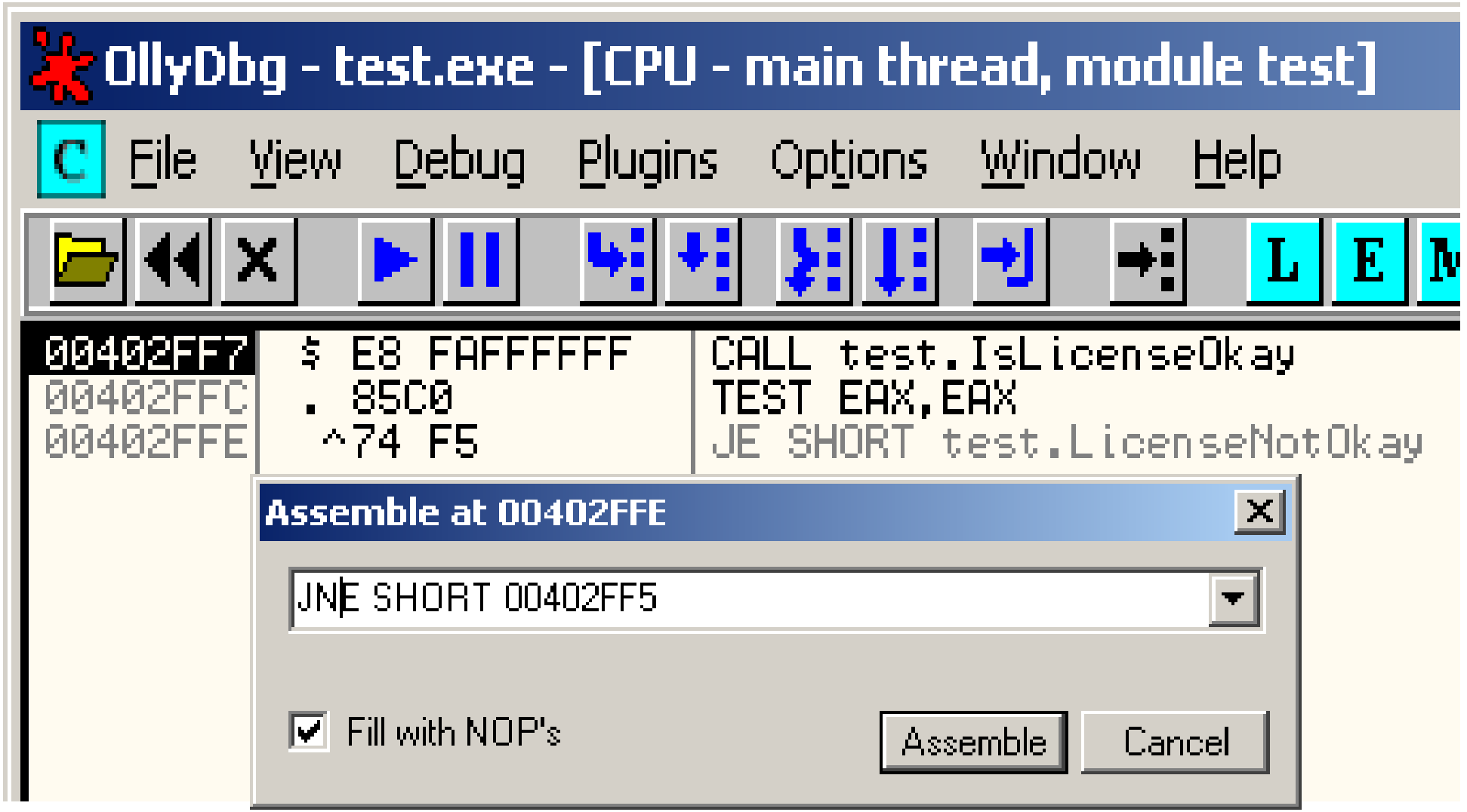
Debugger


OllyDbg - test.exe - [CPU - main thread, module test]
File View Debug Plugins Options Window Help
00402FF7 $ E8 FAFFFFFF CALL test.IsLicenseOkay
00402FFC . 85C0 TEST EAX,EAX
00402FFE ^74 F5 JE SHORT test.LicenseNotOkay

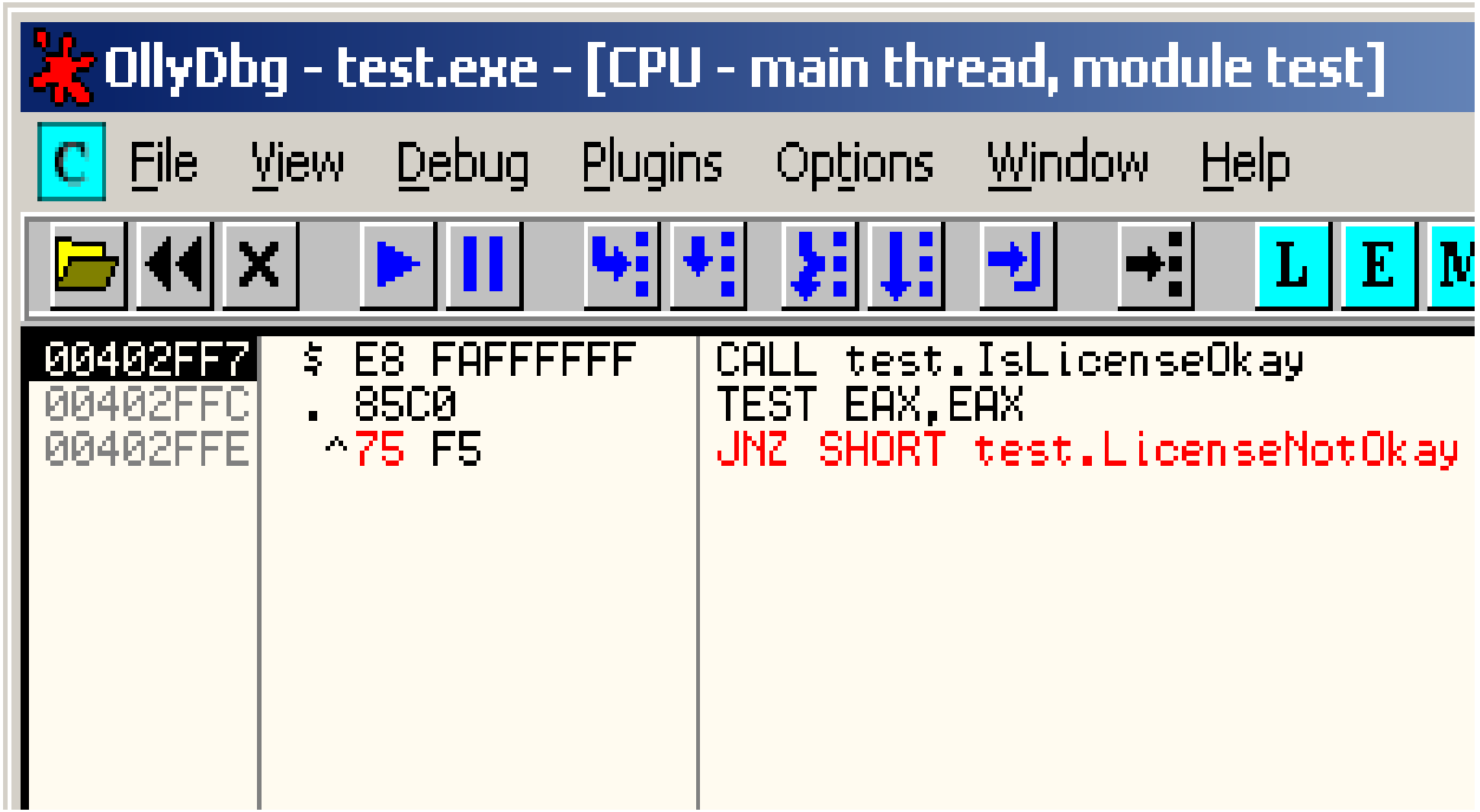
Debugger


OllyDbg - test.exe - [CPU - main thread, module test]
File View Debug Plugins Options Window Help
00402FF7 $ E8 FAFFFFFF CALL test.IsLicenseOkay
00402FFC . 85C0 TEST EAX,EAX
00402FFE ^74 F5 JE SHORT test.LicenseNotOkay
Assemble at 00402FFE
JE SHORT 00402FF5
Fill with NOP's
Assemble
Cancel

Debugger


OllyDbg - test.exe - [CPU - main thread, module test]
File View Debug Plugins Options Window Help
00402FF7 $ E8 FAFFFFFF CALL test.IsLicenseOkay
00402FFC . 85C0 TEST EAX,EAX
00402FFE ^74 F5 JE SHORT test.LicenseNotOkay
Assemble at 00402FFE
JNE SHORT 00402FF5
Fill with NOP's
Assemble
Cancel

Debugger


OllyDbg - test.exe - [CPU - main thread, module test]
File View Debug Plugins Options Window Help
00402FF7 $ E8 FAFFFFFF CALL test.IsLicenseOkay
00402FFC . 85C0 TEST EAX,EAX
00402FFE ^75 F5 JNZ SHORT test.LicenseNotOkay

Ako sa brániť

- Kontrolný súčet strojového kódu programu
- Zaistiť kód v pamäti proti zápisu
- Skúšať či zostal zaistený
- Detekovať bežné programy ktorými sa kód prepisuje (debuggery a iné)
- Aktívna ochrana do OS

Virtuálny stroj (VM)

- Hostiteľský program: VMware, VirtualBox, Xen, ...
- Všetky ochrany zlyhávajú. Hostiteľ môže ľubovoľne prepisovať pamäť VM
- VM sú naprogramované aby fungovali čo najrýchlejšie, nie pre dokonalú emuláciu
- Niektoré „špecialitky“ vo VM pracujú inak ako na skutočnom počítači
- Beh vnútri VM možno detekovať

Obfuskácia

- Nahradenie strojového kódu funkčne ekvivalentným ale ťažko zrozumiteľným

Obfuskácia

```
call IsLicenseOkay
test eax, eax
jz   LicenseNotOkay
```

```
push -788
lea eax, [IsLicenseOkay]
call eax
test edx, eax
cmc
add eax, [esp]
cmp eax, -787
jb LicenseOkay
pop eax
je LicenseNotOkay
jmp LicenseOkay
```

Zhrnutie

- Licencovanie tak ako vyplýva zo zákonov je technicky neuskutočniteľné
- Každú ochranu možno prelomiť pri dostatočnom úsilí
- Na kvalitnú ochranu treba tím dobrých programátorov a veľa času

Situácia v praxi

- „Domácke“ ochrany prelomené ihneď a každým
- Veľmi rozšírené programy odolajú rádovo dni
  - Bežne je ochrana prelomená ešte pred oficiálnym zverejnením (0-day)
- Stredne rozšírene programy môžu vydržať rádovo mesiace
- Málo známe programy majú šancu zostať neprelomené

Ďakujem za pozornosť

Martin Mocko
email: vid512@gmail.com