Safeguarding and eduroam

Considerations for Further Education colleges

Scope

This document is intended for Technical managers wishing to explore the topic of safeguarding minors and vulnerable adults on eduroam, particularly in respect of users roaming away from the home campus to locations where the eduroam service provides unfiltered access to the internet. The background to the issue is considered together with an appraisal of how the key elements of eduroam support the safeguarding of users and how eduroam deployment may be tailored to suit the policy in force at the individual organisation.

Background

eduroam is the popular roaming user network access authentication service that provides users with secure, authenticated, seamless internet access at the majority of education and research organisations in the Janet/Jisc community in the UK and in the NREN communities throughout the world. By using a single Wi-Fi profile and unique set of credentials for each user, access to the service is enabled at any participating organisation. Each member organisation adapts its own network to support the service and benefit from use of the technology and the roaming capability/visitor access service afforded to users and guests.

eduroam services typically allow users to gain unfiltered access to the internet. It is this access to the 'raw' internet that causes concern for some in the Further Education and schools community where the duty of care for minors and vulnerable adults is particularly relevant. As is permitted in the eduroam(UK) policy and technical specification, a number of FE colleges have implemented 'walled garden' filtered eduroam services for users when at their home campuses to provide a safe browsing environment locally. However these colleges may be concerned that eduroam credentials could be used elsewhere where those precautions are not in place and so enable vulnerable users to gain unsupervised access to 'raw' internet.

Jisc's position is that the safeguarding policy an organisation adopts is a matter for the organisation itself to determine as it interprets and applies the relevant laws and regulations. The organisation issuing the credentials has the relationship with the user to whom the credentials are to be issued, and in particular has the verified knowledge as to the age and/or whether the individual might otherwise be considered vulnerable. Neither Jisc as the central operator nor other venues offering a visitor eduroam service have that knowledge. Therefore, the duty of care lies with the home organisation of the user(s) concerned to apply its policy and to grant or restrict eduroam credentials to its users accordingly. The options open to the organisation are described below.

Benefits of eduroam

eduroam offers secure and seamless internet access for users as they roam between service locations, however it is the technology on which the service is based that provides the key to its support for the safeguarding of users.

Benefits for the organisation:

- eduroam uses **standards based technology** (802.1x/WPA2 Enterprise) and is completely platform agnostic. This means that organisations are not locked-in to particular vendor(s) for their network/Wi-Fi provision.
- **Wireless network security**. WPA2/AES is the most secure encrypted Wi-Fi technology available today; emerging protocols such as WPA3 will be supported as they are implemented. Other solutions may put the organisation or the user at risk; open systems provide no accountability and any unencrypted user traffic is exposed; captive portal systems are at risk of Man-in-the-Middle attacks leading to credential harvesting and traffic exposure. A further consideration is that only authenticated, known users are provided with network access and IP connectivity is only provided on the eduroam service after authentication of the user
- **Accountability and logging**. eduroam's requisite user authentication, IP allocation and MAC address logging assures an audit trail for uniquely identify individual users should a breach of regulations be reported or malicious activity detected – whether the user is on campus or roaming to other eduroam locations.
- **Simplification of Wi-Fi network management**. In scenarios where a large number of Wi-Fi networks (SSIDs) have been implemented to a support a variety of user groups with diverse security profiles, network resources requirements and levels of safeguarding/filtering, eduroam can greatly simplify Wi-Fi network management and reduce the number of SSIDs that have to be supported. This can be achieved by using dynamic VLAN selection. The same network services (VLANs) can be utilised, but connection of the authenticated user is decided based on the college AD security groups. A reduction in number of SSIDs results in improved wireless performance too.
- An example of an efficient deployment would be: SSIDs: eduroam; non-eduroam guest network; on-boarding/remedial network. VLANs: staff managed device users; staff BYOD device users; eduroam students BYOD users (internet filtered); eduroam guests (unfiltered/filtered); non-eduroam guests; on-boarding/remedial network.
- eduroam provides a seamless **solution for Bring Your Own Device** (BYOD) by using the college user credentials for authentication, which can be deployed on personal devices as well as the college devices. This allows the organisation to apply security and access controls and an appropriate level of safeguarding for all devices connected to the network.
- **Improved security of guest network access provision**. With eduroam deployed, visitors from other eduroam organisations gain automatic guest network access at your campus, thereby the need for you to provide and manage temporary AD accounts for such visitors may be eliminated, depending on how your current guest network access system works. Whilst you may still wish to provide guest network facilities for non-eduroam guests, reducing the number of temporary accounts (which can be shared or stolen) that you issue is a clear security benefit.

- **Single Wi-Fi and shared authentication service for multi-campus/merging colleges.** Colleges with disparate network services at multiple campuses e.g. during a college merger process, can use 802.1X/eduroam as part of the process of merging IT systems. The technology supports migration through the use of a single authentication system and transition from multiple to a single organisational identity realm.
- **Facilitation of managed guest access systems**. Jisc may adopt or develop an 'eduroam visitor access (eVA)' system which would greatly simplify the creation and management of temporary eduroam accounts for visitors from the Jisc community who have not yet joined the eduroam family. The system enables guest account creation privileges to be devolved to designated 'host' members of your organisation and removes the need for creation of accounts in your AD.

Benefits for the individual:

- Users will love the **seamless, all device single sign on solution**. In addition, the need to authenticate every few hours or every day, typical of captive portal systems, will be a thing of the past.
- Staff will be able to **collaborate more effectively with partner organisations and with less hassle** because they will not have to seek guest access at the visited site.

Putting Safeguarding and eduroam into perspective

eduroam may be deployed in a variety of ways and can be tailored to meet the needs of the further Education community in respect of safeguarding users. This section aims to foster a broad understanding of the issues.

- There are three (user facing) aspects of the provision of eduroam, the Wi-Fi/network service offered to visitors, the Wi-Fi/network service offered to your own users on campus and the Wi-Fi service generally available to your own users when they go to other eduroam service providers. All of these if course are available through the single eduroam SSID. However, all three aspects are tailorable, up to a point, to comply with your own policies and each can be provided or not, independently of the others, (except a home user eduroam Wi-Fi service must always be paired with an eduroam service for visitors).
- You differentiate between your home users and visitors through the realm component of the username, so the first decision in the authentication process of your RADIUS server is whether to process the request locally, which is done for your own users or to forward visitor requests to the eduroam national proxy servers.
- The service for visitors, aka 'Visited service', must comply with the Technical Specification and so be subject to authentication request and IP assignment logging together with the provision of internet access that supports the most commonly required applications, e-mail, HTTP, HTTPS, Citrix, VPN. You may apply content and URL web filtering, but you must not apply SSL/TLS interception proxies since these fundamentally breach the security of users' network traffic. Note that the service you offer requires visitors to accept your Acceptable Use Policy although monitoring of the online activity of visitors is not in keeping with the spirit of eduroam and the provision of guest services. To address concerns in this context, Visitor's connection events are logged and in conjunction with the logs kept by the home organisation of the visitor, the identity of visitors can be established in cases where abuse of network access privilege has occurred and co-operation with authorities is required.

- The service for your own users at home, however, is not subject to all of the above requirements. This is because when at the home campus, eduroam applies simply to the authentication and logging process. Through dynamic VLAN assignment you can connect your own users to services tailored to their security, safeguarding and resource access profiles. If you have yet to deploy eduroam, these can be an existing in-house network services and can be restricted, filtered and monitored as you wish.
- A potentially useful bonus from eduroam deployment is that some web-filtering solutions can use the local accounting information generated to further granulise internet access. This means that the college can apply existing filtering, plus enhanced controls within the home campus eduroam service.
- Visited Services: the service that your users experience when roaming to other sites will be the research and education-friendly service that was established in the early days of eduroam. These provide a standard Tech Spec compliant environment for users, reliable and appropriate for the Janet community. Visited services may or may not be filtered. There is presently no agreed or technically consistent way of managing roaming user connectivity into filtered/unfiltered services nor of selectively making an authentication decision based on location the user is roaming to. Another difficulty is that users expect eduroam to 'just work everywhere'; unfortunately there is no method of informing the user why an authentication is refused by the Home organisation, and without this, selective authentication is not a viable service element.
- Whilst you can't control at which service location your roaming users will be able to connect, you can decide for which users or user groups you enable roaming capability. You could restrict eduroam connectivity for all users to your home campus or restrict roaming capability, for instance, to staff and/or over-18s.
- It is worth noting, that access to unfiltered internet services is widely available – via home broadband services, at open free Wi-Fi service venues, even some captive portal ones and of course though 3G and 4G via smart phones/tablets. And these public services lack the key security advantages that even unfiltered eduroam services provide - the wireless is encrypted, man in the middle attacks are preventable, only authenticated used share the network, all connection event are logged and users are traceable.
- Safeguarding users should not be seen simply as something that can be solved with technology. As above, vulnerable users can readily gain access to 'raw' internet services. User education is key to ensuring safety when online. An appreciation of secure (HTTPS) browsing, certificate usage, password security, wireless encryption, risks associated with captive portal systems and the intrinsic risks in social media, should form part of all students' education.

Solutions for Safeguarding

There are a number of options open to the 'Home' service eduroam provider for meeting the challenges presented if your safeguarding policy requires restricting access for some users whilst allowing the college as a whole to benefit from the ubiquitous eduroam roaming service and the underlying 802.1X technology.

- A broad brush solution would be simply to exclude users you consider should not be enabled to use unfiltered services at other sites from your eduroam service. This would be simply achieved by restricting which (AD/LDAP) user (security) groups you provide roaming eduroam credentials to. It would be an imperfect eduroam deployment, but you could continue to provide a legacy non-eduroam home user Wi-Fi service for

students or under-18/vulnerable students whilst providing a roaming capable service to staff and/or other students together with the eduroam SSID for such in-house users and visitors.

- A better variation on the above would be to deploy an eduroam-as-the-primary-SSID-based solution, but restrict which (AD/LDAP) user groups you provide roaming eduroam credentials to. You could configure your RADIUS server to only authenticate 'vulnerable' user groups when connecting on the college eduroam service and to reject access requests sent via the national proxy servers. An alternative approach to this would be for 'vulnerable' users to be provided with .local credentials e.g. **userID@camford.local** This approach would have the advantage of avoiding authentication requests being sent from visited organisations to the national proxies in the first place (avoiding undue load on the service). ***With this geo-restriction approach it would be essential for user-education to be conducted to manage the expectation of users and to ensure that disappointment and dissatisfaction were avoided.***
- Organisations are permitted to work collaboratively to deliver eduroam, so in situations where colleges are merging, not only can eduroam play a part in the process of merging network access control, but a shared walled garden VLAN can be created or a home walled garden service could be extended into the other organisation through the use of a site-to-site VPN.
- This collaborative approach can also work where colleges that are geographically close agree to each provide home-like protected/restricted networks with equivalent levels of content and URL filtering that visitors from the other college will be connected to based on realm information in the outer identity or Operator-Name. In this scenario, the colleges involved have the assurance that their safeguarding standards apply at least within the institutions that their students are most likely to visit. Of course it has to be accepted that the students can gain unfiltered access should they visit eduroam locations outside the protected access zone.
- The above approaches apply to username and password based credentials (which can be readily copied between devices). There are other more technology-heavy solutions which could be considered in conjunction with certificate based credentials. One solution would be for the college to provide managed devices to users and to only support certificate-based authentication methods. By pushing profiles/configuration via MDM systems such that all web browsing went through proxies that the college managed or controlled, web browsing would be as if it was at the 'home' site. This could be achieved with VPN technology so ALL internet traffic was channelled back so no matter where students roamed using such managed devices, the college would be able to enforce its IT policies in this regard.

Further Support or advice

If you wish to learn more or discuss with Jisc staff:

- Email discussion list : **https://www.jiscmail.ac.uk/cgi-bin/webadmin?SUBED1=EDUROAM-FE&X**
- Implementation issues and questions via direct email: **help@jisc.ac.uk** with subject :"eduroam-FE"
- FE eduroam Implementation Workshop. Contact your college account manager https://www.jisc.ac.uk/contact/your-account-manager to register your interest in attending and for details of the next available workshop in your area. Or contact **help@jisc.ac.uk** with subject : eduroam-FE and the workshop team will respond directly.