Device specific credentials to protect from identity theft in Eduroam

Bernd Decker[1], Marius Politze[2], Ramona Renner[3]

[1] IT Center RWTH Aachen University, Seffenter Weg 23, 52074 Aachen, decker@itc.rwth-aachen.de
[2] IT Center RWTH Aachen University, Seffenter Weg 23, 52074 Aachen, politze@itc.rwth-aachen.de
[3] IT Center RWTH Aachen University, Seffenter Weg 23, 52074 Aachen, renner@itc.rwth-aachen.de

Keywords
Eduroam, OAuth2, SaaS, Security

1. ABSTRACT

To reduce the impact of security vulnerabilities of Eduroam the Eduroam Device Management was implemented at RWTH Aachen University. The service allows to create device specific credentials to be used as credentials when connecting to the Eduroam network. Users can create credentials, get an overview of their credentials already created and can disable network access for each device individually via a web interface. A first device manager was developed for users of RWTH Aachen, the current implementation considers the creation of device specific credentials and supporting processes for other universities within a federation.

2. Introduction

New trends like the Internet of Things, Wearables and BYOD pose new challenges to existing IT infrastructure and applications. Especially the increasing amount and heterogeneity of devices demands changes on existing IT systems. Further degrees of automation are required to successfully operate existing IT infrastructure and applications. Eduroam allows students and researchers to access the network at their home as well as remote institutions and therefore forms a basis for many of the services offered at the university.

Consequently, in the past years the number of devices accessing the internet using Eduroam increased steadily. Not only do more users access the network but also the number of devices used is inclining. The wide spread of mobile devices results in students and academic staff owning more than two devices on average, that can use Eduroam. To reduce the impact of security vulnerabilities of Eduroam discussed in (Bunsen, 2016) the creation of device based credentials for Eduroam was also implemented on the infrastructure for secure access to personalized data (Politze & Decker, 2014). Eduroam credentials can be retrieved using a man in the middle attack. The main risk of the identity theft originates from the fact that Eduroam credentials are mostly the same credentials as for other university services. For example e-mail or the campus management system, which are therefore also affected by the security issue in Eduroam. To reduce the risk of identity theft, the credentials are randomly generated per device and are not changeable by the user. Therefore it is guaranteed that they are not usable to access other university services. Even though the generation of credentials and set up of Eduroam on the device currently requires several manual steps the service endpoints to generate device based credentials have been added to the infrastructure for mobile services. This allows in a future version to automate the setup process using an app directly on the mobile phone.

3. Current State

RWTH Aachen University offers a device credentials generator for its members. A web based application that allows students and staff to create unique login names and passwords for each of their devices using only a web browser. Of course this has to be done before accessing the Eduroam network. However, there are several options to generate credentials: for example, the students can use their

mobile phones internet access or can even generate their credentials at counters of the IT-ServiceDesk found in several places around the university.

The application uses the web service infrastructure described in (Politze, Schaffert, & Decker, 2016) and uses OAuth2 (Hardt, 2012) to manage which applications have an authorization to create Eduroam credentials for the user. This on the one hand allows users to gain more control over which application is accessing their data and on the other hand allows easier replacement of the components used such as user interface or backend services.

Accounts created are intended to be used only on a single device and are completely randomly generated. In the backend systems however the associated user accounts are saved. While this cannot prevent an attacker from getting the Eduroam credentials, these credentials cannot be related to any users' personal data. This does not solve the initial problem of the man in the middle attack described in (Brenza, Pawlowski, & Pöpper, 2015) but reduces the impact on other university services if credentials have been hijacked.

Furthermore, users get an overview of the credentials and devices already created and can, in case of selling or losing the device, disable Eduroam network access by removing only the device-specific credentials from their account.

One Problem that was raised during the first phase of the project was a lack of understanding of the impact of the security problem on the part of users. Another problem was that users found the user interface presented not very intuitive. These two problems compared to just entering the users' credentials when connecting to the network led to confusion and dissatisfaction for the users that already knew the previous login process. To encounter these issues, the user experience was reworked and more value is added by presenting additional usage information to the user in the current implementation of the device manager application.

4. Federated Device Management

While the first approach of the device manager was only intended for users of RWTH Aachen University, the current implementation considers offering the creation of device-specific credentials for Eduroam for other universities within a federation. This is achieved by extending the current infrastructure but also by using means that are already being used by federations such as the DFN AAI (DFN e.V., 2017). The device manager can then be offered as a software as a service to other institutions within the federation.

To comply with this requirement several extensions to the current process have to be defined which could previously be handled internally. The main issues addressed are the lifecycle of created logins and the ability for local administrators or help desks to support their users when using a federated Eduroam device management service (Grzemski & Hengstebeck, 2017).

Lifecycle management is done in three different stages: (1) when the user logs in, the identity provider presents a unique user id and a flag telling the service if the user is eligible to use Eduroam. This is usually the case for students or employees who are able to login but not for alumni who may retain their login after graduation or guests. (2) After six months without activity, the created Eudroam passwords are cleared. This is done to comply with the usual semester based organization that many academic institutions follow. (3) If more fine granular control is desired passwords have to be kept alive by the participating organization. This is performed using a white list containing all user ids that are currently eligible to access the network.

To enable local support for the users the supporting organs of the participating organization need access to some of the information logged when using Eduroam. From the experiences of the IT-ServiceDesk at RWTH Aachen University it was clear that especially the information logged during authentication of the user in the Eduroam network are crucial for support. Participating organizations therefore get access to current authorization logs of their users allowing them to trace login problems for example caused by misspelled passwords, wrong settings on the client or network abuse. This functionality is also provided as a web application.

5. Further Enhancements

In order to raise acceptance of the users to perform the additional steps to connect to Eduroam, the user experience should be as satisfying as possible. Apart from the gain in security the users should be provided additional value when using Eduroam device credentials when compared to signing in with their user credentials.

The newly created web interface, as shown in Figure 1, is supposed to be easy to use. It offers creation as well as management of existing devices and short explanations on how to set up Eduroam on the device. After login, the user is able to create new device credentials or set a new password to an existing device account with three clicks. The interface was created with mobile access in mind, such that creation of new devices is easily possible using smartphones and using mobile network.

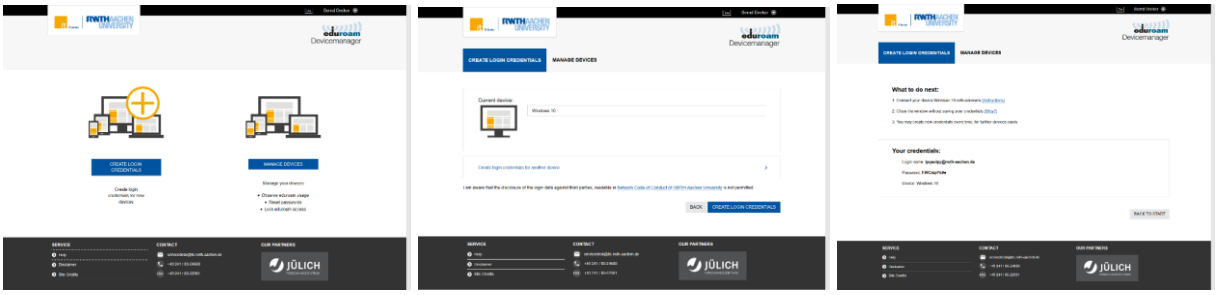

Figure 1: Three clicks to create a device-specific account

Additionally, to the reworked user interface the user is now offered to view a history of the login attempts of the device. This is similar to the information presented in support scenarios but is extended by some personal information like the approximate location during login. In contrast to the support cases, the data presented to the user is extracted from the accounting logs and is preserved for 14 days. During this time historic data can be viewed by the user. Afterwards the data is anonymized and deleted after 30 days.

The login information for each device provides additional value to the user when using the device management. Users may individually check why their device is currently not connecting to Eduroam or can check where their device has been used. In case of irregularities that would also occur when the password was hijacked, the users are able to react by resetting the compromised passwords. Figure 2 shows the data presented to the users in this step.

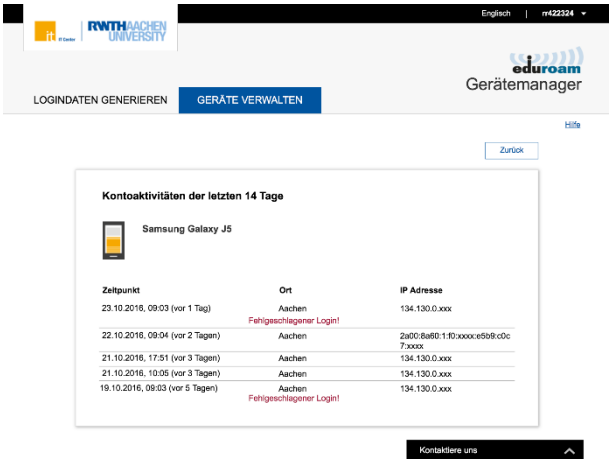

Figure 2: Overview of current devices

6. Future Work

Especially on mobile platforms a relatively slow internet connection is available using the mobile network. Using the current SOA, an Eduroam setup application would need to transfer only few kilobytes of data to create a new account. This would make it easier to connect new devices to Eduroam. Furthermore, this would also allow to automatically configure the current device. Depending on the target platform, the process of configuring the network settings on the devices is very different. Maintaining a multitude of different applications would pose an additional challenge on the overall project. Platforms for which this kind of applications are offered therefore have to be selected carefully.

Currently the Eduroam Device Manager is running at RWTH Aachen will be rolled at Jülich Super Computing Centre as a project partner. A pilot phase is used to gain more insights into running the software as a service which will then be used to further enhance the service. Afterwards the service will be made available for other cooperating institutions.

7. REFERENCES

Brenza, S., Pawlowski, A., & Pöpper, C. (2015). A practical investigation of identity theft vulnerabilities in Eduroam.

Bunsen, G. (2016). Eingrenzung von Risiken durch Diebstahl von EduroamCredentials. In P. Müller, B. Neumair, H. Reiser, & G. Dreo, *9. DFN-Forum Kommunikationstechnologien* (pp. 107–113). Bonn: Gesellschaft für Informatik e.V. (GI).

DFN e.V. (2017). *DFN-AAI - Authentifikations- und Autorisierungs-Infrastruktur*. Retrieved March 16, 2017, from https://www.aai.dfn.de/

Grzemski, S., & Hengstebeck, I. (2017). Future challenges for quality-assured IT support through cooperative structures.

Hardt, D. (2012). *The OAuth 2.0 Authorization Framework*. RFC Editor.

Politze, M., & Decker, B. (2014). RWTHApp: from a requirements analysis to a service oriented architecture for secure mobile access to personalized data. Umea.

Politze, M., Schaffert, S., & Decker, B. (2016). A secure infrastructure for mobile blended learning applications. In J. Bergström, *European Journal of Higher Education IT 2016-1*. Umeå.

8. AUTHORS' BIOGRAPHIES

Dipl.-Inform. Bernd Decker is deputy division lead of the IT process support division at the IT Center of RWTH Aachen University since 2011. He received his degree in computer science at the RWTH Aachen. From 2006 to 2009 he worked at IT Center as Software Developer and since 2009 as lead of the development team. His work is focused on IT solutions for processes in the field of E-Learning, E-Services and campus management systems.

Marius Politze, M.Sc. is research associate at the IT Center RWTH Aachen University since 2012. His research is focused on service oriented architectures supporting university processes. He received his M.Sc. cum laude in Artificial Intelligence from Maastricht University in 2012. In 2011, he finished his B.Sc. studies in Scientific Programming at FH Aachen University of Applied Sciences. From 2008 until 2011, he worked at IT Center as a software developer and later as a teacher for scripting and programming languages.

Dipl.-Medieninf. Ramona Renner is software developerin at the IT Center of RWTH Aachen University since 2016. The focus of her activities lies on user experience und accessibility. She recieved her diploma from Technische Universität Dresden in 2016.