Submitter Information

      Name:                  Michelle Wangham

      Email:                 michelle.wangham@rnp.br

    Submission Information

      Session Title:        **GIdILab:  Experimentation Lab for Trust**

      Session Abstract:

        NRENs offer services related to Identity and Access Management (IAM), including R&E National Federation, Eduroam, and other federated services. However, services under operation cannot be used for exploratory research, which could compromise their security in production. We noted that researchers in RD&I projects devoted a reasonable amount of time setting up identity  management infrastructure to run their experiments and, thus, discard their exploratory environments when research is done. Setting up a proper infrastructure for experimentations in IAM may be more arduous and time-consuming than the research investigation itself. Furthermore, developing applied research in the IAM area requires a scalable, distributed, controlled, and reliable environment to enable exploratory study.

        This presentation introduces GIdLab, a service maintained by the RNP to run experiments related to IAM technologies. GIdLab  offers specialized RD&I consultancy in IAM with a tailor-made experimentation lab that provides a set of authorization and authentication infrastructures (AAI) and an eduroam environment ready to be used by researchers and software developers. This service was born  as an initiative from the IdM technical committee from RNP. Since 2013, more than 70 Brazilian RD&I projects have been using the GIdLab infrastructure and consulting.

        GIdLab offers for researchers an infrastructure composed of: (1) an entire Shibboleth federation, known as CAFe Expresso; (2) a repository with a set of virtual machines and Docker containers  to build Shibboleth providers; (3) a SAML Federation that uses  SimpleSAMLPHP framework; (4) an OpenID Connect environment that uses MITREId Connect and Keyclock; (5) an Eduroam testbed; and  (6) a first-level customer service via RNP Service Desk and specialized technical service to assist the researchers and developers. The GIdLab infrastructure is open for experimentation and implementation of new technologies and solutions under investigation.

        CAFe Expresso, designed along the lines of CAFe (Brazilian R&E  federation), provides standard Shibboleth IdPs with LDAP service  populated with fictitious users with different attributes. It  also offers a dynamic discovery service, a metadata aggregation  service, and service providers hosting PHP, Java, and Python demo applications. A SATOSA proxy for translation between  authentication and authorization protocols and a COmanage  platform are also available for experiments with collaborative organizations. CAFe Expresso interoperates with the SimpleSAMLPHP federation, and it is integrated via proxy with OIDC providers.

        The Eduroam testbed is the first worldwide initiative to offer an authentication and authorization infrastructure for experimentation based on RADIUS, the IEEE 802.1X protocol, and  the Eduroam service. Since May 2018, the Eduroam testbed has been provided by the GIdLab infrastructure in order to provide an environment for researchers and professionals experimenting technologies/solutions in wireless networks. The configuration of the Eduroam testbed has three levels of RADIUS servers: local, national (federation), and top-level confederation.

        In the last part of the presentation, we are going to describe  an e-Science R&D&I project that used the GIdLab to develop and test a solution for virtual collaboration management. LINEA

        (https://www.linea.gov.br/) is a Brazilian initiative supported by the three National institutions: the National Observatory  (ON), the National Laboratory for Scientific Computing (LNCC), and the National Education and Research Network (RNP), created to provide researchers  from the astronomy area ways to survey  with large volumes of data. This GIdLab project developed for LIneA explored ways to enable virtual collaborations and their  management, including user lifecycle under these collaborations,  and a proxy solution for integrating federated authentication and Social Logins to LIneA services. This project was concluded  in six months, with activities from  the developers from LINEA  executed according to the guidance of the GIdLab team.

        The breaking news is that we would like to promote the GIdLab to be an international Experimentation Lab. Anyone interested in contributing, please feel free to contact us during the event.

    Topic Area

      Primary Track:         Identity & Access Management