

## ***Archiving Data in a Firewall Intrusion System***

### ***Overview***

When the systems integration division of Concert Communications Company wanted to offer a secure Managed Firewall and VPN capability over their existing internet service, they naturally went to the experts – Checkpoint Software of Israel and UK based storage management experts, K-PAR Systems.

Concert needed to store all activity on the managed networks in a safe manner and K-PAR were selected for their systems integration experience. Because of the highly innovative nature of the system Concert wanted K-PAR to be directly involved in the installation and training of the software.

### ***The System***

Concert manages the firewall systems of a number of their corporate customers remotely from two global management centres. For legal reasons the group chose to log the firewall activity and configuration data on non-tamperable media which would be retained for a period of over five years. After an extended test period the group selected recordable CD media in a jukebox environment.

The Concert InternetPlus network consists of a high bandwidth Internet backbone and delivery to site over a choice of transports: frame relay, X21, V35, local ISP, public network or leased line. All the firewalls are SUN workstations running Solaris.

Security information, consisting of exposure analysis and detected intrusion attempts, firewall logs, policies and configuration details as well as throughput statistics and customer reports are logged on a per customer per site basis in a normal directory structure. This information is recorded at pre-determined times (or when more than 100 Mbytes has been collected) using K-PAR's ***Archimedia*** software.

***Archimedia*** is an archive and storage management package designed to work with the latest CDR and optical jukeboxes. ***Archimedia*** enhances the usability of jukeboxes by transparently caching data on the hard disk and allowing the user to access the jukebox as one big disk,

simplifying system management. Other packages required *Concert* to format the data before sending it to the drives to make the CDs; **Archimedia** handles all this as a background activity.

"The systems allows us to automate the process of keeping a secure audit trail", commented Richard Davison, Development Manager for the Concert project. "Before we had to rely on a 9GB disk and regular tape back-ups, which got us going but was hardly a long term solution. This is scalable, reliable and simple to manage." The new system has been operational since August 1999 and is expected to double in size every two years.

The CD jukebox selected was from leading European manufacturer Plasmon Data. *Concert* selected the Plasmon D-240-24 with 4 readers and 2 CD recorders inside each box. The Plasmon D series has a swap time of 4 seconds and allows 156 Gbytes of data to be stored on-line.

For reliability and security the group decided to enable the CD mirroring facilities of the K-PAR software so that two copies of each disk are manufactured, one is immediately exported and held in a secure off-site facility. For legal reasons the integrator decided that all firewall activity should be stored on a legally admissible tamper proof media such as CDROM. In addition, *Concert* chose to use a 9GB RAID disk array for the Jukebox cache and intend to permanently cache certain key files. "Eventually, the jukebox will fill up and we will start exporting CD's at this stage, we don't want to lose time finding off-line CD's if we ever have to restore a firewall quickly" said Richard Davison.

## **FireWall Software**

The requirement to protect a network from intrusion and unauthorised activity has for a long time been seen as one of the most critical aspects of enterprise security management. Check Point Firewall-1 is an industry standard in the Firewall marketplace with strong encryption and VPN "tunneling" capabilities. *Concert* enhance this technology with real -time intrusion detection which monitors the firewall and alerts on suspicious activity, and an exposure analysis service which tests and reports on a site's vulnerability to "hack". Events are classified and summarised in order of priority, enabling the manager to see at a glance the nature of any intrusion or vulnerability.

## ***K-PAR Systems***

***K-PAR Systems Ltd*** of Bristol UK the experts on CD and optical disk technology. The group has been operating since 1989 and has provided leading edge solutions for some of the worlds leading corporations. Companies using the technology included BMW, Rover, Opel, National Westminster Bank and Reuters.

K-PAR's expertise is not only in software development but also in ensuring that the overall system meets user requirements and performs according to specification. K-PAR has been involved in the development of a number of bespoke systems in the defense, medical imaging, video-on-demand and pre-press markets where existing technology was deemed to be too slow or inappropriate.

## ***Concert Communications Company***

Concert, a wholly owned subsidiary of British Telecommunications PLC with offices in Reston, Virginia, is the leading provider of global telecommunications services. Today, Concert serves about 4, 700 customers accounting for nearly \$3 billion in revenue under contract, and its network reaches 800 cities in 52 countries. Concert services are available through 47 distributors worldwide.



**174 Cheltenham Road, Bristol BS6 5RE UK**

**Tel:+44(0)117 9421141 Fax:+44(0)117 9420564**

**Email: [sales@k-par.com](mailto:sales@k-par.com) Web: <http://www.k-par.com>**