UK e-Infrastructure Security and Access Management Working Group

Date: Friday 14 March 2014

Venue: Jisc Meeting Room, Brettenham House, 5 Lancaster Place, London, WC2E 7EN

Present:

Stephen Booth (EPCC), Darren Hankinson (University of Manchester), Alan Real (University of Leeds), Andrew Cormack (Janet (Chair)), John Chapman (Janet), Henry Hughes (Janet).

Apologies:

Paul Kennedy (University of Nottingham), Andrew Richards (University of Oxford), David Salmon (Janet), Phil Kershaw (NERC / STFC RAL), David Kelsey (STFC), Dave Britton (GridPP), Jeremy Sharp (Janet)

1. Actions from previous meeting
    1. Janet to set up email list
        i. DONE. uk-e-infrastructure-security@jiscmail.ac.uk
    2. Revise draft TOR and circulate with the aim of reaching agreement by email or at next meeting.
        i. DONE. Final agreed version circulated to list on 17/02/2014.
    3. Janet to talk to Dave Kelsey about personal certificates via IGTF and Janet Certificate Service.
        i. Agreement to add requirement to Janet Certificate Service procurement.
    4. Produce an initial outline draft specification for what identity provider hosting, a virtual organisation service and a home for the homeless might look like.
        i. DONE. Draft document circulated to list on 04/04/2014.
    5. Janet to talk to "SKA (Square Kilometre Array)" as a large scale project to see if their activity and requirements could help define example use cases.
        i. SKA presented at Daresbury at a meeting attended by AC. Feeling is that it may be too early to engage with them as a source of use cases.
    6. Write up proposed deliverables, timescales and circulate for comments.
        i. Discussed as Agenda item in today's meeting.
    7. Joint REFEDS/EGI/UK e-infrastructure discussion - David Kelsey to follow up.
        i. Ongoing
    8. Janet to establish small team to offer practical advice to projects in early 2014. E.g. what should DiRAC be doing?
        i. DONE. AC, JC and Rhys Smith (Janet) met with Jeremy Yates, Jacky Pallas and David Fergusson. Related meetings have also taken place with the Farr Institute.
    9. Janet to poll for dates of next meeting.
        i. DONE. Meetings arranged for Friday 14th March; Thursday 12th June; Friday 3rd October
    10. Janet to use the discussion around mapping of the technical landscape as the basis for a document that the group could keep under regular review.
        i. DONE. Added to https://community.ja.net/groups/uk-e-infrastructure-security-access-management-wg/wiki/draft-e-infrastructure-landscape

2. Report back from project discussions – Andrew Cormack
    1. AC presented feedback summarised from meetings eInfrastructures and attending the Project Directors' Group.
    2. Slides and a summary paper will be available on the Community Group.
    3. We should:
       - identify common requirements
       - reuse existing stuff where we can
       - guide development of new stuff where efficient
       - use "specials" when needed
    4. An analysis of AC's 'Common User Lifecycle' slide shows that it is an accurate summary.
    5. SB stated that EPCC want to log people in via UK federation, but there is a need to tie the anonymised service-specific identifier back to a real name for the PI. They currently use email as an identifier. There are technical solutions to allow the mapping of identities. E.g. email received with a clickable link that when followed allows log in via a federated credentials which are mapped to the account.
    6. SB has had problems registering with the UK federation – **Action 1**: Janet to provide assistance with registering to join the UK federation.
    7. DiRAC and ARCHER use SAFE. Farr are also interested in looking at this. Can this be factored out as an authorisation stage as Farr want 2 factor plus other requirements? – **Action 2**: Janet to arrange a meeting between SB and Rhys Smith to discuss Moonshot and SAFE.
    8. Typical workflow shows delegation is to PI NOT to Home Institution - which differs from European discussions that have been about "what extra attributes can the Home Institution provide?". However, links between group members may have consequences on Home Organisation - misbehaviour needs to be linked to the home organisation not just the PI.
    9. Links to Home Organisations are also needed for statistics generation for REF – to report usage by organisations. Demonstrating ROI is becoming more important politically.
    10. Diamond want to use OrcIDs to determine usage. David Wallom has published a paper about the Oxford infrastructure and gets anyone who uses it to cite that paper. He can then check who has cited the paper to determine usage.
    11. SAFE for DiRAC can be seen as being a DiRAC VO management system.
    12. Some eInfrastructure VOs will be short-lived as they are used to answer one research question, but others may be required for longer and the same VO may be needed for different eInfrastructures.
    13. The ARCHER process starts with a research grant. They receive a letter from EPSRC with a name of a PI and a length of time that can be allocated. The PI is given the tools to bring people in.
    14. Policies for access need to include legal and ethics committee requirements. Farr, for example, need the ability for individual patients exclude their data from being used by particular research projects.
    15. When determining policies we need to highlight which bits would not be available to a Social Identity, for example.
    16. Home for the homeless - not needed anymore as you can use Social Ids, Umbrella, or just username and password.

17. A centrally hosted VO management system is more of a requirement. Can such a system act as an IdP of last resort? Do eInfrastructures care if an identity is not backed up by a contract?
18. Can authentication be passed in the workflow? E.g. a researcher wants to run a batch job on ARCHER and when complete have it automatically sent to JASMIN without the researcher having to be online.

3. Information presentations
    1. Henry Hughes, Janet – External drivers: a report from the EU Cybersecurity Strategy High Level Conference
        i. See slides on Community Group – **Action 3** HH, PL and AC to add slides to Community Group
        ii. 'Standards' mentioned a lot, but more likely to mean processes.
        iii. 'Refreshingly frank' use case from Deutsche Telekom Group. In response to attack they have changed all their internal processes with a security first approach. Have done as much as they can now, but need more automation and intelligence in infrastructure.
    2. Paul Lewis, Cranfield University – Practical steps for eInfrastructure Security
        i. See slides on Community Group – **Action** 3 HH, PL and AC to add slides to Community Group
        ii. Why are we doing this AIM and Security stuff? To tick a box or to achieve a real impact?
        iii. Risk of nation states attacking our systems is relatively low compared to the benefits they will get from Intellectual Property etc.
        iv. What are WE protecting? Need to know what we have got to know what needs protecting.
        v. You can manage risk by: Checklists; Processes; Standards; and NOT managing them - just accept the risk.
        vi. The Critical Security Controls for Effective Cyber Defense could be tweaked for HPC infrastructure. Assessing your infrastructure against these controls demonstrates an assurance to an appropriate standard.
        vii. Security skills assessment is key as lots of people have 'qualifications' that aren't worth the paper they are written on.
        viii. Risk registers are not necessarily the best way to communicate risk. Need to continually update and evaluate. The AS/NZ 4360 diagram is good for explaining risks.
        ix. Science DMZ - recognise you have different requirements from different infrastructures - Department full of Windows machines vs HPC infrastructure.
        x. Need to block the most relevant threats to you - use cases/scenarios good for this. E.g. misuse/abuse by students more of a risk than external threats.

4. Group discussion: what deliverables should the WG aim to produce?
    1. Security:
        i. Profile one of our infrastructures against the SANS/CPNI Top20 controls. (The RUGIT report on the applicability of the SANS/CPNI Top20 controls

to a University environment has been published at http://www.rugit.ac.uk/meetings/presentationsnotes/november2013/)

ii. How to define scope?

iii. The Farr Institute need higher assurance, but can we define a general level of assurance? Is there a set of science use cases that *are* suitable for a generic eInfrastructures? Can we define a baseline standard? E.g. university logins plus Moonshot. What is this suitable / not suitable for?

iv. Need to identify risks FIRST - THEN we can work on mitigation

2. Incident Response:
    i. Need better communication of security issues.
    ii. EGI-CERT put Red Teams onto systems to highlight weaknesses – **Action 5** AC to share EGI-CERT information
    iii. Should there be an HPC-Cert?
3. Operations side:
    i. 'Typical' operation has a PI with a research question. They require certain resources to answer the question (infrastructure and data). The data may need to be pushed to somebody or some other eInfrastructure. An eInfrastructure Provider may need to say if they can do this. Funder may need answers that all operational parts are okay before funding the research.
    ii. Farr != eInfrastructure. It is *a* national infrastructure with different governance and different requirements.
    iii. Janet is planning a Threat Information Pilot to drive up reporting of incidents and better provision of information about threats. This will allow prioritisation and provide a focus on active incidents.
    iv. Janet wants to provide a better system for distribution of threat intelligence. Will look at what can be done to the Janet infrastructure to collect information and what can be deployed at institutions - like IDS. Systems are expensive so want to move them around the network to where they are needed most. Janet will develop a suite of services - not just PEN testing.
    v. Can this group provide best practice recommendations for firewall rules?
    vi. AC wrote a good document a few years ago that is relevant - https://community.ja.net/library/janet-services-documentation/grid-support and https://community.ja.net/library/janet-services-documentation/deploying-grids - **Action 6** AC to circulate link to deploying grids documents and identify what needs updating.

5. Actions
    1. Janet to provide assistance with registering to join the UK federation.
    2. Janet to arrange a meeting between SB and Rhys Smith to discuss Moonshot and SAFE.
    3. HH, PL and AC to add slides to Community Group
    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.
    5. AC to share EGI-cert information
    6. AC to circulate link to deploying grids document https://community.ja.net/library/janet-services-documentation/deploying-grids and identify what needs updating

6. Date of Next Meeting
    1. Date of Next Meeting: 12 June 2014 at Holborn Bars, London (http://www.deverevenues.co.uk/en/venues/holborn-bars/)