Aftermath

In this particular incident, the initial tip-off led directly to the departmental network containing the compromised hosts. This information is not always so readily available, since IP spoo?ng can also be used to simulate traffic from machines on many different networks. Such a situation could be handled by repositioning the network monitor on the backbone (at M' in the diagram, for example), and again examining the source MAC addresses of attack packets (but note that performance is likely to be a concern, with monitors dropping traffic at gigabit speeds). In this case, the MAC address will identify the router (R1, R2 in our diagram), and hence the sub-network from which the traffic originates. It is, however, much better to take a preventive approach and use egress ?lters on the departmental routers to prevent spoo?ng of non-local traffic [6] [1].

We had some further success using the Nessus remote security scanner [7] [2], which can detect a number of inactive DDoS agents, handlers and other backdoors. Several were located and steps taken to secure them.

Although this description relates to the technical aspects of responding to a particular incident, it is worth emphasising that these steps are primarily reactive in nature. The greatest challenge facing our institution now is to develop our organisational controls and improve awareness of security issues. Only by tackling the much broader problem can we hope to see the frequency of such events signi?cantly reduced.

Links
[1] https://community.ja.net/library/janet-services-documentation/references-3
[2] http://www.nessus.org/products/nessus/