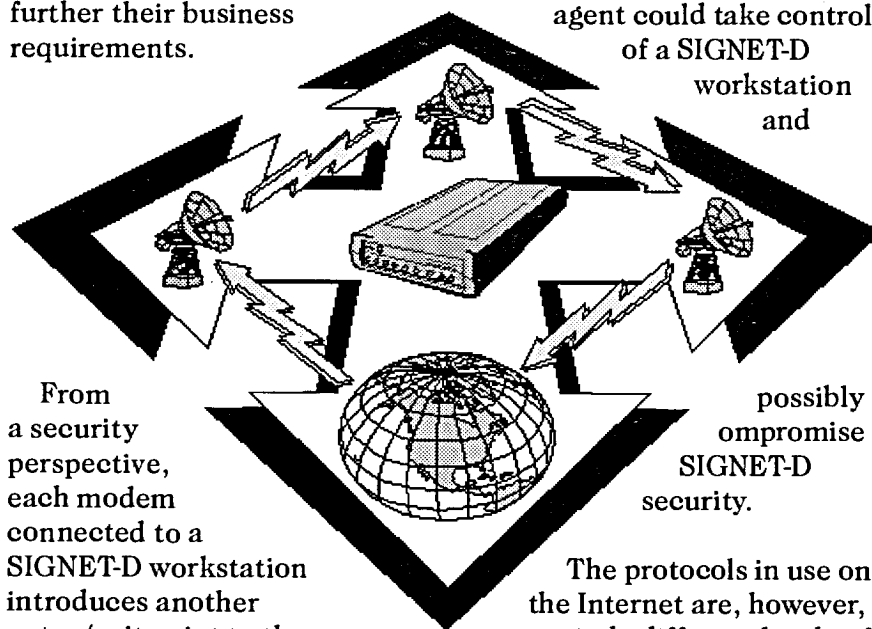# I Just Hooked Up
My Shiny New Modem!

Not so long ago, modems were used by relatively few people to access on-line information services or to transfer data. The increased popularity of the Internet has meant that many more people are now using modems to dial up their Internet Service Provider (ISP) to "surf the net," both for leisure and also to further their business requirements.

From a security perspective, each modem connected to a SIGNET-D workstation introduces another entry/exit point to the network, and thus a point of vulnerability. Prior to accessing the Internet, typical dial-out requirements normally involved unidirectional control protocols, with the calling side controlling the sessions. For instance, you might call out to a local electronic bulletin board system (BBS), and while you downloaded something from that system to your workstation, the control of that session belonged to your workstation. As a result, and where there is no Departmental "modem pool" functionality, it was considered an acceptable level of risk to allow modems on telephone lines configured for outbound dialing only. In this way, we had a reasonable level of assurance that no external agent could take control of a SIGNET-D workstation and possibly ompromise SIGNET-D security.

The protocols in use on the Internet are, however, an entirely different kettle of fish. By nature, they're designed to be bi-directional as opposed to unidirectional. If you have an Internet account with an ISP, you may be familiar with the terms SLIP and PPP. They are two types of protocols that are designed to allow modems to connect over the Internet, and if you have World Wide Web access through your modem to your ISP, you're most probably using one of these two protocols. The bi-directionality of these protocols means that, regardless of who initially called whom, regardless of whether it was on a dialout line only, information can pass both ways on the line. For this reason, the use of modems on SIGNET-D workstations to access the Internet is prohibited. Users still have the option of using standalone microcomputers for this purpose, and the imminent introduction of the "firewall" will enable direct Internet access from the SIGNET-D desktop, thus negating the need for a modem. Users may still use modems from SIGNET-D where it remains a requirement and is sanctioned by ISC, such as at micro-missions through encrypted X.25 connections.

Should you put your modem in the back corner of your closet never to be seen again, and live your life in a Luddite island of solitude? Of course not. Should you understand what possible threats to your environment and information your modem use will introduce? Of course – so that you may assess the level of risk and decide on appropriate courses of action.