Published on *Jisc community* (https://community-stg.jisc.ac.uk)

Security measures within the Janet backbone

5.1 Policy Filtering in the Backbone Routers

As noted in the previous section, any filtering decisions that were made by the Janet backbone routers would inevitably apply to all sites connected to the network. Any decisions to filter would therefore need the agreement of the whole Janet community. It is unlikely that such agreement could be reached for any service, and the benefits would be extremely limited. In particular, filters applied at the backbone routers would not, in most cases, protect organisations from each other. Sites would therefore need to duplicate the filtering at their own routers to protect them from hostile users elsewhere on the Janet network.

The Janet AUP [1] prohibits certain types of use of the network: however, these prohibitions are not of the kind that can be enforced by network filtering. In any case, the AUP has exceptions for activities performed in the cause of legitimate academic research so it is hard to make a definitive statement that any particular traffic flow is contrary to the AUP.

For these reasons, it has been decided that it is not appropriate to use filtering in the backbone routers as a measure to implement security policy for sites connected to the Janet network. Customers of the network may opt-in to filtering provided by some Janet services [2]. Filters may be used in the backbone for operational reasons, as described in the next section.

5.2 Operational Filtering in the Backbone Routers

Although filtering for policy reasons is not appropriate, there are good operational reasons to implement filters in the Janet backbone routers. The most obvious of these is to protect the routers themselves against attack. Filters may also be implemented if they are an effective way to resolve or mitigate operational problems, for example if a Denial of Service attack is in progress, either directed against hosts connected to the Janet network or using those hosts to attack a third party. Janet is designed as an open network with a very high capacity, multiply connected resilient infrastructure. This architecture means that we can't always stop all sources of attack, but we do endeavour to block and filter Denial of Service attacks when they are detected. In many cases attacks are best filtered on an institution's network where application level filtering is becomes a feasible proposition.

In accordance with the Janet Security Policy [3], these filters will usually be temporary and may be installed at the request of sites, the Janet CSIRT or the Janet Network Operations Centre.

5.3 Source Level Routing

Source Level Routing (SLR) is an IP routing technique that allows the originator of an IP datagram to specify the precise route that delivery should take through the network (as opposed to letting the routers on the network determine the route based on their routing tables). It is implemented by placing in each IP datagram a list of addresses of routers to be traversed to get to the destination. SLR is intended for use in circumstances where there are exceptional routing arrangements that may not be known to intermediate routers.

At present there seems to be no legitimate need for SLR to be used across the Janet backbone. There is, however, a possibility that the technique might be used in an attack to assist in impersonating a trusted host. The Janet backbone routers have therefore been configured to reject any packets that attempt to use SLR. This decision will be reviewed in future if it is believed that SLR could be of significant operational use within Janet. Sites that are concerned about the possible hostile use of SLR should also configure their own routers to reject such packets, since a packet will only be recognised by the routers named in its delivery route. If an SLR packet passes through a Janet router on the way between two designated routers then it will be discarded.

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/security-measures-within-janet-backbone

Links
[1] http://community.ja.net/library/acceptable-use-policy
[2] https://community.ja.net/library/janet-services-documentation/janet-and-internet-filtering-technical-guidance
[3] https://community.ja.net/library/janet-policies/security-policy