Janet eduroam security measures

PB/INFO/067 (05/07)

Security was a major requirement in the design of eduroam, to ensure that organisations that provide visitor facilities, and the guests who make use of them, are not exposed to additional risks outside their control. eduroam should present fewer risks than the existing ad hoc arrangements for guest users. This factsheet explains the security measures within eduroam and how organisations can use them to protect their own security.

Network Architecture

Good security practice requires that any visitor network services should be separated from the utility campus network, with a router or firewall controlling network traffic between them. The visitor network should normally be treated as untrusted, outside the organisation's security perimeter, giving access only to services designed for use from offsite (at least until the users have been authenticated). eduroam users, whether using wireless or wired connections, should be treated in the same way with a filtering router or firewall between them and the internal network. Visitor sockets or terminals on the wired network may be segregated by using different physical segments, static virtual local area networks (VLANs) or 802.1X assigned VLANs based on the authenticated username.

Technical Controls – Misuse

The eduroam Technical Specification allows organisations to implement default-deny firewalling for both inbound traffic to their networks and outbound traffic from their visitor facilities. For inbound traffic, the only requirement is to let an organisational RADIUS proxy server (ORPS) communicate with the national RADIUS proxy servers (NRPS). eduroam membership does not require an organisation to allow any traffic into its internal network, nor to offer particular services to its own users. Each organisation retains the free choice of which applications (webmail, virtual private network, etc.), if any, it makes available to its own users when they are offsite; this decision should be based on the organisation's own requirements and risk assessment.

The organisation may also apply default-deny filtering to outbound traffic generated by guests. The eduroam specification requires only that a site hosting guests must allow the following minimum set of protocols to pass from the guests' computers, via JANET, to the guests' home organisation. All other protocols may be blocked if required.

- **Web browsing:** HTTP, HTTPS
- **File access:** passive FTP, passive SFTP, Andrew File System (AFS)
- **E-mail:** LDAP, LDAPS, IMSP, IMAP4, IMAP3, IMAPS, POP3, POP3S, SMTPS, Submit
- **VPNs:** IPv6 Tunnel Broker NAT traversal, IPSec NAT traversal, Cisco® IPSec, PPTP, OpenVPN, SSH

- **Terminal server access:** RDP, VNC, Citrix

(Full details of these protocols and the ports involved are contained in the eduroam Technical Specification.) Without this requirement there would be no guarantee that a guest user would be able to use offsite services provided by their home organisation, and the support load for both home and visited organisations would be greatly increased. With this requirement, offsite services that are provided using the listed protocols should work from any eduroam visitor facility.

Organisations whose policies require them to apply content filtering or rate limiting for guest users are permitted to provide their eduroam service via application proxy servers, but are required to publish this fact on their eduroam web pages so that guests and home support staff can identify the cause of any problems that might arise with those applications that require a direct connection.

Policy Controls

As well as technical controls, the eduroam Policy allows organisations to regulate the behaviour of visiting users and to ensure that any misuse of the system can be traced and dealt with.

The IEEE 802.1X network access system that is used by eduroam requires users to authenticate themselves before they can send any IP packets beyond the local visitor network. When an organisation confirms that one of its users has been authenticated successfully, the eduroam Policy requires that organisation to then take responsibility for any breach by that user of either the eduroam Policy or the Acceptable Use Policies of either JANET, the home organisation or the visited organisation. Home organisations are required to retain logs of authentication requests for at least three months. Therefore, a visited organisation that records which authentication decisions relate to which locally allocated IP addresses can subsequently ask the appropriate home organisation to deal with any complaint arising out of its users' activities.

The eduroam Policy requires users to respect the policies of visited sites and to cease any activity which they are informed is in breach of those policies.

For short term problems, visited organisations have the technical ability to suspend visitor access for users from a particular home organisation. Depending on the technology used, they may also be able to suspend an individual user's access. Since such measures will disrupt the operation of eduroam, organisations are required to notify eduroam operations staff of any such action. eduroam will then assist both organisations involved in resolving the problem.

Technical Controls – Protecting Credentials and Communications

Any remote access service carries some risk that users' credentials and other information may be exposed as they pass across network and computer equipment that is not under the control of the home organisation. eduroam uses technical controls to reduce the risk during its login process, but users and home sites should also take precautions to protect subsequent traffic.

The IEEE 802.1X options mandated by eduroam ensure that when users authenticate to the

service, their credentials are transferred from their computers to their home sites over an end-to-end encrypted tunnel. Provided the user's computer is configured to verify that it is talking to the home site authentication server (this is normally achieved by validating an X.509 certificate on the server) before sending the user's password, the password cannot be discovered by any intervening network or computer, even if it has been compromised.

Once a user has logged in to eduroam their communications are treated like any other remote connection across JANET and the Internet. eduroam does not encrypt this traffic. If users or sites need it to be protected they should use an encrypted VPN or the secure HTTP protocol..

References

- eduroam Home Page: http://www.ja.net/roaming [1].
- Connecting Wired and Wireless Networks: http://community.ja.net/library/advisory-services/connecting-wired-and-wireless-networks [2].

Links
[1] http://www.ja.net/roaming
[2] https://community.jisc.ac.uk/library/advisory-services/connecting-wired-and-wireless-networks