E-COMMERCE OVER CABLE: PROVIDING SECURITY FOR INTERACTIVE APPLICATIONS

Tony Wasilewski
Scientific-Atlanta, Inc.

Abstract

Digital CATV networks now being deployed offer the promise of a rich application environment that goes beyond broadcast and I/PPV.

E-commerce applications that extend the revenue-generating possibilities of the network also bring new issues and challenges. Many of these challenges are security-related and create requirements for authentication, encryption, simplified key management and message integrity.

Public key cryptography can help meet these new requirements as well as provide the basis for the "many-to-many" security relationship that is necessary to support scalable, spontaneous E-commerce applications.

A contemporary approach to CATV security will include support of a Public Key Infrastructure (PKI).

BACKGROUND AND NETWORK OVERVIEW

Security in broadband networks, including CATV HFC networks, can be enhanced by means of a technology called public key cryptography. Cryptographic methods have been used for many years to secure networks of various types, but numerous advantages are afforded by using a public key method in conjunction with more traditional secret key approaches. In particular, contemporary security needs include support of electronic commerce. Public key cryptography is particularly useful in supporting and improving this particular application. Furthermore, the body of standards for public key technologies is growing, and the development of the Worldwide Web has brought about some commonality in implementations.

There is already a broad base of commerce activity occurring electronically. Home shopping networks, such as QVC and the Home Shopping Network, where goods are purchased via television advertising and telephone ordering, is a multi-billion dollar per year industry. On-line Internet shopping in 1998, totaled $8 Billion in consumer transactions according to Forrester Research. Business-to-business transactions on-line are considerably higher. This indicates a strong interest by consumers and businesses in shopping/procuring through networks.

While the convenience of "mouse and network" shopping continues to lure an increasing number of users, security is still a major concern. According to *Internet World*, in a survey of 1000 Americans carried out by ISP NetZero, 53% cited "privacy and security" as the top concern about on-line shopping.

As cable modems and digital set-tops become increasingly deployed, routed IP addressing schemes are becoming the norm on broadband CATV networks. In the past, to communicate with home terminals, connectionless "single-wire" addressing was typically used. In this approach, equipment in the headend merely appends the terminal's address to a message and puts the message on the (usually single) downstream carrier. Then all terminals in the system must filter through all the messages in order to find the one(s) addressed to it. In modern broadband networks, the communications model has become more complex.

New network models have placed new security demands on digital cable networks This is being driven by new connection-oriented and IP subnetted configurations as the schematic in Figure 1 illustrates.

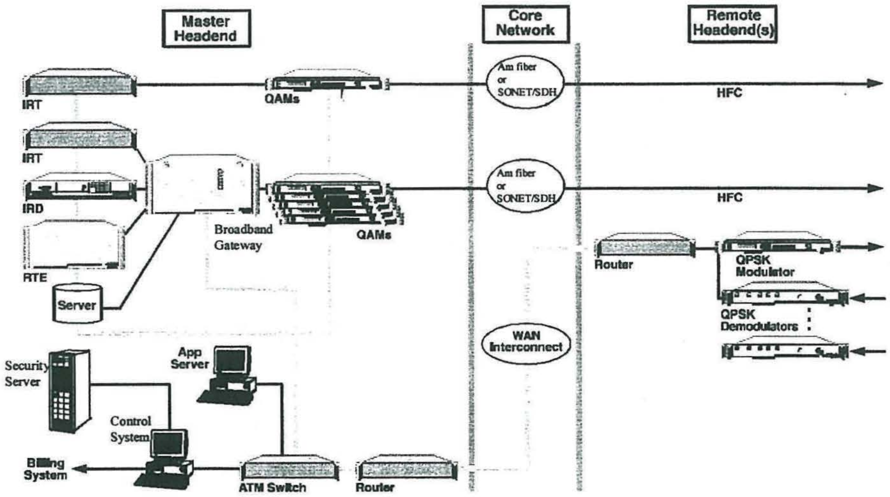


Figure 1 - Digital Broadband Network

New services such as E-mail, interactive shopping and video-on-demand (VOD) are utilizing architectures in which an ATM (asynchronous transfer mode) or SONET (Synchronous Optical Network) may be employed as the wide-area transport supporting servers of all types that transmit digital files as well as entertainment content. Such applications can be hosted in regional centers which send information through the network using various types of broadband gateways and local and wide-area routers. That information is further routed through smaller nodes which handle both downstream and upstream information to/from televisions and/or personal computers at the consumer side of the network.

These trends and the services they support contribute to changes in basic network security relationships. In broadcast-only services (whether digital or analog), such as satellite or traditional cable, there exists a one-to-many security relationship in which the operator of the network establishes an account with each subscriber in the network and provides authorization for each. In most cases, this is accomplished using secret-key-based security systems.

With the advent of two-way interactivity, this relationship is changing. Subscribers want to access a scalable and dynamic electronic-commerce environment. To support this type of interaction, the security relationship must become many-to-many since each subscriber may want to make transactions with a different set of merchants or service providers. The secret key-only approaches that have been traditionally deployed in many conditional access systems do not support this new relationship mode as well as public key methods.

Further inspection of Figure 1 illustrates how the network offers new possibilities. In the center, a large-scale transport system such as AM fiber, SONET and/or ATM is linked with various gateways that can bring in digital satellite, off-air, other locally-encoded signals and server-based digital content. Internet services can, of course, be delivered in such a network as well.

These services can be multiplexed for transmission by broadband gateways and then processed for further transmission through modulators in the access network. In the figure, quadrature amplitude modulation (QAM) is shown, and the signal runs over the HFC network to the subscriber premise.

Finally, at the subscriber premise, a receiving decoder (set-top) using MPEG-2 and other standards is employed. These set-tops can support reverse path communications with many servers or service providers. This multitude of new connection possibilities makes support of a many-to-many security relationship desirable.

EXAMPLES OF EMERGING E-COMMERCE APPLICATIONS

Examples of possible e-commerce services that can be offered over CATV networks is shown in Figure 2.

- On-line ticket sales
- Home catalog shopping
- E-auctions
- E-gambling
- Local fulfillment (pizza, flowers, stamps)
- Travel services
- Affinity (loyalty programs, cross-selling)

Figure 2 - Possible CATV E-commerce Services

The popularity of E-commerce over the Internet has been a proving ground for the introduction of similar applications into the home. However, with the advent of sophisticated HFC networks that support IP traffic and home terminals that can run the operating system, middleware, applications and security services to support them, the cable industry is perhaps better positioned than ISPs which use the PSTN to deliver these services to the consumer.

WHY LEGACY SECURITY APPROACHES ARE NOT SUFFICIENT

It is important, when preparing to launch new E-commerce applications, to examine legacy security methods to understand to what extent they do or do not provide adequate support. Three examples are used here to illuminate some of the issues. The first case involves communication over the Internet; the second looks at key management in CATV networks; and the third reviews the transmission of sensitive consumer information such as credit card numbers over a network.

Case 1): The basic Internet protocols exhibit many security weaknesses. Security was not foremost in the minds of the original designers of transmission control protocol/Internet protocol (TCP/IP). First, there is an inherent lack of privacy both in IP itself and in other layers upon which it typically depends. For instance, lower-layer protocols such as Ethernet are broadcast and session-oriented protocols such as File Transfer Protocol (FTP) provide no protection of content while in transit. Second, authentication is lacking. In general with IP, the user sends packets labeled with a source and a destination ID. The recipient has to trust that the packets really come from the labeled sender because there is no means to authenticate the sender of the message. In addition, the authentication and integrity of the data itself is in question because other than simple checksums for basic error detection, there are no means available to safeguard against malicious tampering.

Case 2): Key management in cable TV networks is typically achieved in an unauthenticated manner. Many cable TV systems have security systems that employ secret-key or "symmetric" encryption. In these systems, when messaging home terminals, the same key is required at both at the encryption and decryption sites. Thus, a network operator must maintain a database of all secret keys for each set-top. These databases can be vulnerable to attacks that can compromise system security through unauthorized access to the keys. Even if the operational databases are reasonably well-protected, keylists can be stolen during shipping. Using this key information, clones of legal terminals can be made that have the same keys in them. These clone terminals will then respond to messages intended for the legal device, such as the authorization of services, etc. Thus, protection (secrecy) of these home terminal key databases is of utmost importance.

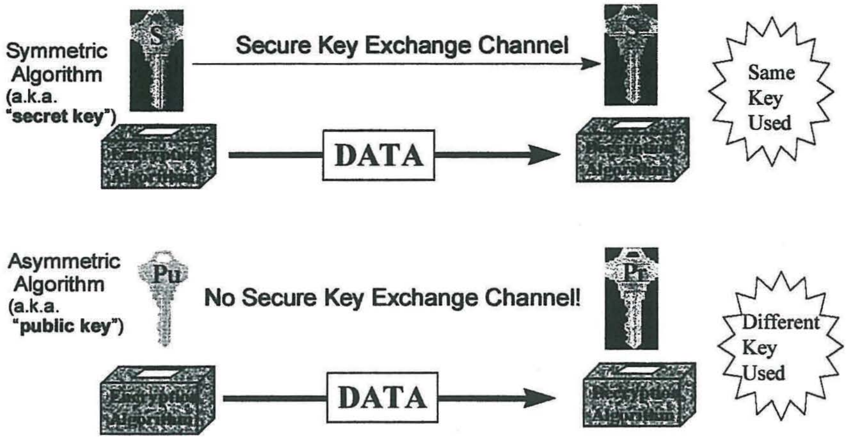
Employing such a secret terminal key database also inhibits multi-site control of the security function, because distributing the secret keys to many locations makes them potentially more vulnerable. A distributed control scenario simply has more places to physically protect since copies of the key database are replicated. This may also have negative implications for "retail" scenarios.

Case 3): As noted above, consumers' concerns about the protection of vital personal or financial information is the major concern of current on-line shoppers. In order to complete an on-line purchase with a credit card, the buyer's credit card number must somehow be transmitted to the on-line merchant. This could be done by telephoning the merchant in advance or during the transaction to send the number. However, by requiring such actions, some of the main advantages of on-line shopping are lost. In particular, the spontaneity of impulse buying is disrupted and scalability is limited since it would be impossible for the buyer to be "introduced to" all possible merchants, in advance.

HOW ADVANCED CRYPTOGRAPHY CAN ENABLE E-COMMERCE

Public key cryptography is an approach that can provide many advantages in support of emerging applications on HFC networks. Figure 3 shows the fundamentals of public key cryptography and contrasts these with secret key cryptography.

Symmetric vs. Asymmetric Ciphers



Symmetric Algorithm (a.k.a. "secret key")

Secure Key Exchange Channel

S

DATA

Same Key Used

Asymmetric Algorithm (a.k.a. "public key")

Pu

No Secure Key Exchange Channel!

Pr

DATA

Different Key Used

Figure 3 - Public Key vs. Secret Key Cryptography

Figure 3 shows that, in a secret key cipher such as the data encryption standard (DES) or DVB Superscrambling, the same key must be used by the sender and the receiver to encrypt and decrypt the message. The process begins with plain text (i.e., an unencrypted message). The key is then applied and the plain text is run through an encryption algorithm. This produces cipher text which can be sent with confidentiality over a network. At the receiving end, the same key must be applied by the receiver to recover the plain text again. The implication is that a secure channel is needed to get this key from the sender to the receiver. If the key were transmitted openly, it could be recovered by unauthorized entities through simple network "snooping" and then used to read messages encrypted with it.

Public/private keys -- which are called asymmetric because the encryption and decryption keys are different -- are mathematically related to each other. What one key encrypts, the other matched key can decrypt. Anyone with the private key can decipher any message encrypted with the corresponding public key and vice versa. The RSA algorithm is an example of this method. Usually, the private key is securely stored so that it may not be easily discovered or altered. This allows messages to remain private to the holder of the private key and also supports another function called digital signature, which will be discussed later.

A major advantage of public key methods is that the public component of the key pair can be published. It can be known by all parties and does not have to be kept secret. It can be put in a global directory where is can be easily accessed on an as-needed basis. Knowledge of a public key can not be used to derive the value of its matched private key.

The public key method provides much better support of a multiple service provider or merchant scenario in the sense that no pre-established relationship between each service provider/merchant and each user is necessary. Security issues associated with secret key databases are eliminated because the public keys can be shared and published openly. Thus, they cannot be stolen because they are already well known.

Use of Public keys is also the best way to provide digital signature services and authentication of users. Digital signatures and authentication allow spontaneous connections between users and service providers or between users in a peer-to-peer mode even though the parties may not know of each other in advance. If they are registered in a public-key database, they can exchange secure messages and be sure that the message author is truly the entity it purports to be.

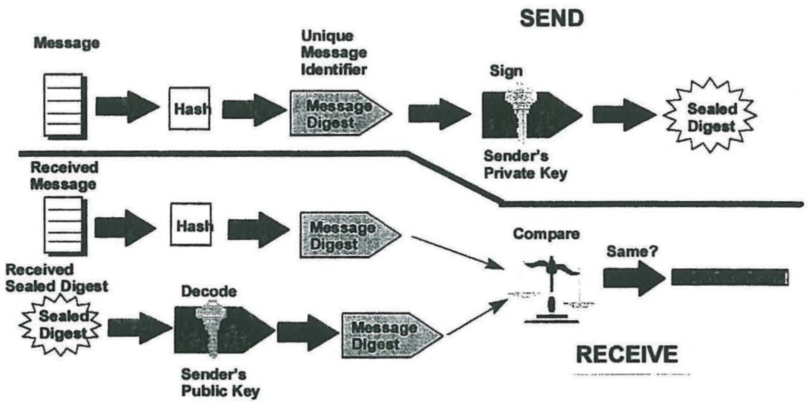


Figure 4 - Fundamentals of Digital Signature

Figure 4 illustrates the authentication process. A message -- it could be a long message, a file, or maybe just an e-mail -- is run through a one-way hash function, This function produces as output a much smaller token (typically 128 or 160 bits) which is called a message digest. This token is a unique identifier of the original message. However, merely knowing the digest does not allow discovery of the message. In addition, because of the design of the hash function, an adversary cannot even formulate an alternative message which produces the same message digest. This makes an attempt to provide a false message extremely difficult.

The message digest is validated and bound to the sender by digitally "signing" it. This is accomplished by encrypting it with the sender's private key. A message encrypted with the private key can be unraveled with the corresponding public half of the key. Because the sender's private key is used -- the one that is not published and that only the sender knows – this provides a way for the sender to put his or her unique digital signature on the message. Each user's private key transforms the message digest in a unique way to produce a "sealed digest". This sealed digest is appended to and sent along with the message.

To verify a digital signature, the receiving terminal simply goes through the inverse motions to process it: receive the message, calculate the message digest in the same way as the sender, and use the public key of the sender to decode the sealed digest. The recipient then compares the transmitted digest with the locally calculated one based on the received message content. If these two quantities are the same, then the recipient knows two things: 1) the identity of the sender is that of the owner of the public key used to decode the "sealed digest" and 2) the original message has not been altered. Note that the message itself need not be encrypted in order for the digital signature to work.

Secure hash functions require very special design. Some examples are MD5 (RFC 1321) or SHA-1 (FIPS PUB 181-1).

While, public key methods offer distinct advantages, it should be noted that there are licensing and intellectual property issues that must also be considered. In contrast, many secret key ciphers are in the public domain and may be used royalty-free. There is also a requirement to provide digital certificates, a certification authority and a public key infrastructure to effectively us public key methods.

CERTIFICATES, CERTIFICATE AUTHORITIES AND THE PUBLIC KEY INFRASTRUCTURE

Data integrity and authentication of correspondents are great advantages offered by public-key cryptography. However, to trust digital signatures, users must have reliable means of obtaining public keys to use in signature verifications. This is done using digital certificates.

Digital certificates are tamper-proof bindings of a public key and the owner of that key. They usually include a "distinguished name" related to the owner, an expiration date, and other data. The "distinguished name" can be a set-top address rather than a subscriber name. Billing information can then be used to link a subscriber with the terminal.

Trust is established by a Certificate Authority. The Certificate Authority is the entity that applies its digital signature to each certificate. Since there are relatively few Certificate Authorities, their public keys can be trusted by publication in open venues, via software distribution (such as in Web browsers) or over the Internet. Then, users can determine the validity of any given certificate by checking that it bears the signature of a trusted Certificate Authority. Clearly, the private key belonging to a Certificate Authority must be guarded carefully.

All of the functions needed to effectively use a public key-based system are collectively known as a "Public Key Infrastructure" or PKI. The principle functions of a PKI are:

- Key Generation
- Storage
- Key transfer (shipping)
- On-line public key repository
- Key renewal (changing)
- Data Recovery (lost keys)
- Retiring keys

Figure 5 shows a structure of a PKI suitable for use in contemporary CATV networks.

A CATV PKI includes not only set-top keys but also keys that the network operator can use to exert control over the set-tops and to enforce its digital signature. In fact, an MSO can have both a corporate-level signature and a site-specific signature. The corporate-level signature can ensure complete control over set-tops in all its systems and to prevent "migration" of set-tops to systems of other operators. The site-specific signature can be used to differentiate control in one headend or system from another.

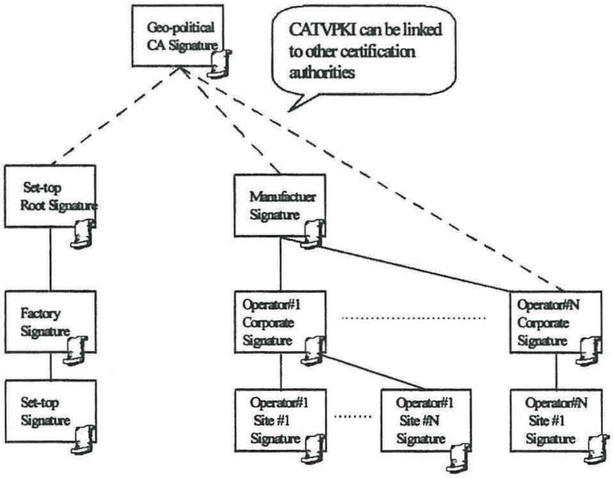

Geo-political CA Signature
CATVPKI can be linked to other certification authorities
Set-top Root Signature
Manufactuer Signature
Factory Signature
Operator#1 Corporate Signature
Operator#N Corporate Signature
Set-top Signature
Operator#1 Site #1 Signature
Operator#1 Site #N Signature
Operator#N Site #1 Signature

Figure 5 - CATV Public Key Infrastructure (PKI)

The set-top is initialized with corporate-level and site-specific "key certificates". It then can check signatures of messages and accept those from the network operator, but reject those from other sources. This is a significant tool in preventing authorization spoofing by pirates but has the further advantage that the operator can also allow or deny access to the set-top by other service providers or merchants. This can be accomplished when the operator validates the digital certificate of a merchant. The set-top can then access and trust the merchant, but otherwise will not attempt transactions with that merchant.The PKI can also be used to link the network operator's signatures and those of the set-tops with a larger universe of E-commerce. Indeed, through the signature mechanism "chains of trust" can be established. For example, a "geopolitical" certificate authority such as Verisign, GTE Cybertrust or governmental agencies certify the keys of MSOs, set-tops and merchants so that by checking a short sequence of signatures, spontaneous E-commerce relationships can be formed quickly. These relationships can also be dynamic.

Flexible PKIs allow changing the "chains of trust". Thus, even though the manufacturer may participate in the signature PKI (as shown in Figure 5), it is perfectly feasible to eliminate this connection. In this case, however, the manufacturer can no longer provide services such as re-keying set-tops when needed, such as in the sale of a headend or system to another operator.

USEFULNESS OF A HYBRID APPROACH

As noted, there are many advantages derived from public-key cryptographic methods, but traditional secret key approaches still have important application in CATV networks. High-speed data, such as Internet data or compressed digital video, still benefit from secret key algorithms such as Harmony DES or DVB Superscrambling because they are much faster. DES, which is a symmetric key algorithm, will run perhaps 100 to 1,000 times faster in the same implementation (hardware or software) than a public key algorithm will. The optimum approach, then, is to use both public-key and secret-key technologies in the appropriate combination. Such a hybrid approach, benefits from the authentication and digital signature capabilities of public key methods in areas such as key exchange and verification of software downloads. At the same time, the speed of secret key algorithms can be exploited to provide confidentiality of large quantities of high-speed data.

LICENSING AND INTELLECTUAL PROPERTY ISSUES

Public key cryptography has several patents associated with its use. Having been invented in 1976, the patents typically have expiration dates ranging from 1997-2000. Licensing of these patents is required for commercial use of public-key technologies. Check with your conditional access vendor, since these licenses may already be included in the product.

OTHER ISSUES TO CONSIDER

As with other technologies, public key cryptography must be implemented properly to deliver its full benefits and selecting standards-based implementations promotes interoperability and economies of scale. Thus, two areas should receive particular attention when the use of public key methods is contemplated:

1) use/existence of relevant standards
2) secure packaging

STANDARDS

Relevant standards in this technology area include a few that are stable, but also many that are still under development. The Internet Engineering Task Force (IETF) is actively engaged in this quest and has defined a security architecture for the IP layer (RFC 2401). Called IPSEC, more information can be found at: http://www.ietf.org/html.charters/ipsec-charter.html. Some of the important methods they are considering at the network layer include: authentication headers (AH), encapsulated security payload (ESP) and Internet Key Exchange (IKE). At the session layer, the well-known secure sockets layer (SSL/TLS) has become widely used in Web applications. At the application level secure multipurpose Internet mail extensions (S/MIME) has gained some acceptance.

The ITU-T X.509 series recommendation already includes a standard for public key certificates. DAVIC, the Digital Audio Visual Council, has published Part 10 of DAVIC 1.2 which includes general security interfaces and tools for multimedia applications. MasterCard and VISA have been leaders in specifying e-commerce secure electronic transactions (SET - http://www.setco.org/).

An "informal" but widely referenced standard is the public key cryptography standard (PKCS) published by RSA Laboratories http://www.rsa.com/rsalabs/pubs/PKCS/index.html. Developed in conjunction with representatives of many computer and communications firms, it gives excellent recommendations on how to use a wide array of public key techniques and includes such important topics as message padding. A more formal effort to establish procedures governing the use of public key cryptography is the Institute of Electrical and Electronic Engineers (IEEE) P1363 which passed its first ballot on April 2, 1999. (http://grouper.ieee.org/groups/1363/)

SECURE PACKAGING

To promote interoperability and retail availability of good security for networks, physical packaging becomes important. For physical security devices a popular standard is ISO 7816. This is the most universal reference for smart-card technology. It now comprises a series of six parts, covering mechanical, electrical, and protocol interfaces of these hardware tokens.

The Personal Computer Memory Card International Association (PCMCIA) package is also a choice in this area. Indeed, the DVB Common Interface, NRSS-B and OpenCable POD all use this basic form factor. Also known as PC-Card, this standard provides a uniform and convenient physical form factor and a flexible 68-pin interface with considerable provisions for software-based configuration of the package.

Certificate Authority equipment must also have highly tamper-resistant packaging.

CONCLUSION

With good protocols and an appropriate combination of public key and secret key approaches, CATV security systems can effectively and safely enable many classes of broadband networks to securely deploy digital services and robustly support E-commerce applications.

Tony Wasilewski is Chief Scientist, Subscriber Networks Sector at Scientific-Atlanta, Inc. His contact information is:

5030 Sugarloaf Parkway
Lawrenceville, GA 30042
Phone: 770-236-5004
Fax: 770-236-3080
E-mail: tony.wasilewski@sciatl.com