



University of the
West of England

MODULAR PROGRAMME

ASSESSMENT SPECIFICATION

Module Details

Module Code	Run	Module Title
UFEEJ6-10-3	08SEP/1 TB2	Advanced Distributed Systems
Module Leader	Module Tutors	
Ian Johnson	Ian Johnson	
Component and Element Number		Weighting: (% of the Module's assessment)
B1		25%
Element Description		Total Assignment time
Coursework		6 hours + lab time

Dates

Date Issued to Students	Date to be Returned to Students
12/02/2009	5th May 2009
Submission Place	Submission Date
PROJECT ROOM - 2Q30 (Help Desk open 9.00 - 6.00pm)	2nd April 2009
	Submission Time
	2.00 pm

Deliverables

As per the attached specification

Module Leader Signature

Ian Johnson

You must work individually for this assignment.

SSL (Secure Sockets Layer) is a technology for securing socket based distributed systems originally developed by Netscape. This is supported by many libraries and languages on most platforms, and whilst this was only a defacto standard it has been revised into a formal standard (as an RFC) as TLS (Transport Level Security)

Your assignment this term is to design and implement a small, SSL enabled client server application. This may be any application, and may be written in C or Java. Support for Java will however be far more limited than for C.

However: You will need to demonstrate the functionality so...

It is suggested that a minimal http server (based for example on linuxsocket.org's http-ls server) is developed so that interaction with a standard web browser can be demonstrated. This will allow you to just develop a server, based on an existing framework.

Main features required:

- Fully chained (i.e you start by creating a certification authority) X.509 certificates for both client & server.
- Client and Server authentication.
- Cipher negotiation.
- Screen based feedback for the steps in and outcome of the SSL handshake.

The examples and documentation that are provided on the website for this module use Linux, openssl, and C. To compile the examples from the SSL tutorial you will need to modify the makefile.

Deliverables:

1. Source code for your project, signed off by your tutor to prove (2). 20
2. A demonstration of your project. 20
3. Your project displays the steps of, and outcomes of the certificate validation and cipher selection. 10
4. Demonstration against a standard web browser 10
5. A report (around 1500 words expected, 4000 words absolute maximum)
 - a. The issues and problems you have encountered in implementing your application. In particular you should explain how you created your certificate chain 10
 - b. A detailed explanation of how SSL/TLS technology works. This should pay particular attention to ciphers, key negotiation and the use of certificates. 30

References:

Thomas, S A; *“SSL & TLS Essentials: Securing the Web”*, Wiley 2000

Rescorla, E; *“An Introduction to openssl programming”*, RTFM Inc. (available from module web page)