Wireless security

- Network Authentication Methods
- eduroam

While wired networks tend to rely, at least in part, on physical restrictions on connection to the network to protect the privacy of communications and the accountability of messages sent by them, wireless traffic must be assumed to be ‘public’ since radio signals leak beyond the physical bounds of buildings and effective remote eavesdropping equipment is readily available. As a result, wireless LANs typically implement a higher standard of security (including data encryption and audit trail) than wired infrastructure (for more information see the Wireless Security Factsheet [1]). Furthermore, as a network service aimed particularly at mobile devices and users who may have made use of other networking contexts with less protections in place, WLANs must also be resilient against inimical software on the client nodes themselves (e.g. Trojans and viruses). For this reason, it is rarely appropriate to connect wireless and wired networks together without some form of filtering and access control at the junction between the two network technologies (see the Connecting Wired and Wireless Networks Factsheet). Even the most secure WLANs rely to a degree upon responsible user behaviour to retain their integrity, both when accessing the local infrastructure and when using potentially less secure networks elsewhere (see the Factsheet Safe Use of 802.1x Wireless Networks [2]).

Network Authentication Methods

Given the potential hostility of the wireless environment, a robust audit trail is essential to fulfil both network management and some legal obligations. The first step in this trail is to identify the connecting user reliably. Currently, there are two main authentication methods for accessing wireless networks:

- 802.1x-based
- Web-based redirect

802.1x is a port based IEEE OSI layer 2 authentication method between a mobile node and an access control device, either a switch on a wired network or an access point in a wireless context. Robust encryption and mutual authentication make 802.1x the current leading security option for controlling network access at the edge. By providing a framework able to support a number of authentication technologies, 802.1x can accept various proofs of identity, be they token-based, conventional username and password, or certificates. 802.1x also allows the access control device to grant different types of network access depending on who the authenticated user is, or the patch level and anti-virus status of their device (e.g. unpatched systems could be assigned to a quarantine VLAN until the condition is remediated).

When users attach to a network that uses **web redirection** authentication, they get a docking IP address (and associated local network configuration) via DHCP, but are initially unable to

receive and send traffic outside a restricted domain, typically gaining access only to web pages about the organisation or service and to a web-based SSL-encrypted login interface. To gain access beyond this, users must launch a web browser which will be redirected automatically to the authentication web page. Once username and passwords have been entered and authentication is successful, users are then granted external access in accordance with the organisation's policy (e.g. by client-specific dynamic access control on an authentication appliance or by VLAN reassignment).

eduroam

Both 802.1x and web-based redirect typically rely on existing separate authentication servers, so local users can authenticate using their normal login credentials. However, eduroam [3] can also be used, if organisations wish, to allow guests from other participating JANET-connected organisations to authenticate and gain access to JANET using their home login credentials. eduroam [3] provides the means to tunnel an access authentication request securely from the visited organisation's network access server to the guest's home organisation for evaluation, and to return a response. By handing off the authentication in this way, the visited organisation is spared the administrative burden of identifying the user and managing temporary accounts, and receives a guarantee from the home organisation that the visitor is a current member in good standing by virtue of any 'access-accept' response returned.

eduroam policy [4] requires that guests must respect the policy of the local site they are visiting as well as abiding by the JANET Policies and those of their home organisation.

JANET may only be used to provide network access for guests who are visiting the organisation for educational or research purposes. Organisations that wish to provide network access to members of the public, for example delegates at commercial conferences or users of other facilities of the organisation, must not use JANET for this. Other options are described in the Factsheet on Guest and Public Access [5].

Links
[1] http://community.ja.net/library/advisory-services/wireless-security
[2] http://community.ja.net/library/advisory-services/safe-use-8021x-wireless-networks
[3] http://www.ja.net/eduroam
[4] https://community.ja.net/library/janet-services-documentation/eduroam-policy
[5] http://community.ja.net/library/advisory-services/guest-and-public-network-access