CHARON-VAX application note

AN-029 Recommendations Regarding Security of CHARON-VAX Host Platforms

Author: Software Resources International Date: 16 June 2004

Applies to: All CHARON-VAX versions **Platform:** Windows hosts.

The problem

VAX customers, accustomed to the legendary security and stability of the VMS operating system, often express concern about the WINDOWS PC host upon which the CHARON-VAX emulator is layered. In this document we make a series of recommendations to assist customers in achieving the highest level of security and stability on the PC replacement platform for your VAX.

The recommendations

The following recommendations are considered good practice in all PC systems but make particular references to CHARON.

Since the CHARON-VAX emulator should be the sole layered application running on the WINDOWS PC platform, the first security measure is to disable all unnecessary WINDOWS services, especially those designed to enable Internet access, such as IIS and DHCP. Disable/unbind the Client for Microsoft networks if the "Windows Network" is not in use. This is similar to dedicating the Network card solely to CHARON. See Application Note 33 for Required Windows Standard Services.

In addition, all unnecessary ports can be closed to external communications (for example, ports 137-139). In taking such steps care has to be taken not to leave the host system in an inoperable state. If in doubt consult Windows help and Windows security guides. An excellent additional reference site for a thorough discussion of concrete steps to reduce risk may be found at Gibson Research Corporation's website www.grc.com

Once the PC replacement platform has been secured as much as possible by shutting down services and ports, the next step is to examine all the machines to which the CHARON-VAX PC is connected, and how they are connected. If the Ethernet adapter(s) on this PC platform only have the NDIS driver enabled for DECnet, then it is only possible to communicate with the PC via DECnet via the emulated VMS OS, meaning it is impossible for a virus to arrive/attack at the PC level.

If an Ethernet adapter on the PC replacement platform uses the TCP/IP protocol, closer scrutiny must be applied. The IP protocol can be used in either LAN or WAN environments without necessarily enabling or sanctioning Internet access. If the customer has a TCP/IP-based corporate LAN or WAN, a firewall should be implemented to sit between these IP nodes (including CHARON-VAX) and prospective attackers. A sophisticated firewall will provide a number of functions, including the ability to shut down inbound/outbound ports for Internet protocols such as HTTP (i.e., no web surfing), SMTP (i.e., no Internet email), FTP (i.e., no file transfer), et al. Other functions of a firewall may include NAT address translation and other forms of address redirection.

If all of the above measures are in place there should be no need to be run virus protection on the PC platform. If the customer still wishes to implement this additional layer of protection, then CHARON-VAX should be shut down before a virus scan can be run.

These recommendations are important because CHARON is a Windows application and although when the PC platform is penetrated, the action of any virus, worm or Trojan will in the first instance be limited to the WINDOWS layer and will not directly penetrate the VMS operating system, it might generate extreme load on Windows, kill processes or delete files.

See also Application Note 35 for further details of the CHARON-VAX Ethernet adapter security.

[30-18-029]