bartkozpoznania

Bartko's Blog

Extracting digital signature (PKCS7) from signed PE files

Filed under: Code — Leave a comment
2013/08/22

Here we go with extracting a digital signature in PKCS7 format from a Windows PE executable file signed with Authenticode (attached signature) using Python with pefile module.

```
import pefile

def extractPKCS7(fname):
    '''A function extracting PKCS7 signature from a PE executable

    This function opens the file fname, extracts the PKCS7
    signature in binary (DER) format and returns it as
    a binary string
    '''

    # first get the size of the file
    totsize = os.path.getsize(fname)

    # open the PE file
    # at opening time we do not need to parse all the information
    # so we can use fast_load
    ape = pefile.PE(fname, fast_load = True)

    # parse directories, we are interested only in
    # IMAGE_DIRECTORY_ENTRY_SECURITY
    ape.parse_data_directories( directories=[
        pefile.DIRECTORY_ENTRY['IMAGE_DIRECTORY_ENTRY_SECURITY'] ] )

    # reset the offset to the table containing the signature
    sigoff = 0
    # reset the lenght of the table
    siglen = 0

    # search for the 'IMAGE_DIRECTORY_ENTRY_SECURITY' directory
    # probably there is a direct way to find that directory
    # but I am not aware of it at the moment
    for s in ape.__structures__:
        if s.name == 'IMAGE_DIRECTORY_ENTRY_SECURITY':
            # set the offset to the signature table
            sigoff = s.VirtualAddress
            # set the length of the table
            siglen = s.Size

    # close the PE file, we do not need it anymore
    ape.close()

    if sigoff < totsize:
        # hmmm, okay we could possibly read this from the PE object
        # but is straightforward to just open the file again
        # as a file object
        f = open(a,'rb')
        # move to the beginning of signature table
        f.seek(sigoff)
        # read the signature table
        thesig = f.read(siglen)
        # close the file
        f.close()

        # now the 'thesig' variable should contain the table with
        # the following structure
        #   DWORD       dwLength          - this is the length of bCer
        #   WORD        wRevision
        #   WORD        wCertificateType
        #   BYTE        bCertificate[dwLength] - this contains the PKC
        #                                    with all the

        # lets dump only the PKCS7 signature (without checking the ler
        return thesig[8:]
    else:
        return None
```

Once the signature is is extracted, information on digital certificates can be obtained using openssl:

```
openssl pkcs7 -inform DER -print_certs -text
```

There is a really good document on the format of Authenticode signatures in PE file available from Microsoft.

Tags: digital certificate, digital signature, pefile, python

Comments RSS (Really Simple Syndication) feed