Motivation for logfiles

Without collecting and analysing logfiles, it is impossible to know what is happening on a computer system or service. There will be no indication of faults and misuse and when they finally result in complaints from users, there will be no evidence to show the cause of the problem or how it can be cured. Failure to keep logfiles therefore leads rapidly to an unreliable system on which users will naturally be unwilling to rely for any critical function. Reliable systems can only be achieved if their performance is recorded and action taken to prevent or remedy problems. Logfiles also provide information about the usage of a service, and allow upgrades or alternative provision to be planned and installed before the load on the existing system becomes a critical problem.

As well as these internal pressures to deal with problems, there are also likely to be external pressures. Wide Area Networks, such as Janet, are shared resources and a problem on one computer or site can soon affect others. For example, a fault that causes excessive network traffic is likely to cause congestion for others as their traffic competes for the finite bandwidth and routing resources available. In cases of misuse it is common for an individual at one site to attack systems or users at others, or for a compromised computer to be used to send spam, participate in denial of service attacks or host unwanted services such as phishing or copyright distribution sites. If reasonable requests to deal with problems are not satisfied then the responsible site is likely, at best, to suffer a tarnished reputation in the eyes of its peers. The Janet community, and the policies that support it, require its members to behave responsibly and not to cause unnecessary problems for others or harm the good reputation of the Janet network. More widely, many organisations and networks now employ blacklists to restrict traffic from sites or networks considered to be a frequent source of problems. An organisation that finds itself on one of these blacklists may have difficulty sending e-mail or other traffic and may have to spend considerable time and effort to be removed from the list.

In extreme cases failure to deal with problems, whether arising from the lack of logfiles or inability to use them, may even lead to legal cases. Service providers have paid large damages to individuals or companies harmed by the actions of their users. At present we are not aware of any cases where educational organisations have been held liable for the computing activities of their students, but solicitors have expressed their view that courts might indeed find against the organisation. Another area where legal action might arise is in negligence: it has been suggested that if an organisation had been warned of a problem but did not deal with it then subsequent victims might have a valid claim against the organisation.

In the case of faults, the best that logging can offer is the early detection and resolution of problems. However, in cases of misuse there is good reason to believe that a publicised practice of recording and analysing logfiles and dealing with those who misuse the system may itself be an effective deterrent. Logfiles can therefore act as a preventive measure, reducing the number of problems experienced by users and system owners. Logfiles enable an organisation to improve its service to its own users and maintain a good reputation with others. In the near future, it appears likely that logfiles and a process to use them may be

essential to defend against threats of legal action. It is important to note, however, that simply keeping logs is unlikely to be sufficient. It is also important to have processes for checking them, analysing the information they contain, and dealing promptly and effectively with problems.
