High Performance Network Security Methods: Comparisons and Case Studies

Dan Winkelstein
Celotek Corporation
danw@celotek.com

This paper describes various information security methods used today, as they relate to privacy. The various security methods are compared in terms of encryption strength, performance, delay/jitter, scalability, management, and inter-networking. Case studies of CellCase™ ATM VPN systems installations highlight the advantages of ATM-SEC based security over host-based or network layer security solutions. This paper is intended as a guide for technical managers who need to implement security and want to understand the advantages and disadvantages of the various security solutions available. It offers constructive guidance for implementing the appropriate security solution based on specific application requirements.

1.0   Overview

Celotek Corporation is the leading manufacturer of high-speed Virtual Private Networking (VPN) security solutions for commercial Asynchronous Transfer Mode (ATM) networks.   Celotek provides ATM security (ATM-SEC) via its line of hardware-based cryptographic systems.

The following paper focuses on security related issues associated with privacy. All security methods have advantages and disadvantages. The various security methods are compared in terms of encryption strength, performance, delay/jitter, scalability, management, and inter-networking. This paper examines the threats imposed on information privacy and surveys some of the common security methods used to overcome these threats. Data collected from the ATM security installations described throughout this paper demonstrate that ATM-SEC can be the best security solution for perimeter security where latency, speed, and strong encryption are the most important criteria. In addition, this paper discusses some of the technical design challenges encountered during deployment of secure ATM VPN solutions.

1.1   Threat Model

The most important design element of a commercial grade security system is to first identify the security threat. Yet, this tends to be the step that is the least understood. In the military, huge amounts of resources are spent to understand the enemy, his capabilities, weaknesses, and motives. Unfortunately, in a commercial setting, the enemy is far less obvious. Information security issues include privacy (encryption and authentication), access security (e.g. firewalls or intrusion detection systems), and denial-of-service attacks (e.g. ping or TCP setup storms). Each of these security issues represents a different type of enemy, thus, a different threat model. This paper focuses only on security issues associated with privacy.

The threat model for privacy assumes that confidential information is being transmitted across an unsecured network. It is also assumed that the threat is an "outsider" threat. This means confidential information is at risk for interception while it traverses the network outside of a trusted Local Area Network (LAN). Typically, the untrusted network is a Wide Area Network (WAN) or Metro Area Network (MAN) that begins at the point-of-presence to a public switched network.

The ability of an "outsider" to intercept confidential information while it is traversing the WAN or MAN can take the form of:

- Wire-tapping
- Packet redirection
- Unauthorized multicasting
- Redirection to service or maintenance ports
- Spoofing (pretending to be the intended recipient)

None of these methods for intercepting confidential information is particularly difficult for a person who is technically competent and familiar with the operation of the WAN. Private line facilities, provided by a third party carrier, are nearly as susceptible to these types of attacks as public use carrier facilities.

1.2   Security Perimeter

1.2.1 Physical Partitioning

The classical approach to building a secure network is to define a "physical security perimeter". Inside the physical security perimeter, people and equipment are trusted, therefore, information may remain in the clear "red region". Outside the physical security perimeter people and equipment are not trusted, therefore, all information must be secured "black region". A single trusted device crosses the physical security perimeter at each point of presence to the untrusted network. This device encrypts cleartext data on the red side and decrypts ciphertext data on the black side.

The definition of the physical security perimeter has security ramifications for the following:

- Type of encryption
- Management of the security
- Speed of operation
- Impact to dataflow

Confidentiality of data in a single LAN can be maintained through physical security alone. However, most networks are comprised of more widely dispersed elements. Cost and practicality prevent most enterprises from physically securing WAN resources. Instead, sensitive data is encrypted before it is transmitted into the public network and decrypted after it is received from the public network.

1.2.2 Logical Partitioning

A second method of developing a network security architecture is to define a "network security layer". Information transmitted below a specific layer in the ISO-OSI Protocol stack is encrypted. Information above the specific layer is in the clear. This type of architecture also has security ramifications for the type of encryption, management, speed of operation, and impact to dataflow. Implementations of encryption exist at the Physical Layer, Link Layer, Network Layer, and Upper Layers (session, presentation, or application).

Encryption at the physical layer is only appropriate for networks with a common physical layer infrastructure (such as point-to-point links or RF transmission) and, therefore, is not applicable for a general network. Physical layer encryption, however, is very effective for certain broadcast networks such as cellular wireless networks where only certain portions of the network are perceived to be vulnerable.

Link layer encryption, such as ATM or Frame Relay, has the advantage of permitting security for multiple packet protocol types. Link layer encryption tends to have higher performance and lower latency than network layer or upper layer encryption methods. This layer of encryption also effectively hides network layer end-station addresses. A disadvantage of link layer encryption is that it requires a homogeneous network at the link layer for all secure endpoints in the network.

An advantage of network layer encryption is that it supports networks with heterogeneous lower layer interconnections. For instance, network layer encryption would work for passing network layer packets

(e.g. Internet Protocol (IP) datagrams) between sites with different physical and logical link layers point-of-presence to the service provider (e.g. ATM at OC-3c at the headquarters and T1 frame relay at a remote site).   In addition, network layer encryption provides the ability to hide end-station addresses by implementing network layer tunneling or Network Address Translation (NAT). A disadvantage of network layer encryption is that it requires a store-and-forward encryption method and, therefore, will be slower, have a higher latency, will introduce more jitter into the data stream, and will be very processor intensive (for processor-based VPN designs). This store-and-forward approach is required to accommodate variable length data, misordered packets, fragmented packets, and other effects associated with a connectionless network layer.

Higher layer encryption (application, session, or transport) is excellent for application end-to-end encryption since it requires the end host to perform the encryption and decryption process. Higher layer encryption is not generally used for high-speed encryption gateways or VPN products. Since higher layer encryption is performed at the end-host it may have significant security management challenges. Higher layer protocols provide no security of end-station addressing.

1.3   Common Approaches to Security Partitioning

There are several commonly used methods for defining the physical and logical partitions for encryption. The following are classifications of various types of commercially available approaches to security partitioning.

1. Host-based security at an upper layer protocol. Examples include Secure Socket Layer (SSL) for transaction oriented traffic and Pretty Good Privacy (PGP) for e-mail messages.
2. Host-based network layer security such as IP security (IP-SEC) transport mode.
3. Transport/Network layer firewalling VPN technology. This approach is typically implemented using end-station address hiding with firewall products.
4. Network layer gateway security. An example of this type of security is IP-SEC based VPNs. IP-SEC encryption devices can be physically located at various points in the network such as:
   a) Traversing Ethernet segments
   b) Sitting between routers
   c) Acting as adjuncts to routers
   d) Installed as part of a router
5. Link layer security at the point-of-presence to the WAN. Examples of this type of security are:
   a) ATM-SEC based VPN boxes sitting at the point-of-presence to an ATM link from the service supplier
   b) Frame Relay based VPN boxes sitting at the point of presence to a Frame Relay link from the service supplier
6. Physical media layer security provides point-to-point encryption over a shared media. Examples of this type of security include encryption of digital data carried via a wireless network.

Each of these approaches to security has advantages for different type of applications. The following diagram summarizes the current state-of-the-art implementation for these various solutions.   The different approaches to security are compared in terms of the following:
1. **Security** - the strength of the encryption and authentication algorithms. The metrics used are:
   - none
   - 40-bit DES: weak encryption
   - 56-bit DES: medium encryption
   - 112-bit or 168-bit triple DES: strong encryption
   - MD5 or SHA-1 with 96-bit hash: strong authentication
2. **Throughput** - the speed of operation for encryption and authentication.
   - slow: a significant performance impact exists for using encryption for most applications
   - medium: a performance impact exists for high bandwidth applications
   - fast: a negligible performance impact exists for nearly all applications
   - line rate: the performance is sufficient for the medium and has no impact on applications

3. **Delay and jitter** - delay is the time it takes a packet to transverse a security gateway and jitter is the variation in delay.
   - high: a significant impact for most real-time applications
   - medium: a negligible impact under low loads and low bandwidth, a noticeable impact for high bandwidth applications or under high load conditions
   - low: a negligible impact for real time applications
4. **Scalability** - does the state-of-the-art implementation scale work well for large networks? The complexity of management, key exchange, and interoperability with infrastructure increase with the size of the network. The factors listed below tend to limit the size by which the network can grow.
   - point-to-point
   - low: appropriate for small networks since complexity increases exponentially with the size of the network
   - medium: appropriate for small to mid-size networks, complexity increases super-linearly with the size of the network
   - high: appropriate for large networks, complexity increases linearly with the size of the network
5. **Management** - centralized or distributed
6. **Applications** - example applications that would be well suited for the particular implementation
7. **Inter-networking** - Applicability for inter-networking to lower layer networks, particularly link and physical layer networks in the WAN

Encryption Implementation	Security	Throughput	Delay and Jitter	Scalability	Management	Applications	Inter-networking
Physical layer encryption	weak encryption	line rate	low	point-to-point only	none	Wireless	physical layer specific, link layer independent
Host-based application layer	medium encryption no authentication	slow	high	low	distributed	E-mail e-commerce transactions	physical layer and link layer independent
Host-based IP-SEC	medium to strong encryption strong authentication	slow	high	low	distributed, will be centralized in the future	Any IP-based data communication	physical layer and link layer independent
Firewalling VPN-based on NAT	none	medium	high	medium to high	centralized	Access control only	physical layer and link layer independent
Gateway-based IP-SEC	medium to strong encryption strong authentication	medium to slow currently, getting much better	high	medium to low currently, getting much better	centralized	Any IP-based data communication	physical layer and link layer independent
Router-based IP-SEC	medium to strong encryption strong authentication	slow currently, getting a little better	high	low currently, getting much better	centralized	Any IP-based data communication	physical layer and link layer independent
Gateway-based ATM-SEC	strong encryption strong authentication	line rate	low	high	distributed now, centralized in the future	Voice, video, data, legacy, bit-transport data service (BTDS)	physical layer independent and ATM link layer specific
Gateway-based Frame Relay	medium encryption authentication is implementation dependent	line rate (1.5Mbps or less)	medium	medium to high	distributed or centralized based on implementation	data,voice, legacy	physical layer independent and Frame Relay link layer specific

1.3.1 Host-based

Host-based encryption is optimal for applications that are low bandwidth, time-insensitive and where the security perimeter is at the host. E-commerce transactions and e-mail are two examples of applications where host-based encryption is appropriate.

Typically, host-based encryption is software-based and, therefore, is limited by processor speed, data movement efficiency, computer architecture, operating system, system load, and many other factors. Modern RISC (or CISC) processors are not particularly efficient at bit scrambling or bit operations, which are generally part of symmetric data encryption algorithms such as DES. Hardware-based accelerator cards can increase the performance over software-based solutions by transferring the encryption process to specialized hardware. However, the performance of a host-based system will always be limited by architectural limitations such as bus bandwidth, memory bandwidth, interrupt processing, context switching, operating system scheduling, etc. Host or computer-based security technology can never be as fast as an equivalent hardware-based security technology developed for security functions.

The following diagram (Figure 1) illustrates the inefficiencies of host-based systems. For each inbound packet, data must traverse the system bus at least three times and the processor generally performs at least two buffer copies for each packet transversing the system. Outbound packets have exactly the same inefficiencies.

Figure 1. Data movement for incoming data within a computer for host-based encryption
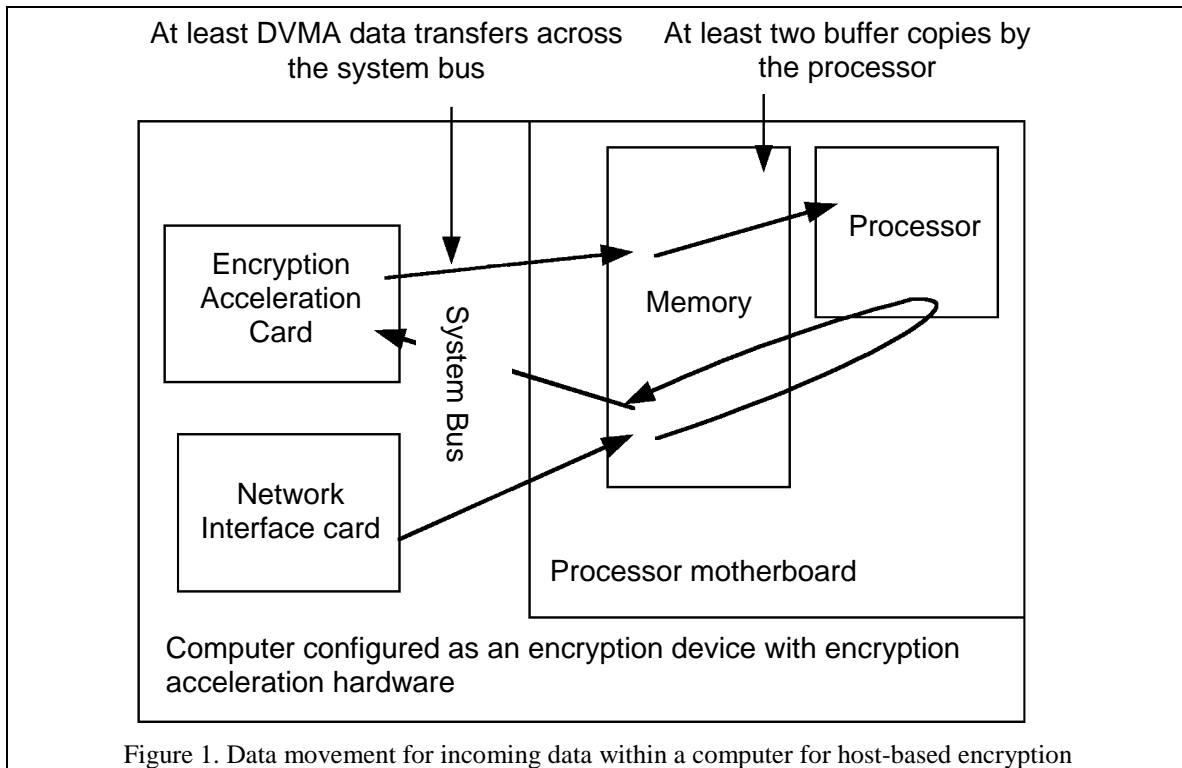
Host-based encryption generally implies a host-based security policy. For a large enterprise this can be unwieldy and cumbersome to manage and control. Furthermore, if the security requirements are cumbersome, individual users may choose to bypass the security altogether.

Host-based encryption also typically requires users who are knowledgeable about encryption. This is very uncommon. Systems like PGP require the user to generate and distribute public keys out-of-band to intended recipients. Systems like SSL provide no authentication of source or recipient. This means that while the data is encrypted as it traverses the network, the identity of the end recipient is unverifiable.

IP-SEC host-based encryption solves some of the problems of key-exchange and authentication. Management of host-based IP-SEC security can be centralized, although this is not required. IP-SEC software-based implementations tend to have a low throughput. Some performance gains are achieved with encryption acceleration hardware.

1.3.2 Transport/Network Layer Firewalling VPN Technologies

This approach to security is an incomplete solution as it provides hiding of end-station addresses, but absolutely no encryption of data. It is inappropriate to call this type of technology a privacy solution for network security. With or without network address translation, firewalling technology is excellent at access control, however, it is inaccurate to refer to firewalls as a privacy solution. Network address translation or IP-packet encapsulation does not scramble or encrypt the data in anyway. Therefore, all sensitive data remains in the clear as it transverses the unsecured WAN.

1.3.3 IP-SEC Based Security

Network layer security is typically IP-SEC based security. IP-SEC can be implemented as a VPN unit or integrated into a router. This approach to encryption is excellent for an IP-datagram application in which bandwidth, latency, and delay are not a factor. These approaches are also useful in networks with a wide array of link and physical interconnects (e.g. ATM/OC-3c at headquarters, T1/Frame Relay at branch offices, dial-up modems for home offices).

1.3.4 Router-Based Network Layer Security

Router-based IP-SEC solutions combine the functionality of a router and the operation of a VPN into a single entity. This can be less expensive than deploying each unit separately.

These systems use processors within the router to provide encryption, authentication, and management. Presently, the performance of router-based IP-SEC security solutions is limited to 4-10Mbps; however, performance will improve as IP-SEC hardware acceleration is added to routers. IP-SEC, in general, and router-based solutions, in particular, induce delay and jitter. IP-SEC is, by definition, a store-and-forward operation and, therefore, subjects packets to increased delay and increased delay variation (jitter). Delay and jitter make real-time applications such as voice and video (particularly interactive voice and video) extremely difficult.

Router-based network security violates the traditional model for security where there is physical separation of information between the trusted network and the untrusted network. Security is maintained only by ensuring that the router is configured correctly so all information going between the trusted and untrusted networks passes through the encryption sub-system. This requires that the network administrator also be the security administrator. Some organizations prefer to keep these functions separate.

1.3.5 VPN-Based Network Layer Security

For security, management, and performance reasons, it is sometimes preferable for a VPN solution to be a separate entity from an edge router.   A gateway/VPN-based solution is typically superior to a router-based solution with respect to performance, speed, delay, jitter and scalability. This is because the solution architecture is optimized for encryption as opposed to packet routing.   Additionally, security management can be separated from network management.

For many IP-SEC based VPN solutions, the solution can be placed either behind the router, inline between routers, or as an adjunct to a router or switch port. The inline placement maintains the red/black separation of information, whereas, for the adjunct or behind the router placement, there is no clear red/black separation and security is maintained only by ensuring that the router is configured correctly. If the IP-SEC based VPN solution is placed as an adjunct to a router point or behind the router, it does not need to have routing functions. Furthermore, the choice or choices of WAN interfaces is much more flexible as WAN interconnection issues are deferred to the router.

If the IP-SEC based VPN solution sits at the edge of a network (point-of-presence to the WAN), it must participate in routing protocols. This means an inline VPN box must provide support for routing protocols and routing options for all packets. Also, if NAT is enabled it must occur in the VPN box, since NAT hides both IP addresses and upper layer protocols. Routing functions increase the complexity of an inline IP-SEC implementation. Increased complexity can mean lower performance, higher costs, or increased management requirements.

1.3.6 Link Layer Security

Link layer security implementations are typically found in a VPN or in security gateways. These gateways typically sit at the point-of-presence to the WAN and provide good red/black security partition between the trusted LAN and the untrusted WAN.

In general, link layer security gateway solutions are superior to network layer solutions in terms of speed, scalability, delay, and jitter. This is because link layer solutions do not require a store-and-forward approach to encryption. Link layer security solutions are also appropriate for mixes of non-IP data traffic. Thus, if a network consists of a mix of data, voice, video, and legacy traffic, link layer security provides the most direct mechanism to provide encryption for all these different traffic types.

Link layer solutions, however, only operate on homogeneous points-of-presence to the networks. This means link layer security is only appropriate if all endpoints requiring security interface with the network at the ATM or Frame Relay layer. The point-of-presence to the network, however, may be a mix of different physical media (e.g. OC-3c or OC-12c at headquarters, T3 or T1 at branch office, xDSL at the home office). There are some technical challenges associated with ATM layer security. These challenges include provisioning issues associated with bandwidth management for cryptographic synchronization and in-band key exchange.

2   Case Studies for ATM VPN

Unfortunately, there is not one security solution that is best for all applications, all the time. There are, however, certain applications where one type of security solution is better than another. This section focuses on those applications where ATM-based security is appropriate.

2.1   Case Study - Voice, Data, Legacy, and Redundancy

A major customer of Celotek is currently using ATM to carry voice, IP data, and X.21 legacy network data over a truly redundant WAN between multiple corporate sites, and an even larger number of remote sites. The entire ATM network is redundant to the point that there are multiple carriers that interconnect the corporate sites. IP data traffic is internally load balanced between two routers at each corporate site. Voice and X.21 legacy traffic is also load balanced between two Nortel Passport[*] switches at each site. These switches multiplex IP data with voice and legacy traffic onto ATM. Voice and X.21 legacy traffic is encapsulated onto ATM using Nortel proprietary Bit Transparent Data Service (BTDS) techniques. The output of each switch is multiplexed voice, data, and X.21 legacy traffic over ATM at STM-1 rates (155Mbps).

The ATM/STM-1 rate traffic from each switch goes to a Celotek CellCase™ ATM VPN device that provides strong encryption for each active virtual path (VP) or virtual channel (VC) independently. The following diagram (Figure 2) illustrates some of the operation of this network.

---

[*] Passport is a registered trademark of Nortel Inc.

Celotek Corporation **Telephone: 919-462-1900**
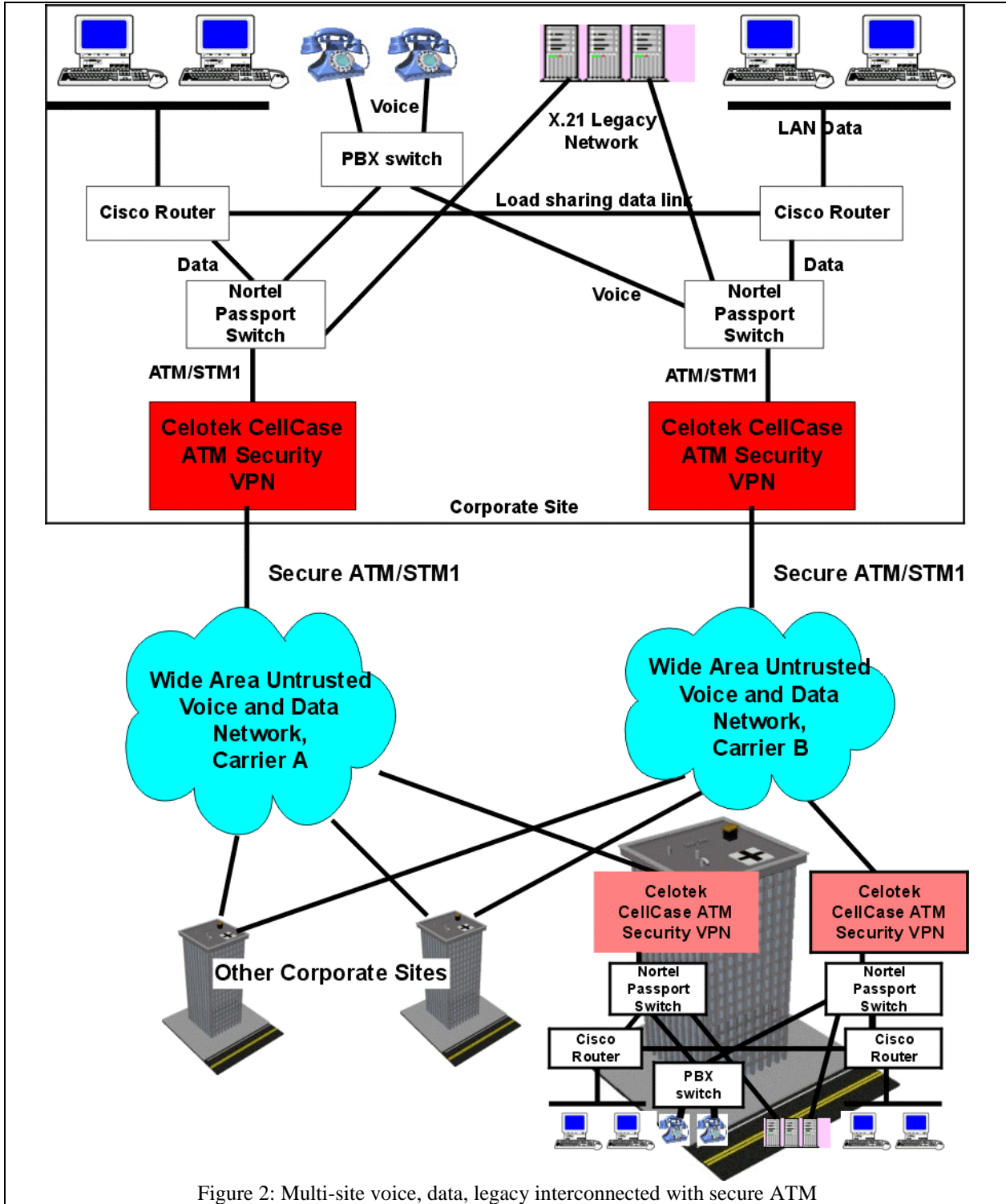**www.celotek.com**

Figure 2: Multi-site voice, data, legacy interconnected with secure ATM

In this particular network, the customer chose ATM-based encryption, as opposed to other methods of security because of the following factors:

1. The data transmission rate was very high and a method of encryption that provides full STM-1 line rate encryption was required.
2. The WAN was a true switched multi-point network, as opposed to point-to-point services. This means the customer needed a method of encryption that was compatible with switch services.

3. The customer had a large number of independent traffic streams and required separate encryption for each stream.
4. The customer was running a mix of IP data traffic, voice, and legacy data traffic over the same WAN. All of these types of traffic required security.
5. The customer had applications that required security with very low latency and very low jitter.
6. The customer required strong encryption technology (168-bit key triple DES or equivalent).
7. The customer expected the network bandwidth requirements to grow substantially over the next few years.

ATM layer encryption is a good choice for this customer. By using encryption at the ATM cell layer for each VP or VC, the security process is entirely transparent to the data transport mechanism. All data security management functions can be centralized to one device at the point-of-presence to the WAN for each carrier. The CellCase ATM VPN device provides 168-bit key triple DES encryption to the payload of each cell, while leaving the cell header in the clear. The cell header contains only local routing information that is not encrypted in order to maintain transparency with the existing ATM networking infrastructure. There is no security or privacy implication to keeping the cell header in the clear.

Since each VP or VC is encrypted separately, there is strong encryption for each communication channel regardless of the media type. Encryption at the ATM layer runs at STM-1 line speed for the CellCase product. The CellCase product also introduces negligible delay and jitter to the traffic stream. Thus, there is no impact for real-time sensitive data such as voice carried over a WAN.

2.2   Case Study - Data Communication Over Satellite

Another Celotek customer had a very high bandwidth medical application that required encryption. The United States Health Insurance Portability and Accountability Act (HIPAA) requires that patient information transmitted over a network be protected. One mechanism to provide this protection is encryption of the data. This particular customer is using the ACTS Satellite for communication of large quantities of medical data between multiple, distant sites. The customer chose to encrypt the data at the interface to the ACTS satellite equipment. The following diagram (Figure 3) illustrates the data network used by this customer.

Figure 3: Multi-site very high-speed secure communication over satellite
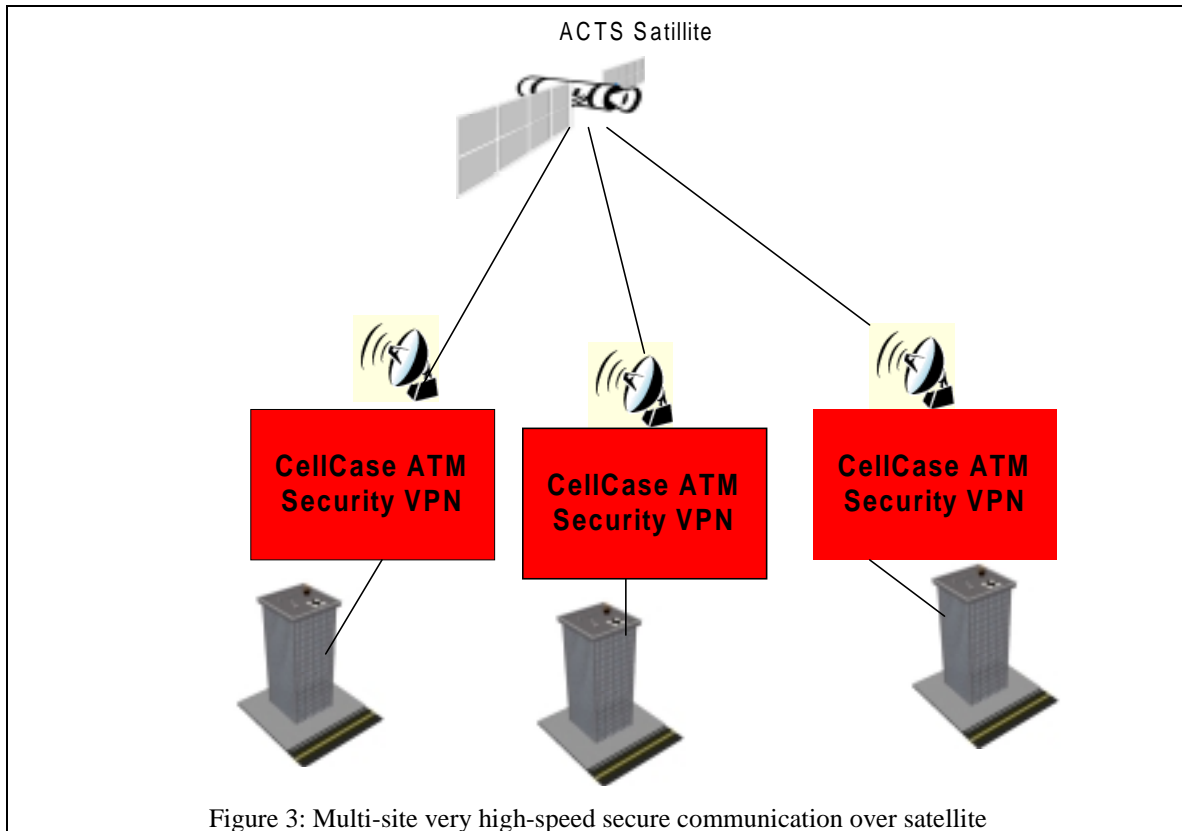
In this network, the customer chose ATM-based encryption, as opposed to other methods of security because of the following factors:
1. The data rates were high and were expected to get higher.
2. The sensitivity of the data required strong encryption using triple DES.
3. The existing data network was an established ATM-based network based on satellite communication. The introduction of encryption had to be accomplished without changing the network infrastructure.

ATM encryption is an ideal choice for this customer. By using encryption at the ATM cell layer the customer was able to provide strong encryption at speeds up to 155Mbps. Given the sensitivity of the information being transmitted over an inherently untrusted network, the customer required strong encryption. The Celotek CellCase ATM VPN provides 168-bit key triple DES encryption for each independent data stream. The customer's traffic patterns tended to be a very bursty transmissions with very large amounts of data at high data rates. The CellCase product provides strong encryption at line speed, independent of the burstiness, size, or data rate.

This particular customer had also invested a substantial amount of money in the infrastructure for data transmission between remote sites. Security at the ATM cell layer, at the point-of-presence to the ACTS satellite equipment, required no changes to the existing data transmission infrastructure. Furthermore, the system allows network services and data rates to grow without impacting the security architecture.

One concern the customer had was the effect of very large latency and the relatively high bit error rate associated with satellite transmission. It was found that the Celotek key exchange protocol was not adversely affected by the long satellite delay. It was also found that the cryptographic synchronization required for counter mode would recover adequately, even with the high relative bit error rate of satellite (as compared with fiber transmission media.) ATM layer encryption also had no effect on the physical layer transmission of data over the ACTS Satellite.

2.3   Case Study - Return on Investment

The final case study illustrates the return on investment (ROI) of the CellCase ATM VPN. In this particular situation a customer had two campus networks separated by a short distance (about 700m). Originally they wanted to install private line facilities between the two campuses for high-speed voice, data, and video applications. The underlying network at each campus is ATM.

When the customer requested private line facilities between the campuses from the local service provider, the customer was told there would be a 6 to 9 month delay before fiber could be installed in the ground. To accelerate this process, the customer installed a small line-of-sight microwave network between these two sites that operated at 155Mbps. By installing the CellCase ATM VPN to secure the data between these two sites over the microwave link, the customer was able to complete the network in much less time. The customer found the ROI for using the CellCase ATM VPN to be less than one year when compared with the cost of installing a private line facility. The CellCase ATM VPN was paid for in less time than it would have taken the local service provider to even install a private line facility. The following diagram (Figure 4) illustrates the CellCase ATM VPN in place of a private line facility.
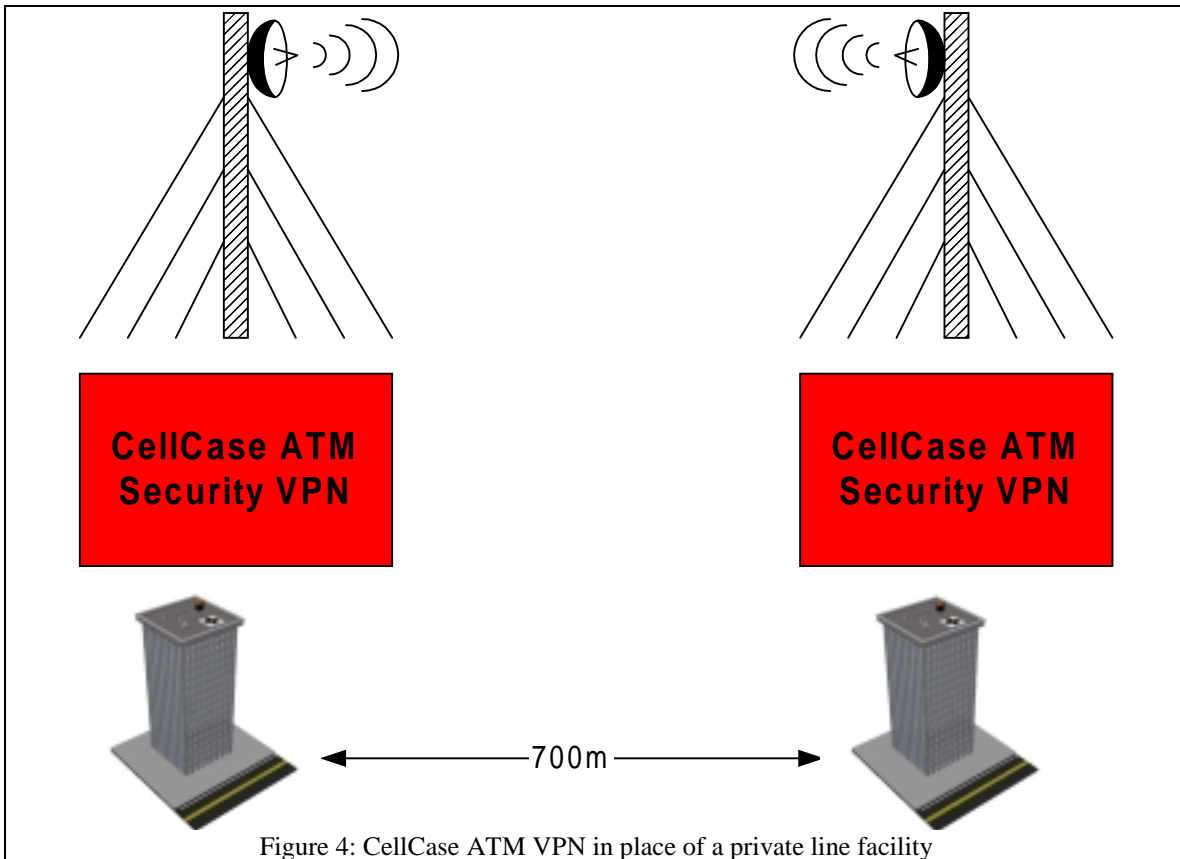

Figure 4: CellCase ATM VPN in place of a private line facility

The choice of ATM security was a good business and technology decision for this customer for the following reasons:
1.   The cost and time of installing a private line facility was larger than the cost of encrypting the traffic at the ATM cell layer.
2.   The customer had a mix of voice, video, and data over ATM at each campus. Only a link or physical layer encryption mechanism would be appropriate for this mix of traffic without changing the underlying network.
3.   The customer had an unsecured ATM network between sites.
4.   There is no performance impact on traffic when encryption at the ATM cell layer is introduced.

5. The network and security implementation can grow seamlessly to include other sites connected by microwave, private lines, or a public carrier.

3 Technical Challenges

3.1 *Interaction with Cryptographic Synchronization Messages*

One of the technical challenges associated with adding security for networks with mixed data types is the interaction found between encapsulated constant bit rate traffic, traffic shaping/policing, and cryptographic synchronization. Some constant bit rate (CBR) services encapsulate voice or legacy traffic onto ATM cells (e.g. BTSD). Some implementation of encapsulation CBR services seems to have an extremely low tolerance to cell delay variation.

The CellCase ATM VPN provides two modes of cryptographic operation as defined by the ATM Forum Security specification V1.0: Electronic Code Book (ECB) and Counter Mode chaining. ECB is a straight mapping between cleartext and ciphertext for a given key. Counter Mode chaining provides for hiding of cleartext patterns by encrypting a key-stream and exclusive-ORing the encrypted keystream with the cleartext to produce ciphertext. The ATM Forum specifies a means to maintain cryptographic synchronization over a Counter Mode channel by use of cryptographic synchronization cells. These cells are defined as end-to-end OAM security cells that are transmitted in-band on Counter Mode channels.

Celotek has encountered very rare packet loss associated with encapsulated CBR service that was being encrypted using Counter Mode. This packet loss did not correspond to ATM layer cell loss. It was theorized that the problem was the interaction between the traffic pacing requirements in the network, the insertion of cryptographic synchronization cells, and the tight cell delay variation tolerance of the encapsulating switches. By introducing cryptographic synchronization cells, the traffic pattern for encapsulated CBR traffic was subtly changed. Apparently very small changes in cell delay variation in the network can introduce packet loss in some encapsulating CBR implementations. The packet loss rate was so low that there was no performance impact to the customer's applications.

3.2 *ATM Forum Standards Issues*

Another technical challenge encountered while installing ATM-SEC encryption systems is the interaction between cryptographic synchronization messages and network routing equipment. The ATM Forum specifies that cryptographic synchronization messages must be carried in-band using end-to-end security OAM cells. The ATM Forum standards also require that cell order must be preserved while traversing all ATM switching equipment. An instance was uncovered in which a major router vendor had a bug in their implementation of the standard where cell order was not preserved for OAM cells. Under certain circumstances, the router would extract an OAM cell from the cellstream and re-introduce the cell at a later time. This caused the CellCase units to loose cryptographic synchronization. Once this problem was fixed with the router vendor's implementation, the customer encountered no problems with encryption. ATM switch and router vendors should be compliant with the ATM Forum Security specification V1.0, particularly with respect to the handling of security OAM cells.

Conclusion

This paper provides an overview of some of the common encryption methods used today. No one method is ideal for all networks, applications, and traffic patterns. ATM encryption, including the CellCase ATM VPN system, is a good choice for networks that have a mix of IP data, voice, video, and/or legacy traffic, particularly when the existing infrastructure is switched ATM. ATM encryption is also a reliable choice when performance and minimal latency are critical. Finally, ATM security makes good business sense-- important information is reliably secured, while providing an excellent return on investment.

About Celotek

Celotek's high performance, high-speed VPN security products and technology continue to be integrated into networks across the globe. More information about the company, products and sales offices can be found at www.celotek.com. Celotek is headquartered in the Research Triangle Park area of North Carolina, USA. In addition, Celotek has sales offices on both the West and East Coast of the United States, and an international sales office in the United Kingdom.

Bibliography

1. Schneier, Bruce. "Applied Cryptography". 2nd Edition, John Wiley & Sons, NY, 1996
2. af-sec-0096.000, "ATM Security Framework 1.0", ATM Forum"
3. af-sec-0100.000, "ATM Security Specification Version 1.0",
4. Kent, S., R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, Nov 1998
5. Alan Amrod, "VLANs Authenticated VLANs and firewalls, How they relate to the United States Health Insurance Portability and Accountability Act", Xylan, Jan 1999
6. "Encrypting ATM Firewalls", Celotek Corp, 1997
7. "Microsoft Privacy Protected Network Access: Virtual Private Networking and Intranet Security", Microsoft Corp, 1999