IT University of Copenhagen

(Thesis)

Information-Flow Secure Programming on Matrix: A Case Study

Authors:
Ans Uddin anud@itu.dk

Supervisor:
Willard Rafnsson

Co-supervisor:
Carsten Schürmann

February, 2018

1 Background

1.1 Information Flow Control

Confidentiality

Integrity

The Lattice Model

Noninterference

Static policies

Dynamic policies

Declassification

Taking some specific information and changing it to a lower security classification.

Identify: What to classify, who declassifies, where the declassification happens and when the declassification happens

1.2 Matrix

Architecture

Client/Server API

End-to-end Encryption

How is E2E managed?

2 Analysis

This chapter consists of two parts. The first part will provide an evaluation of the Matrix security model and relies heavily on the paper *A Formal Security Analysis of the Signal Messaging Protocol.* and a preliminary analysis of the IFC tools and the selected tool.

2.1 Evaluation of Matrix security model

Matrix provides end-to-end encryption by using the Olm library which is an implementation of the Double Ratchet algorithm known from Signal Protocol. As mentioned in xx Matrix uses the Megolm library for group chat which is layered on top of the Olm library. This evaluation will primarily focus on the Double Ratchet algorithm.

By evaluating the Signal Protocol we can derive the same evaluation for Matrix as well.

2.2 Survey of IFC Tools

JIF

Fabric

Paragon

JSFlow

Not possible to use Matrix library with JSFlow because of missing support for libaries such as require (in node). Also overhead with configuring JSFlow to be the interpretor.

Swift, SIF, FlowR, JFlow, LIO

Selection of IFC tool

The selection of the IFC tool used for developing the prototype is based the following defined parameters. The selection of IFC tool put emphasis on the practical usage in combination with Matrix.

Paragon analysis

2.3 Summary

In this chapter the Matrix security model has been evaluated. Matrix provides end-to-end security and uses the Double Ratchet algorithm by Signal. The evaluation found that there are no major flaws in the design. To achieve end-to-end security the endpoints need to be secured as well [13] this leads us to the chapter's second part. The chapter analyzed information-flow control tools and justifies the selection of Paragon which the prototype is programmed in.

Bibliography

[1] Op imod 90.000 ansatte kan kigge i din journal - Indland. URL `https://jyllands-posten.dk/indland/ECE6715461/op-imod-90000-ansatte-kan-kigge-i-din-journal/`.

[2] Adgang til sundhedsdata - sundhed.dk. URL `https://www.sundhed.dk/borger/service/om-sundheddk/om-portalen/datasikkerhed/andres-dataadgang/adgang-til-sundhedsdata/`.

[3] CWE - CWE-359: Exposure of Private Information ('Privacy Violation') (3.2). URL `https://cwe.mitre.org/data/definitions/359.html`.

[4] Journal fra sygehus. URL `https://www.sundhed.dk/borger/min-side/min-sundhedsjournal/journal-fra-sygehus/`.

[5] Google Plus Will Be Shut Down After User Information Was Exposed - The New York Times. URL `https://www.nytimes.com/2018/10/08/technology/google-plus-security-disclosure.html`.

[6] Kontrol af opslag - sundhed.dk. URL `https://www.sundhed.dk/borger/service/om-sundheddk/om-portalen/datasikkerhed/portalens-beskyttelse-af-data/kontrol-af-opslag-e-journal/`.

[7] FAQ | Matrix.org. URL `https://matrix.org/docs/guides/faq`.

[8] 91,000 state Medicaid clients warned of data breach | The Seattle Times. URL `https://www.seattletimes.com/seattle-news/health/91000-state-medicaid-clients-warned-of-data-breach/`.

[9] Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila. A Formal Security Analysis of the Signal Messaging Protocol. *Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017*, (November):451–466, 2017. ISSN 13484214. doi: 10.1109/EuroSP.2017.27.

[10] Laurinda B. Harman, Cathy A. Flite, and Kesa Bond. Electronic Health Records: Privacy, Confidentiality, and Security. *Virtual Mentor*, 14(9):712–719, sep 2012. ISSN 1937-7010. doi: 10.1001/virtualmentor.2012.14.9.stas1-1209. URL `http://virtualmentor.ama-assn.org/2012/09/stas1-1209.html`.

[11] P. D. Pacey and J. H. Purnell. OWASP Top 10 - 2017. *International Journal of Chemical Kinetics*, 4(6):657–666, 1972. ISSN 10974601. doi: 10.1002/kin.550040606.

[12] Fiza Abdul Rahim, Zuraini Ismail, and Ganthan Narayana Samy. Information privacy concerns in electronic healthcare records: A systematic literature review. In *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, pages 504–509. IEEE, nov 2013. ISBN 978-1-4799-2487-5. doi: 10.1109/ICRIIS.2013.6716760. URL `http://ieeexplore.ieee.org/document/6716760/`.

[13] Andrei Sabelfeld and Andrew C. Myers. Language-based information-flow security. *IEEE Journal on Selected Areas in Communications*, 21(1):5–19, 2003. ISSN 07338716. doi: 10.1109/JSAC.2002.806121.

[14] The Government, Local Government Denmark, and Danish Regions. *The Digital Strategy - A stronger and more secure digital Denmark*. Agency for Digitisation, 2016. ISBN 9789400769250 | 9400769245 | 9789400769243. doi: 10.1007/978-94-007-6925-0_9. URL `https://en.digst.dk/media/14143/ds{_}singlepage{_}uk{_}web.pdf`.