CODE REVIEW

1. R KNOUR , MILO “KNEDLICI: DUMPLING”
   * Code not commented
   * No call tracking at server
   * Could not execute chat session.
   * Threads in server for different client connections?

**Problem identification**: C\_1

**Severity:** medium

**Practicability**: Deviation from proposed architecture

**Description of the problem**: Architecture proposed peer to peer communication. But Implementation works through the server.

**Proposed solution** :

**Problem identification**: C\_2

**Severity:** low

**Practicability**: Exhaustion of resources. Easy to exploit unknowingly

**Description of the problem**: Memory leak. Line 665: packethash variable.

**Proposed solution**: Deallocate variable ater use.

**Problem identification**: C\_3

**Severity:** low

**Practicability**: Exhaustion of resources. Easy to exploit by making multiple chat sessions.

**Description of the problem**: Memory leak. Line 147: leak in public function. The pointer 'mAesKey' is not deallocated before it is allocated.

**Proposed solution**: Deallocate variable before allocation if pre allocated.

**Problem identification**: C\_4

**Severity:** high

**Practicability**: Will effect communication operations.

**Description of the problem**: Client waits on input stream. If some other client tries to communicate during the time, it will affect the communication.

**Proposed solution**: Either poll the input stream or wait for it in separate thread. Wait only until some other client initiates a connection.

**Problem identification**: C\_5

**Severity:** high

**Practicability**: Will effect communication operations.

**Description of the problem**: Client terminates after one chat session.

**Proposed solution**: Make persistent client. It should terminate when user asks so.

**Problem identification**: C\_6

**Severity:** high

**Practicability**: Easily exploitable by packet capturing. Replay and Man in middle attacks.

**Description of the problem**: Unencrypted channel for connection establishment

**Proposed solution**: Use secure channel

**Problem identification**: C\_7

**Severity:** low

**Practicability**:

**Description of the problem**: Memory allocation not checked.

**Proposed solution**: Check the value of pointer after memory allocation.

**Problem identification**: C\_8

**Severity:** low

**Practicability**:

**Description of the problem**: Return value of functions not checked

**Proposed solution**: Check the return value of functions.

**Problem identification**: C\_9

**Severity:** low

**Practicability**: Can effect performance of system

**Description of the problem**: No mechanism to ensure uniqueness of client identifier

**Proposed solution**: Unique client identifiers shall be either issued from or verified at a central authority.