EBU

OPERATING EUROVISION AND EURORADIO

Item 4.6
TC-SPG 18430 inf.

R 139

BEST PRACTICE FOR HANDLING A/V STREAMS PROTECTED BY THE BISS EN-CRYPTION SYSTEM

Внимание!

- Данный перевод **НЕ** претендует на аутентичность и может содержать отдельные неточности.
- Оригинал этого документа находится по адресу: http://www.ebu.ch

ПЕРЕДОВАЯ ПРАКТИКА ОБРАБОТКИ A/V ПОТОКОВ, ЗАЩИЩЕННЫХ СИСТЕМОЙ ШФИРОВАНИЯ BISS

Женева
Июнь 2013

Рекомендуемая практика по A/V потокам, защищенным системой шифрования BISS

EBU, учитывая, что:

1. безопасность, предоставляемая A/V контенту системой условного доступа BISS, зависит от целостности сеансных слов, известных только системе вещания Евровидения (кодерам и декодерам),
2. нынешняя вычислительная мощность потребителей может быть достаточна для осуществления успешных своевременных атак методом грубой силы на сеансные слова в зашифрованном транспортном потоке,

и что

3. наличие долговременных повторяющихся и предсказуемых значений типа “Null / Padding Packets” в A/V потоке повышает уязвимость шифрования потоков.
4. безопасность любой системы условного доступа можно повысить принятием соответствующей операционной практики,

Рекомендует:

5. **Поставщикам оборудования рассмотреть следующие реализации:**
   a. Для режима передачи с постоянной скоростью потока (CBR), где используются «нулевые пакеты» для поддержания требуемой скорости на уровне PES, заменить их значение случайной последовательностью.
   b. Для режима передачи с переменной скоростью потока (VBR) удалить заполняющие (нешифрованные) «нулевые пакеты» на уровне TS.
   c. Возможность выбора шифрования для каждого PID (PES).
   d. Аудио дорожки, кодированные в Dolby E, должны быть не зашифрованы.
6. **Операторам соблюдать следующую операционную практику:**
   a. Шифровать контент только в начале прямой передачи.
   b. Все установочные и тестовые сигналы должны передаваться незашифрованными. Для тестирования шифрованного тракта сигнала перед прямой трансляцией необходимо использовать съемку с камеры, уникальную для каждой трансляции, заранее записанные сигналы использовать НЕЛЬЗЯ.
   c. Сеансное слово необходимо менять в каждом сеансе передачи.
   d. Персонал в передающих пунктах никогда не должен разглашать сеансные слова третьим лицам, независимо от того, кто это может быть. Все запросы на сеансные слова должны отправляться в EVC.
   e. Всем авторизованным принимающим сторонам для использования в событии должна быть передана пропускная фраза, что сеансное слово нужно запрашивать у EVC во время прямой трансляции.

07/06/2013