ENCRYPTION-BASED SECURITY SYSTEMS
What Makes Them Different and How Well are They Working?

Anthony J. Wechselberger
Vice President, Engineering

OAK Communications Inc.

Introduction

Over the past half dozen years a new genre of secure audio/video transmission equipment based on the application of encryption technology has developed. The use of encryption has been made possible by advances in technology in several areas. Developments in semiconductors and microprocessors and the evolution of low cost digital communications and processing techniques has been married to newer industry trends such as addressability, satellite television broadcasting, and pay-per-view, which demand enhanced security.

This paper will discuss some of the fundamental aspects of how encryption technology can be used to secure program delivery, why cryptographic methods are different from traditional scrambling techniques, and how their proper application offers long term solutions where other approaches fail. We will then test these arguments by looking at how products featuring encryption-based approaches to security are doing in the marketplace.

Historical

A microcosm of what later became an industry trend took place within Oak Industries in the early 1980's. This was the battle against signal theft on both legal and technological fronts. We were rapidly expanding our subscriber base in STV in 1980 and, while vigorously pursuing pirate activity on the legal front, were experiencing severe piracy problems in our large Los Angeles and Chicago markets. It may be surprising, but the scrambling approach being used in those days was more complex than many types still going into new cable installations today. Yet we estimate at least 50,000 illegal pirate boxes existed in our subscriber base of some 380,000 in Los Angeles alone. Illegal STV boxes were selling for $200 to $400 and were generally built from scratch. This for one channel of premium programming, when over-the-airs were readily available for free! So at Oak we learned early to respect the degree to which pirate activity could organize and be technology-wise.

We sought a technology solution to the piracy problem through the application of encryption, and in 1982 launched our new Dallas, Texas and Portland, Oregon STV operations with the world's first commercial use of a security system based on true encryption principles. Also that year we introduced ORION, Oak's broadcast-quality satellite security system. The STV markets didn't survive long enough for a true test of their encryption systems (they were on the air for only about a year), but ORION is still in use today, with approximately 20,000 units in both commercial programming and private network use. We now market our Cable Sigma product line which applies similar encryption technology to the cable environment.

With the industry looking to protect satellite broadcast of premium programming services by the adoption of a de facto standard, and the private sector (networks) also widely utilizing scrambling, we see a technology solution to the theft problem on a broader scale today. Pirate activity is also being combatted legally and procedurally by companies (e.g. General Instrument vs. "Cooper et al") as well as by collective industry efforts with groups such as the Coalition Opposing Signal Theft (C.O.S.T.).

Today, a cryptographic approach to securing television transmissions is accepted as the contemporary method. Yet all products described as using encryption principles are not created equal. As we're seeing today, encryption systems can and have been compromised. The test of longevity will be those which are able to recover from a compromise once it has happened. So how does one know if a system is technically secure, or secure enough, or by what margin? How does one get past buzzwords or generalisms in developing a figure of merit on a subject as esoteric as encryption? It's not as difficult as it might seem, once a few basic themes are examined.

Three Tests for True Security

The discussion will center around three areas, each a fundamental prerequisite before the system can qualify as "cryptographically" secure. These are:

1. What is being secured? That is, what aspects of the total information transfer process are being (or, more importantly, are not being) protected by the use of encryption?
2. What are the actual encryption algorithms, and how are they used?
3. How was key management problem solved?

Unfortunately one of the areas that gets most attention in security studies is many times the least important, at least in entertainment applications. That is number (2) above. It happens to also be the most esoteric, that is, most difficult for the layman to evaluate. For the moment let's just say an "algorithm" is the lockbox that mathematically envelops or encloses the information such that it cannot be recovered without a "key". The encryption algorithm all by itself must be evaluated in terms of its ability to withstand "breaking". Once encrypted by, or through the use of the algorithm, the information must not be able to be recovered by analyzing the algorithm, or the resultant encrypted information. With today's computers and high speed logic, it is straightforward to design and implement algorithms which are low cost, and extremely "hard" or difficult to break; although you may need some expert help in this part of the evaluation. The most popular algorithm in commercial use today is the "DES" or Data Encryption Standard. DES is only an algorithm. It's use does not a secure product make by any means.

Items (1) and (3) above ensure that the algorithm is put to work properly. It is the objective of an encryption-based system to 1) "bottle" up or secure the information (in our case, programming and subscriber management information) by encrypting it, and 2) ensure that no back doors exist allowing the information to be recovered by any means other than decrypting the encrypted information at legitimate receiver sights by 3) using a secure key management scheme alongside our secured signal.

When studying encryption systems one always comes back to key management, as we'll see when we look at real world systems. Since we said that by definition the only way to recover the secured information is by using the algorithm key, the system must provide for convenient, dependable and secure methods of distributing decryption keys to legitimate receivers to recover the broadcast information.

Test Examples

Let's now look at some specific examples of the above concepts in cable or satellite programming distribution networks. First, we'll look at why traditional "scrambling" methods fail the first of our three tests for total systems security.

Consider a contemporary addressable scrambling system having scrambled programming and one or more control or addressing channels. When considering the piracy issue, which includes any kind of unauthorized access to programming, note that the control channel or channels have no relationship (as far as the pirate is concerned) to the service being purchased. One of the first questions to ask then about a scrambling system is what is the function of the control/authorization channel? That is, how is it related to the scrambling approach if at all?

In most systems the control channels direct the decoder to decode or not to decode as a function of either the channel tuned, or the tier of a given program. Critical to the issue is whether any information contained in the control channel is required in the decoding process. If not, the control channel can be ignored when attempting to pirate the signal. Likewise, if the scrambling technique or decoder circuitry easily succumbs to one-time defeats (e.g. a hardwired defeat), the control channel content is of no interest. Such is the case when descrambling can be accomplished by observation of the scrambled signal alone, while ignoring the control channel information.

What about "time-varying scrambling"? Time-varying scrambling adds a dimension of change to the scrambling process such that the decoder will not properly decode at all times unless it appropriately follows the change. Is this better security? To a degree, yes. But if the attribute that changes has few or trivial differences, then no real barrier to defeat of the system is actually created. Consider the pirate entrepreneur who wishes to build a "universal decoder". Most positive scrambling systems use one of several techniques of suppressing the horizontal sync pulse. ("Positive" systems are those that actively scramble the premium signal, and thus require a decoder. "Negative" systems remove the signal from the unauthorized viewer through traps or signal path switching). Whether the system's scrambling is at RF or baseband, our pirate's universal decoder can quite easily be designed to reconstruct the sync pulse and completely ignore all control channel information, time-varying or not.

This discussion is gearing us toward a theme: In programming distribution, security is a systems issue. The simplest method of defeat will be the path followed by the would-be pirate. The system must therefore be viewed from several angles and an adequate threshold against compromise developed for each. In so doing, one must ask what information (timing, control data, circuitry, etc.) is available at the receive location that can be used to get around (not through) the secured or encrypted material. There is usually an amazing amount of data available to tap. How much added security is afforded by random video inversion of the picture for example, if a simple-to-detect "flag" exists in the vertical interval indicating current polarity? Is any security afforded in an addressable system simply because it's addressable? Not if it's easier to address (authorize) the box yourself than it is to open the box up and tamper with circuitry. This is our first test then, the notion of the "back door" entry to information. Why worry about breaking the encrypted audio out of your satellite receiver, for example, if it's coming out of your local cable drop in the clear?

The Encryption Algorithm

We'll now digress momentarily to discuss some details of what constitutes the encryption algorithm, and how keys or key variables are used. The encryption algorithm executes a "digital processing" function. The actual entity that undergoes encryption must be in a digital format. The output of the algorithm can then be used to perform other random processes, if desired.

CLASSICAL CRYPTOGRAPHIC SYSTEM

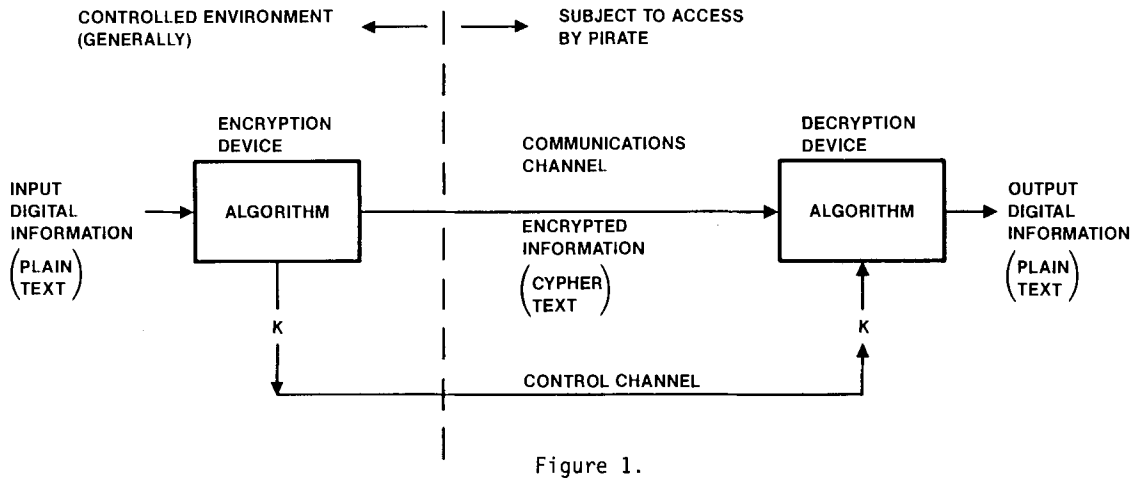

Figure 1.

In a conventional encryption system (Figure 1), a digital bit stream (the information) is passed through the algorithm that transforms the input into a seemingly unrelated output bit stream. The transformation that is performed is a function of the "key variable", and in a conventional system the same key is used at both the transmit side where encryption is performed and the receive side where decryption is performed. A different transformation is implemented whenever the key changes. The key is a digital word of many bits (generally in the range of 24 to 64 bits), so 2^n (where n is the number of bits in the key) different transformations are possible by varying the key. In a properly designed algorithm, all keys are equally strong (i.e., resistant to "cracking") and no detectable relationship exists between the input data, output data or key variable. Each combination of key bits represents a completely different scrambling "mode" and there is no such thing as "almost having the correct key". The key must be exactly correct or no decryption is possible.

The process of encryption must, of course, be reversible. That is, applying the same key at the receiver must restore the original information. The original, non-encrypted data is called clear or plain text, the encrypted data is called cipher text. So during transmission (i.e., between headend and decoder), only non-intelligible cipher text is available to the would-be tamperer. If the decoder doesn't have the proper key, no message or clear text will be obtainable, even if the pirate has the hardware. Further, in a properly designed system based on cryptographic security principles, we can give the pirate just about anything he wants: hardware, access to, and knowledge about the control channel, schematics, any firmware, and even the crypto-algorithm itself. The only doorway to information access, in our case programming, should be through the key variable (no back doors, right?). Controlling access to the key variables is thus essential. This is called "key management" and is the basis for what ultimately makes or breaks the security of a cryptographically-based system. The cryptographic or encryption algorithm, therefore, can be thought of as a lockbox. The message is encrypted or locked by the algorithm, and can only be unlocked by the same algorithm, which means the identical digital key must be used for decryption.

Now that we have discussed some essentials, the value of encryption as a mechanism for security will be more readily evident. For encryption simply enables a complex security problem, in which many variables (audio, video, control) must be secured, to be reduced to simple protection of a few digital keys. Figure 2 summarizes these and other advantages of digital encryption.

Key Management Problem

The third of our three tests for security asked about the key management problem. Encryption alone will not assure the security of information in any network in which it's used unless the key management problem is carefully addressed. In the broadcast scenario, the problems of key variable distribution are particularly challenging (in comparison

ADVANTAGES OF DIGITAL ENCRYPTION AS A BASIS FOR SECURITY

- IMPLEMENTED WITH INEXPENSIVE DIGITAL HARDWARE
- ENCRYPTION REQUIREMENTS INTEGRATE NICELY INTO THE ADDRESSABLE CATV ENVIRONMENT
- EASILY AND NATURALLY BECOMES TIME VARYING
- SECURITY IS NO LONGER MANIFESTED IN PROPRIETARY CIRCUITS
- LEVEL OF SECURITY ACHIEVED CAN BE ORDERS OF MAGNITUDE ABOVE ANALOG SCRAMBLING APPROACHES OF EQUIVALENT COST

Figure 2.

to applications where only point-to-point situations exist). It probably has occured to the reader by now that, if access to working hardware is given the pirate, it is little trouble to determine what digital key is being used for decryption. Recall that previously it was stated that one-time defeats won't be allowed. Therefore, the encryption/decryption keys must be changed from time to time. The time interval depends on the key length, the ability of the encryption algorithm to resist analysis by computer, the expected accessibility of keys and the motivation of the system's enemy.

In an addressable system, the control channel is the obvious choice for a key distribution path. (Alternate methods might be by courier, mail, etc.). But one can't just go broadcasting the new keys throughout the network. They must remain private to all but authorized decoders. The solution for controlling key access is to encrypt the keys for transmission. By transmitting decryption keys in an encrypted form throughout the system, we have not really solved the key distribution problem, however, because to decrypt these keys requires yet another key. Such is the notion of "multilevel key distribution" (Figure 3). Various information exchange networks utilize different solutions to a multilevel approach. In the television broadcast environment, either satellite or CATV, the requirements dictate that: 1) when the keys are changed (updated), all decoders (and encoders too) must do so at the same time; 2) the system operation must ensure that all decoders have had the new keys properly delivered, decrypted and prepared prior to engaging them; and 3) only authorized decoders are able to perform (1) and (2).

In fact, many types of information passing through the control channel are candidates for encryption. Authorization or tiering data, for example, also should be considered "sensitive" information since, as pointed out earlier, it can easily be locally synthesized and fed to the decoder by simple digital hardware or any home computer. Such control channel manipulation by other than the legitmate network controller is just as dangerous a form of tampering as hardware tampering. Attempts to subvert the system by such address channel tampering is called "spoofing". Integrated within the operational framework of the system must be a fully developed methodology for key distribution and protection against spoofing.

Spoofing can take several forms, depending on how the pirate is attempting to fool the box. Control channel mechanisms must be in place to:

1) Prevent the insertion of illicit control data.
2) Prevent the deletion of valid control data.
3) Prevent the modification of valid control data.
4) Prevent the replay of control data.
5) Prevent box swapping between systems and geographic areas, and ensure stolen boxes are, or become useless.

If the first two tests or prerequisites to a secure system have been properly attended to, one has a totally secure system -- for the moment. It's the ability of a system to refresh key variables securely that will then enable it to be secure over time.

The "Key Question"

In a general sense, all control data having to do with enabling or directing box functions can be thought of as a form of keys. Virtually all systems in use today rely on a hierarchical or multilevel key distribution process as previously described. At the time boxes are installed they are brought on line by being given certain information (current keys) which allows them to join the network. Thereafter, having joined or signed up, they

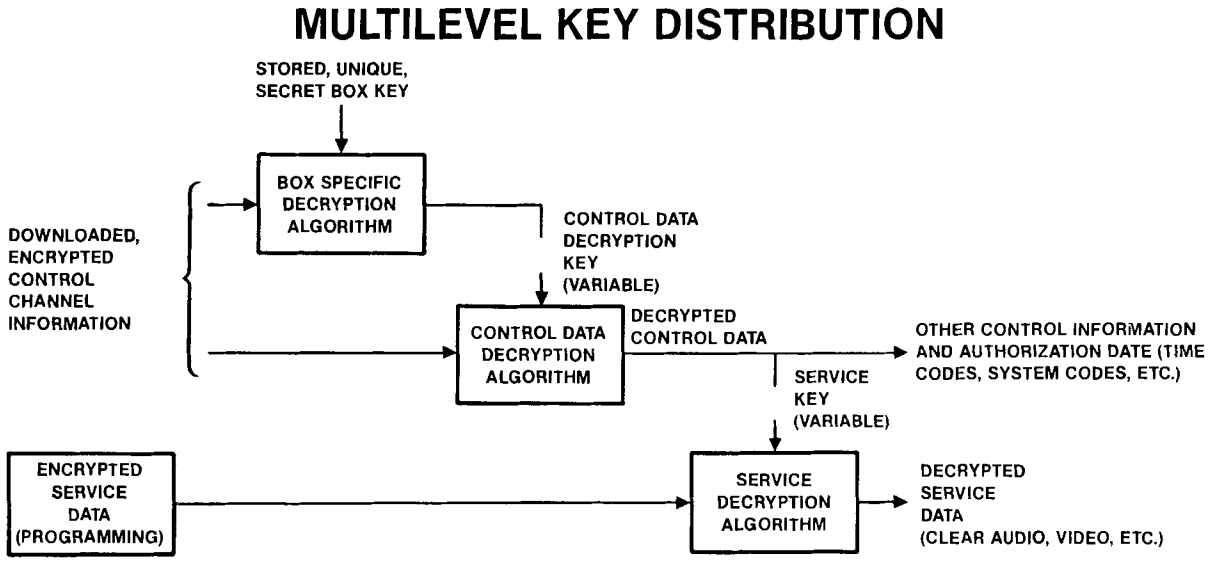

Figure 3.

are kept on line by being included whenever new network enabling codes (authorization codes, security codes, time codes, channel codes, program codes, keys, etc.) are distributed. The updating process must be performed securely, otherwise illegitimate boxes can listen in and update themselves too. Remember, having satisfied our first two tests, all boxes, legitimate or illegitimate, must have these decryption codes or key information before the signal can be recovered. If the network is distributing new keys encrypted, they must then be decrypted under existing keys already in the box. If existing boxes are suspected of being copied (cloned), then one has to consider the probability that the cloned boxes also received the updated codes or keys.

Now one of the most important points of this paper: Since all systems operate in multilevel key distribution formats, where new authorization data is distributed encrypted under "old", then how is it possible to really maintain security at all? It isn't, unless each and every decoding box has something fundamentally different about it from all other boxes. (Now we're back to the "one-time-defeat" idea). The multilevel key distribution process must begin at its most fundamental level by distributing information uniquely to each box, and then build further layers on that initial unique information. This requires a unique code or "box key" for every box, which is unknown by any other box. Thereafter, the network can always fall back to rebuilding its key levels by starting over with each box, leaving out of the redistribution or rebuilding those boxes which are known to have been cloned, stolen, etc. With the cloned box not reauthorized, all of its offspring are also up the proverbial creek.

One final comment about this notion of box uniqueness. When looking at any system purporting to have "encryption-based" security, don't let its manufacturer side-step the question of box differentiation. Without the equivalent of a box key, which is never broadcast over the control channel (because it must be encrypted under "something" to do so), the system is fundamentally, and by cryptographic standards, absolutely insecure. That the process is "too complex" or "proprietary" is the usual argument when such questions are asked. These notions are basic to any sound crypto system and they are not complex at all. Now let's look at our industries' experience with encryption products, and see why good system designs which take into account all three of our tests are so important.

The Real World Test

This paper began by noting that encryption-based systems have been commercially utilized only since 1982. Within that period, however, over a half dozen major types of products have seen extensive utility in several marketplaces. However, only three products have had exposure to the extent that significant piracy efforts have been mounted; these are the Oak ORION and General Instrument VideoCipher 2 (VC2) satellite products and the Oak Cable SIGMA system. The Oak STV SIGMA, SA B-Mac, Oak/Leitch Video Polaris, and GI Starlock systems are not believed to have ever been compromised, but have not had the exposure time and/or appropriate audience to have been really tested.

We'll make a distinction now between a system compromised and a system broken. A "compromise" is a temporary condition which can be expected to develop, and has developed, for both the ORION and VideoCipher products. "Breaking" the system would be a condition where the headend no longer has the ability to overcome the compromise, or deauthorize a decoder. This has not happened. After four years of operation and over 160,000 units installed, our Cable SIGMA system has yet to have shown evidence of any compromise.

In the cat-and-mouse game between manufacturers and pirates, the compromise of ORION and VideoCipher have been much ballyhooed in the press. It makes great gossip! But you will not hear companies like Oak and General Instruments actively responding to claims and challenges by individuals or organizations involved with the illegal activity of stealing programming. We will be quietly going about the business of ensuring that appropriate measures are taken to update keys and deauthorize modified or cloned boxes as they are discovered.

Let me now describe what has been in process in Oak's ORION system with our major customer CANCOM, for several months. CANCOM, the Canadian Satellite Communications company, chartered by the Canadian Radio and Telecommunications Television Commission, has been using ORION since 1982 to secure eight channels of television programming to CATV systems and individual homes. Approximately 15,000 decoders are currently on line.

Our knowledge of modified ORION decoders at the time of this writing indicates that most approaches have caused the boxes to simply ignore tiering alteration commands. This is a trivial compromise to overcome from the headend, and not nearly as sophisticated as either the cloning or "Three Musketeer" attacks that VC2 has seen. We are currently in the process of performing a "cycle change" on the CANCOM system. In Oak vernacular, this means the complete rebuild or redistribution of the network decryption keys. ORION has the attribute that each box stores a secret, and unique box key under which this is done. This has never before been executed on the CANCOM system, as the headend control system has only recently been upgraded to perform this function. The original design, however, planned for this exercise and there are no decoder modifications required. Any illegal decoders still operational after the cycle change can be assumed to be clones. A subsequent cycle change will then be performed, with clones thus identified eliminated from the redistribution process. Why this simple technique can work effectively is because it's computer-controlled, passive (that is, a background function) and very easy to invoke. Pirate boxes can always crop up, but once discovered can always be shut down.

This total redistribution is not possible with any system that does not have the equivalent of a box key. If, at the deepest or most fundamental level, boxes are manufactured with hardwired keys

or key seeds, once uncovered, these seeds will cause the redistribution process to be insecure and thus piratable. It may take a while -- we didn't see any significant piracy in ORION for three years -- but pirates will eventually break any system with hardwired or hardcoded keys.

Summary

The level of sophistication and organization behind the attacks currently being mounted against VC2 should lend credence to arguments that "OK" security is really not OK any longer. The cable industry should in fact take a lesson from what is happening in the satellite arena and understand why. The why is really economics. As cash flow from services increases, either through new revenue generators (IPPV and home shopping!) or increased audience, the motivations for system subversion (not just signal theft) will also increase. Along with the tests for security reviewed above, Figure 4 outlines additional considerations that relate to areas such as internal threats from employees, increased sophistication of the enemy, and advances in the state of the art.

Oak and our equipment manufacture competitors have spent a great deal of time and energy over the past two or three years educating our industry with respect to the merits of encryption. There is a tendency on the part of some manufacturers to confuse the issue by jumping on the bandwagon, claiming encryption processes are employed when what is really being done is trivial to undo under some of the examinations we looked at earlier. When such products are defeated, together with the publicity about products featuring true encryption getting compromised, the public and our industry gets naturally confused, and misled, and it is the consumer who eventually gets duped in the process.

The success that Oak, and other companies may enjoy (literally, sometimes) in combatting piracy is due to proper attention to theory and practical considerations in the application of true encryption principles. This paper has discussed some basic attributes and prerequisites of those principles, and reviewed how they can be employed to take advantage of the resultant system strengths.

GRADING A SYSTEM'S SECURITY

- KNOW THE FULL RANGE OF POSSIBLE ATTACKS
- DO NOT UNDERESTIMATE THE ENEMY
- BE AWARE OF TECHNOLOGY ADVANCES
- UNDERSTAND THE BASICS OF ENCRYPTION
- UNDERSTAND THE APPLICATION OF ENCRYPTION

Figure 4.