IT University of Copenhagen

(Thesis)

Untitled Thesis Project

Authors:
Ans Uddin anud@itu.dk

Supervisor:
Willard Rafnsson

Co-supervisor:
Carsten Schürmann

February, 2018

Contents

1 Introduction

1.1 Problem Formulation

Matrix is an open standard protocol for messaging over HTTP and synchronizing data. Matrix provides secure real-time communication over a decentralized federated network. Matrix secures data by providing end-to-end encryption. However in the presence of end-to-end encryption, apps can still leak through their application logic; a content-filtering chat bot running at the receiving end of an end-to-end encrypted connection can leak anything it receives from this connection.

Leaks through the application logic can be prevented with Information Flow Control (IFC). IFC prevents leaks by enforcing policies for secure information flow in a program. There exist tools (e.g JIF, Paragon and Fabric) that aid in building software with secure information flow.

1.2 Method

The objective of the project is to do a case study on the security of Matrix, apply IFC tools to improve the Matrix security model and demonstrate the improvements.

A successful project is one that fulfills these criteria:

- Evaluation of Matrix security model
- Survey IFC tools to improve the Matrix security model
- Implement a prototype distributed system running on Matrix, using the chosen tools
- Demonstrate improvements to the Matrix security model

2 Background

3 Method

4 Results

5 Conclusion

Appendices

Bibliography

[1] Website example. `https://google.com`. Accessed: xxxx-xx-xx.

[2] John Doe. *Lorem ipsum*. Unknown, 2018. ISBN 0521865719, 9780521865715.