UK e-Infrastructure Security and Access Management Working Group

Date: Thursday June 12th 2014

Venue: Holborn Bars, London

Present:

Stephen Booth (EPCC), Alan Real (University of Leeds), Andrew Cormack (Janet (Chair)), John Chapman (Janet), Henry Hughes (Janet), Paul Kennedy (University of Nottingham), Andrew Richards (University of Oxford), David Salmon (Janet), David Kelsey (STFC), Jeremy Olsen (Francis Crick Institute), Jens Jensen (STFC).

Apologies:

Phil Kershaw (NERC / STFC RAL), Jeremy Sharp (Janet), Darren Hankinson (University of Manchester), Steven Newhouse (EBI), Paul Lewis (Cranfield University).

1. Actions from previous meeting
    1.1. Janet to provide assistance to SB with registering EPCC to join the UK federation.
        1.1.1. ONGOING
    1.2. Janet to arrange a meeting between SB and Rhys Smith to discuss Moonshot and SAFE.
        1.2.1. ONGOING
    1.3. HH, PL and AC to add slides to Community Group.
        1.3.1. HH and AC published. Waiting for PL.
    1.4. All members to look at The Critical Security Controls for Effective Cyber Defense Version 5.0 (http://www.counciloncybersecurity.org/practice-areas/technology/) and apply to their infrastructures.
        1.4.1. See item 9.
    1.5. AC to share EGI-cert information
        1.5.1. See item 2.
    1.6. AC to circulate link to deploying grids document https://community.ja.net/library/janet-services-documentation/deploying-grids and identify what needs updating
        1.6.1. DONE

2. EGI-CERT
    2.1. DK talked through some slides prepared for an EC review outlining EGI-CERT activities.
    2.2. See slides published at https://community.ja.net/groups/uk-e-infrastructure-security-access-management-wg/document/egi-security

3. Report on items of interest from TNC14
    3.1. Lots of group management options - need a protocol rather than software.
    3.2. GÉANT research pilots (DARIAH, Elixir, Umbrella) – similar issues: attribute aggregation, user friendliness, credential translation, attribute release, LoA, homeless users, bridging communities, non-web browser.
    3.3. User interface design for AAI – informed attribute release (Ken Klingenstein).

3.4. Virtual Campus Hub awareness raising needed – 3 countries working together and discovered the pilot institutions weren't in their country's federation.

3.5. IdP in the cloud – developed by Italian NREN GARR. No link to site IdM therefore low "LoA". Could connect to a site LDAP, but no one's asked them to do that yet.

3.6. Some IdPs in the US say they have to dispose of authN record immediately due to privacy concerns so not possible to use logs to deal with incidents.

3.7. See also JC's TNC and REFEDs notes at https://community.ja.net/groups/access-and-identity-management-aim/article/highlights-tnc14 and https://community.ja.net/groups/access-and-identity-management-aim/article/taking-aim-dublin-view-refeds

4. Generic model for an eInfrastructure

4.1. At a recent Project Directors' Group (PDG) meeting - AC talked through a Draft Model (see https://community.ja.net/groups/uk-e-infrastructure-security-access-management-wg/document/draft-general-model-e).

4.2. Basic federated authN gives you currency and accountability.

4.3. Enhanced federated authN is needed for certain services e.g. Farr

4.4. Group management part needs to be High Availability as lots of real time use. Maybe a central cloud hosted HA instance?

5. Update on Janet/Farr Institute working groups

5.1. Janet is working with the Farr Institute and partners on a pilot project to demonstrate high assurance networking and AIM.

5.2. The plan is for an overlay network. We will put in the groundwork for security certification, but we are not going for full ISO27001 certification.

5.3. If you want to run an HA service you have to be able to control the environment in which traffic is being moved - end to end control of the transmission path. We are doing an encrypted overlay so we have to have boxes at the edge in an accredited space in the home organisation and we have to manage the key management from end to end. The end sites can do whatever they want over the connection including a second level of encryption so Janet can't access the content.

5.4. For the access and identify management element three use cases areas have been defined:

5.4.1. Use case A: Dementia Study - There is a theory that statins are protective against dementia. The Clinical Trials Service Unit (CTSU) at the University of Oxford has a dataset from a consented cohort of participants, with sufficient identifiers (e.g. name, date of birth, postcode and NHS number), who were randomised to 5 years of statin or matching placebo. The study has completed. The study plan is to gather evidence of dementia, together with date of record from a range of sources collated at CTSU. This pilot will initially look at authenticating potential collaborators for involvement in the Research Proposal. This will then lead on to providing access to the requested data as listed above but collated and held by the CTSU e.g. using Moonshot for file transfer / SAML for web access only. The objective of use case A will be to enable a researcher to use their home credentials to authenticate in order to request the creation and delivery of collated datasets (with local multifactor authorisation – likely to include Google Authenticator, SMS, Hardware tokens) with the aim of demonstrating the benefits of federated authentication.

5.4.2. Use case B: HPC Pilot. This pilot will enable researchers from HeRC and N8 institutions to access the Leeds University large shared memory computing facility using their home institution credentials. By the end of 2014 this pilot will have demonstrated that researchers can use their home credentials to access the N8 HPC, HeRC and DiRAC facilities. This pilot will build on existing work within the Janet Moonshot pilot.

5.4.3. Use case C: eMedLab Pilot. eMedLab is to be a health research facility at a shared offsite data centre, currently in procurement, created by The Francis Crick Institute, the Sanger Institute, the European Bioinformatics Institute and UCL Partners, including University College London, Queen Mary University London, and the London School of Hygiene & Tropical Medicine. Funded by a grant from the MRC Medical Bioinformatics call, eMedLab will help the project partners to analyse human genome data and medical images, together with clinical and other physiological and social data. The eMedLab pilot will demonstrate how a common AAI will allow researchers to access different datasets using a common credential with authorisation based on the specific access rights and security needs of the data sources.

6. Moonshot update

6.1. Pilot picking up speed. Janet central infrastructure - Trust Router - now on a new virtual platform and starting to connect end sites – Cambridge and Cardiff connected, Glasgow imminently. Very shortly we will be connecting Kent, University of Murcia and Diamond Light Source.

6.2. We have a meeting next week with Advanced Research Computing at Oxford with colleagues from UCL and Southampton to get them started with Moonshot.

6.3. Doing some training with European partners in the GÉANT project later this month with delegates from the NRENs from Switzerland, Croatia, Spain, France, Finland, Slovenia, the Netherlands and Hungary and also some institutions from the Netherlands.

6.4. Aiming for a production service in Q1 2015 targeted initially at research institutions, but with a plan to scale up to include more diverse institutions and supporting more applications.

7. Comments on Authentication paper

7.1. There was general agreement on the paper

7.2. Detailed comments are requested by email with a view to gaining emailed agreement for publication. – **Action** ALL to feedback detailed comments on AuthN paper to AC by 21/7/2014

7.3. UK federation Rules has an optional section (Section 6) for sites to declare that they can trace users. This is shown by a flag in the metadata. Question: Do any other federations make a similar assertion in metadata? Does the UK federation flag get passed via eduGAIN? REFEDs has done some work on this – see https://refeds.terena.org/index.php/Federation_Policy_Best_Practise_Approach – **Action** on Janet to determine if other federations can do traceability in the same way as UK federation Section 6.

8. AAI information gathering - Discussion and tentative conclusions on group management

8.1. There are lots of group management solutions.

8.2. A single grand plan won't work, but some protocol as a default would be good and if that didn't work then point to point would be needed.

8.3. Should leverage SAML if possible.

8.4. VOMS uses attribute certificates.

8.5. Referring to AC Draft Model diagram - need to define how to 'drain the Swamp'.

8.6. Diagram needs updating from 'Service' to 'Services + Workflow'

8.7. Mapping identities is a priority. We need a way to tie up accounts at different sites e.g. ensure the same Moonshot id gets mapped to the user's Cambridge account and their Edinburgh account.

8.8. Need to support requests – “Can I be a member of this group?” “Can I have access to this dataset?” A simpler solution is an out of band request to be invited to access a data set.

8.9. **Action** on AC to draft skeleton document addressing group management.

9. Security information gathering - Work through Top 20 controls

9.1. Top 20 Controls are not a standard, but a framework for discussion.

9.2. The Group discussed how relevant each of the Controls are to an e-Infrastructure. AC will decide how best to document this. **Action** on AC to document Top 20 Controls discussion.

9.3. Need a pre-approved range of firewall ports dependent on service / networks. e.g. research vs library

9.4. RUGIT work started with dirty network and said different parts will need some controls applied.

9.5. Trying to draw a perimeter between control plane and where the user is. Assumption is users will do some bad stuff that we will deal with by policy and there are some controls that we need to manage to prevent more severe things happening.

9.6. Partition between react and prevent.

9.7. Use of Controls always has to come back to risk assessment.

9.8. Firewalls are there to protect yourself from things you don't know are running,

9.9. Vulnerability testing tells you where your policies aren't being implemented, pen testing is used to tell when your policies aren't working.

10. AOB

10.1.This week we have published a draft Jisc Security Products and services strategy and plan – this is similar to the AIM strategy and plan published in January. The drafts are out for open public consultation until September. We will also likely have a webinar and face to face meetings - possibly in conjunction with UCISA. Comments are requested from this Group. See www.tinyurl.com/jiscsecurity .

10.2.Jens offered to write up positive case studies e.g GridPP and DiRAC; and EUDAT working with multiple countries.

11. Agreed Actions

11.1.Janet to provide assistance to SB with registering EPCC to join the UK federation.

11.2.Janet to arrange a meeting between SB and Rhys Smith to discuss Moonshot and SAFE

11.3.AC to draft skeleton document addressing group management.

11.4.Janet to determine if other federations can do traceability in the same way as UK fed Section 6.

11.5.ALL to feedback detailed comments on AuthN paper to AC by 21/7/2014

11.6.AC to document Top 20 Controls discussion.

11.7.JJ to provide short case studies on the Community Group.

11.8.JC to Poll for dates for next meeting (aiming for end Jan 2015)

12. Date of Next Meeting

12.1. 3 October 2014 at Jisc's London Office at Brettenham House, 5 Lancaster Place, London, WC2E 7EN (http://www.jisc.ac.uk/contact#tab-5-1).