SAND2006-4149C

An Architecture for Multi-Security Level Network Traffic

Edward L. Witzke, Steve Gossage, Dallas J. Wiener
Sandia National Laboratories[1]
Albuquerque, New Mexico
{elwitzk, sagossa, djwiene}@sandia.gov

Abstract: Increasing availability and decreasing prices of encryptors raise the question, "Can secure and regular network traffic be carried over one infrastructure?" If this is feasible without compromising the security of network data or attached systems, benefits in both money and reliability can be realized. This paper examines the trends in encryption hardware, presents a possible consolidated architecture, highlights potential benefits, and discusses obstacles and details that would need to be worked out before wide-spread adoption.

Keywords: Network Architecture, Encryption, Network Security

Problem Description

Currently, sensitive or classified communications in most business or government installations are carried over a separate network from unclassified or open traffic. This requires duplicate (and generally parallel) infrastructures, and duplicate sets of design, maintenance, and troubleshooting personnel. This traditional model is shown in Figure 1.

We present for examination, an alternative that has the potential to save money through reduced duplication, and increase network reliability through reduction of network complexity and quantity of components. This consolidated model is summarized in Figure 2.

In this model we propose carrying secure and open traffic over the same infrastructure. This could be accomplished by using encryptors to convert classified or sensitive information to nonsensitive information that can be freely mixed with open traffic. The resulting classified network consists only of short tail circuits and individual systems or enclaves.

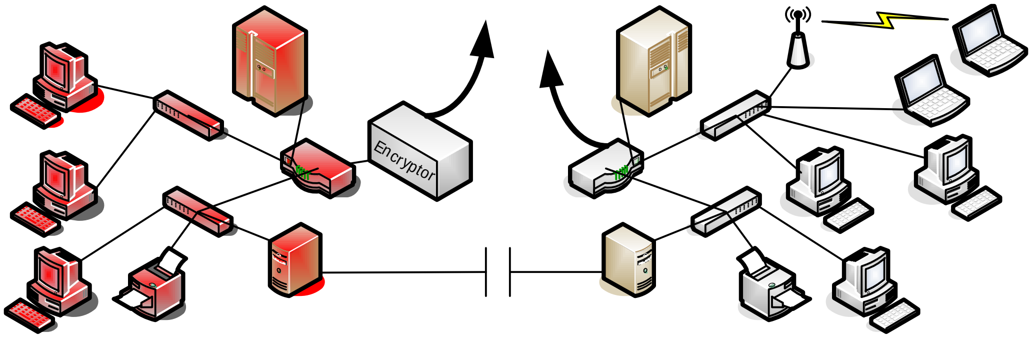

Figure 1. Traditional model for security separation in networks.

[1] Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

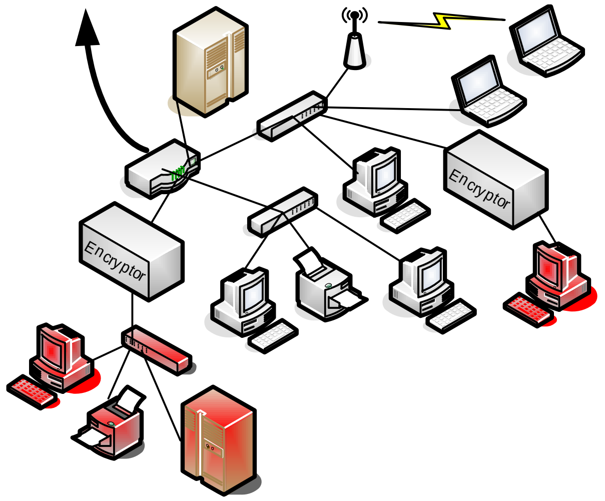

Figure 2. Overview of the consolidated model for multi-security level network traffic.

Encryption Product Evolution

A Type 1 encryption product is a classified or controlled cryptographic item, endorsed by NSA, used for securing classified and sensitive U. S. government information *when appropriately keyed*. Commercial encryption products typically use algorithms registered by the National Institute of Standards and Technology (NIST) and published as a Federal Information Processing Standard (FIPS PUB), such as AES (Advanced Encryption Standard) [1], which is FIPS PUB 197.

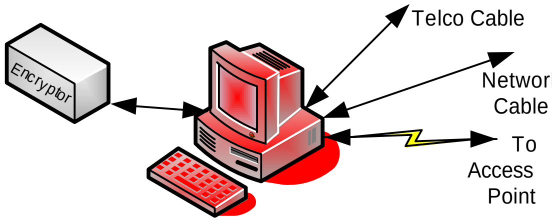

Figure 3. Attached encryptor.

Commercial encryptors implementing the Data Encryption Standard (DES) [3] or Triple DES have been available as software products, programmable logic cores, and hardware products. The hardware products can operate as an attached device (see Figure 3) like the Secure Session Encryptor from Communication Devices Inc. [2] or as an in-line network encryptor (see Figure 4). DES is now deprecated, and while Triple DES is still allowed for the protection of Federal information, NIST encourages the use of AES instead. In-line network encryptors using AES, like the Datacryptor® series from Thales [13] or the SafeEnterprise™ Ethernet Encryptor family from SafeNet Inc. [11], are now available to compliment the AES software modules that have been on the market. Encryptors from both of these families operate at 10 Mbps, 100 Mbps, and 1 Gbps.

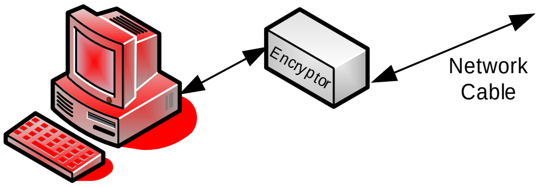

Figure 4. In-line network encryptor.

A HAIPE (High Assurance Internet Protocol Encryptor) working group has been developing an interoperability specification to define future generations of Type 1, IP-based, network encryptors, which enable a suite of secure, IP-based applications. This specification ensures interoperability between HAIPE compliant network encryptors that are manufactured by different vendors.

There are several companies manufacturing Type 1 HAIPE-compliant encryptors. Two of them producing products suitable for this architecture are General Dynamics C4 Systems and L-3 Communications Systems.

The TACLANE™ family [4] of Type 1 Ethernet encryptors from General Dynamics operates at rates from 7 Mbps (TACLANE Classic) through 100 Mbps fast Ethernet (TACLANE-Mini) to 1 Gbps (TACLANE-GigE). These come in a variety of form factors to support a variety of installation needs. These units are priced and sized appropriate for tactical applications, protecting single systems or small-to-medium enclaves of systems. On the horizon is the TACLANE-Router [5], which combines a HAIPE network encryptor with integrated routing capabilities provided by Cisco 3200 routing technology.

The RedEagle™ family [10] of Type 1 Ethernet encryptors from L-3 Communications operates at rates from 100 Mbps (RedEagle KG-240) through 1 Gbps (RedEagle KG-245) to 10 Gbps (RedEagle KG245X). These encryptors are similar to each other in form factor and fit conveniently into a standard equipment rack, although they could be placed on a desk or tabletop.

Prices of Type 1 encryptors are dropping, when viewed in terms of dollars per Mbps (Megabit per second). From the 1984 vintage KG-84 that came in at about $133,000/Mbps to the current KG-245X at about $4.50/Mbps, we have seen an improvement of nearly 30,000 in the price-to-performance ratio. This is illustrated in Figure 5.

Type 1 encryption of network data is not just limited to wired network computers any longer, as IEEE 802.11 wireless Type 1 encryptors, such as those from Harris Corporation [7], are now available. The Harris Type 1 wireless encryptors come in two varieties. One of them is a link encyrptor, providing full link encryption from wireless client to access point (SecNet 11® PC Card and Wireless Bridge). This is an 802.11b device operating at signaling rates up to 11 Mbps. The other kind of wireless encryptor from Harris provides end-to-end encryption, encrypting only the data payload, thus permitting data routing through a non-secure network infrastructure (SecNet 54™). The SecNet 54, in its initial configuration, is an 802.11a/b/g device supporting signaling rates up to 54 Mbps. The SecNet 54 is a HAIPE compliant encryptor.

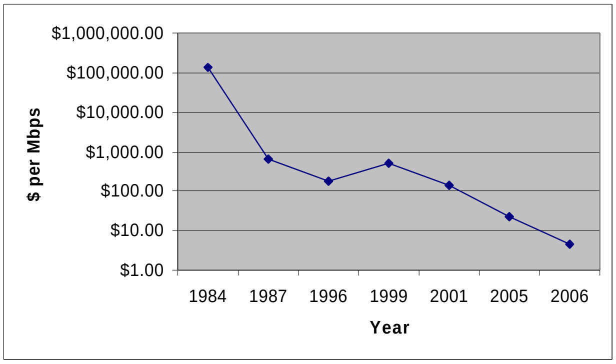

Figure 5. Encryption cost in Dollars/Mbps.

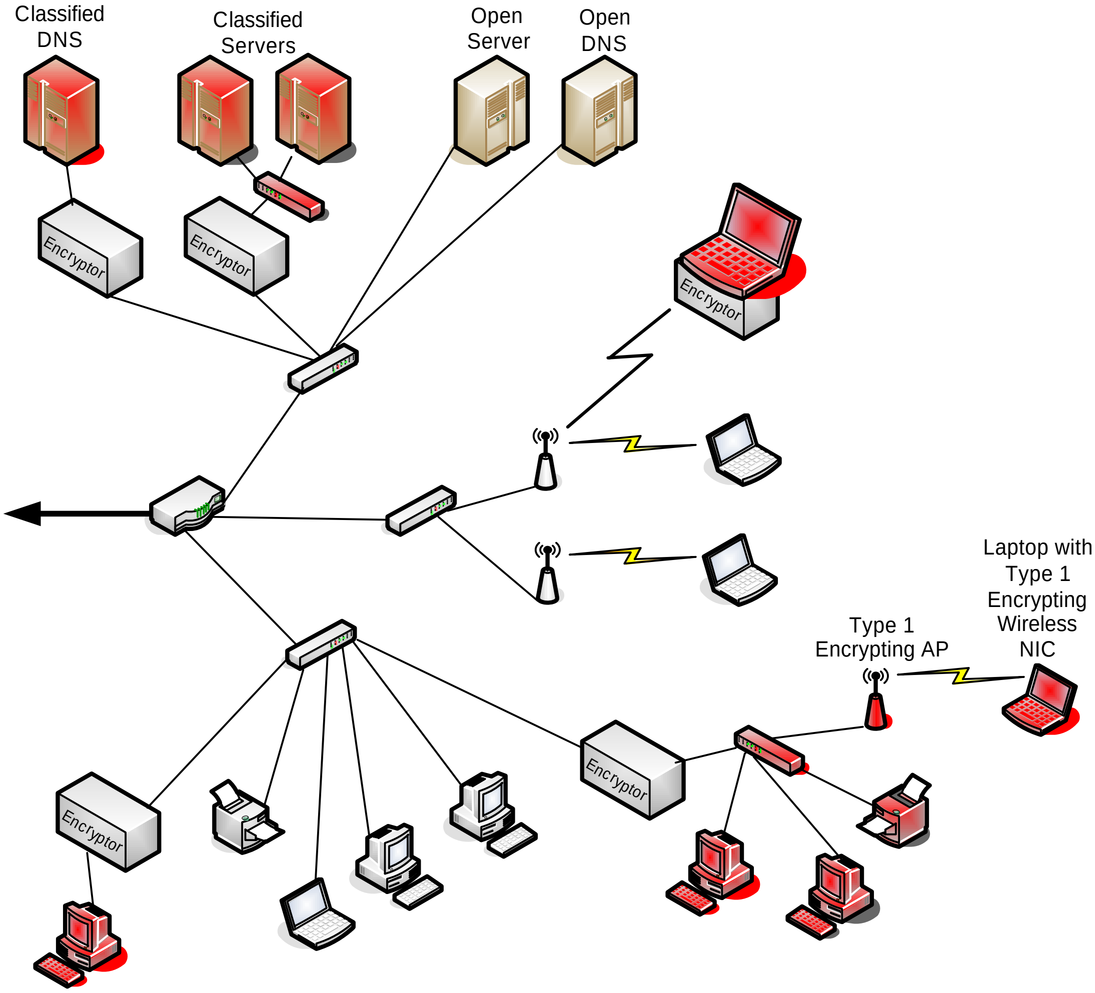

Figure 6. Detailed view of the consolidated network architecture.

Future configurations of the SecNet 54 are expected to support other transmission methods [8] including wired Ethernet and 802.16 WiMax

Although encryptor size, price, and ease of use are considerations, the key to a new consolidated network architecture is the interoperability between encryptors from different manufacturers, which is provided by being HAIPE compliant.

A Consolidated Network Architecture

In the consolidated network architecture, shown in Figure 6, the lengths of the classified or sensitive network segments are minimized by the use of local encryptors. Unlike the traditional network architecture where an entire classified network is build and placed behind one large, high capacity encryptor, the consolidated architecture uses smaller, more easily managed encryptors in front of specific classified systems or enclaves to reduce the amount of classified network infrastructure.

A small encryptor can protect an individual workstation (as shown in the lower left portion of Figure 6), an individual server (shown in the upper left of Figure 6), an enclave of servers (top of Figure 6), or an enclave with workstations and a printer (lower right of Figure 6). Small encryptors can also provide the over-the-air link encryption between a laptop and an access point (right of Figure 6), or end-to-end encryption between a laptop (upper right of Figure 6) and wired network components, such as the protected workstation in the lower left of Figure 6. Note that in the case of link encryption the AP decrypts data destined for another device and it only gets re-encrypted if it leaves that protected enclave. The laptop employing end-to-end encryption can communicate through infrastructure that is also carrying non-sensitive, unencrypted traffic to an encryption-protected workstation, server, or enclave.

Network topologies with encryptors may favor hub and spoke distributions instead of the three tier (core, distribution and access) topology commonly deployed, although a multi-tier distribution system may still work, as illustrated previously in Figure 6. There must still be a limited amount of duplication in the network, as in today's architecture. A classified Domain Name Server (DNS) will probably be needed (located behind an encryptor) to provide name-address translation service to classified network nodes.

The major advantage is that in the consolidated architecture, there is only one set of switches, routers, and communication links (fiber optic, copper, or air) to maintain and troubleshoot. Classified tail circuits can be reduced to very short lengths, the quantity of classified network switches decreased dramatically, and classified routers might be completely eliminated. The addition of encryptors and the support structures that they need will offset some of the lifecycle cost savings achieved through the consolidation of wiring and communications devices.

Finally, an architecture as that shown in Figure 6, is not without precedent with respect to network standards. In his book [9], Kou describes how security mechanisms like encryption map into the OSI reference model for communications (ISO 7498-2). Encryption is a key element for preserving data integrity and secrecy.

Benefits

As noted above, the consolidated security architecture benefits from containing only a single set of network equipment to maintain and troubleshoot. This decreases overall system cost by requiring less equipment, requiring fewer resources to operate and maintain the network, and by decreasing system complexity.

This architecture also increases overall functionality by providing quick, useful, and even simultaneous access to both secure and non-secure network resources from a single location.

Adding secure network links and devices to a new area containing only non-secure equipment becomes viable with this consolidated architecture. Existing equipment such as wireless access points and network switches can be used to extend network service to new secure enclaves.

The use of encryptors also helps to mitigate identity spoofing, sniffer-based attacks, and man-in-the-middle attacks. If a mixture of encryptors were used, Type 1 protecting classified information and commercial encryptors protecting all other data, then the network would be much more resistant to attack.

Obstacles and Issues

There are still many obstacles to overcome and open issues to be addressed. Some of these are fertile areas of research, but the authors feel none of them are insurmountable. A sampling of them are listed here:

- Cryptographic synchronization loss is a major contributor to poor performance and down-time in encrypted networks. The consolidated network infrastructure places a high premium on system and network component availability. In order to remain synchronized, encryptors demand a greater level of bit integrity from the network than unencrypted networks. Some cryptographic algorithms and modes of operation will eventually come back into synchronization if only flipped or stuck bits have been encountered. If bit count integrity has been lost (such as through dropped packets) the communicating devices will likely need to be resynchronized, unless each packet is separately synchronized. If an encryption system is not able to readily detect out-of-sync conditions, resynchronization can be performed prophylactically, although this introduces additional overhead.

- Small and portable Type 1 encryptors permit rapid deployment in areas where secure communication is required. The flexibility in deploying these encryptors in open areas such as offices, laboratories, field test sites, etc. however, increases the complexity in physically securing these devices when unattended. Vigilant consideration must be given to the methods for ensuring these devices are not accessible to unauthorized parties.

- Increasing the number of secure enclaves adds to the burden of ensuring the secure devices are configured and operated correctly. More and disparate secure devices in the field (or network) can increase the chances of a human-error adversely affecting the security of the system. Typical enterprise networks will need to add operations processes to facilitate effective management and deployment of encryptors.

- Key management is always an issue in networks containing encryptors. Key generation, distribution, and revocation are problems that grow at least as fast, or faster than the number of encryptors in the network. Public key negotiation, on-demand session key generation, and over-the-network key distribution techniques can ease these growing pains.

- Troubleshooting is more demanding in an encrypted environment because encryptors increase network complexity (e.g. different type of equipment, key management issues, resynchronization problems, etc.). Troubleshooting events, such as connectivity failures or poor application response time, become even more difficult when using link encryption, where the network headers and data payloads are encrypted. This can adversely affect trouble resolution time and cost.

- Need-to-know (NTK) separation must be maintained between various users of classified data. Just because two people hold a security clearance of the same level, does not grant each one of them the right to see the other's data. They might have a common need to know. If not, each individual must demonstrate a need to know before being allowed to access the data. In the consolidated architecture presented in Figure 6, some of the data might need to be doubly encrypted, first by a commercial encryptor to provide the NTK separation, then by a Type 1 encryptor to provide the national security protection.

- Presently, the development and production lifecycle of encryptors lags the timeline of the introduction and deployment of network devices, which creates pressure to maintain a fixed set of capabilities for longer periods of time. Encryptor technology is typically a generation behind communication network technology in terms of throughput. Because of this, the network may not exhibit as much technology push, as the periods for network equipment replacement and updating stretch out to match the pace of encryptor technology. Therefore the encrypted network may not always have the most current feature set and state-of-the-art performance.

- How would new encryption technology affect the enterprise? Just as IEEE 802.11i is a giant step above WEP (Wired Equivalent Privacy), what might be enabled by new encryption products, ideas, standards, and paradigms? What about new ways of using existing technology, such as IPsec?

Summary and Path Forward

In this paper, the authors have brought forth the idea of consolidating sensitive and nonsensitive information together on a common network through the use of tactical encryptors protecting individual systems or small enclaves of systems. This decreases costs by requiring less equipment, requiring fewer resources to operate and maintain the network, and by decreasing system complexity. This consolidated approach is not without issues. Many of these would make excellent research projects and smooth the way toward implementation of this consolidated architecture.

In addition to the specific issues discussed in the previous section, there are several general foundation items that need to be analyzed. The details of lifecycle cost in the consolidated infrastructure need further analysis. The topology alternatives, such as tiered vs. hub and spoke, need to be further explored. Finally, the capabilities of the various pieces of encryption equipment need to be examined in greater detail and verified.

As encryptors become fully HAIPE compliant, as they become even easier to use, and as encryptor prices drop yet further, a consolidated network architecture, as presented in this paper, may become a reality.

References

1. *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, National Institute of Standards and Technology, Gaithersburg, MD, November 26, 2001.

2. Communication Devices Inc., http://www.commdevices.com/sse.htm, 2001.

3. *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3, National Institute of Standards and Technology, Gaithersburg, MD, October 25, 1999.

4. General Dynamics C4 Systems, http://www.gdc4s.com/networkencryption, 2005.

5. General Dynamics C4 Systems, http://www.gdc4s.com/documents/Encryptors_PIB1.pdf, 2006.

6. Gerber, Cheryl, "Converging on Network Security," Military Information Technology, Vol. 8, Issue 1, (online edition, http://www.military-information-technology.com/article.cfm?DocID=384), Feb 9, 2004.

7. Harris Corporation, http://www.govcomm.harris.com/secure-comm, 2006.

8. Harris Corporation, http://download.harris.com/app/public_download.asp?fid=1015, 2006.

9. Kou, Weidong, Networking Security and Standards, Kluwer Academic Publishers, New York, 1997

10. L-3 Communications Systems-East, http://www.L-3com.com/cs-east/ia/redeagle/ie_ia_redeagle.shtml, August 16, 2005.

11. SafeNet Inc., http://www.safenet-inc.com/products/encryptors/ethernet.asp, 2006.

12. Tarman, Thomas D. and Edward L. Witzke, Implementing Security for ATM Networks, Artech House, Norwood, MA, 2002.

13. Thales e-Security, http://www.thales-esecurity.com/ProductsServices/DC2K_IP.shtml, 2004.