APPROACHES TO SECURITY AND ACCESS CONTROL FOR DIGITAL CABLE TELEVISION

Claude T. Baggett
Cable Television Laboratories, Inc.
Louisville, CO 80027-1266

Abstract

This paper addresses the several design trade-offs which should be considered by a system operator in selecting a security and access control sub-system for protecting digital television signals on cable television systems. Factors are discussed which have a strong impact on the strength, adaptability, and cost of such systems. The principles discussed in this paper apply whether the primary source of security and access control in the subscriber home is found in a set-top decoder, a decoder interface unit, a home server, or as an insertion in an MPEG-capable computer or television receiver.

SCOPE

This paper will address the options which system operators should consider in choosing a security and conditional access system for their digital television signals. It will not address cryptographic and key handling processes in depth, but only as required to explain the trade-offs in system selection.

BACKGROUND

There are a number of options and design trade-offs which must be considered in order to optimize the digital security and access control functionality to cable system needs. Some of these decisions have only minor impact on the quality of the security sub-system, but others will have a pronounced affect on the robustness, integrity, usefulness, cost, and extendibility of the chosen system and its deployment. A "one size fits all" approach to the functionality and features of the security and access control system is not appropriate because of the great variation in cable system size, services, operating philosophy, and access to capital.

In analog television, there is basically only one decision which must be made for access control; that is, whether to descramble the incoming signal or not. The same descrambler in the set-top converter is used whether the system has one scrambled channel or many. The sophistication and depth of the scrambling mechanism is limited because the analog signal is very difficult to reconstruct without leaving unacceptable artifacts in the visible picture. Therefore, with only one, very limited, process to protect the analog television signal, meaningful security is difficult. Some later systems, which use line shuffling under the control of a modern cryptographic system and hard-encrypted audio, are much superior in this aspect, but are costly and have come too late relative to the advent of digital television.

To protect digital signals, four basic mechanisms are utilized. First, a cryptographic algorithm is defined for the headend which will take the digital signal and scramble the binary characters so thoroughly that no practical amount of analysis will regain the original signal. This same mechanism is used to reconstruct the signal in the subscriber home. If this were all that was possible with digital scrambling it would still be of great benefit because of the depth of the obfuscation of the signal and the fact that it can be restored to its original, pre-scrambled, condition without degradation. However, digital security is much more versatile than that.

The second basic mechanism is the electronic key—literally a long binary word—which controls the scrambling and descrambling processes in the cryptographic unit. The cryptographic algorithm itself is useless without the electronic key. Furthermore, unlike analog scrambling, a different electronic key can be used for differentiated services. Multiple keys can be used to protect a tier of services, a single digital channel, or a specific string of digital data such as a control channel, a pay-per-view event or a multimedia display. Keys can be symmetric, meaning that the same exact binary word is used to scramble and descramble the digital data; or they can be asymmetric, meaning that the key used to descramble the signal is different from the one used to scramble it. Keys must be generated, managed, protected, transmitted, and utilized, thus forming the key management and distribution system which is the most critical part of the security process.

The third basic part of this system is called the entitlement/authorization message or matrix. Originally, this was just a matrix of two columns by the number of rows equal to the number of occupied channels on the cable system. If a given channel had a binary one in the second column it was authorized for descrambling, and if a zero was placed there the customer was not authorized to receive it. This matrix was encrypted for transmission and stored in the secure microprocessor in the access control system. Now, a cryptographic system, somewhat like the master key systems used in buildings, can be devised which convert the simple authorization matrix into a cryptographic process, thus making it much more difficult to defeat.

The fourth part of the system is a secure signature mechanism. Secure signatures make it possible to guarantee the identity of the sender of the digital message and to verify that the message has not been modified en route. This is especially useful in key distribution, certain control messages, and in purchasing.

The specification of these four mechanisms involves the consideration of the intended application, technology issues, threats and countermeasures, governmental policy and regulation, costs, and desirable additional features.

DEFINITION OF TERMS

The following terms are either used in this paper or are considered important to the understanding of digital security systems.

Algorithm: A mathematical process which can be used for the scrambling and descrambling of a data stream.

Authentication: The process by which one party can ascertain with certainty the identification of another party.

Authorization Coding: A digital word which describes the personality or service access capability of the subscriber decoder unit. This code word, which is based on the service access authorized by the billing system, determines which keys are distributed to each customer, and is required at the subscriber decoder to authorize the descrambling of any specific program.

Conditional Access System (CA): The complete system for ensuring that cable services are accessible only to those who are entitled to receive them, and that the ordering of such services is not subject to modification or repudiation.

Cryptanalysis: The science of recovering the plain text of a message without access to the key (or electronic key in electronic cryptographic systems).

Cryptographic Duty Cycle: The maximum secure capacity of a cryptographic process, based on total data throughput on a single key vector.

Descrambling: The process of reversing the scrambling to yield usable pictures, sound, and data services on a cable system.

Electronic Key: The term for data signals which are used to control the descrambling process in subscriber decoders. There are at least three types of electronic keys referenced in this Recommendation, including those used for television signal streams, those used for protecting control system operations, and those used for the distribution of electronic keys on the cable system. While the Authorization

Coding is effectively a key, it is treated separately in this section.

Encryption: The process of scrambling digital signals to avoid unauthorized access.

Host: A device with generalized functionality where modules containing specialized functionality can be connected.

Integrity: The ability of a function to withstand being usurped for unauthorized usage, or modified to yield unauthorized results.

Intrusion Resistance: The ability of a hardware object to deny physical, electrical, or irradiation-based access to internal functionality by unauthorized parties.

Module: A small device, not working by itself, designed to run specialized tasks in association with a host.

National Class Laboratory: The primary source for cryptanalysis in a national government.

Non-Repudiation: A process by which the sender of a message cannot deny having sent the message.

One-Way Hash: A mathematical process or algorithm whereby a variable-length message is changed into a fixed-length digital word, such that it is very difficult to calculate the original message from the word, and also very difficult to find a second message with the same word.

Pay-Per-View: A payment system whereby the subscriber can pay for an individual program or programming period, rather than for a full-period terminated service.

Piracy: The act of acquiring unauthorized access to programming materials, usually considered for the purpose of reselling such access to illegal subscribers.

Public Key Cryptography: A cryptographic technique based upon an asymmetric two-key algorithm, private and public, wherein a message is encrypted with the public key but can only be decrypted with the private key. Knowing the public key does not reveal the private key. Therefore, Party A would devise such a private and public key, and send the public key openly to all who might wish to communicate with Party A, but retain the private key in secret. Then, while any who have the public key can encrypt a message for Party A, only Party A with the private key can decrypt the messages. Also known as a Private-Public Key (PPK) system.

Scrambling: The process of using an encryption function to render television and data signals carried on a cable system unusable to unauthorized subscribers.

Secure Signature: A mathematical process by which the origin and integrity of a transmitted message can be ascertained. This means that the originator cannot deny having sent the message, and the receiver can determine if the message has been modified.

Transport Stream: An MPEG-2 (Moving Pictures Expert Group) or other data digital transport stream.

DESIGN CONSIDERATIONS AND TRADE-OFFS

Since this paper will not address cryptographic algorithms in depth, it appears useful to dispose of this topic first. For many years now, the approved civilian cryptographic process in the United States has been the Digital Encryption Standard, or DES. DES has several operational modes in order to be as widely applicable as possible. The National Institute of Standards and Technology (NIST), the government agency responsible for civilian cryptography, has approved DES for use through approximately 2003, but plans to have a new encryption standard in operation by that time. This does not mean that the DES equipment in the field will suddenly cease to function or become more vulnerable, but that NIST will no longer support it.

DES is only one of many hundreds of electronic encryption algorithms which have been devised, each with its target application, strengths and weaknesses. Many of these are appropriate for the encryption of digital television signals, therefore a choice of these on merit would be difficult indeed. The North American cable industry has decided to begin their digital television transmissions using the GI DigiCipher 2® system, which is DES-based. This does not preclude an operator from deciding on another algorithm if so desired, or starting with DigiCipher® at the outset and changing to another algorithm at a later rebuild.

The important issue for being empowered to choose from multiple algorithms is to be able to select or change systems without undue cost or operational impact. An operator may decide to change cryptology for several reasons, including:

1) The security has been compromised and pirating has begun;

2) Unit reliability has deteriorated to an unacceptable level; and

3) The operator wishes to add new services which the existing suite of security equipment cannot protect.

This issue leads to the first design trade-off question in this paper, which is:

Removable and replaceable versus built-in security

In the past, analog descrambling converters have always had security-related circuitry as an integrated part of the unit. Removable and replaceable descrambling circuitry has never been important in analog television because that circuitry represented an important portion of the overall cost of the box, and a pluggable interface to the descrambler is not cheap or easy. With digital decoders, the security represents a relatively small portion of the cost of the unit, and the interface for digital data is a well known and practiced science.

There are three basic approaches to the architecture of the security system as far as its placement is concerned. In case one, the digital security circuitry can be integrated into the digital circuitry in the MPEG-2 decoder unit. Case two has the security functionality totally placed in a removable module, such as a PCMCIA card, with an open architecture interface to the host device. Case three is a hybrid of the first two wherein the security sub-system is built into the decoder unit, but an open architecture interface is provided so that the internal system can be replaced by a pluggable, replaceable one.

The fully integrated decoder unit with no external socket for replaceable security probably represents the path of least initial cost to the operating system. However, if and when the security requires replacement, the entire decoder unit must be replaced, representing hundreds of dollars rather than tens of dollars for a PCMCIA removable security module. The other problem with this approach is that it is not responsive to the Telecommunications Act of 1996. This law states that set-top decoder units must be available at retail to the subscriber, but not the security element used by the cable system. This law necessitates making the security circuitry removable if the cable operator is not to totally lose control of the security of the cable programming. If the security circuitry is not removable, then the consumer electronics manufacturer will decide which security is adequate to protect the cable business, and there will be only one algorithm available.

The totally removable security element is responsive to the Telecommunications Act, and provides the cable operator a cost-effective way to replace the functionality when the need occurs. The proposed PCMCIA module has adequate capability to provide all of the needed functionality and additional features demanded by the marketplace and has an interface which is more than adequate for the needed control and data transfer. There are three separate efforts underway to standardize the interface between the removable module and the host device. These are the Digital Video Broadcasting (DVB) Common Interface Specification being planned for Europe, which uses a pin-depleted version of the PCMCIA card, the National Renewable Security Standard (NRSS) of the United States which includes specifications for both the PCMCIA module and the ISO-7816 chip card, and the security working groups within the Society of

Cable Television Engineers (SCTE) Digital Video and High-Speed Data Subcommittees of the SCTE Engineering Committee.

To define an interface between the security module and the host system, three separate issues must be determined. First, the physical form factor of the module must be specified along with the number and placement of the connector contacts or pins which provide the physical interface between the two entities. Second, the electrical specifications regarding powering, grounding, logic levels, and clock speeds must be set. Finally, the format of the data, and the command set which controls the interface and integrates operations must be determined.

The NRSS specification stops at this point and makes no attempt to define the exact security functionality contained within the removable module, preferring to leave this determination to the marketplace interaction between the cable operator and the equipment vendor. The DVB specification attempts to go further and define the exact security algorithm and feature set to be used by the operator. If DVB were accepted worldwide it would mean that every cable system, broadcaster, satellite deliverer, and MMDS operator would have the exact same cryptographic function for security, but that they use an electronic key unique to their system. The best advice from cryptoanalysts in the US and elsewhere is that this is a foolish undertaking as it would dramatically increase the worldwide vulnerability to the pirating of communications signals. However, there appears to be no strong reason why the interface specification between the NRSS and DVB standards cannot be harmonized and efforts are underway in the NRSS subcommittee at this time to accomplish that task.

The specifications generated by the SCTE subcommittees will no doubt reflect some of the work which has already occurred in NRSS and DVB, with further tailoring of the requirements to cable industry needs. However, the DVB and NRSS work specifically targets the interface of MPEG-2 signals and may not be optimized for other data transmissions used on cable systems. Therefore, efforts are beginning in the Security working group of the High-Speed Data Subcommittee of the SCTE to define a new interface, perhaps somewhat like NRSS and DVB, which will specifically meet the needs for the data transmission infrastructure on cable. It is probable that the results of the SCTE efforts will yield the proper purchase specifications for the cable television and data industry.

In-band, out-of-band, and hybrid control channels

Traditionally, the control channel for analog descrambling converters has been carried on an out-of-band separate carrier located in the downstream cable passband. Since that portion of the control channel dedicated to security and access control primarily was dedicated to a single issue, allowing the descrambler to turn on or not, overhead on the channel was minimal relative to that required for digital security. Satellite, MMDS (Multichannel Multipoint Distribution Service), and SMATV (Satellite Master Antenna Television System) delivery systems for MPEG television signals use an in-band control channel scheme wherein the packets for security or other control functions are inserted into the transport packet stream. At the receiver, a Program Identification Filter (PID Filter) examines the headers of the incoming packets and routes them according to their content, video, audio, or control. Packets called EMMs (Expanded Memory Manager) and ECMs (Error Correction Mode), which contain key and authorization codes, are routed to the cryptographic processor. It is also possible to do an amalgamation of these two systems where certain control functionality is carried on an out-of-band carrier, and security packets are contained in-band.

Note that the in-band signals carried with each MPEG transport stream apply only to that channel whereon they are carried, and each MPEG television channel has its own peculiar security packets. On an out-of-band control channel all of the keying and authorization data applying to all digital channels are carried on the single carrier. There are pros and cons to each of these approaches. The in-band system requires a packet inserter in the headend for each encrypted digital channel. While this seems like an unsupportable complication, it must be remembered that each encrypted digital channel also has a digital encryption device at the headend. Adding the ability to insert packets at that point represents an extremely small increase in complexity. For programming sources, such as Headend in the Sky™ (HITS) where re-encoding at the headend may not be necessary, the insertion of ECMs and EMMs can be accomplished at the uplink facility and no additional complexity is required at the cable headend. The out-of-band carrier represents a system vulnerability in that if the signal is jammed or otherwise fails, the entire system, including every encrypted channel, also fails at the next key change. Whereas with the in-band system, the failure to rekey only affects the single channel where the problem occurs. There also is some question as to whether cryptographic synchronization can be supported during rapid key change intervals with the single out-of-band carrier.

All of this relates back to a basic security consideration for multichannel digital television on cable. As explained earlier, if you have a proper functioning decoder unit, there are still two key elements required to decrypt a program; the cryptographic key and the authorization code. Suppose a security and access control system uses the same cryptographic algorithm and electronic key to secure every differentiated channel on the system. This means that the correct key is present in the home terminal equipment to decode every program on the system. The only feature preventing that from happening is the authorization code which sets the personality of the decoding unit. This therefore negates much of the advantage of digital security by making it work just like existing analog descrambling converters, meaning, turn them on and they decrypt, turn them off and they don't. The biggest advantage is found in using different cryptographic keys for each differentiated service or tier of channels. This means that each differentiated service or tier is encrypted completely differently from any other, and if a subscriber doesn't take a certain service, the key to decrypt it is not even present in the home terminal.

Now, what does this mean for in-band versus out-of-band control channel architecture? If each pay service, each pay-per-view, and each differentiated tier of channels has its own unique cryptographic key—which is changed on a fairly rapid basis during each day—a huge overhead is placed on the out-of-band channel during key update periods, which is fairly continuous. Additionally, an extra burden is placed on the home decoding unit to ensure crypto-synchronization during key change periods. Since the proper key is sent in conjunction with the secured video and audio in the in-band case, crypto-synchronization is virtually automatic.

It is also unclear at this time how cable systems which have implemented ATM (Asynchronous Transfer Mode) transport structures for voice, data, and video can accomplish out-of-band control, since, by definition, all control is in-band.

There is a hybrid solution which may actually be the best choice of all in these design considerations. This is where the EMM and ECM packets are sent in-band with the MPEG transport stream, but all other control signals are sent over an out-of-band channel. This takes the burden for key distribution off of the out-of-band control channel, but still facilitates other control functions. Besides the home terminal unique control signals sent on the out-of-band channel, other signals such as pay-per-view promotionals, local clock, channel maps, purchasing communications, program guide updates, security and usage audits, messaging, etc., could then be easily transported on this channel in a global fashion. Sending certain control keys over the out-of-band channel may facilitate the compartmentalization of large systems into sub-key regions, to reduce the marketing area of the subscriber/pirate, and to provide a unique point of leverage in disenfranchising cloned home terminals.

Public-private and symmetric key systems

In Public-Private-Key (PPK) systems, an algorithm is used which has two different keys, one called private and the other public. The public key is sufficient to encrypt a message for transmission, but the private key is required to decrypt that message. So, if Party A wishes to receive communications from Parties B, C, and D, Party A will send them the public key part of the key-pair, while keeping the private key strictly to himself. Whenever B, C, or D wishes to communicate a message to A, they encrypt it with the public key and transmit it to A. Note that while B, C, and D, all have the same public key, they cannot read each other's messages to A because they do not have the private key. Party A can read any message from B, C, or D because the private key has been retained. In a cable system, Party A would be the headend, and Parties B, C, D, etc., would represent the subscribers with digital descrambling converters. The headend would send to each subscriber its public key so that each subscriber terminal could communicate toward the headend either on the return plant or via telephone return, if two-way communications is desired. Each subscriber terminal would also send its public key to the headend, or do so at the time of converter issuance and activation, so that the headend could communicate uniquely to each of the subscriber terminals. This would allow the unique control of each unit individually. It would also be possible to have a second PPK system in which the public key from the subscriber terminals are all the same, thus allowing a single global message to be sent containing material that all receive, such as clock, channel map, etc.

Symmetric key means that the exact same single key is used for encryption and decryption. This is much simpler than the PPK approach, but only if you have a method for delivering that symmetric key to each legitimate customer without it being revealed to unauthorized subscribers. With symmetric key, each differentiated channel or tier would have just one key per key period and the problems of key distribution in a PPK environment are eased. The probable best answer is once again an amalgamation of the two systems. Suppose a cable operator used a PPK system to protect the current operating symmetric keys during their distribution to those subscribers who are authorized to receive them. The symmetric key, encrypted by the public keys from authorized subscribers could then be delivered without unauthorized subscribers being able to discern them. Since the changing of symmetric keys is not required on a continuous—but more of an intermittent—basis, the overhead in the control channel from the PPK system can be lessened.

Taking this one step further on any given system there are a limited number of perturbations in the possible service personalities available to the subscribers. Then, each home terminal could be differentiated based on the service personality group into which it falls. All home terminals of the same service class could be keyed similarly, if pay-per-view and purchasing is split out and handled separately. This advantage would fall apart in a completely a'la carte service rendering.

Anytime a rekeying message is directed to the home terminals (if it is sent under a secure signature mechanism) at least the terminal can ascertain that the message is from the headend and that it has not been modified en route.
One other problem with PPK systems as the single system for encryption in cable television is that the operations are more complicated and require more processing and transmission time. This overhead increase could become an important factor in control channel access in a PPK-only system.

There are a number of iterations in design concept based on the use of PPK and symmetric key systems. The important thing to the cable operator is to understand how the system works, and the amount of overhead left in the control channel to allow future subscriber-base expansion without a required rebuild of the CA system. It must be said that the use of any of these systems does not obviate the clone terminal threat. In that case, the clone terminal is configured cryptographically just like the pirate's legitimate terminal and each time the legitimate terminal is given a new key; the clones are likewise updated. Other countermeasures are required in addition to the ones discussed here to resolve this threat.

Form factor trade-offs

This subject was partially discussed above, but a few more words are required for completeness. There are two worldwide accepted module formats which are candidates for use in cable operating systems, the PCMCIA card and the ISO-7816 chip card. Either one could be made to work for the most simple conditional access applications. The ISO-7816 card is basically limited to a single 25 square mil integrated circuit, which is nonetheless adequate for a straightforward decryptor, such as DES. It may not be adequate to house a simultaneous decryptor/encryptor and secure signature unit with adequate storage for several keys, even with limited or no additional features. There are only eight contracts on the card for interface, which means that the data must be streamed onto and off of the card in serial format. This card has been tested at 50 Mbps serial input/output with good reliability. However, since the security card is intended to be inserted into the socket and left there for long periods of time, perhaps years, it is not known how corrosion at the point of contact between the socket and the contact pad would impair this data rate.

The PCMCIA card has sufficient contact pins so that the input and output data can be sent in byte-parallel, or at least nibble-parallel, format, thus reducing the impact of corrosion impairment on a single pin. The module also has considerably more volume than the ISO card, thus facilitating more complex security schemes and multiple features.

Another option for cable would be to define its own unique module form factor and pin configuration. While this has some desirable features, it presents almost insurmountable problems at the cable/consumer electronics/computer interface, and in the end, would not likely represent any real advantage over using the proven and widely deployed PCMCIA card.

DEPLOYMENT OPTIONS

While we are discussing options for moving into the digital security era on cable, a few words regarding deployment are in order. No matter what approach is chosen, everyone in the industry understands that this transition is going to be costly and given to a certain amount of operational disorder.

Here are some options to consider, with probable results:

Table 1: Deployment Options for Digital Scrambling

Option	Probable Result
Ignore digital, stay analog	Be driven out of business.
Co-carry both analog and digital scrambled services along with analog unscrambled basic.	Inventory proliferation; Pirates still steal analog services; Wasted spectrum; Reduced incentive for customer to move to digital tier.
Keep unscrambled analog basic only; Carry all scrambled services on digital system.	No descrambling analog converters required; All pirating stopped or deferred; Improved pictures with digital incites customer to move to digital tier.

For example, suppose a system was capable of 66 channels, being divided into 30 channels in a basic unscrambled analog tier, with the balance scrambled and apportioned into an expanded basic tier, and some number of pay and pay-per-view services. If you chose to approach your digital transition according to the third option above, you might consider the following channel breakout:

1) 30 Unscrambled Analog Basic Tier Services

2) 16 Channels (96 MHz) of Open Spectrum Dedicated to New Digital Data Services such as High-Speed Data or Telephony

3) 120 Digital Scrambled Channels (20 - 6 MHz Channels at 6:1 SDTV Compression)

Only those subscribers taking pay services of any kind are required to have the digital decoder units, which they can rent or purchase from the cable company, or purchase at their consumer electronics retailer. In either digital case, the cable operator is responsible for furnishing the removable security and access control module to each pay customer. In this scenario, the operator has had a net increase of 100 standard definition digital channels, has retained the 30 channels of analog basic programming for the transition period, and has netted an additional 96 MHz for further digital service development. A similar case can be made for systems with fewer channels which result in similar proportional gains. To be economically feasible, this scenario supposes that the system operator acquires the digital programming channels in a format suitable for available home terminal units without having to decode and re-encode each digital channel in a new MPEG format, but does require that trans-encryption is performed for every scrambled digital channel.

CONCLUSIONS

Competitive issues require cable operators to make the move to digital as expeditiously as possible. Enhancements in security and picture quality will directly or indirectly off-set some of the transition costs. Digital transmissions from competitive sources are already operational so cable is behind in deployment. It is absolutely necessary that cable deploy digital services as soon as possible to stop erosion of the customer base. There are a number of options for security and access control which should be considered by a cable operator based upon unique and individual system and company requirements.

When considering the purchase of a security and access control system with which the cable operator has no direct experience, it would be well to consider using the services of a communications security certification company to examine the proposed system for compliance to the purchase specification and to ascertain any unadvertised vulnerabilities which the system may possess.