ADDRESSABLE SECURITY

AL CLARK

CYBERTECH, INC.

OVERVIEW

The leading edge of operational security technology is found in the military. The methods used 20 years ago included an electronic circuit coupled with the physical act of using a courier to alter the operational characterisitc of the electronic equipment used.

Today we are addressing the issue of security in Cable Television in terms of controlling both the presence of video signal and clarity along with user environmental sampling and transmitting.

In the past and in the present, control of video has been employed by the physical act of using a person to place hardware at the pole and/or in the home. We are now seeing the beginning of the use of electronics to replace the manual function of that operational activitiy and a higher degree of the control function.

In that the Cable Industry is on the verge of becoming a part of a global communication network an overview of other network security requirements is in order.

Those networks are:

1. Satellite
2. Land lines (Phone companies)
3. MDS
4. STV
5. Cable
6. Mushroom return links

Mushroom is a term the Author is using to express the use of a limited distant transmitter used by a person to transmit to a series of geographic dispersed receiving locations. These locations would be the uplink to a Satellite network or go into any other networks. The person or entity could be mobile or stationary.

Business data processing communication has used in some cases a formula that is a De facto standard. This formula takes clear data at the transmit point and scrambles it into garble that is non-readable. At the receive site the formula is reversed and the garble is converted back into clear text. Other means of security at the business or individual level involves software (passwords, etc.) and hardware. As Cable interfaces to these networks the same techniques and standards will be received.

PRESENT TECHNOLOGY

Cable Television is now addressing security at the home level in terms of control of the video signal. The control is performed by a micro-processor in an intelligent tap or an intelligent convertor. Security is based upon using a unique address for each of these devices.

Programming of the micro-processors can be altered by sending software code down the cable system if RAM (random access memory) is used. If PROM (programable read only memory) is used the alteration of the code can be changed by using a person in the field or in the office.

To support the use of these devices by a Cable company requires a very co-ordinated effort at the operational level.

As customer orders are received at the cable office they should be handled one time for requirements. The order should be entered on a computer that can handle billing, operational and control functions or pass electronically the information to another computer or computers for those functions.

The billing system must have the design to support Multi-tiered service. History of the transactions should be stored by each tier for clarity and because of the different types of service cable will be selling in the future, billing should read the history file by each tier and by each transaction to produce an itemized statement for customer acceptance.

The billing system should pass to operations the necessary paper work if a person is needed to install or alter the service. If a person is not required, the billing/or entry process should electronically pass control signals to satisfy all required needs.

FUTURE

The next step in security within the Cable Industry should encompass manufacturing economics and techniques to support software control at a level to defeat economic emulations.