ELECTRICAL AND INFORMATION TECHNOLOGY | FACULTY OF ENGINEERING | PRESENTED 2023-06-21

THESIS WORK Profile Based Access Control Model Using JSON Web Tokens
STUDENTS Mustafa Albayati, Aslan Murjan
SUPERVISOR Ben Smeets (LTH)
EXAMINER Thomas Johansson (LTH)

Access control for complex Internet Of Things (IoT) networks

POPULAR SCIENTIFIC SUMMARY **Mustafa Albayati, Aslan Murjan**

With advances in computing technologies, IoT devices can be more capable than ever. Some of these devices offer advanced functionalities and run complete operating systems, not very different from the one you are using right now. This thesis work addresses the access control challenges surrounding a large network of such devices.

Access control is a mechanism that regulates who or what can view or use resources in a computing environment. Role Based Access Control (RBAC) is one of the simplest access control solutions, where a user is associated with one or more roles that specify the type of user he/she is. It's widely used for it's simplicity. The roles can be anything. You as a student, teacher, parent, child have roles of your own, with your own rights and limitations. Roles in a computing environment similarly define the users rights and limitations on the device. This is a very straight forward approach. A user is added to a device and given a role. However, as the capabilities of the device increase and the use cases get more and more complex, the generalization of roles are rendered insufficient. A student can tutor their friends and a teacher keeps on learning. Just like life, access control is not always black or white.

For our solution, we started with moving the user out of the device. In a large network, it's not practical to add and manage users on each individual device. A central server was put in place to handle user identities. Next, we replaced roles with profiles that can better address the individuality of the user. These profiles are also placed on a central server and provide a fine grained definition of what a user is allowed to do on the device. The profiles were designed from a user first mindset. Giving the system administrator the opportunity to customize permissions based on the needs of the user. By removing the user and the access definitions out of the device, they can be managed on the go and let the device act as a passive receiver of instructions, without prior knowledge. Furthermore, when a user wants to perform a task on the device, he/she first send a request which the device checks against the profile in order to determine if the requested task is valid and then creates a ticket representing that task. Just like in the cinema, a ticket can only be used once for a single movie. This approach narrows down what is allowed to be done on the device at any given time, by only allowing single, authorized, tasks.

To finish the cinema metaphor, the entire system can be summarized as following. You want to watch the new blockbuster movie and go online to book a ticket. Days go by and it's finally the big day. You identify yourself at the counter (the device) where the booking is confirmed through the knowledge from the booking system (the server). Now with your ticket in the hand, you can enter the theater (the service) and enjoy the movie.