Name: Cezar Augusto Contini Bernardi
Student ID: 140139
Obligatory exercise 4
2014-10-06

Task:

- **Find vulnerabilities in the SecureDesktop application.**

1. Report

First of all, I tried to compile the Secure Desktop source code using Lazarus 1.2.4 and Free Pascal Compiler 2.6.4. I tried it to better understand how the program works. Unfortunately I was not able to make it happen with either of those.

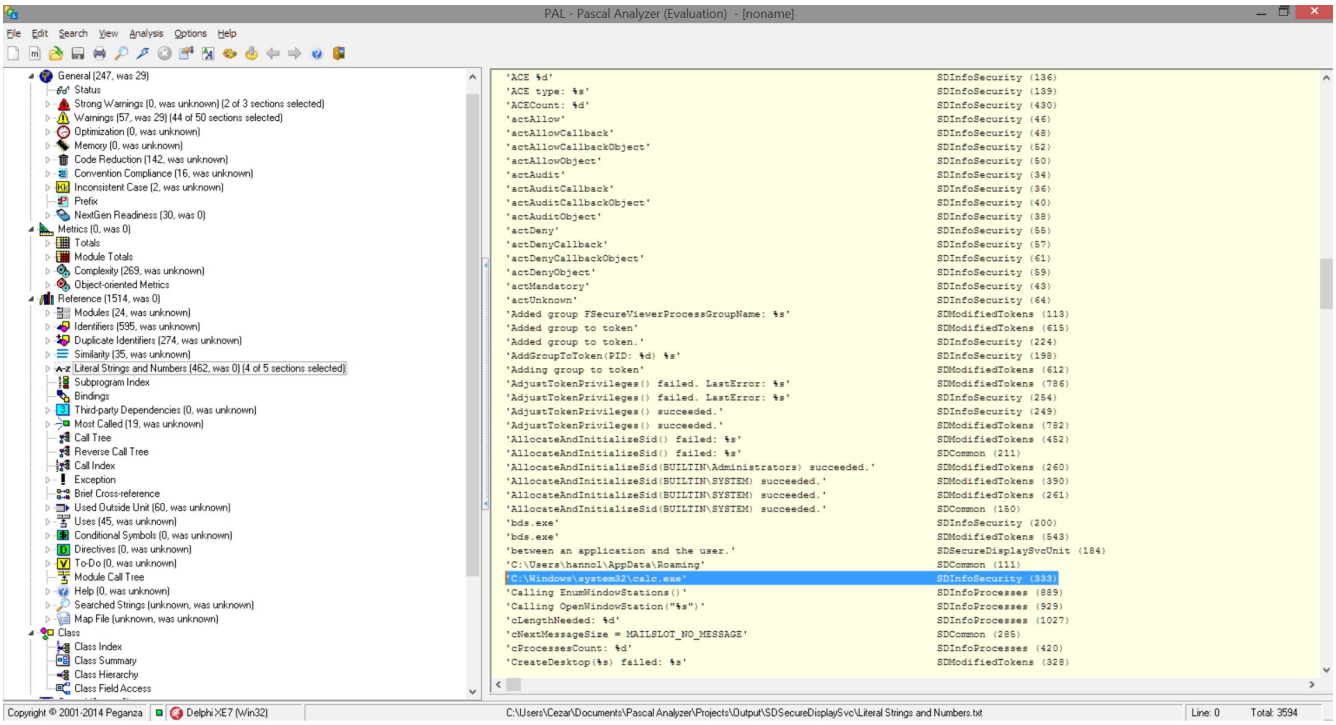
Moving on, I found Code Healer as an option for static analysis of delphi code, however, I couldn't find a free option to use/test. I also found Pascal Analyzer 7.

On Pascal Analyzer (PA, to simplify) I was able to see literal strings on the code. With this info, I found out some hard coded paths, leading to files or executables.

The line 333 of the file SDInfoSecurity.pas has an example of this.

```
if SDCreateProcessWithTokenOnDesktop('C:\Windows\system32\calc.exe', '',
    hNewToken, 'Default') then
```

It could lead to security issues in a situation where the executable would be moved or modified with malicious code. On this issue, a solution that I can think of is to include the needed execuble inside the instalation folder of the program and code it as a relative path, as well as check on the execuble to be sure it is not modified. It could be done with a hash function like MD5 or SHA-256.



Pascal Analyzer 7

Another programming issue is on line 111 of the file SDCommon.pas where a username is hard coded in to the path.

StrPCopy(pszAppDataPath, 'C:\Users\hannol\AppData\Roaming');

I don't see how this would be a security issue, however, this program will not work outside the environment it was created.

There is also a filename hardcoded on file SDCommon.pas, line 23.

BackgroundBitmapFileName = 'Background.bmp';

Later on, this constant is utilized without any check, leading to a possible threat, by having the file modified by an atacker. Again, a hash check could prevent the issue.