# The Cost of Policing Security Incidents on the Central VAX Clusters

Breaches of security on the central VAX clusters (VXCERN and VXENG) come to the attention of the support staff at approximately a rate of one incident every two months. Due to the vast number of different accounts being used per day on VXCERN in particular (around 1300), it is reasonable to assume that there are a number of unauthorised activities that are never detected. In fact, several years ago, the infamous Computer Chaos Club boasted that, outside prime shift, the number of hackers on the VXCERN service outnumbered *bona fide* users! (This was thought at the time to be a wild exaggeration!)

Each detected incident varies in seriousness, from the simple use by a CERN user of an account he is not authorised to access, to the deliberate use of several accounts by a non-CERN user for nefarious activities. The manpower invested in policing incidents is made in accordance with the perceived severity of the attack. For the simple mis-use of an account this typically involves making contact with the group administrator concerned, and deciding on an appropriate action, for example blocking the account, or creating the user a valid account of his own. In the case of the serious attack, the costs are considerably greater. The paragraphs that follow describe one particularly unpleasant attack that was made on VAXes not just in the CERN Computer Centre, but across the CERN site, Europe and even to VAXes in the U.S..

In November 1991, a routine test of checksums on system images on the Aleph Offline Cluster, alerted the system manager there that a rogue version of the SYSMAN utility was installed. He promptly began tracing all remote accesses made to his cluster, and informed the Central VAX support team of the details. Checksums were then run on the Computer Centre VAXes, revealing that many of them were also hosting the rogue image. In the meantime, it was realised by careful inspection of the accounting data on all affected machines, that several users with no privilege had somehow been running with all privilege bits set. Telephone conversations with the system managers of the major VAX clusters at CERN revealed that the rogue SYSMAN was widespread. Work began in parallel to discover which user accounts had been compromised on all systems. This involved around eight system managers. In addition, work began on disassembling the rogue image in an effort to understand what it did. The CERT in the U.S. were informed that a major security incident was happening at CERN, and their advice was requested.

The accounting files on the central machines revealed a catalogue of severe hacking activity that had been going on since early in 1991. Moreover, the attacks were continuing as the support team worked. In the end, after approximately four man-weeks of integrated effort on the part of all system managers involved, all accounts know to have been hacked were blocked, and all copies of the rogue image, and associated hacking software, had been removed.

During the hacker's activity, many calls to outside laboratories had been made, using public networks, the use of which is charged to CERN by the PTT. It is estimated that the real cost of the calls made by the hacker amounted to a sum rather less than ten Swiss Francs. The CPU time involved was negligible in the sense that it was used typically outside normal working hours, and in any case amounted to very little. The hacker created several directories on disk in most accounts he used, and placed there his "hacker's toolkit" of software. Again, the use of disk space must

be considered negligible in the context of impacting the total space available on the machines involved. Finally, the inconvenience and lost time for the owners of the hacked accounts should be taken into consideration when evaluating the cost of this hacking attack. Several accounts were blocked, requiring the real owners to go to some trouble to have them re-activated. The lost time could be conservatively estimated at one physicist-day, integrated over the users involved.