Dissertação de Mestrado em Engenharia Informática (2017/2018)

Title

Protocols for Encrypted e-Mail

Supervisor: Prof. Paul Crocker

Email: crocker@di.ubi.pt

Description

End to end security has been popularized for instant messaging applications such as WhatsApp. Secure E-mail systems however are still largely based on traditional encryption technologies such as S/MIME and OpenPGP. These traditional systems lack usability, in the sense of easy and automatic setups. Alternative protocols based where all the necessary steps for key exchange can be taken by the senders and recipients e-mail clients automatically, without the need for user interaction, are an interesting alternative.

This thesis will survey current and forthcoming technologies such as Key Continuity Management (KCM) or “pretty easy privacy”. The next focus will be on completing and extending an existing protocol for usable secure e-mail communication. The final phase will be be an analysis and evaluation with regard to security, usability and resilience against typical attacks and comparison to the other surveyed solutions.

Work Plan

1 Literature and State of the Art Review

2 Review of existing solutions

3 Review of Microsoft Outlook Development and API’s

4 Implementation and Development of the existing Solution

5 Security Analysis

6 Writing of the Dissertation.