Poster: WebMaDa 2.0 - Automated Handling of User Requests

Corinna Schmitt, Dominik Bünzli, Burkhard Stiller
Communication Systems Group CSG, Department of Informatics IfI, University of Zurich UZH
Binzmühlestrasse 14, CH-8050 Zurich, Switzerland
[schmitt|stiller]@ifi.uzh.ch, dominik.buenzli@uzh.ch

***Abstract*—Today users want to monitor their networks remotely and adjust privileges immediately. Addressing the first request is not a big problem anymore, because many applications offer such solutions by default (e.g., via a special app to be installed or a browser-based solution). The immediate privilege handling is the challenge nowadays, because usually a global administrator in the background needs to be included in the workflow. This is required, because he is the only person who has the full overview of the tool the network is included. In general this is a nice idea, but introduces delays to the privilege management depending of the number of networks linked to the system, in total. WebMaDa 2.0 overcomes this bottleneck by introducing an automated request handling solution to a web-based framework for monitoring sensor networks remotely as well as supporting privacy and immediate handling of privilege requests.**

***Keywords*- WebMaDa, automation**

I. Introduction

Today, many different devices are connected with each other building small networks that are part of the Internet of Things (IoT). Such networks are designed for individual solutions specialized for a specific purpose (e.g., environmental monitoring, health monitoring). Devices used show heterogeneity concerning hardware and software and are linked to a specialized solution allowing analysis and visualization of data collected. This itself is nothing really new within the IoT community. But the requests of users and network owners changed over time towards (1) mobility support, (2) ownership and controlling of data, as well as (3) updating granted privileges immediately.

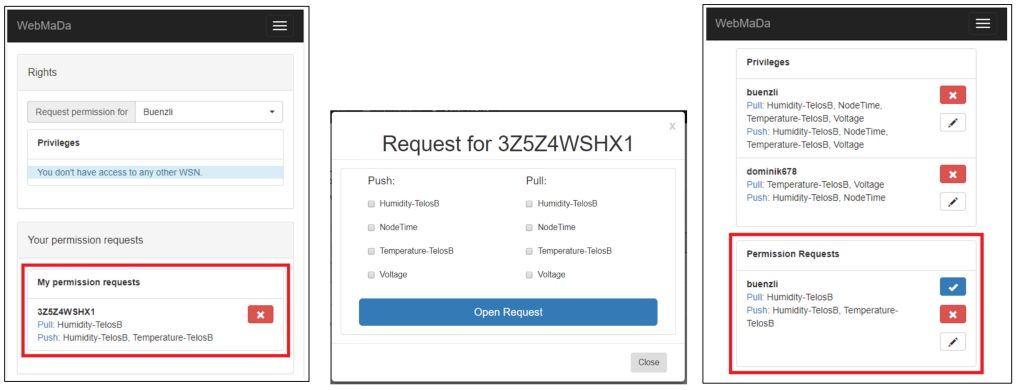
Many specific solutions are in place addressing the mobility request installing a special application on the mobile device. In general this is a good solution, but these solutions usually have special requirements to the operating system of the device and can exhaust the device quickly when running. The later can be overcome by integrating energy saving solutions, but still the applications require much memory of the device. To overcome this, web-based solutions are thought of beeing most suitable, because they only require Internet access and a browser installation on the device. Fortunately, both can be considered to be available by default on mobile devices. Furthermore, the code base only has to be updated in one place, thus reducing the cost for maintenance. The urge for control and ownership of the collected data is manifesting itself more and more in the minds of users. This is due to increased media coverage of data abuse caused by data leaks and the possibility of having data analyzed and visualized by third-party providers. Together with this situation comes the users' request to update granted privileges to manage access to the data collected. This is challenging, because access granted to applications can hardly be revoked or updated immediately if at all. Thus, the call for solutions supporting data and access control immediately arise. The aforementioned three issues (1)-(3) are addressed by WebMaDa, a Web-based Management and Data Handling Framework for sensor networks. The development started in 2014 with a basic support of mobile access to owned sensor networks allowing visualization of collected data in a flexible and hardware independent manner [2]. In 2016 WebMaDa received an update addressing the general request of fine-grained access management and pulling data in emergency cases [3]. The drawback was that each request (e.g., create networks, access to foreign networks, to view or pull data) required interaction of a global administrator introducing delay into the system. This drawback has now been solved in WebMaDa 2.0 [1] by automating the request handling within the system allowing immediate handling without the involvement of a global administrator. At the same time, the request for privacy and controlling data access is respected as every action that affects access rights is logged in the database.

In Section II, the main design decisions taken are presented leading towards the implemented WebMaDa 2.0 solution. Section III summarizes the new features of WebMaDa 2.0 highlighting the benefits and practical issues, as well as giving a hint to future improvements.

II. Design and Implementation

In order to handle any request received immediately an automated solution is required. This solution must support (1) user creation, (2) access request to foreign networks, and (3) password reset. Furthermore, for addressing privacy and controlling of the data (4) transparency must be assured by including a detailed logging system into the infrastructure.

Addressing the first three requests an automated mailing solution was integrated into WebMaDa 2.0. If a new user wants to use WebMaDa he needs to register by filling out the registration form. By submitting the form, the user creates an invitation request that is stored in the database. At the



(a) Requestor view (b) For for requesting access to data (c) Network owner's view of pending request

Figure 1: Graphical views during data access request

same time, the administrators receive a notification that a new request has been created. If the request is accepted by the administrators the user will receive an invitation which can be used to complete the registration. Otherwise, a message will be sent informing that the request has been rejected. After this, the user is able to create new networks or request access to foreign networks when not yet having permission as shown in Figure 1a. The latter is done by creating a permission request filling out a form (cf. Figure 1b). The form is received by the backend. Here a mapping between the selected network by the unique WSN Identifier (ID) and the stored owner address is performed resulting in mailing the request to him. The owner receives a mail with the request and a personalized link to handle it within WebMaDa (cf. Figure 1c). The owner can now grant the access, update the request or deny it. In return, the requester receives the result andl a log entry is created in the backend's database addressing the transparency request. Same procedure is followed if after time the network owner updates granted privileges. In case a registered WebMaDa user looses the password, a request can be placed via the corresponding form. The filled in data of the form is then compared to the logged entries in the database. If the check fails, no action is performed as not to provide a single bit of information wheter a user exists or not. Otherwise, the user receives a link to reset the password. In order to ensure transparency, the updating of a password also triggers the creation of a log entry.

III. Summary, Practical Issues, and Benefits

WebMaDa 2.0 supports the original functionality developed in 2014 and 2016. This is extended by an automated mailing solution to handle incoming requests immediately and, thus, reducing delays in the system each time an administrator interaction was required in earlier versions.
The designed and implemented solution is user-friendly due to its intuitive design in the graphical environment including easy understandable instruction to conclude the workflow (e.g., request data access, register new user). All steps are following a global process starting with a form that need to be filled out with respective information required, checkup with stored information if applicable, and updating database with new information (e.g., new user information, new networks, granted/updated/revoked privileges). In order to address the general privacy request of users the administrator is only involved when new users are registered or an existing WebMaDa user should become administrator of WebMaDa for the case the original administrator needs a representative. Addressing the transparency concerns of users, any changes are logged within the database with required information (e.g., timestamp, what was done and by whom). All this logging information can only be accessed by the network owner or the global administrator.
Looking from a practical perspective all user requests are addressed within WebMaDa without having drawbacks on performance of WebMaDa assuming several networks hosted at the same time. Due to the fact that WebMaDa 2.0 is still web-based, no new special requirements to the mobile device exist and the solution is still hardware and software independent.
Further developments are conceivable with regard to session timeout similar to banking systems, two-way authentication besides mailing using SMS, and further flexibility in visualizing data collected.

References

[1] D. Buenzli, "Efficient and User-friendly Handling of Access Requests in WebMaDa," Bachelor Thesis, Communication Systems Group, Department of Informatics, University of Zurich, Zurich, Switzerland, Jan. 2018.

[2] M. Keller, "Design and Implementation of a Mobile App to Access and Manage Wireless Sensor Networks," Master Thesis, Communication Systems Group, Department of Informatics, University of Zurich, Zurich, Switzerland, Nov. 2014.

[3] C. Schmitt, C. Anliker, and B. Stiller, "Pull Support for IoT Applications Using Mobile Access Framework WebMaDa," in *IEEE 3rd World Forum on Internet of Things (WF-IoT)*. New York, NY, USA: IEEE, Dec. 2016, pp. 377–382.