

Enhanced network security protects war-fighters' platforms



By John Wemekamp



The rollout of planned Network Enabled Capability (NEC) by a number of nations' armed forces highlights the need for renewed emphasis on security. Networks are being implemented that encompass all levels of information and intelligence exchange from strategic planning, logistics, battle groups, and sensor and weapons platforms down to the tactical deployment of individuals. These networks will support not just national interests, but will also be required to support interoperability between allies and coalition partners with all the attendant issues of language, politics, culture, dissimilar assets, and doctrine. IPv6 has been selected as a secure backbone for the U.S. Global Information Grid (GIG), yet many more measures will be required to provide network integrity, data protection, and intelligence security in order to prevent attack or unauthorized access.

At the higher layers it is the responsibility of an application, its administrators, and users to maintain security. Applications are designed to prevent unauthorized user access and constantly monitor for malicious interference from insiders or disgruntled users. Shared applications over the Internet can make use of Transport Layer Security (TLS) or the earlier Secure Sockets Layer (SSL) to provide security within the application itself. These methods use authentication, keys, and encryption negotiated between servers and authorized clients.

Secure IP communications

Of course, it is at the application level that issues of culture, language, and doctrine are addressed. Similarly, TLS and SSL implementations are often specific to each type of application, putting them beyond the scope of the typical COTS vendor's product portfolio. However, IP has demonstrated vulnerabilities to a number of different attack types at routers, switches, and servers. Consequently, this is where COTS vendors' products can be used to advantage, introducing defensive technologies to protect sensitive

network assets. The most common forms of attack are sniffing, planting, connection hijacking, and Denial of Service (DoS). *Sniffing*, or eavesdropping, happens when the unprotected packet payload can be read by an intruder without the communicating nodes' knowledge. *Planting* uses a similar technique to replace the payload with either modified data or malicious code such as a *Trojan Horse*. *Connection hijacking* occurs when an attacker is able to spoof a node into believing it is connected to a legitimate network node. Hijacking can be further developed to *DoS*, where the hijacked node is, for example, a server connection that is then bombarded with access requests. These swamp the server and prevent access by legitimate clients.

“ The sheer size of the existing installed IPv4 base currently without IPsec, coupled with the diversity of developing national NEC efforts, exposes vulnerabilities to attack at the IP level. ”

IPsec was developed to address many of these vulnerabilities. IPsec introduces authentication, keywords, and encryption to the network layer, independent of any applications running on the network. It is equally applicable to IPv4 and IPv6, though its use is only mandated for IPv6. IPsec imposes additional processing overhead for authentication and encryption/decryption of the packet payload, often requiring retrospective upgrading of existing IPv4 equipment to be fully IPsec compliant. The sheer size of the existing installed IPv4 base currently without IPsec, coupled with the diversity of developing national NEC efforts, exposes vulnerabilities to attack at the IP level.

Intra-platform network security

Secure Virtual Private Networks (VPNs) such as intra-platform networks on ar-

more vehicles, Unmanned Aerial Vehicles (UAVs), aircraft, and naval vessels require strong perimeter defense if they are to provide a safe and secure backbone network. At the same time these platforms will be participating in shared applications as part of the networked battlefield and provide broader network access for communications, interoperability with partners, logistics, and support. Access protection from threats to IP integrity can be enhanced by the addition of a stateful firewall, IPsec/L2TP secure tunneling support, Network Address Translation (NAT) routing to detect IPv4 addressing irregularities, and intrusion filtering. The PMC-110 CryptoNet module from Curtiss-Wright Controls Embedded Computing (CWCEC) shown in Figure 1 is an example of such an enhanced security module, designed to complement an embedded switch or router to secure a VPN.



Figure 1

IPsec provides the basis of a secure environment for IP communications, though it will be many years before it can be implemented universally. Many new intra-platform networks can be implemented entirely in IPv6, as mandated by the DoD, using COTS equipment; however, they will inevitably be exposed in order to participate in the broader NEC and Internet environments. Until network layer communication is considered safe, adding further protection at vulnerable points is the most practical and affordable solution to enhanced network security.

To learn more, e-mail John at john.wemekamp@curtisswright.com.