CEN5515/4406 Network Security Project

**Title**: Assigned Project: Secure Instant Point-to-Point (P2P) Messaging

**Group Members:** Tao Ma, Dillon Prendergast

**Description**: In this project, you need to design a secure instant messaging tool for Alice and Bob (like gtalk, skype or icq chat). The system supports the following functions

• Alice and Bob can use the tool to send instant messages to each other.

• Alice and Bob share the same password (or passphrase), they must use the password to set up the tool to correctly encrypt and decrypt messages shared between each other.

• Each message during Internet transmission must be encrypted using a 56-bit key

**Design Questions:**

**With a 56-bit key, what cipher you should use?**

DES uses 56-bit encryption so it would make sense to use a variant of DES.

**DONOT directly use the password as the key, how can you generate the same key between Alice and Bob to encrypt messages?**

PBKDF2, Password-Based Key Derivation Function 2, was created to generate a key using a password for PKCS#5.

DK = PBKDF2(PRF, Password, Salt, c, dkLen)

* *PRF* is a pseudorandom function of two parameters with output length *hLen* (e.g., a keyed HMAC)
* *Password* is the master password from which a derived key is generated
* *Salt* is a sequence of bits, known as a cryptographic salt
* *c* is the number of iterations desired
* *dkLen* is the desired bit-length of the derived key
* *DK* is the generated derived key

This allows the password to be used for password generation without the encryption/decryption to be clear by knowing only the password due to the use of a salt. It is also compatible for 56-bit keys in DES and capable of running 1000s of iterations quickly and is used in WPA2.

**What will be used for padding?**

PKCS#5 padding scheme pads with each bytes equal to the number of padding bytes. I.e. 4 bytes of padding would be 04 04 04 04. This scheme was created as an 8-block variant of PKCS#7 for DES. This is easy to detect errors in a single byte or padding bytes being lost because the length is apparent in all bytes.

**How should Alice and Bob set up an initial connection and also maintain the connection with each other on the Internet? (You may refer to socket/network programming in a particular computer language)**

With socket programming in python we can open a connection on a constant port that will allow constant listening and transmitting data between Alice and Bob. The messages will pass through the connection as ciphertext only, with encryption/decryption happening on Alice and/or Bob’s end.