Authorization Aspects of the Distributed Dataflow-oriented IoT Framework Calvin

Tomas Nilsson, *Faculty of Engineering at Lund University* *June 2016*

Many applications benefit from using several devices at the same time for the execution. As a device owner you want to be able to control who is allowed to access your device. As a user you want your application to move to other devices if access is denied. The framework Calvin will handle it all for you!

People talk a lot about the *Internet of Things* (IoT), where everything that can benefit from a connection will be connected. This is expected to largely influence everyday life and opens up many opportunities for creating smart products and applications that dynamically adapt to the current environment.

Calvin simplifies distributed applications

The open-source framework *Calvin*, developed by Ericsson Research, simplifies the development of so-called *distributed applications*, where different parts of the application are executed on different devices. It can for example be a tiny IoT device which sends sensor data to a more powerful device where the data is processed in some way. Such distributed applications may be complex to write, but Calvin will help you.

A Calvin application uses building blocks called *actors*, which perform certain tasks. You create an application by defining how data flows between different actors. When an application starts it is not always decided on which devices the application will execute. Calvin can move, or *migrate*, parts of the application to other devices without interrupting the execution.

Calvin handles the difficulties of transporting data between different devices and creates the illusion that the application is running on a single device when it is in fact running on multiple devices. For an application developer it is therefore as easy to develop a distributed Calvin application as developing a regular application which runs on a single device.

Access control based on attributes

A device owner usually wants to only allow some users or applications access to the device. The focus of this thesis work has been to extend Calvin with authorization functionality, which means controlling who is allowed to access different functionality on devices.

An application started by a specific user may for example be allowed to access some functionality on the device between 8:00 and 17:00 every day if the user is a manager at a certain company and the device is located in the same country as the user. As this example indicates, there may be several attributes involved when you decide if access should be permitted or not.

The authorization framework that has been added to Calvin enables access decisions based on many different attributes about the user, the application, the device, and the current environment. Policy rules are evaluated against attributes to get an access decision.

The solution is very flexible and compact to make it suitable to a wide variety of devices. Access control can be performed locally on the same device, but it is also possible to let another device make the decisions on behalf of devices that are not able to handle access control on their own.

Migrate when access is denied

If access only is given until a certain time of the day, Calvin will try to migrate the denied part of the application to another device when the access permission expires. It is migrated to a device where access is permitted, if such a device exists, so it can continue running. Everything is handled automatically by Calvin. The user does not need to change anything or stop the application.

This feature, and all the other parts of the implemented authorization framework, is available on Github as part of the Calvin project. Download the code from `https://github.com/EricssonResearch/calvin-base` and test all the benefits that Calvin offers.