Project: Solution to POODLE SSL Flaw

1 Introduction

The Secure Sockets Layer (SSL) protocol is based on an asymmetric encryption and a symmetric block cipher method. In September 2014, a flaw of SSL 3.0 was disclosed by the Google Security Team. An attacking method, namely Padding Oracle On Downgraded Legacy Encryption (POODLE), successfully catches plaintext encrypted in a Cipher Block Chaining (CBC) mode at the rate of no more than 255 tries per byte provided that one (man-in-the-middle) is able to manipulate the transmission and change the ciphertext at will between the sender and receiver .

2 Problem Statement

In this project, the students are required to present a prototyping two-phase SSL system between the sender and receiver.

In the first (handshake) phase, relying on a public-key cryptosystem, the authentication procedure is able to verify the communicator's identities and exchange the encryption key of the symmetric block cipher in the second phase. The RSA algorithm is chosen and implemented in this public-key cryptosystem. A possible implementation of the authentication procedure can be based on a one-way function, such as the HASH algorithm. The authentication procedure is required to be immune against the dictionary attack and the replay attack.

In the second (symmetric block cipher) phase, the plaintext is encrypted in a CBC mode by using the DES algorithm. The symmetric encryption procedure is required to be immune against the POODLE attack. Find out what is the Padding Oracle Attack first.

Demonstrate your system via a technical report. Proper commenting is important, as well as applying good English writing practices.

3 Deliverables

The project must be carried out in groups of not more than 2 students. Each group member must hand in an individual report. You will be assessed on the following deliverables:

1. A complete technical report that contains the following:
    - A detailed description of your implementation (diagrams, descriptions, etc.), why a particular approach was taken, the limitations as well as advantages and disadvantages of the chosen approach.
    - Discuss how to defend your cryptosystem from the POODLE attack.
    - Discuss how to defend your cryptosystem from the dictionary attack and the replay attack on the authentication procedure.
    - Problems in the design and implementation.
    - An appendix detailing the division of work between team members, the milestones used to manage the project and a signed-off section, by both team members, of the work division.

4 Hand in details

Assessment comprises a written report. The deadline for the report is on the 25th of August.

5 Assessment

- 50% for the report.
- 50% for the success of the design, which is determined as follows:
  - 10% Implementation of a public-key cryptosystem based on the RSA algorithm.
  - 5% Implementation of a symmetric cryptosystem based on DES.
  - 5% Implementation of the CBC mode.
  - 10% The cryptosystem is immune against the POODLE attack.
  - 10% Implementation of an authentication procedure based on the HASH algorithm.
  - 5% The authentication procedure is immune against the dictionary attack.
  - 5% The authentication procedure is immune against the replay attack.

6 Plagiarism

The report is an individual effort, equivalent to an exam; so if there is the slightest indication of copied or plagiarised work all parties, i.e. the offender and supplier of information, will be given zero and reported to the University Disciplinary Committee.