DOI: 10.7250/eunis.2013.048

Bootstrapping OAuth for mobile apps using QR codes

Giralt, V[1], Baleriola, M[2], Pérez-Martín, I[3] , Muñoz, A[4] , Canca, J[5]

[1]Central ICT Services, University of Málaga, Málaga, Spain, victoriano@uma.es
[2]Central ICT Services, University of Málaga, Málaga, Spain, baleriola@uma.es
[3]Central ICT Services, University of Málaga, Málaga, Spain, ipm@uma.es
[4]Central ICT Services, University of Málaga, Málaga, Spain, alfredomunoz@uma.es
[5]Central ICT Services, University of Málaga, Málaga, Spain, joaquin@uma.es

Keywords
Mobile apps , QR codes , Oauth , identity management.

1. ABSTRACT

The current trend to do as many things as possible using mobile devices prompted the University of Málaga Central ICT Services to plan the development of mobile apps that would allow access to student data stored in the student management systems. Allowing access to personal data required strong authentication of the users and a secure way of storing credentials in otherwise insecure devices. Most mobile devices used by the student population have cameras that can scan QR codes and act on them. So, inserting a QR scan in the application installation process was an easy way to go. The initial application is able to send alerts to the registered handsets and allow for reviewing published exams results. The app got over two thousand registered devices in five days.

2. REQUIREMENTS

The main requirements for the system were:

- Offer secure access from mobile applications to web services providing business logic functions of various University ICT systems. Initially, the student management system for publishing examination results.
- Send notifications to the registered handsets with ability to discriminate individual users and groups.
- The users should not enter their University credentials in the handset, as the University is trying to train the users into not entering their credentials in any place different from Identity Provider, as part of a phishing awareness campaign.
- Create a registration process that is as user friendly as possible.
- Be platform neutral. This requirement had to be postponed if we wanted to be ready for the first semester exam results, because we already had a trained Android developer at hand for a first proof of the concept.

3. ADOPTED SOLUTION

OAuth was adopted as the access control method for protecting web services because the protocol does not require the user credentials to be stored in the mobile device and because there are available implementations in many programming languages. The problem was how to associate the user identity to the OAuth tokens.

QR codes are ubiquitous and Android users are trained to use them, as many applications are published with installation URLs as QR codes in web pages. So, we decided that the OAuth tokens would be presented in a WebSSO (Web Single Sign On) protected page inside our identity panel as a QR code that the application would scan. This will be the only data stored in the mobile device and, if the user decides so, protected by a PIN code.

DOI: 10.7250/eunis.2013.048

The Android system sends alerts using the WebSockets protocol, so the system has a server for such protocol and the application registers its location with the OS once installed. Thus, every time the device is connected to the Internet, a connection is established to the notifications server and the user receives any pending and subsequent alerts.

Then, the flow for using the application is as follows:

- User connects to the University identity management panel using her normal credentials for the WebSSO,
- Finds the list of the available mobile applications.
- Selects an application to install in a device. It is possible to have several devices associated to one user for any given app.
- Either the application has been already installed in the device or a QR code with the installation URL is presented.
- The first time the application is run, it gives instructions on how to reach the registration page and offers a "scan" button.
- The user informs the registration page that he is ready to register the application and taps the "scan" button on the device.
- The code is scanned associating the user and the handset, providing visual feedback both on the device and the registration page.
- The application is ready to access the user information without further requiring any credentials.

At any time the user can revoke access either from the device or from the registration page, for example, if she forgets the PIN or the device is lost. Registrations can be limited in time according to institution policy and application requirements.

4. RESULTS

The first application has been taken from the concept to deployment in less than three months, really much less, as the period included the Christmas break that lasts for two weeks in Spain. All requirements have been met except the platform neutrality.

Teachers now have the ability to notify students when any results are available or send any other kinds of messages with delivery acknowledgement and a certain degree of immediacy.

User feedback has been very encouraging and adoption has been fast paced, with over five thousand installations in the first two days of availability and over two thousand continuous connected devices in five days after release.

5. FUTURE

The main objective for the near future is to port the application to a development system that will allow for platform neutrality, most probably using PhoneGap. Once this has been achieved, the next step will be to increase the number of applications and services. Further into the future, the idea is to offer a skeleton application to anyone willing to offer identified services to members of the University.

6. REFERENCES

PhoneGap website (2013). PhoneGap framework. Retrieved May 1st, 2013, from: http://phonegap.com/

Hammer-Lahav, E., Ed. (2010). RFC 5849: The OAuth 1.0 Protocol. April, 2010. Internet Engineering Task Force. ISSN: 2070-1721

DOI: 10.7250/eunis.2013.048

7. AUTHORS' BIOGRAPHIES

V. Giralt is the systems manager for the University of Málaga. Graduated as an MD from University of Málaga in 1986, and became a member of the University IT team in 1987 as a programmer. Has worked as a programmer for the University and as a systems administrator both for the International University of Andalusia (1990-1995) and the University of Málaga. Chairs the technical committee of the Confia identity federation for the Andalusian public universities and the Groningen Declaration Executive Committee. Member of the steering committee of RS3G EUNIS task force, member of the European Committee for Academic Middleware, member of the TERENA EMC2 task force, acting as co-chair during 2012, member of the RedIRIS identity task force, member of the SSEDIC EU expert network on electronic identity.

M. Baleriola has a degree in Computer Science Engineering and also a Master degree in Software Engineering and Artificial Intelligence from the University of Málaga. He started writing books about ethical hacking and Linux in the 90's. In early 2000's he landed in web programming and near 2008 he met Django and fell in love with Python. Nowadays he is working as a sysadmin and developer in Central ICT Services of the University of Málaga. He was one of the developers of a virtual microscope software presented as TERENA 2009 and EUNIS 2009 that obtained the III Educational Innovation Award at the University of Málaga in 2010.

I. Pérez is a Computer Science Engineer with a Master degree in Software Engineering and Artificial Intelligence, both at the University of Málaga, who began his career as an ERP consultant and web developer. Since 2008 he works at the University of Málaga as a developer, mainly in Python/Django and as a systems administrator, using the main identity systems like OAuth, Shibboleth, SAML and PAPI, with LDAP, VMS and OpenVZ infrastructure. He also offers his services as a freelancer and teaching the virtues of Django as a teacher. Previous occupations: ERP consultant at O&S Consultores. He was one of the developers of a virtual microscope software presented as TERENA 2009 and EUNIS 2009 that obtained the III Educational Innovation Award at the University of Málaga in 2010.

A. Muñoz has a degree in Computer Science Engineering and also a degree in Technical Engineering in Computer Management from the University of Málaga. Since 2006 he's gaining experience in everything related to Java, Oracle and Android (J2EE, Oracle database, Oracle Application Server, Android SDK, JSF, Hibernate,...). At present he works as J2EE developer in Central ICT Services of the University of Málaga. Previous occupations include Isoft Health in the E-siap project based on Javax Swing and RMI Technology, CGI Group, NÁCAR Information Technology. SL. Working for Vodafone España with J2EE technology. He participated in the development of applications that got ORACLE Spain's best management software project award and Computer World's award for citizen impact in 2007.

J. Canca has a degree in Mathematical Sciences. He has been Assistant Professor at the Languages and Computer Science Department. He is currently the CIO of the University of Málaga and has been the director for the ICT services for the past fifteen years. Member of the working groups eGovernment and Government IT in the IT Commission of Spanish Rectors Conference.