Assignment 1 Specification

Course: Masters in Engineering MIOT BN535M

Module Code: H6016

Module Title: Secure Communications

Email: francis.long@itb.ie

Lecturer's name: Francis Long

Latest date for Submission:

Date Assignment given out: 13/2/19
Report: 0.01am Wednesday April 10th 2019, Demonstrations 10th April 2019

% of total CA marks allocated: 20% **Max Group Size 3 (group project)**

General Requirements for Students:

1. A proportion of assessment marks is allocated to presentation. All assignment scripts must be word-processed, where appropriate.
2. Assignment scripts must be submitted via link on Moodle. Email submissions will not be accepted.
3. All relevant provisions of the Assessment Regulations must be complied with.
   Penalties for late submission of assignments are as follows:

   20 % per day penalty for assignments submitted after the deadline.

4. Extensions to assignment submission deadlines will only be granted in exceptional circumstances only. The appropriate "Application for Extension" form must be used and supporting documentation (e.g. medical certificate signed by a medical doctor) must be attached. Applications for extensions should be made directly to the Programme Leader **in advance** of the deadline date.
5. Assignments that exceed the word count by up to 1000 words will not be penalised.
6. Students are required to refer to the assessment regulations in their Student Guides and on the Student Website.
7. TU Dublin ITB / Blanchardstown penalises students who engage in academic impropriety (i.e. plagiarism, collusion and/or copying). Please refer to the attached referencing guidelines for information on correct referencing.

Secure Communications, BN555M Full Time

Secure Communications H6016	
Assignment 1	
Value	20%
Group Project	Group (max 3)
Assignment date	13/2/2019
Assignment Due	Report: 0.01am Wed April 10th 2019 Demonstration: Wed April 10th 2019
Deliverables	1.Report 1.Demonstration 5 min

Network communications by default are not secure and are vulnerable on a number of levels.

For this assignment you are asked to research report and demonstrate secure communications on a network. Identify vulnerabilities and ways to exploit those vulnerabilities as network traffic such as email, ftp, http etc crosses a network. Follow this up by identifying and implementing techniques and technologies to mitigate against those exploits, and then test the defence mechanisms.

Deliverables:

Set up a client-server system (s) (no marks for this).

For the report you must examine three communication vulnerabilities, such as man-in-the-middle, arp poisoning, arp flooding etc, wired, wireless (WPA etc.). Here is a list to choose from.

ARP Poisoning
WPA Wireless Cracking
MAC Flooding
Session Cookie Hijacking
Any Man in The Middle Attack
Denial of Service Attack

For the live demonstration, only one vulnerability need be demonstrated (not arp poisoning). The live demonstration must include a mitigation technique.

In the report and the demonstration you must include steps you have taken to mitigate against vulnerabilities, and demonstrate how you can attack the defences (encryption, switch security, anti-mitm, certificates etc.)

Write a report on your research and findings (approx. 6000 words (one report per team)). Report should be written in an academic style, and full referenced using the Harvard referencing system. This will be submitted via Turnitin, and should follow the usual rules for plagiarism (submission link to follow).

Submission will be via TurnItIn (link available later).

The usual rules on plagiarism apply and any plagiarism will result in a grade of zero. Late submissions are subject to a daily penalty of 20%. Your attention is drawn to ITB's Plagiarism Policy Guidebook, available on Moodle. This covers cheating, attempts to cheat, plagiarism, collusion and any other attempts to gain an unfair advantage in assessments. The work you submit must conform to those regulations.

Marking Scheme

Assessment Criteria	**% weighting for each problem part**
Research and review of issues and solutions for secure communications on wired and wireless networks.	20%
Effective research and implementation of these attacks and solutions, demonstrating a full understanding of both attacks and defences.	30%
Extra relevant research/context	10%
Balanced, well-thought-out and original conclusions/effective understanding and demonstration	20%
Proper references	10%
Overall quality of report	10%
(Total)	100%