Петров Д.М. КИТ-М120Б

Лабораторна робота № 4

Захист від зміни бінарного файлу

Мета: Навчитися підписувати виконувані файли.

Індивідуальне завдання

- створити сертифікат
- проінсталювати його в систему, щоб він був "довіреним"
- використовуючи проект будь-якої попередньої роботи, виконати підпис виконуваного файлу за допомогою утиліти SignTool (або JarSigner) (інші варіанти повиннні бути оговорені з викладачем)
- виконати верифікацію підпису (бажано на рівні самого кода при завантаженні додатка):
- чи є підписаний сертифікат валадним
- чи не було (бінарної) зміни файлу та його код цілостний

Цифровий підпис програми потрібен для того, щоб захистити програму за допомогою вказівки вашого авторства. Як тільки програма отримає спеціальну цифровий підпис, вона не може бути змінена третіми особами. Якщо людина спробує внести свої зміни в код програми, цифровий підпис тут же стане недійсною. Власне, в цьому і полягає суть Code Signing.

Додатки, що мають цифровий підпис, є верифікованим і не викликають підозр у користувачів. До них лояльно відносяться різні антивіруси і брандмауери. Такі програми дуже рідко потрапляють в карантин.

В процесі лабораторної роботи був створений сертифікат. Для того щоб підписати ним файл необхідно додати сертифікат в операційну систему. Після того за допомогою утиліт можна підписувати.

codesign -s lab04 server

За допомогою утиліти codesign був підписаний файл server.

```
[danilpetrov@MacBook-Pro bin]$ codesign -dv --verbose=4 server
Executable=/Users/danilpetrov/Safe_Programming/lab04/bin/server
Identifier=server
Format=Mach-O thin (x86_64)
CodeDirectory v=20100 size=26135 flags=0x0(none) hashes=813+2 location=embedded
VersionPlatform=1
VersionMin=659200
VersionSDK=659206
Hash type=sha256 size=32
CandidateCDHash sha256=8b491f9767ecd6ff29bab8811271ef7c468131c7
CandidateCDHashFull sha256=8b491f9767ecd6ff29bab8811271ef7c468131c7f8eae7c59331a005ce5756eb
Hash choices=sha256
CMSDigest=8b491f9767ecd6ff29bab8811271ef7c468131c7f8eae7c59331a005ce5756eb
CMSDigestType=2
Page size=4096
CDHash=8b491f9767ecd6ff29bab8811271ef7c468131c7
Signature size=1610
Authority=Lab04
Signed Time=24 Nov 2020, 11:49:24
Info.plist=not bound
TeamIdentifier=not set
Sealed Resources=none
Internal requirements count=1 size=84
```

Висновок

Навчитився підписувати виконувані файли.