

DVB Security: Why Bother?

Ken McCann

ZetaCast



ZetaCast



ZetaCast

Who is ZetaCast?

Independent technology consultancy company

- Specialising in digital TV systems

ZetaCast directors have each over 15 years experience of digital TV, including

- Leading design team for the world's first real-time MPEG-2 encoding system
- System integration and for digital terrestrial, cable and satellite systems
- International project management

Overview

Introduction

Some definitions

Development of DVB Security Solutions

Practical Issues with DVB Security

The Regulatory Environment

Conclusions

Content Protection wasn't needed in the Good Old Days



1970s



1980s



1990s

Conditional Access (CA)

Controls access to **broadcast content at time of delivery**

- Scrambles content in a way that can be descrambled only by an authorised receiver
- Primarily designed to support the pay TV business model

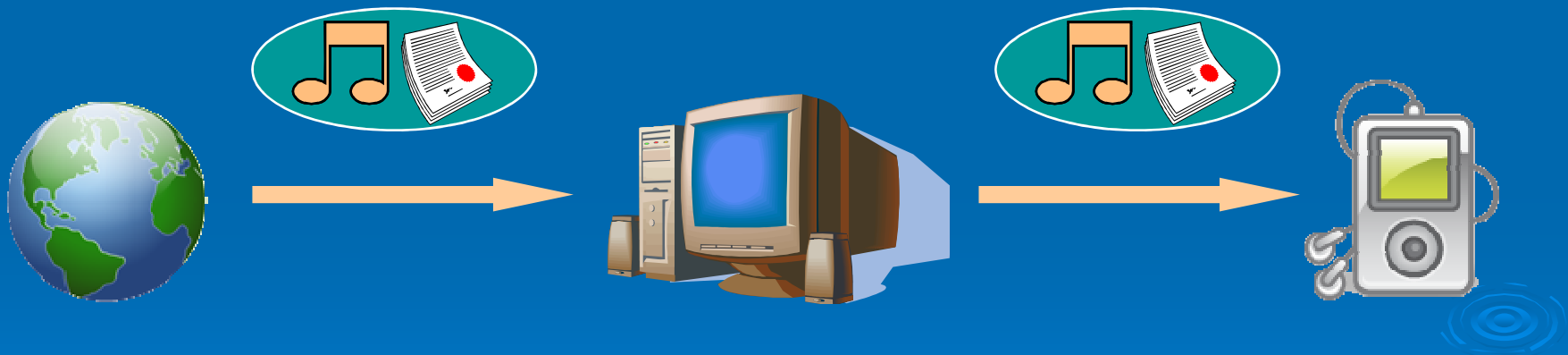


“a technique used to protect a programme or a number of programmes from unauthorised viewing” – Ulrich Reimers

Digital Rights Management (DRM)

Controls use of the **received content**

- Defines rules to ensure that viewing, storage and copying is consistent with the rights granted by the content owner
- Primarily designed to control usage of downloaded content

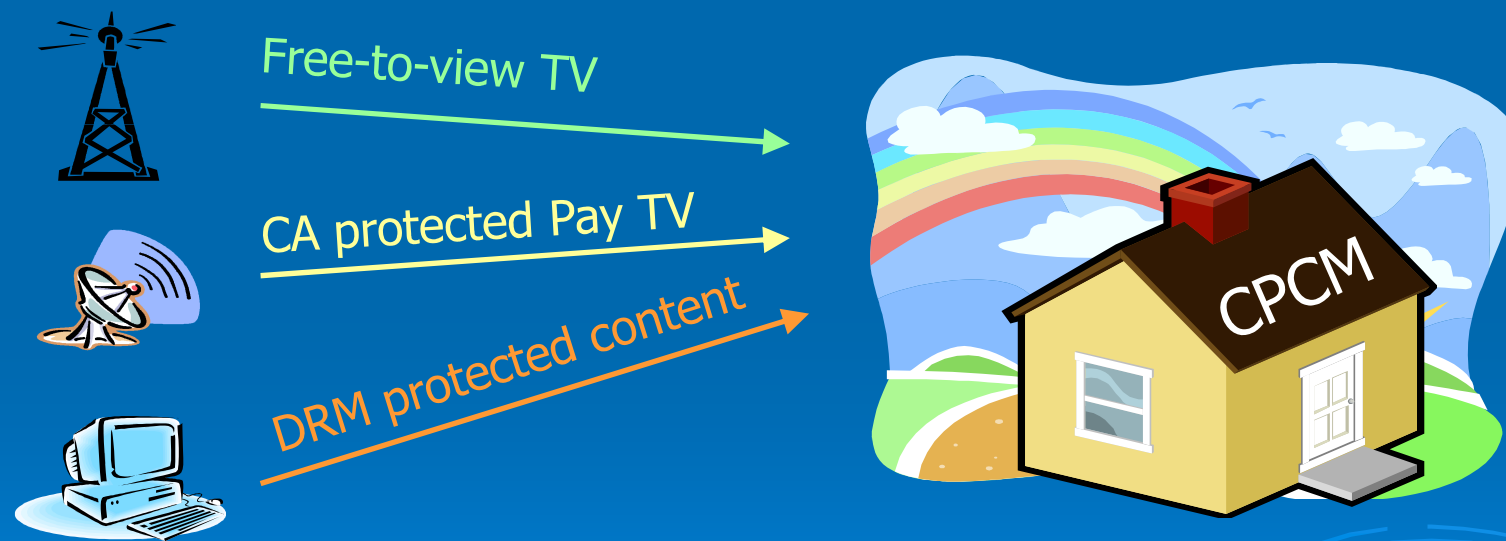


“access control technologies used by publishers and copyright holders to limit usage of digital media or devices”
– Wikipedia

DVB-CPCM

An **interoperability framework** that gives integrated access to content delivered using various CA or DRM systems within the home

- Content Protection and Copy Management of commercial digital content delivered to consumer products



“a stealth attack on consumer rights and competition” —
Cory Doctorow, EFF

Development of DVB CA

Pay TV applications led the way in the early days of DVB

- Business model requires a means of ensuring that viewers who do not pay for specific premium content cannot access it
 - Adequate level of security
 - Cost effective implementation

Two opposing views on how to achieve this in 1993

- Proprietary solution, developed behind closed doors
- Fully standardised CA environment, developed openly

Compromise was

- “CA Specialist Group” in DVB
 - Membership restricted to accredited cryptology experts
- DVB Common Scrambling Algorithm (CSA)
- Proprietary means of generating and delivering Control Words
 - The “keys” to the encryption, which change periodically

Common Scrambling Algorithms

Initial DVB Common Scrambling Algorithm specified in 1994

- Uses 64 bit keys
- Designed to resist brute force attacks for at least a decade
- DVB CSA v2 restricted to 40 bit keys
 - at request of some government agencies

DVB CSA v3 specified in 2007

- Uses a 128 bit key
- Algorithm is based on two block ciphers
 - AES128 and the DVB-confidential XRC
- Designed to be sufficiently robust to protect high value content for at least another decade
 - Backwards compatible with CSA v2
 - Designed to be hardware-friendly but software unfriendly

Some Practical Issues with DVB-CA

Simulcrypt

- Architecture that allows a service to be transmitted with the entitlement messages for multiple CA systems
- Decoder supporting a particular CA system can extract the relevant entitlement messages and ignore the others.

DVB Common Interface (CI)

- Standardised interface between a set-top box or integrated digital TV (IDTV) and a removable security module
- Idea is to allow alternative CA systems to be plugged in
- But few CA modules are available in practice

Common Interface Plus (CI+)

- Work to address security and cost concerns began in DVB
- Failed to reach consensus within DVB
- CI+ Forum formed outside of DVB

EU Regulatory Issues

The Good, the Bad and the Ugly?

Conditional Access Directive

- Created common standard of legal protection to fight CA piracy
- Provides legal framework to underpin pay TV market

Universal Services Directive

- Requires IDTVs to be fitted with standardised interface
 - In practice means Common Interface (CI)
- But there is a lack of CA modules
 - Results in consumer paying extra without gaining useful functionality

Some countries have a levy on digital storage media

- Evolved from levy on analogue tapes
- Wide disparity in the level of charges within the EU
- Is this still appropriate with digital Content Protection?

Conclusions

There is a range of security options, supporting different business models

- No Security
- Conditional Access
- Digital Rights Management

Regulation struggles to keep up with evolving technologies

- Some historical anachronisms remain

In standardisation there is a natural tension between

- Economies of scale offered by a fully standardised solution
- Enhanced Security offered by a partially standardised solution with proprietary elements

Conflicting views on content protection are deeply entrenched

- Different application areas have different approaches
 - Can cause problems with convergence technologies, e.g. mobile TV
- DVB was more successful in providing elegant and coherent solutions when considering a less diverse set of applications