



Information assurance for critical national infrastructure

Critical National Infrastructure depends on information networks for effective operation. Cost-effective Information Assurance to protect these networks is therefore essential. This article proposes how this might be achieved

The value of information on Critical National Infrastructure (CNI) networks means that they are now exposed to the same range of attack as military and financial networks. But these networks are as vulnerable to accidental damage as to hostile action. Ensuring both the resilience and security of all CNI networks is therefore critical to the nation's ability to function and demands the same level of high assurance protection as has hitherto been the preserve of this "high threat" club.

CNI network functionality must, therefore, march hand in hand with corresponding improvements in its protection. IA, and its well known elements (confidentiality, integrity, availability, authentication, and non-repudiation), are all critical in

protecting and maintaining CNI network infrastructures in a fully functioning and effective state.

However funds to pay for required improvements are currently limited. The Comprehensive Spending Review 07 calls for significant government expenditure reductions and similar budgetary constraints apply to the private sector. The need for modern, secure and resilient information networks appears therefore to clash with its affordability.

But squaring this circle is not impossible. New technologies offer solutions and differing CNI sectors offer lessons in improving CNI network security and resilience while also reducing costs. This article offers suggestions of how CNI network confidentiality and availability can be improved at reduced

cost using the concepts of Protected Core and Resilient Networks.

Protected core networks

Network confidentiality is generally assured by the use of encryption. Traditionally, where encryption is used, networks support separate security tiers, each supporting voice and data through segregated Local Area Networks (LANs). These are encrypted through the Wide Area Network (WAN) using point to point link encryption.

The costs of providing separate cabling and equipment for each security tier, the provision and management of link encryption across the WAN and the use of permanently connected or dialup circuits are high and result in inefficient network utilisation. However, just as Internet Protocol (IP) has enabled the

“New technologies offer solutions and differing CNI sectors offer lessons in improving CNI network security and resilience while also reducing costs”

voice and data convergence, a new breed of encryption solution permits security tier convergence. This simplifies encryption device management and offers a more cost-effective information confidentiality solution.

High Assurance IP Encryption (HAIZE) devices, now the mandated IP Cryptographic Standard for military use by Five Eyes nations and expected shortly to be mandated for Government use, work in a similar way to IP routers. When a user of one community needs to connect to a user of another community, HAIZE devices discover each other and establish Security Associations (SA) across the network, thousands of which can be maintained simultaneously.

EADS has brought to market the first such UK HAIZE 3 device, ECTOCRYPT™. Designed to support multilevel secure interconnection of LANs through an unclassified, or Protected Core, network, ECTOCRYPT™ eliminates the need for bulk encrypted point to point communication links or Virtual Private Networks (VPN) encrypted point to point tunnels. ECTOCRYPT™ can also be employed in LANs at building and campus level to eliminate separate cabling and ducting currently used to isolate information of differing classifications. In both cases, this collapses the need for separate security networks with significant infrastructure and support cost savings.

Encryption management

The number of link encryption devices required for current security architectures and the distribution and accounting of encryption equipment and key material presents a significant management and cost overhead for any secure network.

ECTOCRYPT™ permits centralised management and distribution of key material, including “over-the-air” re-keying. In addition the device design means that it can be handled at a lower level than COMSEC when not filled with key material and so authorised commercial couriers can be used to despatch equipment. Cost savings associated with these reduced managerial overheads enabled by ECTOCRYPT™ are substantial.

EADS has also developed a Voice Gateway on the ECTOCRYPT™ platform providing 120 channels of secure voice (up to TOP SECRET). This allows Departments to exploit secure SCIP (and subsequently VoIP)

technology and provides backward compatibility with legacy government standard Secure Voice systems, including BRENT in the near future. The device allows considerable flexibility in the use of a variety of secure voice devices, achieves significant cost savings over the current dated secure voice technologies, which is increasingly expensive to support, and provides a cost-effective solution to the management of legacy secure voice devices.

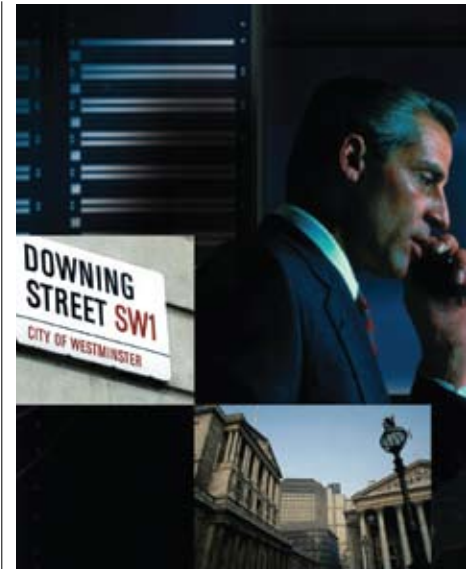
Resilient networks

The HAIZE-compliant ECTOCRYPT™ platform enables the disaggregation of the architecture from a rigid set of fixed or dial up connections. A range of network types can therefore support the underpinning connectivity. So in the ultimate (perhaps not advisable) extent the Public Internet could be the connectivity of choice. More likely it is possible to create networks that take advantage of architectures now commonly in use in banks and stock markets at considerably lower cost and with greater resilience than traditional secure networks.

Commercial companies have successfully contracted for highly resilient networks designed to support specific business requirements, with up to triple redundant links for guaranteed availability. Furthermore, the experience of these companies, such as banks, is that this can be achieved at substantially lower cost than traditional networks and with better visibility and assurance of resilience. Such innovation can now be adopted by government safe in the knowledge that it can be effectively protected by capable HAIZE devices.

Protected Core and Resilient Networks offer a simplified, multi-level secure and highly resilient CNI capability at substantially lower cost than has hitherto been achievable. Such solutions allow the cost-effective control of confidentiality and assured CNI network resilience. These developments can greatly assist in delivering the government’s Public Sector Network (PSN) initiative while helping to meet the Comprehensive Spending Review 07 targets. ●

Andy Warnes, Campaign Director
EADS Defence & Security Systems
For further details on ECTOCRYPT™ or to comment on this article, contact ukinfo@eads.com
For more information on EADS Defence & Security, visit our website www.eadsdsuk.com



Benefits of Protected Core and Resilient Networks include:

- reduced cost of LAN and WAN communications infrastructure
- reduced cost of encryption device and key material management
- a single collapsed security architecture
- flexible adoption of VoIP with cost-effective management of legacy secure voice terminals
- assured Five 9’s end-to-end availability
- improved operational agility through over the air key distribution and management.

