Mini-Project Security Analysis

Prof.-Dr. Volker Roth

February 17, 2012

Purpose

The task is to analyze the cryptographic strength and the implementation robustness of the chat programs implemented in the course of the previous mini-project.

Rules

There are two ways to earn points:

1. Submit a report that succinctly proves or demonstrates a vulnerability in a chat program implementation.
2. Submit a response that confirms or disproves a vulnerability report.

However, there are a few rules to obey:

Rule 1: No one can submit an analysis for his or her own chat client.

Rule 2: Only the first report of a vulnerability counts.

Rule 3: Only the first valid response to a vulnerability report counts.

Rule 4: In order to claim points, the report or response must be presented in class.

The following counts as a vulnerability report:

- A proof that the cryptographic protocol implemented by a chat client is insecure in the EAV/CPA/CCA indistinguishability model. If the proof requires oracle access then it must be shown that a remote chat client can be abused as an oracle.
- A convincing argument that the chat client can be crashed remotely by another client, best accompanied by a documented script or tool that reliably crashes a chat client remotely.

Scoring

- Each team that submits a valid vulnerability report scores 10 points. A vulnerability report is valid if someone else submits a response to it that confirms the vulnerability.
- Each team that submits a response and confirms a vulnerability scores 5 points.
- The highest scoring team receives 10 extra points.

Submission Format

All reports must be submitted in PDF. They should be sent by e-mail to the referee with the subject line prefix [SECANALYSIS]. The e-mail can contain attachments with a demonstration script or tool (keep it simple).

Submissions which do not follow the rules and formats mentioned above may not be counted.