NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

School of Computer Science and Engineering
College of Engineering

Demonstration of Attacks on SSL-TLS Protocols

POODLE and CRIME Attacks

Student: Iyer Rajagopal Mahadevan **Supervisor: Dr Kian Boon Tay**

Project Objectives:

Secure Sockets Layer (SSL) which was superseded by Transport Layer Security (TLS) is the most extensively used application of cryptography in the day-to-day life of humanity. It is used to secure communication between two parties across the internet ensuring the principles of identification, authentication, confidentiality, and integrity. Over the last decade there have been multiple attacks on SSL-TLS in order to break the encryption and obtain the sensitive information that was encrypted. Some of these attacks focus on implementation errors, or some inherent feature of SSL-TLS.

This project focuses on two such attacks, ***POODLE*** and ***CRIME*** and we will dive deep into following aspects:
Feature of SSL-TLS that is exploited.
How is it exploited (Theory)?
How is it exploited (Proof-of-Concept)?
What is the impact of this attack?
What are some strategies to mitigate this attack?