Advanced Computer Security Final  
Blowfish Lab (W2013)

**DUE: Friday, April 26th 11:59pm EST in the Angel Dropbox**

**Note: This Final Exam requires students to work alone.**

Overview

This take-home final exam provides students a chance to implement a known and trusted security algorithm (Blowfish) into a network security scenario. The task is to create your own, small, instant messaging solution whereby 2 instances communicate with each other over the network, with and without blowfish encryption activated. Network packet analysis tools are then used to capture packets and reveal their contents.

Scenario and Requirements

You have been tasked with setting up a small demonstration lab that will show unencrypted messages being sent between two computers on the same LAN. Using TCP, the payload of your messages will be visible, unless some effort is taken to encrypt them. You will code a small, instant messaging application that will communicate via TCP between two hosts on a LAN. This application must meet the following requirements:

1) Users can send short messages to each other

2) Encryption of the messages must be optional. This is to assist you in demonstrating that the payload being sent in the clear or encrypted on an as-needed basis.

3) IM application uses TCP to send character data (user messages) between hosts. The messages being sent over the network will be sent in the clear (no encryption) or encrypted, at the option of the user.

4) If an IM client receives an encrypted message, it must be displayed to the user as both the encrypted string and the decrypted string, so that the user might compare messages being sent between IM clients.

5) Your IM application must implement Bruce Schneier's Blowfish Encryption Algorithm. Although this algorithm has been improved upon via more evolved implementations/evolutions, it is still quite strong by today's standards, and is suitable for our purposes. <http://www.schneier.com/blowfish.html> is the place to start.

6) Your IM client application should have some method for tracking the resources it takes to encrypt a string of text using the Blowfish algorithm, and must display this metric. This might be something like CPU time/clock cycles, as an example.

In addition to creating this small IM application, you need to be able to intercept and inspect TCP packets to see if the message being sent is encrypted or in the clear. How you achieve this is up to you. You might code your own small 'interceptor' application; you could use Wireshark, or even scour BackTrack Linux for tools to help you out.

# Your deliverables

Create a lab document that will walk the reader through the use of your IM application, and your chosen 'interceptor' method. The audience of the document will use it to setup your IM application in a small LAN environment, and test the effect of using the Blowfish encryption algorithms. A sample 'structure' to the document might look like this:

1) Setup of the IM clients

-testing the IM clients can communicate to each other

2) Setup the packet inspection/interceptor

3) Clear Text Intercept Test

- Test that you can successfully investigate the TCP payload and confirm the message being sent to/from a specific IM client, with no encryption being used.

4) Encrypted Message Intercept Test

- Test that you can successfully investigate the TCP payload and confirm the message being sent to/from a specific IM client, with encryption being used. Does the TCP payload content match the encrypted string for the message?

5) Review Metrics

- Have the reader examine the differential in time it takes (if any is detected) to encrypt and decrypt messages.

## What to Hand In:

Via Angel drop box, in a zip file, please provide:

* Your working, well commented, IM application solution
* Custom interceptor app if you wrote one, otherwise, links to the tool needed to run your lab must be provided in your...
* Lab document. This should be a professional looking/reading document; well formatted, with supporting screen shots (as an example) to demonstrate your tests.

## Marking Guidelines

Effectiveness of your IM application (Meets the requirements) - 40 pts

Quality of your ‘lab book’ (e.g. Setup is clear; testing instructions effective, etc) - 45 pts

Effective Communications Skill (grammar, spelling, etc) - 15 pts