

User Authentication

When things go wrong it is useful to be able to identify the people involved, both the possible victims and those who may have caused the problem. This is as true on computer networks as anywhere else. The aim should be to have all users of JANET identify themselves whenever they are on the network, but in a few situations the cost or inconvenience of achieving this may be unreasonable.

Why identify users?

The *JANET Security Policy* requires that connected organisations exercise 'responsibility about giving and controlling access to JANET'. The Policy does not mandate that everyone accessing the network must log on to it, but leaves each organisation to decide how to control network access responsibly.

Likewise, the law of the land and the expectations of society do not insist that every action be traceable to an individual. There is no legal requirement to identify or record every logon, e-mail, web request or mouse click. However activity on a network can almost always be traced to an organisation. Organisations are expected to behave responsibly and will be blamed if they are not seen to do so. For example:

- JISC (Joint Information Systems Committee) may, in extreme cases, suspend or withdraw the right to connect to JANET if an organisation's behaviour represents a serious threat to other users of the network;
- other users may be reluctant to accept communications from an organisation that does not deal promptly and effectively with problems, for example some JANET sites have found themselves on blacklists that prevent them exchanging e-mail with others;
- in a few circumstances, the courts may fine an organisation or imprison its directors if crimes were committed as a result of their negligence, in other words, if they have not taken reasonable care to avoid causing foreseeable harm;
- more often, courts may require organisations to pay damages to individuals or businesses who have suffered loss or harm because of their negligence;
- society and the press may publicly blame an organisation that fails to meet the standards expected of it.

JISC's Legal Information Service (JISC Legal) publishes an article on the legal liability of universities and colleges at: <http://www.jisclegal.ac.uk/publications/legalRisks.htm>

Organisations should consider the risk of misuse when deciding if any groups of users and systems do not need individual identification. An individual account should only take a few minutes to set up. If the user only needs it for a few seconds then creating and deleting an account may be an unreasonable overhead. However, the convenience of not setting up and managing individual accounts cannot justify a significantly increased risk of harm to others and the organisation.

Harm can be caused by hacking, malicious messages, downloading illegal material and many other types of activity, the scope for which will normally be less where an individual's access is limited to a few systems, rather than the whole Internet. However, if critical internal systems may be accessed then the potential harm should not be underestimated.

How to identify users

The most common way for individuals to identify themselves is to log on when they sit down at a terminal, however this is not the only option. If users have to prove their identity to get into a workstation room then a paper record can be kept of who used which workstation when. Some organisations let anyone see a limited set of web pages but require a login to gain access to other sites or services. However they are collected, records linking a user to his or her IP address should be kept long enough for misuse to be reported and investigated. Further information on recording this information is available at: <http://www.ja.net/services/publications/technical-guides/logfiles.pdf>

If usernames and passwords are used there are a number of ways to issue them. Staff and students of the organisation should have their own local accounts. Visitors may also have local accounts, or authorised staff may be enabled to set up daily accounts for their guests. Visitors from other organisations may be authenticated by their home organisation if both organisations are members of JANET Roaming or another partner in the TERENA (Trans-European Research and Education Network Association) eduroam federation.

Even if individual identities are not checked, access to the JANET network must still be limited to those who are known to the organisation. Knowingly providing network access to strangers is likely to be a breach of JANET policies and to be considered irresponsible by other users of the network. Access may be limited by physical barriers, although this does not work for wireless networks, or by providing a temporary access code to visitors such as conference delegates. Organisations may wish to arrange their networks so that these visitors do not accidentally obtain access to internal resources controlled or licensed by IP address.

Organisations that provide access to networks, and users who benefit from that access, should regard it as normal to require an individual identity. Systems for establishing electronic identity are becoming easier to use and manage. In a few situations there may be a justification for not checking and recording identity but this should only be done after a rational assessment of the risks and benefits.

References

JANET Security Policy:

<http://www.ja.net/services/publications/policy/security-policy.pdf>

JISC Legal Information Service article on legal liability of universities and colleges:

<http://www.jisclegal.ac.uk/publications/legalRisks.htm>

JANET Guidance Note: Logfiles by A Cormack GD/NOTE/008 (02/08):

<http://www.ja.net/services/publications/technical-guides/logfiles.pdf>

TERENA Mobility Task Force glossary and notes on authentication by home sites:

<http://www.terena.nl/tech/task-forces/tf-mobility/>