Security Considerations for Impulse Pay-per-View Systems

Vito Brugliera

VP Marketing & Product Planning
Zenith Cable Products Division
Zenith Electronics Corp.

Richard Citta

Mgr Electronic Systems R & D
Advanced Development Division
Zenith Electronics Corp.

ABSTRACT

Renewed interest in Pay-per-View applications has produced a variety of technologies for implementing Impulse Pay-per-View. Among these technologies is use of store and forward methods with addressable home terminals. There are obvious advantages to store and forward because it allows instant self-authorization of the PPV subscriber addressable home terminal, while permitting slow data communication and retrieval of the PPV buy data, thus avoiding some transaction handling problems with conventional system controllers and billing systems.

INTRODUCTION

The obvious advantages of store and forward approaches also create the opportunity for serious compromises of the scrambling and security of PPV addressable home terminals because:

- addressable home terminal is self authorizing
- valuable transaction data is stored on premise for long periods of time
- communication links between the storage element and the system headend could be vulnerable

To maintain the inherent security of the addressable home terminal under this environment it is necessary to have:

- true dynamic scrambling with constant and reliable data paths
- dynamic encryption of downstream communication
- secure non-volatile storage that is:
  1. unreadable
  2. unalterable
  3. inaccesable
- dynamic encryption of upstream communication

A description of an addressable home terminal system utilizing these criteria will be given.

SECURITY

Each succeeding generation of CATV technology has increased the level of security available to protect cable services from unauthorized reception. The parade of technology goes from mid-band tuning to sync suppression and addressability. As the perceived value of cable service has increased, so has the sophistication of the pirates. The weakest link of each new technology is discovered and exploited. This attack can be very sophisticated or just the result of brute "megatinkering" hours.

Early non-addressable decoders were soon victims of cloned or counterfeit PROM's. The advent of addressable decoders using sync suppression merely changed the battlefield. Sophisticated systems were compromised by a variety of means. More often than not, the box rather than the "system", was the focus of attack. Electronic sophistication fell to physical attack, filling the pirate pipeline with tales of "blue" and "orange" wires. However, even designers learn and the weakest link is less and less obvious. The latest generation of decoders, which have true dynamic scrambling, requiring a constant stream of data from the headend to operate properly, have not been immune from attack.

Impulse pay-per-view is emerging as a new revenue source for cable. The perceived value of this service makes it a target for security compromise. Since some of the PPV technologies utilize self-authorizing decoders, consideration of the entire system security is required if history is not to repeat itself.

History

The basic function of security is to deny unauthorized reception by the subscriber of certain program material. Authorization assumes payment by the subscriber and revenue for the cable operator and programmer. If we consider the history of cable, we find various approaches to security were used.

Early cable operators denied unauthorized reception by translating cable channels to a portion of the spectrum, midband and superband, not tuned by television receivers. A converter was required to translate those channels to frequencies tuned by the television receiver tuner. The introduction of cable compatible television tuning systems made another approach necessary.

The next step in security was the use of traps mounted between the pole and drop to alter the signal. The trap, positive or negative, had to be physically present or removed for proper reception and operation of the television receiver. Traps aged, drifted and in some instances, aided by subscribers or entrepreneural technicians, they ceased to function. Traps, now being rediscovered as "consumer friendly", became burdensome as pay services proliferated and subscriber churn kept trucks rolling.

A more sophisticated approach to security was sync suppression. At first with non-addressable converters, and later with addressable converters. Authorization was provided by a PROM, which could be reconfigured easily. A box changeout was still necessary until addressability came in. The advent of addressability allowed the subscriber's in-home terminal to have authorization levels changed electronically from the headend without the necessity of a truck roll and box changeout.

Sophisticated as they have been, addressable systems have been defeated, most often by attack upon the physical converter itself, and not the "system". A common problem has been that the signal can be interrogated to derive the scrambling parameters. An example is synch information on the aural subcarrier. On the premise that both video and audio need be present, recent approaches have left the video scrambling "soft" with sync suppression, and audio encoded digitally in what are considered "hard" forms of scrambling. This approach offers more security, but at increased cost.

PAY-PER-VIEW

The cable industry has seen the perceived value of the traditional pay services decline. Along with that decline has come a virtual cessation in subscriber pay growth. This phenomena has been attributed to external forces, among them is the rapid growth of VCR ownership and competition from VCR cassettes. VCR cassettes offer VCR owners, convenience, wide selection and choice, and product with earler release windows. This is an enormous market, measured in billions of dollars.

Cable has the ability to share in the revenues of this market through pay-per-view. Addressable technology offers subscribers the opportunity to purchase a single program. Early release of program material, time and date with VCR cassette rental and sale release, adds perceived value to the programming on cable. Best of all, the subscriber need not leave his home to enjoy the event. The ability to enjoy a single event requires that:

1. the subscriber's addressable converter be authorized and deauthroized in a timely manner to coincide with the event

2. the subscriber transaction data be captured by the billing computer for subsequent payment

3. the transaction constraints allow impulse purchase of the event

Satisfying these requirements is possible through a variety of technologies. The return path for the transaction data to reach the billing computer can be either the cable system itself using two-way communication; or the ubiquitous telephone system. Either path technology, if accomplished in real-time, must also deal with dynamic peak loads caused by impulse purchases near the event start.

One of the problems in dealing with real-time is that the very act of authorizing a subscriber can require substantial time:

- transport of the subscriber transaction to the billing computer
- dynamic updating of the billing computer subscriber database record
- transmission to the headend site the signal to the system controller to authorize the subscriber

STORE AND FORWARD

One way of avoiding the technical problems is to:

- allow the addressable home terminal to self-authorize prior to the event
- deauthorize after the event
- collect the transaction data at the addressable home terminal
- system controller database update and encoder command to authorize

These times can be measured in seconds to minutes. That magnitude of time makes impulse situations impossible with conventional technologies. Also, the voice telephone network is not very receptive to peak loads possible under these situations.

Real-time operation requires new approaches to billing technology and system controller design. Successful technologies exist for handling dynamic impulse loads in real-time: either two-way contention systems or ANI passing telephone systems.

- transfer the transaction data from the home to the system headend or billing computer at a time and data rate to avoid the peak loads on the return path or the billing computer

This approach, using an autodialer and telephone return path is the conventional approach to store and forward. Another approach uses the cable plant as the upstream return path, with an RF transmitter instead of the telephone. An advantage of the RF system is that the transmission rate for the upstream data can be faster, allowing more frequent polling.

Store and forward technology is very attractive. It allows the customer to buy programming or events on a true impulse basis, buying the event directly from the addressable home terminal. The stored information is then retrieved by polling the system and recovering it at a very slow rate.

Store and Forward Security

The home is an extremely hostile environment. The realization that value, in the stored transaction data, resides within the addressable home terminal will result in attempts to circumvent system security. To maintain a secure system, the integrity of the stored data must be maintained under adverse conditions. In addition, the decoder must self-authorize only under certain controlled conditions.

Data Integrity

Transaction data is stored in electronic memory, which must be secure. There must be no external access to this memory, and there must not be any way to alter or otherwise subvert the writing or reading of this data.

Encoding data and then placing it in a discrete external EPROM is to court disaster. Despite the mathematical odds against "breaking" the code or algorithm, we must remember that there will be thousands of boxes out there collecting thousands of "megatinkering" hours of assault by amateurs and professionals. The law of large numbers is against you no matter how infinitesmal the odds are.

In the system under consideration the data is stored in non-volatile memory within the controller IC. The controller is a proprietary application specific VLSI, and not available as a standard component. Placing the memory within the controller IC, requiring that essential dynamic data also be stored there, and that access is possible only with encrypted code, increases the security of the data. Only properly encrypted commands, which are in the in-band RF signal, can alter or read the data, making unauthorized attempts to alter the data unlikely.

Data recovery is achieved by polling the addressable converter and transmitting a message to the headend. The return path can be RF, via the cable return path, or the telephone network. This message is dynamically encrypted. Each polling of the box uses a different encryption key, generating a different message, even with the same data stored. This is absolutely necessary for a telephone return path where messages can be easily recorded and played back repeatedly for analysis. The downstream polling message must also be encrypted to maintain the security of the upstream encryption key.

Multi-Level Decoder Control

Positive control of the addressable converter requires that constant data is needed to properly decode the dynamic scrambling. This program related data is encrypted using session keys which are changed periodically. Each authorized addressable converter is individually given a new session key periodically. This provides positive control over stolen, unknown and non-pay addressable converters. Also, non-responding addressable converters where the data channel may have been subverted. The change of session key causes all of these addressable converters to stop decoding.

PPV Authorization Control

There are two levels of authorization possible in the system under consideration. There is one configuration for normal tiering, such as basic or a premium pay. For IPPV, the addressable converter and program must carry a special IPPV authorization level. Thus for proper IPPV authorization the addressable converter requires:

- IPPV program tag
- IPPV authorization
- proper session key
- correct data reception

Exceeding credit limits may deny a subscriber further access to IPPV service, but still provide normal pay services.

Additional Security Considerations

There are advantages to developing a proprietary application specific VLSI, not the least being reliability and cost reduction because of parts count reduction. The more concentrated the functions allocated to the VLSI, the higher the security of the system. The more there is in the VLSI, the fewer "blue" and "orange" wires are available. The VLSI incorporating these criteria is shown in Figure 1. The non-volatile memory is in the lower right hand corner of the chip.

The controller IC was designed to perform the following functions:

- data reception
- decryption
- decoding control
- upstream data generation
- dynamic encryption
- non-volatile memory
- decoder ID

The concentration of all these functions in one IC leaves no "hooks" to grab. The ID or serial number of the decoder is inserted in non-volatile memory at the time of addressable converter manufacture, at which time internal device gates are opened, thereby denying access to the ID resident portion of memory. As a consequence the ID is unchangeable and cannot be read or altered. Similarly, the algorithms for encryption and decryption are located in inaccessable portions of the chip. User accessable portions of the IC exist, providing functions such as tuning system control, IR remote control and favorite channel scan memory.

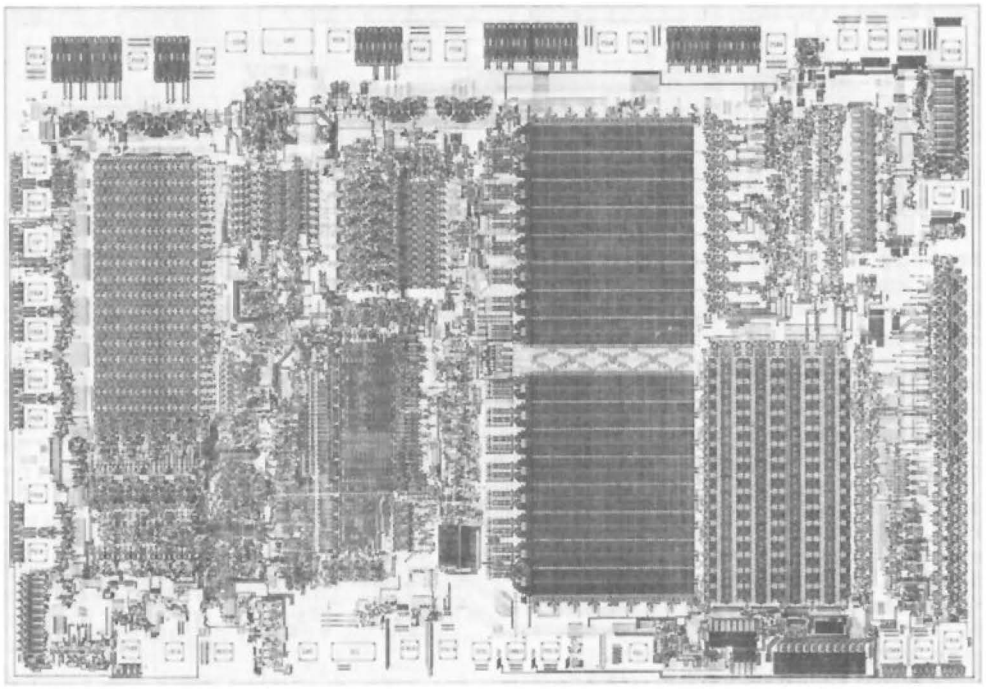

Figure 1. Custom CATV Microtuner with NV RAM

IMPLEMENTATION

An addressable converter using these security criteria for store and forward IPPV applications has been implemented. The addressable converter, by means of an external serial buss, is capable of store and forward IPPV applications, using either the telephone or upstream RF as the return path. The RF implementation, PM-Pulse, has a self contained RF transmitter. Polling occurs at up to 100,000 converters per hour. Polling at such high rates allows a typical system to be polled several times during an event, thereby assuring capture of the event data prior to completion of the programming material. Such fast polling means there is likely to be no data of value in the addressable converter. Verification of the subscriber transaction occurs because of time stamping of data at the headend.

The system polls constantly, and each upstream response from a converter supplies the following information:

- box status
- channel tuned
- authorization bit map.

Thus the box is constantly being interrogated and any unauthorized changes can be quickly noted.

CONCLUSION

Store and forward IPPV systems can be made very secure if the system architecture and hardware implementation are carefully executed. The essentials are:

- dynamic encryption
- dynamic scrambling
- constant and reliable data paths
- secure non-volatile storage
- concentration of functions in proprietary VLSI

The resulting implementation is not only secure, but capable of multiple IPPV approaches. The parts count reduction results in an extremely cost effective and reliable product. A version of this product, without tuner, provides a decoder only function using an existing "plain-jane" converter. Using ANI passing for IPPV provides an extremely low cost approach to PPV.