UCL Log Retention Guidelines

Misuse of the Internet and its systems cannot always be detected immediately. Traceability may be required some time after an event has occurred. This means that it is necessary to keep the logging information in case it is wanted.

Best Practice is to keep the logs required to provide traceability for at least three months. This can involve a significant commitment of online storage space, so it may be necessary to rotate older information onto magnetic tape or other offline storage media.

Often the UCL Computer Security Team (CST) receive requests from external organizations, for tracking evidence of possible criminal activities, and to assist in the tracking and detection of compromised machines. It is therefore important that proper authorisation, auditing and accounting be kept of access to and from UCL resources.

Data protection requirements

The type of data which is logged for traceability is almost certain to be personal data within the meaning of the Data Protection Act (1984 and its 1998 replacement). Even if the data does not identify individuals directly, it can be combined with other data so as to do so; that, after all, is the raison d'être for logging it in the first place. Best Practice is to secure all of the data against casual examination so that only authorised personnel can extract information about users.

One of the Data Protection Principles is that data should not be kept for longer than is necessary for the purposes that have been declared, and naturally it is important to conform to this. However, in the special case of "traffic data" (which in this instance means the records of phone calls made to an ISP) the European Directive 97/66/EC requires (paraphrasing considerably) that the data must be destroyed or anonymised once it is no longer required. The LINX has secured the opinion of the Data Protection Commissioner that an upper limit of six months should apply. After that period traffic data must be discarded or processed so that it cannot be related back to identifiable individuals.

UCL-CST advise that the following points be used as a guideline for correct logging:

- All log collectors (i.e. Syslog servers, Event Viewer Servers) should have accurate time, which will be achieved by using the UCL NTP time servers as a reference clock
- Departments should keep a record of which user is using which machine, with its corresponding IP and MAC address and location.
- DHCP servers should log session times (both connect and disconnect), with corresponding MAC addresses/IP Addresses. If possible, MAC addresses should be tied up to a username.
- RADIUS logs should contain user name, IP address assignment, callback telephone number, session time, etc.
- Web and FTP server logs should contain client IP address, files accessed, request time, query string, etc.
- Email server logs should contain sender/recipient addresses, message date and time, relay hostnames, etc.
- Firewall and IDS logs should contain IP addresses, packet payloads, date and time of connections, protocol used, etc.

(Portions of text taken from LINX BCP guidelines on traceability)