AN-35 CHARON-VAX network adapter security

Author: Software Resources International Date: 3 June 2004

OVERVIEW

Many CHARON-VAX products use a Windows® based host system. These host systems are vulnerable to virus attacks via their network connections. The design of CHARON-VAX networking allows all network access to its host to be disabled, so that any attacks from the network via the network adapter assigned to CHARON-VAX can never influence the host software other than momentarily increase the network load.

Consequently, disabling host based networking is a recommended procedure for all CHARON-VAX installations.

STRUCTURE

The CHARON-VAX network connection seen from VAX/VMS has the following layers:

VAX/VMS

CHARON-VAX-VAX

VAX Ethernet adapter emulation

NDIS5_port

NDIS5 packet driver

Network Interface (NIC) driver

----physical network----

ETHERNET FRAME RECEPTION FROM THE NETWORK

A frame arriving from the physical network is read by the NIC driver into the MS NDIS5 Packet buffer. This packet is directed to every upper binding.

The CHARON packet protocol (NDIS5) driver is the only up link. This assumes that the CHARON-VAX network installation procedure was correctly followed: The CHARON packet protocol (NDIS5) driver was installed and all protocols except the NDIS5 driver are disabled on the adapter used for CHARON-VAX. No additional networking software is installed on the system that intercepts the communication between the NDIS5 port and packet driver.

The CHARON packet protocol (NDIS5) receives the packet from the NIC driver and is designed to redirect it to the NDIS5_port in the CHARON-VAX application without any processing. Note that the frame as read from the physical network is transferred completely without processing of its contents, thus preventing any Windows virus code to be executed.

The only user of the CHARON packet protocol (NDIS5) driver' is the NDIS5_port configured in CHARON-VAX, which delivers in turn the packet without any processing to the emulated VAX Ethernet adapter. Identical to the operation in a hardware VAX, the frame is delivered to the emulated VAX memory.

At this point, only the VAX instruction interpreter can operate on any executable code found in the Ethernet frames, rendering any i86 instruction code meaningless. Furthermore, most Windows system attacks exploit particular vulnerabilities in Windows applications or services that are not visible nor reachable in the emulated VAX environment.

ETHERNET FRAME TRANSMISSION BY VAX/VMS ON CHARON-VAX

The procedure works as receive but in reverse order. As with receive the frame is kept untouched through the whole path and appears on the physical network exactly as it was delivered to the CHARON-VAX Ethernet adapter emulation by VAX/VMS.

ERRORS TO AVOID

Forgetting to disable all bindings to the NIC driver except the CHARON packet protocol (NDIS5) driver. As a result, the other binding (that likely will be Windows applications or services) can potentially receive unwanted traffic;

Some Windows applications can install the filters on top of the NIC driver (in between the NIC driver and the CHARON packet protocol). Typically security software does so to sniff for viruses or unauthorized access attempts. For designated CHARON-VAX adapters these filters are not required (should be removed) to avoid any influence of the host system, and VAX/VMS can itself be configured to do the same without being vulnerable to Windows based viruses.

A CORRECT INSTALLATION ACHIEVES COMPLETE HOST SYSTEM PROTECTION

A correct installation offers an exact replica of the connection of a hardware VAX system to a network, and no packet data is extracted and provided to the Windows host. In other words, the IP frame content is processed only by VAX/ VMS making attempts to attack MS Windows host useless.

When the CHARON-VAX configuration uses multiple NICs, the procedure described above should be repeated for all NICs.

[30-18-035]