From Moonshot to Mars

Insteek: Security + Forensics

 Federated Access to High-Performance Grids using EAP-TTLS

Federated  access to web applications has rapidly gained popularity in the  education and  research community: users from many different  organizations can use their ‘home credentials’ to  authenticate and gain  access to services elsewhere. Product based around the SAML security   assertion markup language (such as SimpleSAMLphp, Shibboleth and  Oracle’s Identity  Manager) facilitate the exchange of user attributes  between identity providers - the users’ home  organization - and service  providers such as file share sites, collaboration portals, and access  to  electronic journals. They all share one basic characteristic: the  applications are 100% web- based. But the oldest and most popular  federated service is not web-based at all. eduroam was setup  already in  2003 to provide cross-domain access to wireless networks, and leveraged  a bit of old  but proven technology: RADIUS. Today it is one of the  most ubiquitous federated services, and  now RADIUS is again the basis  to expand federated access beyond web and wireless to many  more  applications. Project Moonshot is an initiative to develop a single  unifying technology for extending the  benefits of federated identity to  a broad range of non-Web services, including Cloud  infrastructures,  High Performance Computing & Grid infrastructures and other commonly   deployed services including mail, file store, remote access and  instant messaging. The goal of  the technology is to enable the  management of access to a broad range of services and  applications,  using a single technology and infrastructure. It leverages a distributed  RADIUS  architecture like eduroam, but links it to the GSSAPI to  ‘moonshoot’ applications such as  OpenSSH, MyProxy, Windows log-on,  OpenLDAP, etc. In this project, we aim to do the following: - install  and deploy a moonshot environment linked to a test Identity Provider -  deploy OpenSSH and WebDAV service in moonshot mode - extend the OpenSSH  and a WebDAV client with the abil

ity to send an EAP request over  TTLS  through an OpenSSHd server to be authenticated by the test IdP - The  clients and the servers are required to receive the attributes pushed  back by the IdP. - Make the attributes of the IdP available for further  processing by the client and the  service through PAM for further  attribute processing, i.e. mapping to local group rights  and ACLs. -  Extend the attributes returned to the service with group and role  information from a  federated source, i.e. a VOMS service and/or  SURFconext teams. The service needs to  be able to verify the  authenticity of the attributes. The project involved systems  configuration, engineering, and configuration management, and  coding in  the C programming language using the GSSAPI, as well as the associated   documentation effort. Knowledge of security and AAA systems, SSL/PKI  and XML will be  beneficial. The implementation will be scored based on  applying security principles including  privacy preservation for the  end-user.

Deelnemers: 6

Contactpersoon: Oscar Koeroo (okoeroo@nikhef.nl)

Wouter:

De vraag of alle documenten nog langs de QA moeten?

Installeren en neerzetten van een moonshot omgeving gelinkt aan een IdP, OpenSSH en WebDav service in moonshot modeus en uitbreiden naar OpenSSH en WebDav met de mogelijkheid voor een EAP request over TTLS door een OpenSSH server en geauthoriseerd door een test IdP.

Vragen algemeen:

Wat weten we al?

Plan van Aanpak --> Wat wordt er verwacht?

Functioneel Ontwerp --> Wat wordt er verwacht?

Technisch Ontwerp

GIT/SVN?

Afspraak met de opdrachtgever:

E-mail a.s.a.p.

Interessant om te bekijken: SSH config te vergelijken tussen standard openSSH < - >

Vragen Arnim:

ITopia QA

Kunnen wij het XEN cluster van Arnim gebruiken voor productie (test)?

Waarschijnlijk maken: Proof-of-Concept

Vragen opdrachtgever:

Extentie RADIUS server -> RADIUS server -> overal in kunnen loggen

GSSAPI

“Log 1x in, access naar allerlei systemen

Wat is de geschiedenis van het project?

Wat is er al gedaan voor het project?

“Wat moeten wij precies doen?” (niet zo vragen!)

SURFconext is ook al bezig geweest met Moonshot-achtig project

Communicatie met de opdrachtgever

Regelmatig contact voor feedback

Misschien Jabber/IRC

E-mail

In-person?

Moonshot

Vragen aan Arnim: Hebben we ITopia QA?

Wat weten we al?

Extentie RADIUS server -> RADIUS server -> overal in kunnen loggen

GSSAPI

“Log 1x in, access naar allerlei systemen

Waarschijnlijk maken:

Proof-of-Concept

Wat is de geschiedenis van het project?

Wat is er al gedaan voor het project?

“Wat moeten wij precies doen?” (niet zo vragen!)

Kunnen wij het XEN cluster van Arnim gebruiken voor productie (test)?

SURFconext is ook al bezig geweest met Moonshot-achtig project

Plan van Aanpak --> Wat wordt er verwacht?

Functioneel Ontwerp --> Wat wordt er verwacht?

Methodes? Prince2, scrum, DSDM, oid? <-- Prince2?

GIT/SVN?

MoSCoW! Afbakening van het project

Communicatie met de opdrachtgever

Regelmatig contact voor feedback

Misschien Jabber/IRC

E-mail

In-person?

Interessant om te bekijken: SSH config te vergelijken tussen standard openSSH < - > Moonshot

Afspraak met de opdrachtgever:

E-mail a.s.a.p.

PAP

Dear Oscar,

For our Minor Foresic Intelligence and Security, we decided to sign up for the project From Moonshot to Mars. Is it possible to schedule a meeting on the 13th of February, 15:00h? If not, could you suggest a different time? We would also like to know where you would like the meeting to take place. It's possible to meet at the Hogeschool van Amsterdam, or we could meet at the Science park?

For future reference, in what language would you like to communicate?

Kind regards,

Sebastiaan Groot, on behalf of Remy Bien, Ruben Bras, Marvin Hiemstra, Wouter Miltenburg, Koen Veelenturf.