Obligatory Assignment 3 in Software security

Tommy André Evensen
120484
12HBISA

Co-reviewer
Mats Aass Authen

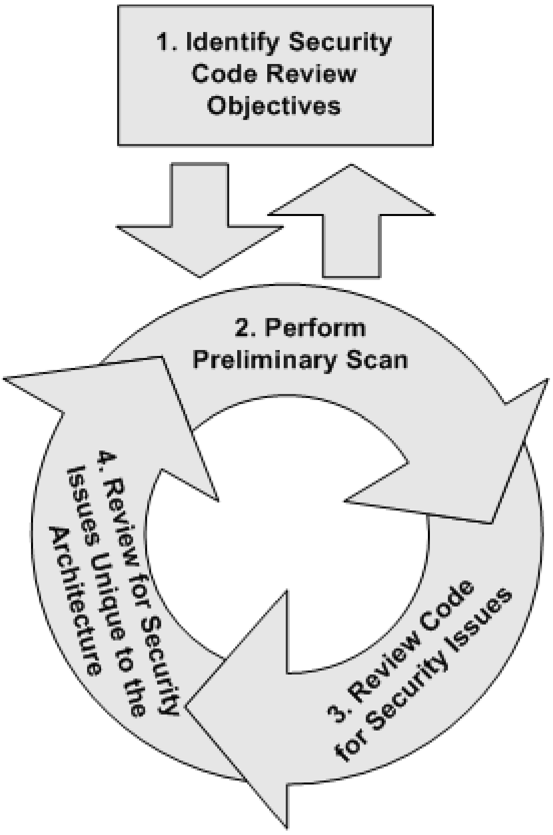
About the task

« Find vulnerabilities in the SecureDesktop application. You find source code and an article in the repository. »

The source code consists of 16 items which is written in Pascal.

Methology

We used the microsofts: Preferm a security Code review for managed code.


1. Identify Security Code Review Objectives
2. Perform Preliminary Scan
3. Review Code for Security Issues
4. Review for Security Issues Unique to the Architecture

(Illustration of the review model http://i.msdn.microsoft.com/dynimg/IC78436.gif *)*

The process includes four steps. The first step was to Establish goals and constraints for the review. The second was to use static analysis to find an initial set of security issues and to improve my understanding of where the most likely will find issues. The Third was to review the code thoroughly with th goal of finding security vulnerabilities that are common. The last step was to look for for security issues that relate to the unique architecture of this program.

My programming skills is limited to what i've learned at Hig so i've had to use a lot of time doing research.

The findings

ID	1
File	Sdinfoprocsses.pas
Threat	Buffer Overflow

Line	153
Short description	If the microsoft username is over 2048, we may have a buffer overflow
Risk	Low

ID	2
File	Sdinfoprocesses.pas
Threat	Buffer Overflow
Line	156
Short description	If the domain-name is over 2048, we may have a buffer overflow
Risk	Low

ID	3
File	Sdmodyfiedtokens.pas
Threat	Buffer Overflow
Line	216
Short description	It places something into a Cstring which is Not alocated,
Risk	Low

ID	4
File	SdCommon.pas
Threat	Hardcoded path
Line	111
Short description	Most people don't have username «hannol»
Risk	High

ID	5
File	All

Threat	Lack of comments
Line	All
Short description	I feel the program would benefit with more documentation in the code
Risk	low

ID	6
File	All
Threat	Open Loggs
Line	All
Short description	I feel the program would benefit with more documentation in the code
Risk	low

ID	7
File	SDCommon.pas
Threat	Bugg
Line	96
Short description	There is a bugg with «shgetknownfolderpath» on some platforms
Risk	Medium

Buffer Overflow
I found 3 places where a buffer owerflow might occour. Although there are som system limmitations that might make it not possible on ID 1 and 2, i thought i should write it down.
But anyway one should not use windows Pchar as its equalent with C strings which is responsible for a lot of buffer Overflow attacks. One should rather use Pascals string, which is basically a heap pointer, which is harder to exploit.

Hardcoded Path
This one was interesting. As most user don't call their users on windows «hannol» this may resoult in a crash. The program should have a dynamic link which works for all users.
%USERPROFILE% \AppData\Roaming
This should make it work on all users.

Comments
As a reviewer, it would be easier to go through the code and understand if the code had comments.

It would be easier for furter developing and maintenance aswell. I saw that the program had commented away some lines so the programmer should know how to do it.

Verbose logging

At many sections and most functions of the application events that have been undertaken or have failed are outputed to a log file. This could expose a potential attacker to a lot of information.

Reffrences

http://msdn.microsoft.com/en-us/library/ff649315.aspx

http://en.wikipedia.org/wiki/Heap_overflow