Acceso condicional en sistemas DVB

Pablo Flores Guridi, pablof@fing.edu.uy

Facultad de Ingeniería, Universidad de la República

IIE

Montevideo, Uruguay

11 de noviembre de 2020

Motivación (I)

- Necesidad de encriptar las señales transmitidas:
  - Que las señales sólo puedan ser vistas por nuestros abonados.
  - Tener la posibilidad de vender paquetes de señales.
  - Tener la posibilidad de vender señales o eventos PPV (por ejemplo partidos de fútbol).
- Existen varios sistemas de encripción, pero ¿alguno de ellos nos sirve?

Motivación (II)

Ejemplo 1 - Sistemas de encripción con clave simétrica:

- Emisor y receptor deben conocer a clave.
- Se utiliza la misma clave para encriptar y desecriptar los mensajes.
- Puede ser peligroso a menos que la llave se actualice regularmente.
- El intercambio de estas llaves conocidas por ambas partes es en general realizado mediante el uso de sistemas con llave asimétrica (llave pública - llave privada).
- Salvo casos excepcionales, ¡no es suficiente para un sistema de *broadcasting*!

Motivación (III)

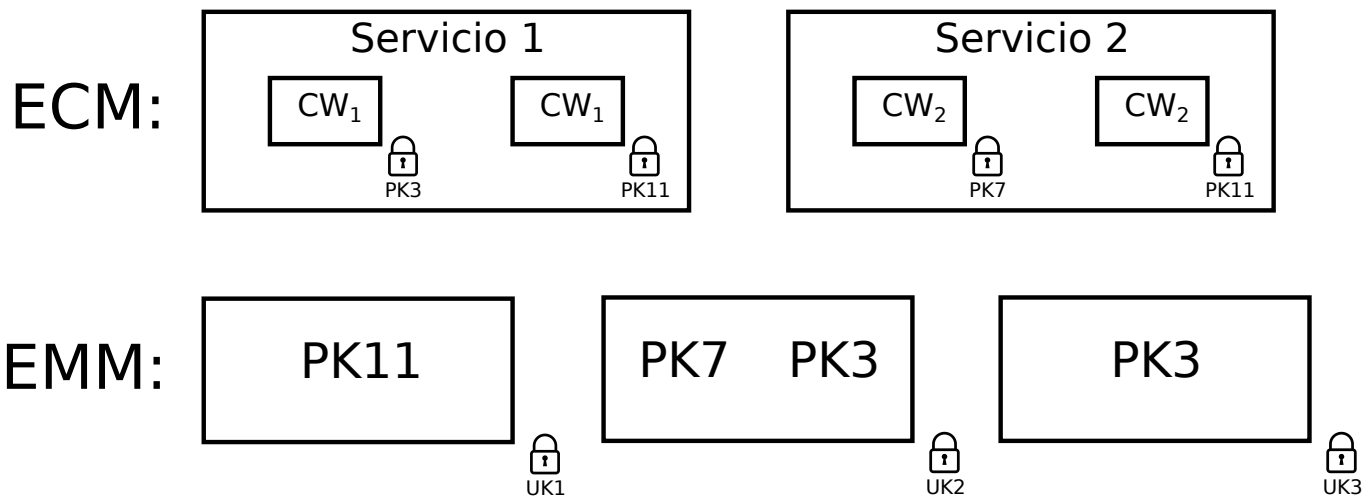
Ejemplo 2 - Sistemas de encripción con clave asimétrica:

- Constan de una llave pública y una llave privada.
- La llave privada es sólo conocida por su dueño.
- La llave pública es conocida por cualquiera.
- Dos casos de uso:
  1. Firmas digitales: verificar que el mensaje fue enviado por el portador de la llave privada.
  2. Encripción: enviar mensajes encriptados (con la llave pública) que sólo pueden ser desencriptados con la llave privada.
- ¡Tampoco es suficiente para un sistema de *broadcasting*!

¿Cómo se implementa la encripción?

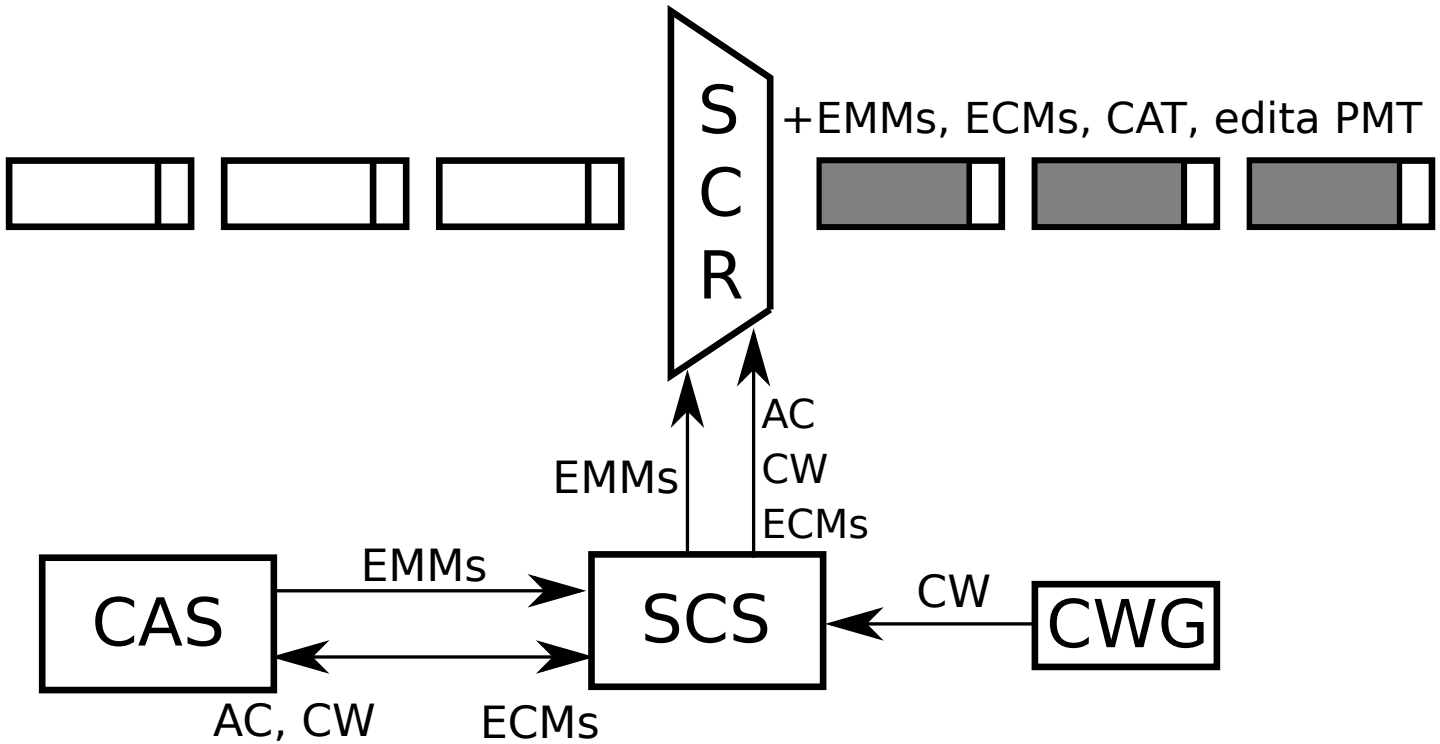
Una llave de encripción y dos tipos de mensajes:

- CW: Control Word.
- ECM: Entitlement Control Message.
- EMM: Entitlement Management Message.



$\Rightarrow$ Su implementación es definida por el proveedor.

Diagrama de bloques



Para discutir en clase...

(1) ¿Cuántos PIDs (*streams* independientes) de ECMs deberá haber en un TS?

(2) ¿Cómo señalizaría ese o esos PIDs? ¿Agregaría una nueva tabla o editaría una existente?

(3) ¿Cuántos PIDs (*streams* independientes) de EMMs deberá haber en un TS?

(4) ¿Cómo señalizaría ese o esos PIDs? ¿Agregaría una nueva tabla o editaría una existente?

(5) ¿Hay alguna otra consideración que haya que tener con el SCR?

Las siglas y sus significados (I)

- Scrambler o Encriptor (SCR):
  - Se encarga de encriptar los ESs.
  - Además multiplexa EMMs, ECMs y CAT; y edita la PMT.
- Simulcrypt Synchonizer (SCS):
  - Componente lógico que sincroniza CWG, CASes y SCR.
- Control Word (CW):
  - Palabra secreta de 64 bits utilizada para encriptar los ESs.
- Control Word Generator (CWG):
  - Módulo responsable de generar CWs de manera aleatoria.

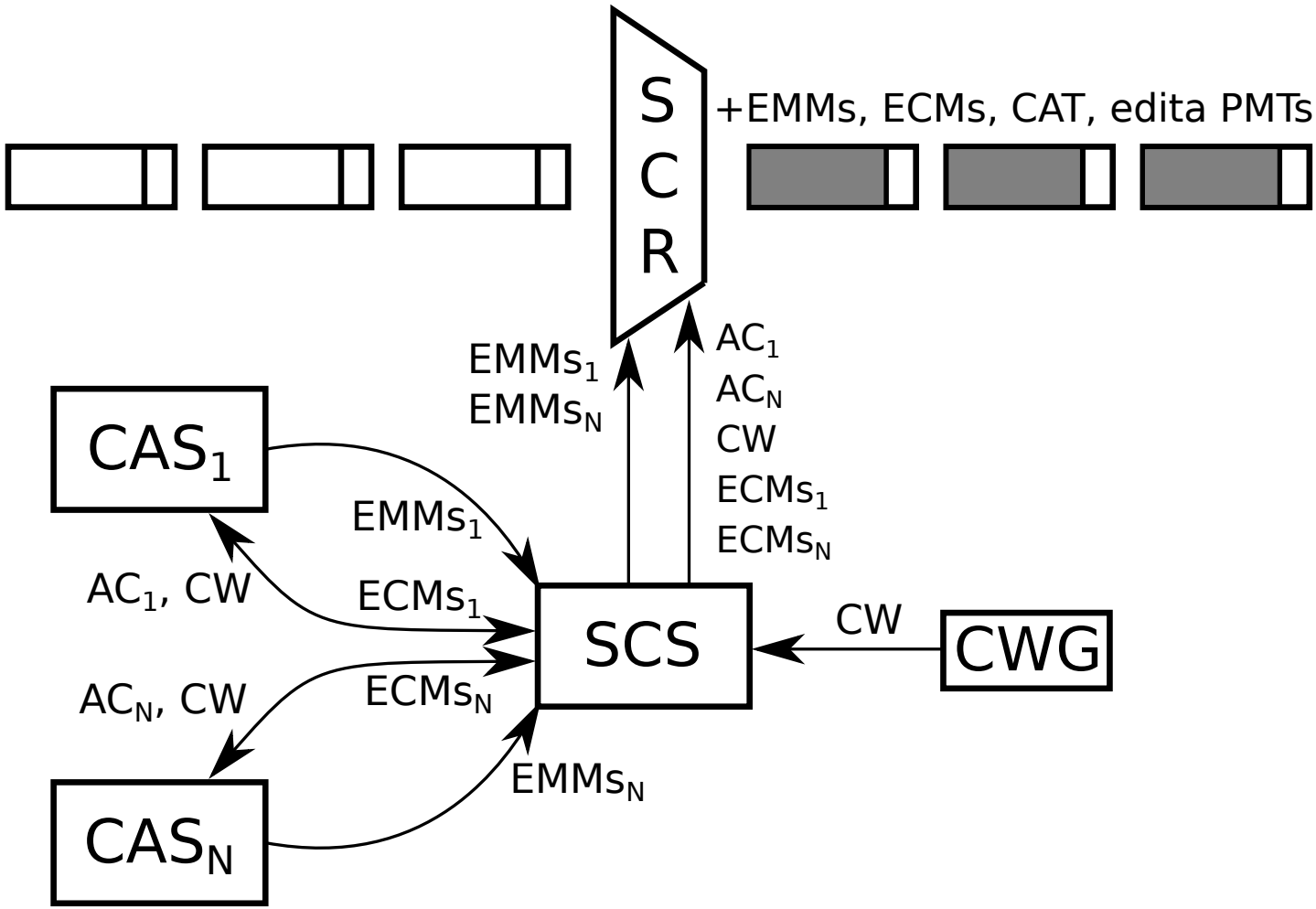
Las siglas y sus significados (II)

- Conditional Access System (CAS):
  - Sistema que controla el acceso de los distintos usuarios a los distintos servicios y sus ESs.
  - Entre otros módulos, consta de un ECM Generator (ECMG) y un EMM Generator (EMMG).
- Access Criteria (AC):
  - Información requerida por el ECMG para generar los ECMs.
  - En general, un AC se corresponde con un servicio.
  - Al encriptar un servicio con un AC determinado, quedan definidos los productos que lo podrán desencriptar.
  - Cada AC "tiene" un conjunto de productos.

Otros conceptos importantes

- Common Scrambling Algorithm (CSA):
  - Algoritmo que se utiliza para la encripción de los Elementary Streams.
  - Utiliza una llave simétrica denominada Control Word.
- Crypto Period (CP):
  - Tiempo durante el cual el encriptor utiliza una determinada CW.
- Subscriber Management System (SMS):
  - Sistema de gestión de usuarios.
  - Almacena, para cada usuario, tarjetas asociadas, packs (productos) y otra información de interés.
  - Envía comandos al CAS indicando relación tarjeta-producto(s).

Simulcrypt con N CASes



Señalización: Conditional Access Descriptor

Syntax	No. of bits	Mnemonic
CA_descriptor() {		
descriptor_tag	**8**	**uimsbf**
descriptor_length	**8**	**uimsbf**
CA_system_ID	**16**	**uimsbf**
reserved	**3**	**bslbf**
CA_PID	**13**	**uimsbf**
for (i = 0; i < N; i++) {		
private_data_byte	**8**	**uimsbf**
}		
}		

- Si se encuentra en la PMT, el CA_PID apunta a los ECMs correspondientes a un determinado CA_system_ID.
  - Si aparece como descriptor del programa, su información es aplicable a todo el programa.
  - Si aparece como descriptor de un determinado ES, su información es aplicable a ese ES particular.
- Si se encuentra en la CAT, el CA_PID apunta a los EMMs correspondientes a un determinado CA_system_ID.

Ejercicio

Basado en lo visto en clase:

1. Diseñe un sistema basado en paquetes comerciales.
2. ¿Cómo implementaría eventos PPV? Hay dos maneras posibles.