

# JANET Roaming Security Measures

Security was a major requirement in the design of JANET Roaming, to ensure that organisations that provide visitor facilities, and the visitors who make use of them, are not exposed to additional risks outside their control. JANET Roaming should present fewer risks than the existing ad hoc arrangements for guest users. This factsheet explains the security measures within JANET Roaming 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). JANET Roaming 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 JANET Roaming 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). JANET Roaming 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, VPN [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 requirement and risk assessment.

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

- **Web browsing:** HTTP, HTTPS
- **File transfer:** passive FTP, passive SFTP
- **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 JANET Roaming Technical Specification.) Without this requirement there would be no guarantee that a visiting 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 JANET Roaming visitor facility.

Organisations whose policies require them to apply content filtering or rate limiting for visiting users are permitted to provide their JANET Roaming service via application proxy servers, but are required to publish this fact on their JANET Roaming web pages so that visitors 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 JANET Roaming 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 network access systems that are recommended for use with the JANET Roaming (either web-redirect or IEEE 802.1X) require 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 JANET Roaming Policy requires that organisation to then take responsibility for any breach by that user of either the JANET Roaming 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 JANET Roaming 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 JANET Roaming, organisations are required to notify JANET Roaming operations staff of any such action. JANET Roaming will then assist both organisations involved in resolving the problem.

## Technical Controls – Protecting Credentials

Any remote access service carries some risks that users' passwords may be exposed as they pass across network and computer equipment that is not under the control of the home organisation. JANET Roaming implements technical measures to protect passwords – however, these can inevitably be defeated by users who do not take sensible precautions. For example, a user who carelessly uses the same password to log on to both their office computer and a third party discussion site cannot be protected by JANET Roaming.

The protocols used by JANET Roaming to transfer passwords from the visited organisation to the home organisation all use encryption. The JANET Roaming specification also requires that encryption is used to protect passwords between the client computer and the visited organisation's JANET Roaming gateway. Organisations providing visitor facilities must ensure that these systems are configured and maintained securely to reduce as far as possible the risk of them being compromised.

JANET Roaming support for VPNs and the option to use IEEE 802.1X authentication protocols allow home organisations to implement their own end-to-end encryption of both passwords and data where these are required. However even the basic JANET Roaming service will protect passwords as well as most internal networks.

## References

- JANET Roaming Home Page: <http://www.ja.net/roaming/>
- JANET Roaming Technical Specification: <http://www.ja.net/roaming/documents/techspec.doc>
- Connecting Wired and Wireless Networks: <http://www.ja.net/services/publications/factsheets/068-connecting-wired-and-wireless-networks.pdf>

JANET® is a registered trademark of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association is the registered user of the trademark. JANET, the United Kingdom's education and research network, is funded by the Joint Information Systems Committee (JISC).