Kodowanie i szyfrowanie sygnałów fonicznych i wizyjnych

Technika rejestracji sygnałów

Zastosowanie szyfrowania

- Ochrona prywatności w zastosowaniach typu VoIP (Voice & Video over IP – telefonia Internetowa, telekonferencje)
- Ochrona praw autorskich (i innych praw majątkowych) – telewizja cyfrowa (DVB), wideo na żądanie (VOD), filmy DVD i BD
- Ochrona danych wrażliwych – dokumentacja medyczna

System DRM (Digital Right Management)

- Szyfrowanie materiału multimedialnego w celu uniemożliwienia dostępu bez prawidłowego klucza
- Podczas próby odtworzenia wyświetlany jest monit o dostarczenie licencji, która zawiera w sobie klucz deszyfrujący
- Różne rodzaje licencji: pojedyncze odtworzenie, pojedyncza kopia, 1 generacja kopii, ograniczenia geograficzne, ograniczenia czasowe
- Użytkownik zakupuje licencję na stronie wydawcy i dodaje ją do magazynu odtwarzacza
- Odtwarzacz weryfikuje licencję i deszyfruje strumień multimedialny

Skuteczność systemów DRM

- Podatność na ataki – błędne założenia technologiczne, usterki programistyczne
- Firmy usiłują cenzurować informacje o błędach i usterkach w systemach DRM za pomocą kroków prawnych

„Dziura analogowa”

- Brak kontroli na wyjściach analogowych odtwarzacza
- Nowsze rozwiązania eliminują „dziurę analogową” poprzez stosowanie tylko połączeń cyfrowych, wyposażonych w szyfrowane interfejsy (np. HDMI wraz z HDCP)
- Sygnał analogowy odtwarzany jest przy znacznie zdegradowanej jakości

Przykłady technologii

- Macrovision
- CGMS-A
- SCMS
- CSS
- AACS
- HDCP

SCMS – Serial Management System

- uzupełnienie połączenia SPDIF o zabezpieczenie przed nielegalnym wykonywaniem cyfrowych kopii
- powstał, żeby zabezpieczyć format DAT (Digital Audio Tape) przed robieniem cyfrowych kopii
  - stosowany także w MiniDisc-ach i DCC (Digital Compact Casette)
  - pierwotnie (1987 r.) planowany był system polegający na wykrywaniu obecności sygnałów w okolicy 3840Hz. Brak tych częstotliwości oznaczałby, że materiał jest zabezpieczony
  - przyjęty w 1992 roku
- rozwijany dla potrzeb telewizji w postaci m.in. broadcast flag

SCMS – Serial Management System

- **profesjonalny sprzęt pozbawiony był zabezpieczenia SCMS**
- w praktyce polega na odpowiednim ustawieniu dwóch bitów w kodzie SPDIF:
  - 00 – brak zabezpieczenia przed kopiowaniem
  - 10 – zakaz kopiowania
  - 11 – możliwość wykonania jednej kopii, ale bez możliwości skopiowania tej kopii
- działanie (za http://www.minidisc.org/)

źródło	**kopia**
analogowe	11
CD	10
cyfrowe, 00	11 lub 00 (zależnie od modelu)
cyfrowe, 11	10
cyfrowe, 10	brak możliwości zapisu

Macrovision Video Copy Protection

- opracowany w połowie lat 80-tych XX wieku w celu zabezpieczenia materiałów wideo przed kopiowaniem
- polega na
  - wstawianiu dodatkowych impulsów synchronizacji w sygnale wygaszania ramki, co zakłóca pracę układów AGC w magnetowidach
  - modulowaniu impulsów przekazujących informacje o kolorze (w systemie NTSC)
- objawiał się okresowymi zmianami jasności i nasycenia obrazu, zrywaniem synchronizacji itp.
- do obejścia za pomocą praktycznie dowolnego wzmacniacza sygnału wizyjnego

Macrovision Video Copy Protection

- na płytach DVD funkcjonował jako **APS** (Analog Protection System) lub jako **Copyguard**
- polegał na ustawieniu odpowiedniej flagi obecnej w plikach VOB
  - po opłaceniu praw licencyjnych
- do obejścia przy pomocy praktycznie każdego oprogramowania do kopiowania płyt DVD-Video

Copy Generation Management System - Analog

- system opracowany dla potrzeb telewizji analogowej
- polega na umieszczaniu w sygnale wygaszania ramki dodatkowego sygnału
- po wykryciu sygnału blokowana jest możliwość nagrywania programu
- używany przez urządzenia DVD oraz różnego rodzaju rejestratory sygnału TV

Copy Generation Management System - Analog

- wykorzystuje dwa bity z 7-bitowego pola
  - kolejne dwa bity dla APS

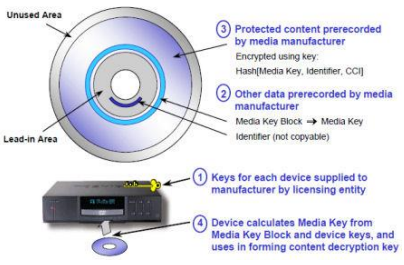
CGMS-A	znaczenie
0 , 0	kopiowanie dopuszczalne
0 , I	wykonano jedną generację kopii, brak możliwości kopiowania
I , 0	można wykonać jedną generację kopii
I , I	brak możliwości kopiowania

Broadcast flag

- dotyczy przekazów cyfrowych
  - obecny we wszystkich odbiornikach standardu ATSC (USA) od 2005 roku
  - w Europie brak standardu
- informuje, czy istnieje możliwość nagrywania danego programu, a także
  - czy można ominąć reklamy
  - czy można zapisać program w wysokiej jakości
  - czy można wykonać kopię z nagranego programu
  - itp.

CSS – Content Scramble System

- opracowany w 1996 roku
- zabezpiecza materiały zapisane na płycie DVD-Video oraz DVD-Audio
  - wymaga „współpracy” nośnika, napędu i oprogramowania do odtwarzania
  - klucz o długości 40 bitów
- obecny wyłącznie na tłoczonych płytach



http://www.manifest-tech.com/ce_products/content_protect.htm

CSS – Content Scramble System

- uniemożliwia skopiowanie danych z płyty DVD na dysk twardy
- stosowanie CSS wymaga uiszczenia opłat licencyjnych
- powiązany z kodowanie regionalnym
- złamany w 1999 roku przez Norwega - Jona Lecha Johansen (w niecałe dwa lata po pojawieniu się DVD-Video)
  - soft o nazwie DeCSS

AACS – Advanced Access Content System

- odpowiednik CSS dla płyt Blu-ray i HD-DVD
- specyfikacja opublikowana w 2005 roku, pierwsze płyty HD-DVD i Blu-ray pojawiły się w I. połowie 2006 roku, zabezpieczenie złamane w grudniu 2006 roku przez „muslix64” (soft o nazwie BackupHDDVD)

AACS – Advanced Access Content System

- podstawowe różnice w stosunku do CSS
  - materiał zakodowany za pomocą „title keys” o długości 128 bitów z użyciem AES (Advanced Encryption Standard)
  - każdy odtwarzacz posiada unikalny zestaw kluczy – *decryption keys* (w CSS grupa odtwarzaczy)
    - teoretycznie można wyeliminować nawet pojedyncze odtwarzacze

AACS – Advanced Access Content System

- wprowadza ograniczenie rozdzielczości na wyjściach analogowych do 960x540 pikseli
- teoretycznie umożliwia zarządzanie procesem wykonywania kopii
- obecnie wersja AACS2 dla potrzeb formatu Ultra HD Blu-ray

BD+

- kolejne zabezpieczenie oferowane przez format Blu-ray
  - jego istnienie przyczyniło się do zwycięstwa formatu BD nad HD-DVD
- rodzaj wirtualnej maszyny za pomocą której można uruchamiać programy zawarte na płycie Blu-ray w celu
  - sprawdzenia poprawności kluczy
  - sprawdzenia czy odtwarzacz jest bezpieczny
  - kontrolować wyświetlane treści
- złamane w listopadzie 2007 roku przez twórców AnyDVD HD

BD Mark

- ostatnie z zabezpieczeń na płycie Blu-ray
- polega na wytłoczeniu na płycie dodatkowych danych (znaku wodnego) identyfikujących źródło i współpracujących z AACS
- ma zapobiegać masowemu kopiowaniu pirackich płyt

HDCP - High-bandwidth Digital Content Protection

- zabezpiecza przed nieautoryzowaną transmisją danych między urządzeniami AV
  - kodowany jest każdy piksel, a klucz (56b) jest uaktualniany co ramkę
- opracowane przez Intela
- korzystanie z HDCP wymaga opłacenia licencji
- teoretycznie możliwość stworzenia czarnej listy urządzeń

HDCP - High-bandwidth Digital Content Protection

- wyróżnia się trzy typy urządzeń
  - źródło (source)
  - odbiornik (sink)
  - repeater
- polega na wymianie kluczy między urządzeniem źródłowym (np. odtwarzacz Blu-ray) i odbiornikiem (np. telewizor LCD)
  - brak obsługi HDCP przez dane urządzenie (odbiorcze) uniemożliwia przesłanie obrazu i/lub dźwięku (lub ograniczenie jakości)
- dostępne urządzenia eliminujące HDCP, włączane między źródło a odbiornik

HDCP - High-bandwidth Digital Content Protection

- złamany w 2001 (przed praktyczną implementacją w jakimkolwiek urządzeniu) przez naukowców-kryptologów
  - w 2010 upubliczniono odtworzony poprzez kryptoanalizę klucz główny HDCP, efektywnie niszcząc cały system
- obecnie rozwijane wersje 2.x (najnowsza 2.2)
  - wykorzystują inne kodowanie (m.in. AES 128)
  - sprawdzają czas transmisji sygnału między źródłem i odbiornikiem (musi być poniżej 20ms)
  - wymagane do transmisji 4k
  - również złamane