Maintaining Control of Controlled Content

David K. Broberg, © November 11, 2000

The Point-of-Deployment (POD) module developed by CableLabs allows the separation of security functions from the digital cable set top box necessary to meet the FCC's *Retail Navigation Order*. The result of this separation is an external POD module that contains all the necessary descrambling circuitry to restore the MPEG stream back to cleartext, so common decoders can be used in a set top box sold at retail (Host). This separation allows each cable operator to maintain a proprietary digital scrambling method to protect the controlled content. It also allows various manufacturers to build compatible Host devices which can be sold at retail. These retail Host devices use the POD interface to allow access to the controlled content regardless of the chosen conditional access (CA) system.

Since the result of descrambling in the POD module is clear MPEG, passing this signal back to the HOST across and unprotected external interface would leave the signal vulnerable to unauthorized access, copying or redistribution. One might argue that since the POD is controlled by the cable operator and tied to an authorized, paying subscriber, no further protection should be necessary. While it is true that the POD only descrambles content that has been specifically authorized for that subscriber, allowing this interface to remain unprotected leaves the signal vulnerable to two basic threats: (1) the device that is hosting the POD, may not be a trusted device and (2) even if the POD can verify that the Host is trusted, something may be snooping on the communications. With the help of the Dynamic Feedback Arrangement Scrambling Technique (DFAST), this interface can be protected against such threats.

It is important for the POD to authenticate the Host device, to ensure the device it finds itself connected to is well behaved. For example, the cable operator has certain contractual obligations to protect the digital programming against theft, redistribution and in some cases unauthorized recording. If the POD was connected to a device that was designed to redistribute the clear MPEG of controlled content over the Internet, the operator might find himself vulnerable to lawsuits or breach of contract.

Without this authentication between the POD and the Host, the POD could also find itself providing services to Host devices that were improperly designed causing harm to the cable network, possibly disrupting services for other paying subscribers or even causing physical damage to the POD module. Unique secrets are stored in the Host which can be verified by the POD module to provide this authentication process which ensures that the POD module will only successfully bind with well behaved host devices.

This authentication process has three steps which are used together to verify the validity of the Host certificate. First the POD checks to see if the certificate supplied by the Host represents a mathematically accurate certificate matching the algorithms supplied by the Certificate Authority (DTLA). If the certificate proves invalid, controlled services are not provided to the untrusted Host device. After the POD successfully validates the Host certificate, the POD is authorized to begin descrambling certain content for the Host.

In the second step, the POD reports the unique Host identification numbers to the cable head-end using the RF return channel, where the Host certificate can be further verified against certificate revocation lists (CRLs) which are stored at the cable head-end. Once the head-end verifies that the Host certificate has not been previously revoked, the head-end sends a host ID validation message back to the POD.

The third step begins while the POD is waiting for the reply message from the headend. The POD requests the Host to provide the authentication key which is derived from the DFAST secrets provided by CableLabs. This key is compared to one also derived in the POD from the same secrets. Only after all three steps have completed successfully is the POD able to send all authorized services to the Host device including those with copy protection restrictions.

Once the Host has been authenticated, it is still important to protect against eaves dropping on the interface. Since this POD interface is external to the box, there is a threat that an extender card could be used on the POD allowing a PC or some other device to capture the copy protected content being passed to a legitimate Host device.

A message system is used by the head-end to identify certain MPEG streams as copy protected. This copy control information (CCI) is used to control the use of the DFAST scrambling on signals returning to the Host after first undergoing CA descrambling by the POD module. Only those MPEG streams that are specifically identified by the head-end as *copy-never* or *copy-once* are rescrambled before being passed back to the Host. Signals controlled by the CA system that have no such copy restrictions, are passed across the interface as clear MPEG.

For those copy restricted MPEG signals, a unique form of scrambling using the DFAST technology in combination with DES encryption is used. This copy protection scrambling relies upon unique secret keys and intellectual property to process those keys provided by CableLabs which are stored in both the Host and the POD. This DFAST technology increases the robustness of the keystream generation process by providing a dynamic process to modify the keystream on both sides of the interface.

A two-part system is used to form a comprehensive copy protection scheme for the POD interface of digital cable systems. The first part consists of an authentication process which is used to validate the Host device ensuring that the destination and behavior of the Host device can be trusted. The second part is comprised of a digital encryption system that makes use of DFAST technology to improve the security of the keystream generation process which is applied using the Digital Encryption Standard (DES) to the content identified by the head-end with copy restrictions.