Security Engineering, Assignment 5. Due date: May 3, 2015

Return Oriented Programming and OpenSSL Certificates

Part 1.

The objective of the assignment is to familiarize you with Return Oriented Programming (ROP). As a part of the assignment you have to write a program that exploits the concept of *Gadgets* that we discussed in the class, to print "Hello World". You should be searching for sequence of 'POP RET' instructions in the libc library which should be used to print "Hello world" using the write() system call (present as a library function in the libc library).

Part 2.

The second part involves modifying assignment 1 so that the clients are now authenticated using X.509 certificates generated using OpenSSL package. You would require to add a CA, similar to the one demonstrated during the lecture. Thereafter the CA signs server and client certificates. The server needs to validate the client certificate so as to successfully allow the connection to proceed. Otherwise the server should terminate the connection. The authentication must be done using OpenSSL library routines. You could use the openssl s_client and s_server packages to help you debug the client and/or server sides of the program.

You must demonstrate to the TAs that the certificates are validated for both the clients and servers. Thereafter, you must also demonstrate how clients with invalid certificates (With some bits modified) or unavailable certificates are not authenticated.

Like the previous assignments, you must correctly handle all errors and corner cases.

You would not be evaluated for the functionalities which were already demonstrated for grading assignment 1.

What you are supposed to submit:

1. C source code for the aforementioned shell server and client programs.
2. Makefile through which one could compile these programs.
3. A write up of what your system does, what all assumptions you made, the inputs that you used to test your program and all the errors that you handled.

Grading scheme:

1. Successful compilation using Makefile – 10 points
2. Use of OpenSSL library routines to perform the client and server certificate validation operations. – 15 points.
3. Successfully using the sequence of POP RET instructions to assemble the gadget that prints out "Hello World" on the screen. – 15 points.
4. Successfully defending against atleast 3 attacks/bugs/errors (e.g. Handling client connections whose certificates cannot be validated, handling connections where the server's certificate cannot be validated) – 7 points (List the bugs/errors/attacks that you defend against)
5. Description of the systems, commands to execute and test the program and the assumptions that you made. – 3 points