

Technical measures scenarios

- eMusic.com
 - members have email address and password to access site
 - uses SSL (Secure Socket Layer) for authenticity of eMusic to customer, privacy of connection between eMusic and customer
 - downloaded files in unencrypted standard (MPEG 1, audio layer 3 -- AKA MP3)
 - accessible with any device/software that decodes MP3
- Archambaultzik, Puretracks, Napster Canada
 - members have name/password to access site
 - downloaded files are in Windows Media Audio (WMA), encrypted using Windows Media DRM
 - only compatible with Microsoft Windows (No Apple, Linux, etc) running Microsoft Media Player
 - files only useable on devices which contain Microsoft keys and run Microsoft software
- iTunes
 - Members have name/password to access site
 - downloaded files are in encrypted standard (MPEG AAC) using Apple keys
 - requires iTunes software (Mac and Windows) which manages downloads and synchronization with devices
 - Files only usable on devices which contain Apple keys and run Apple software
- CDs
 - Red Book Audio file format did not include encryption mechanism
 - All so-called "copy control" on CDs are done with media defects (which behave differently on different devices) or contain software that is intended to be automatically installed (infect) computers while not impacting traditional devices
- DVDs
 - DVD format included encryption, with keys used for region encoding and multimedia data
 - region encoding done in DVD drive firmware, with all DVD drive manufacturers required to sign license agreements with DVD CCA (Copy Control Association)
 - multimedia data encoding in device software, requires manufacturer specific decryption keys created by DVD CCA
 - Encryption is weak enough that decryption can happen without key

- Blu Ray, HD DVD, etc
 - Uses Advanced Access Content System (AACS) "standard"
 - Uses strong encryption, facilitates multiple scenarios
 - Keys can be unique to model (rather than just manufacturer), or in some cases unique to device (broadcast encryption)
 - Entire software stack must conform to requirements of content producers for them to encode their content in your key. This leads device manufacturers and software authors to author for the lowest common denominator (least features to actual customers)
 - Master key has been found/distributed multiple times (Search for "09f9")
- Rogers Digital Cable
 - Uses proprietary PowerKey Conditional Access System, by Scientific-Atlanta
 - Allows for two-way communication between individually keyed set-top boxes and a key server at cable company, allowing different programming to be accessible or inaccessible to individual keys.
 - Only compatible with systems using the PowerKey software, which has been offered as a hardware module to plug into compatible third party devices.
 - Receivers are fully under the control of Rogers, including automatic software updates/etc. Device may be 'possessed' and even 'paid for' by cable customers, but clearly owned/controlled by Rogers. Most people rent.
- Bell ExpressVu / Starchoice
 - Bell ExpressVu uses Nagravision, Star Choice uses a DigiCipher 2-based system
 - Systems have changed over time and required firmware updates
 - Only one-way communication used (less secure)
 - Uses customer specific Conditional Access (CA) SmartCard
 - Firmware upgrades under the control of Bell.
- Sony Playstation / Microsoft XBox / Nintendo *Wii*
 - Security mechanisms involving secure boot where the BIOS will only load and run software signed by the manufacturer.
 - Vendor retains full control over console, allowing them to decide what software can and can not run. Game designers must get approval/digital signature from console manufacturer in order to author/ship games.
 - The term "mod chip" has been used to describe techniques to unlock these devices so that the owner, rather than the manufacturer, can decide what software will run.
- Apple iPhone/etc
 - Similar to game consoles in that Apple retains full control over what software can be installed, requiring app developers to get approval/signatures from Apple
 - Apple iPhone fans call it "jail breaking" when owners unlock the device
- Trusted Computing
 - Specification from the Trusted Computing Group
 - Includes a "Trusted Platform Module" (TPM) that would be included in computer hardware which can do cryptographic operations internal to the hardware (separate from main CPU)
 - Security concepts: Endorsement key, Secure input and output, Memory curtaining / protected execution, Sealed storage, Remote attestation
 - Has both non-controversial security enhancing and controversial security-removing uses
 - It all comes down to the "key" question: who is maintaining the keys, who is the technology being used to secure against
- Many others....