SWINBURNE UNIVERSITY OF TECHNOLOGY

TNE30024

Deploying Secure Engineering Applications Online

Tutorial 5 (week 6)

Secure Communications in Practise

1. Why is the TLS layer typically implemented as a Library at the Application Layer?

2. Within the TLS libraries, how is a server verified by the client?

3. In terms of certificate information, what does the server need to provide to the client in order to allow a connection to be established?

4. When developing a software solution to use a certificate, what information/files does the program need to provide to the TLS libraries?

Socket Programming

For the second half of the tutorial, we are going to write a very short python program to download a web page from a HTTPS server that is encrypted via a certificate.

Note: Here I am going to use a sample code to demonstrate it. This will be similar to the one you are going to use in the lab.

Purpose of the Programming section:

1) Familiarize with python code, library functions and their syntaxes
2) Understand that for a valid connection, the server certificate is authenticated against the stored central repository.

3) Understand that having an invalid connection will cause the TLS library and code to fail

4) Understand that a complete solution (one that you come up with by yourself) would:
   - catch the TLS errors to allow the program to fail nicely rather than crash
   - allow provision of alternate root certificates to accept non-verified connections

Step 1: Create a socket, wrap it with TLS Context and Verifying Connection

Step 2: Downloading a page

Step 3: Connect and Download page from Rule201