Team name	LMMT-SecureDove			
Project topic	SecureDove			
Project repository	https://github.com/LoganKloft/LMMT-SecureDove			
Team members	**Name**	**Email**	**WSU ID**	**Contact**
	Logan Kloft	logan.kloft@wsu.edu	11728076	
	Matthew Gerola	matthew.gerola@wsu.edu	11661224	
	Manjesh Puram	manjeshreddy.puram@wsu.edu	11716685	✓
	Taylor West	taylor.west@wsu.edu	11733958	

SecureDove
Develop an instant messenger that provides secure messaging with explicit confidentiality and integrity defenses (e.g., checking and defeating message hijacking). We will be using a client-server architecture to facilitate multiple clients.

Security Problem:
Messages meant to be private being hijacked and read by somebody else.

I. Initial Security Requirements:

- Messages encrypted
    - Asymmetric Encryption (performed by clients)
- Server resilient to attacks against availability
    - I.e. distributed denial of service

II. Security Goals:

We will strive to incorporate the CIA Triad into our project as we develop our solution.

- **Confidentiality**

This means that we will provide confidentiality by not storing messages sent from one another in a plain text. That way in the case of a message being intercepted, the content of the message will not be learned.

- **Integrity**

For integrity, we will attempt to discover any sort of tampering. Some potential ideas are hashing the messages before sending them and then calculating the hash once again on the other side.

- **Availability**

We don’t plan on handling the case that the server goes down due to a power outage for instance. However, we believe that we can reasonably strive to handle a denial of service attack.

III. Metrics:

How we will measure the success of the project

- Complexity of encryption technique (**Confidentiality**)
- Can we brute force the encrypted messages (**Confidentiality**)
- Add payload to client message and detect whether the other client detects the payload (**Integrity**)
- Put various levels of stress on the server and assess latency of client messages (**Availability**)