

FINGERPRINTING

CONDITIONAL ACCESS SYSTEM SECURITY FEATURE

This solution provides a cost-effective way for operators to combat a type of piracy in which a legal smart card is illegally used to relay descrambled content from a set-top box (STB) into an unauthorized analog network or to other devices in an establishment such as a bar or a hotel.

Fingerprinting is a very effective detection tool, and there is a trend in some countries, such as India, to mandate this implementation. Many content owners in these countries also require operators to implement these measures on broadcast platforms before allowing their content to be aired.

SECURITY FEATURE

Fingerprinting is a mechanism for identifying a specific smart card used to illegally relay de-scrambled content from a set-top box into an analog network. For example, a pirate operator may receive content on an STB with a legitimate smart card, and illegally relays de-scrambled content to other TVs in a bar or to other homes. When this type of piracy is suspected, operators can enable fingerprinting on an STB to aid the identification of the misused smart card, its disabling and possibly the prosecution of the rogue operator. When fingerprinting is enabled, a mark identifying the smart card, i.e. its "fingerprint", is shown on all TVs connected to set-top boxes in the pirate operation. The fingerprint allows investigators to derive the identity of the smart card used to illegally relay content so that the pay-TV operator can disable it. There are two ways to implement fingerprinting: overt and covert fingerprinting. The main difference between the two approaches lies in the way fingerprints appear on screen.

COVERT FINGERPRINTING

When the operator issues a command from the conditional access system (CAS) head-end to enable overt fingerprinting, an ASCII number, representing the hashed version of the smart card serial number, is displayed on all TV screens in the pirate operation. The operator can configure the following parameters for fingerprint display:

- Position of the overt fingerprint on the TV screen
- Size, color and font of the characters used in the overt fingerprint

Investigators communicate the hashed number displayed on a TV screen to the operator, who uses a conversion tool to determine the associated smart card serial number. With this information, the operator can then disable the offending smart card and thereby ending the illegal relay of descrambled content.

COVERT FINGERPRINTING

Covert fingerprinting shares the same concept as overt fingerprinting, except that fingerprints are now hidden on screen, so that they are undetectable by both human eye and fingerprint blocking software. It addresses the challenge of overt fingerprinting, where pirates can sometimes detect and block ASCII-number fingerprints from TV screens, by using readily-available professional logo insertion and removal hardware devices.

In the Irdeto covert fingerprinting feature, a fingerprint is made up of a matrix of dots. Each dot represents a binary 1 of the ASCII character in the hashed smart card serial number. The positions of the dots are weighted, allowing investigators to derive the ASCII number using an algorithm. To make it difficult to block, the matrix of dots can be moved around on screen, and varied in size to cover different percentages of the screen. Operators can configure the following parameters for fingerprint display:

- Number of frames per second for the covert fingerprint
- Duration of fingerprint transmission
- Percentage of the screen coverage by the fingerprint

A person looking at a TV screen will notice very little or nothing of the covert fingerprint. This is because the tiny, scattered dots appear on screen for a very short period of time (less than one tenth of every second, and then only when the fingerprint is active). The dot pattern

can also be randomly moved around when the coverage is not set to 100% of the screen area, making the covert fingerprint virtually undetectable to the human eye.

When the fingerprint transmission is in progress, the investigator uses a video camera to record the display screen at the pirate operation. The investigator then re-plays the recorded video in slow motion (frame by frame) on a video player to view the covert fingerprint. From the play-back video frame, the investigator then copies the covert fingerprinting dot pattern into a conversion tool, which processes the information and returns a corresponding smart card serial number. With this serial number communicated to the operator, the smart card used in the pirate operation to illegally relay descrambled content can be disabled.



Figure 1: An example of a TV screen with a covert fingerprint, at 50% coverage

COMPONENTS

Fingerprinting requires changes in both the operator's CAS head-end and client devices:

- A head-end component must be able to issue either an entitlement control message (ECM) or an entitlement management message (EMM) fingerprinting command to client devices to turn fingerprinting on and configure various fingerprinting options.
- Client devices must be able to support fingerprinting and the associated display options.

CONTROL SYSTEM AT THE HEAD-END

- Irdeto Key Management System (successor of Irdeto Plsys)
- Irdeto Key Server (successor of Irdeto Encryptor)

SECURE CLIENT AT THE SUBSCRIBER SIDE

- Irdeto smart card
- Irdeto-approved set-top box

Contact Irdeto for a complete list of Irdeto-approved devices.