Chapter 5 - Understanding Access Control and Digital Rights Management

Kenny Inthirath

Summary

With the advancement of computing and its pervasiveness within recent decades, the flow of information has never been greater than it is today. With each day that passes, information is only growing, not declining. However, all information is not intended to be viewed, used or modified by the general public. Access control (AC) is the selective restriction of access to a place or other resource [1]. Although the idea or methodologies of access control is certainly nothing new, today’s flow of information should be under scrutiny of some form of access control.

Digital Rights Management (DRM) is a modern implementation based on access control. DRM is intended to protect the intellectual properties (IP) of its creators in today’s world of technology. The pervasiveness of modern technology has empowered end-users in a multitude of ways; not only does modern technology act as an access point to a significant amount of information but technology is able to provide very easy ways to execute, copy and alter said information in an unintended manner. If the content creators wish to protect their IP, some form of DRM must be implemented in order to control use of their content as they intend.

Overview of Access Control

This paper takes a look on a modern day implementation and usage of AC and its importance in DRM. By understanding AC thoroughly, the inner workings of modern DRM systems can be understood thoroughly as well. AC is commonly associated with confidentiality, integrity, and availability of information. We’ll take a general look at what defines an AC system, its usefulness, different implementations of AC in modern systems, and its relation to DRM.

Access control (AC) is the act of controlling access to resources at its most basic level. AC often is used as a ‘what and when’ model of security—that is what/who has access and to when/what can they access? AC in its general understanding can be found in almost every corner of the world. For example, most people do not let strangers in their house, and even if they chose to, the owner of the house still controls who/what has access to their house demonstrating a basic form of access control. While basic in its highest level concept, AC can be a very powerful methodology and is necessary to many information systems around the world.

AC systems have defining security policies that are adhered to by security models which can be implemented through different security methods. A bit confusing at first, an AC framework can be compared to construction plans with each component explained in the following paragraphs.

Security policies are not limited to AC systems but can be found in design processes, network administration, and other like mechanisms to ensure that an entity such as an
organization or system is secure. Security policies are guidelines that do not explicitly tell you how to incorporate those guidelines. Overall goals are there but details are not. Security policies detail documents that express concisely what protection is needed and what defines a secure state for the system. In our construction plan analogy, it is very similar to blueprints of a house where the document represents the overall framework for the construction project but lacks the details to actually build the house and thus it is up to the construction firm on how they wish to build it.

Security models are interpretations of security policies and are the detailed implementation and incorporation of those guidelines. Security models map techniques necessary to enforce the security policies represented by mathematics and analytical ideas. Four common models will be covered in this paper: Mandatory Access Control (MAC), Role Based Access Control (RBAC), Discretionary Access Control (DAC) and Rule Based-Role Based Access Control (RB-RBAC). In our blueprint example, a security model would be the detailed plans on how to carry out construction of the building, electrical, plumbing and various other systems.

Access control methods are techniques used to implement security models that align with the respective model. Methods can be broken down into two categories, Logical Access Control (LAC) and Physical Access Control (PAC). LAC focuses more on AC through permissions and account restrictions whereas PAC utilizes physical barriers to prevent unauthorized access. Each category has various implementations depending on the security model chosen. In our construction analogy, access control methods can be thought of the specific materials to use in the electrical or plumbing system implementation.

**Mandatory Access Control (MAC)**

An access control model that enforces security policies independent of user operations [2]. Only the owner has management of the AC and inversely the end user has no control over any settings for anyone. The two common models associated with MAC are the Bell-LaPadula model and Biba model.

The Bell-LaPadula model was developed and is still in use for government and military purposes focusing on confidentiality. The model works by having tiered levels of security where a user at the highest level can only write at that level and nothing below it (write up), but can also read at lower levels (read down). If one does not have the correct clearance level, then they should not be able to access that information since it should be unassociated with them.
The Biba Model is almost converse to the Bell-LaPadula model and focuses on integrity rather than confidentiality. A user with lower clearance can read at high levels (read up) and a user at higher levels can write for lower levels of clearance (write down). This way higher clearance users can inform lower level clearance users.

**Role Based Access Control (RBAC)**

RBAC provides access based on a position given to an individual in an organization. This model is reminiscent of a many-to-one relation where instead of an individual being assigned many permissions, the individual is assigned a role which has one-to-many relation to the appropriate permissions.
Discretionary Access Control (DAC)

The least restrictive model, DAC gives complete control to any object a user owns along with the permissions of other objects associated with it [3]. While DAC is least restrictive it is also the least secure model.

Rule Based-Role Based Access Control (RB-RBAC)

A model that dynamically changes roles of a user based on certain criteria set by the owner or system. A user may have access during certain time of day, days of the week, etc. While the possibilities are endless for which rules are set, it may quickly become complicated in larger scale systems.

Sandbox

Often times, many different systems, programs and software need to be tested to a certain extent before being production ready. If a system were to be deployed without testing into a real-time environment, many unintended consequences may come of it. Factors such as stability and security are typically the two biggest worries. Good practices indicate deploying these systems into a sandbox environment.

A sandbox creates an environment where resource access is limited in order to isolate itself. Through limited resources, sandboxing can be considered a form of AC. The permissions given are tightly controlled for both incoming and outgoing operations. The term sandbox will not have direct effects on the underlying system and thus users can ‘play in a sandbox’ separate from the rest of the system. When operations are requested, they are checked by the sandbox’s AC system. The design of the AC system will determine how isolated a sandbox environment is and thus the sandbox idea is not limited to one set of policies.
The design of the AC system depends on the software being tested or testing procedures. The goal of a sandbox is eventually integrate the new system eventually in the production environment and thus each sandbox will have different requirements to test and thus different levels of access to different resources.

**Case Study: HPAnywhere**

With the mass adoption of smartphones and other such capable devices, the policy of Bring Your Own Device (BYOD) has become a hot topic in many workplaces and institutions in today’s society. Due to the computational power of smartphones, low cost and wide availability they have increased innovation and productivity in many lives over. The benefits can be carried through a traditional workplace if employees were able to use and have resources provided for their personal smartphones for work. This can potentially cut company cost by not having to purchase as much hardware, but more importantly take advantage of the ability to consume data anywhere, anytime provided by smartphones. However, many security issues are raised when the policy of BYOD is considered. IT departments must make sure that these devices comply with company security standards, compliances and are generally acceptable to use within such an environment.

Hewlett-Packard’s (HP) solution to mobile devices in the work place comes in the form of the HPAnywhere platform. HPAnywhere provides a secure container environment for HTML5 based mini-applications (miniapps). Miniapps are developed using HTML5 ensuring cross platform compatibility between mobile operating systems and are then placed on an HPAnywhere server. Each application has its own Java based backend application that can be called by the miniapp using RESTful webservice which acts as the business logic to a backend resource. The power of HPAnywhere comes with the platform acting as a secure middleman between mobile devices and resources behind corporate firewalls; this intermittent connection creates a secure channel between personal devices and corporate resources in the form a smartphone application.

A user first provides login credentials in the HPAnywhere app for smartphones. The login credentials are connected to a reverse proxy who returns a session cookie allowing the phone to access resources behind a corporate firewall. Once the cookie is received, the user has access to the HPAnywhere server. Since the miniapps are stored on the server, each miniapp is loaded on demand. However, HPAnywhere provides another form of access control in administration of the miniapps.
By pairing a Lightweight Directory Access Protocol (LDAP) group with each miniapp, the user only has access to the miniapps associated with the LDAP group the user is in. This reduces redundancy in providing a single service sign-on solution. Miniapps do not need to implement their own authentication process which would be needed otherwise to ensure that correct access in a normal smartphone environment. Instead, the user is already authenticated by logging on to the HPAnywhere server and then the platform simply checks the user’s role to see if they have access to a miniapp based on their role in the organization as defined by their associated LDAP group acting as a form of RBAC.

Pulling data from another backend resource behind the corporate firewall is also completed by using the single sign-on service provided by HPAnywhere. By having the session cookie, the user is already authenticated into the corporate network and thus can use the same session cookie to authenticate with other backend resources as defined for each miniapp.

The end result is a platform powered through the notion of AC providing a secure solution to the BYOD dilemma. When properly designed, the benefits of an AC system can provide the needed security to enable a highly valuable system in both traditional and innovative ways.
Overview of Digital Rights Management (DRM)

DRM is the practice of imposing technological restrictions that control what users can do with digital media [5]. By explicitly creating barriers in digital goods, DRM acts as an authenticator to ensure correct usage of digital media as intended by the content creator in the interest of protecting their intellectual property (IP). DRM enforces polices after the content leaves the trusted environment of the creator. Essentially DRM tries to recreate such a trusted environment with the end user. By encrypting the content, a damaged good is created. Without a proper trust environment, the content is restricted barricading access leaving unusable content potentially preventing unintended use in-order to protect the IP.

DRM today is commonly associated with music, movies, games and software with the intent of copy-prevention and anti-piracy measures. However, DRM encompasses more than copy-prevention techniques. By acting as a form of AC, DRM technologies monitor the executing, copying and altering digital content. It is an effective enforcement of policies to grant the correct permissions to authorized users.

The DRM system model represents a flow of information and money to four different entities. The content provider is the creator of the digital content and serves two functions:
supplying the protected content to a distributor and the usage rules to a license manager. The distributor passes on the protected content to the consumer and receives payment from the licenses manager. The license manager pays royalty fees for each license sold to the consumer as well as paying distribution for each product delivered to the distributor. The consumer may purchase the product from the distributor but is exchanging money for the digital license.

The system model represents an efficient flow of information and money in the business model aspect of an end-to-end DRM system. More importantly it outlines the flow of two important factors: the flow of information in relation to the flow of money. While not all DRM systems align with the above model, it is a general model that represents most DRM systems at a higher level aspect. Some differences could include the content provider taking on the role of licenses manager and distributor, or even a model where content is free yet still employs a form licensing such as GNU General Public License depending on how the creator defines the content’s policies.

Digital licenses act as the end-user policy in a DRM system. Licenses express the usage rules of the content as defined by the creator. Users do not purchase the IP itself but rather a usage license which often outlines a few common factors such as frequency of access, expiration date, as well as copy and transfer rights. The licenses must match the business model in which the content is to be distributed though schemes such as rental, subscription, freeware, pay-per-use, etc.
History of DRM

While the distribution of copyrighted material is nothing new, there has always been a fear of new media technologies. One of the better known examples comes from a congressional hearing in 1982 where the Motion Picture Association of America (MPAA) proclaims “I say to you that the VCR is to the American Film producer and the American public as the Boston strangler is to the woman home alone” [6]. While hyperbolic in description, it shows the extremity of what the MPAA thought of the VCR at the time and the capabilities many media industries feared. The Recording Industry of American (RIAA) expresses similar sentiments in a 1990 hearing. “For many years, the music industry has been gravely concerned about the devastating impact of home taping “.

While iterations of new technologies were being released, content providers became increasingly skeptical and the fear of unintended and illegal circulation continued to increase. Content media giants begin to war with piracy by forcing prevention measures upon all consumers, legitimate or not. The industry that deemed prevention measures must be taken into account was (and still are) financially and politically strong organizations with seemingly little opposition at the time. It can be said that their interest was in maximizing and securing profits by this new standard they sought to impose by protecting their IP.

One of the first legislation to be introduced was the Audio Home Recording Act (AHRA) in 1987. The arrival of a new audio medium Digital Audio Tapes (DAT) allowed consumers to make their own recordings with quality comparable to compact discs. The recording industry lobbied for legislation in the U.S. that required the production or import of DAT recorders to include copy-control techniques. While the music industry had already opposed home taping, they did not want to integrate such a possibility for this to become a standard in the U.S. Through lobbying, threats, and market pressure, the recording industry was prepared to have strict regulations in the sale and purchase of DAT recorders. One of the consequences of the harsh opposition kept DAT recorders out of U.S. stores for years in favor of the recording industry. Eventually the recording industry and electronic industry came to an agreement that let consumers legal right to make noncommercial recordings for personal enjoyment and manufacturers the legal right to help them do so and eventually became law in 1992. AHRA was quickly outdated.

The rise of home computers as entertainment systems quickly became a reality. A revolution began with royalty-free copying and distribution of music through the ability to burn CDs for use in personal CD players and cars. Even later, the widespread popularity of peer-to-peer systems became prevalent in the home music revolution thanks to the internet. AHRA did not cover the unforeseen revolution and thus the home computer based distribution was unregulated. While there were still AHRA regulated devices and methods to consume music, consumers preferred disc copying and file-sharing methods due to the regulations not present due to its convenience. Thus AHRA became outdated and really only served as a stepping stone into future DRM implementations.

Digital Millennium Copyright Act (DMCA)

Perhaps the most known and controversial copyright law in recent memory, the Digital Millennium Copyright Act (DMCA) was a dramatic change to copyright law due to the
forthcoming digital age. The DMCA criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works. [6], with three different bans or stipulations the first follows as “No person shall circumvent a technological measure that effectively controls access to a work protected under this title” [6]. The second ban prohibits manufacturing, importing and trafficking in tools aid in AC DRM circumvention. The third ban prohibits tools to circumvent DRM systems that do not block access but prevent unauthorized copying or alteration.

By 1994, the internet was becoming more commonplace as the number of users would begin to come into the tens of millions within the next few years. Copyright holders came to fear the age of the internet and quickly developed policies to address of online copyright infringement. Media industries threatened to boycott the internet as a media outlet if stronger copyright laws were not put in place. By seeking to force internet distribution through DRM systems backed by the law, copyright holders were guaranteed an initial form of protection by criminalizing circumvention of the AC provided by DRM systems.

The impact of DMCA created a significant shift in copyright law using it as a means for regulation of technology. AHRA had only regulated a small class of technology whereas DMCA can potentially regulate an infinite number of devices. Any copyrighted work that is digitized can be wrapped in encryption and thus falls under regulation of DMCA.

One of the most notable cases appeared in 1999 when the infamous Napster became a mainstream service. At its peak, Napster had 80 million registered users, and while there had been other forms of file-sharing through a peer-to-peer program, Napster specialized in audio files in the form of mp3. Napster gave the ability to acquire almost all of the music in the world for free. The recording industry began suing Napster which led its eventual shutdown in 2001. Despite the shutdown of Napster, more and more technologies came in its place and while they come and go, they still remain prevalent in today’s world. P2P software is still readily available as well as widely used. While multiple attempt to control its proliferation through legal means, it has not worked.

Media industries began to target the user base by suing copyright infringers creating a large spectacle regarding public relations. Some users sued included single mothers, deceased individuals and even teenage girls. Again, the litigation brought forth did not have much effect on the use of P2P. What ensued was a public relations nightmare for many companies. The public outlook on such cases was ill-received garnering and becoming an object of hatred for many young people and technology enthusiasts across the nation. The public support for to stop copyright infringers are not apparent and continues in that direction today because of the large hindrance created in most DRM systems.

Since DMCA has had such an adverse effect on copyright laws, it began as a precursor to many hot topics surrounding the World Wide Web today. Bills such as the Stop Online Piracy Act (SOPA) or Protect IP Act (PIPA) came from the fundamentals presented in the DMCA. These bills are constantly in the public eye as they represent many issues in user privacy, subjugation to mandatory AC, and other means of scrutiny by the government. Again, those in favor for these bills tend to be large content corporations who seek to shape the landscape through lobbying and litigation. However with the pervasiveness of technology and age of social networks, many end users who would be affected are aware of such moves. There is a constant struggle between both sides to find middle grounds as interest generally differ.
While the DMCA still exists today, it’s not to say that all DRM is negative. There are successful implementations of DRM systems that come to terms with users in a positive manner. One of the biggest issues with DRM today is the hindrance it can provide through strict access and maintenance. When content providers offer a convenient and appealing way to users, many users choose to opt-in due to the ease of use of the model. When content providers force a clunky system onto users, it only harms users in the end leaving distaste.

**Modern DRM Technologies**

**Music**

Arguably the first implementation of forced DRM in digital media, music DRM systems are generally still prevalent in Internet Music but once were found in Audio CDs. DRM systems found in Audio CDs controlled access from the media player’s perspective. Some implementations included installing software on a user’s computer without notification [11]. There were cases where the DRM software had significant vulnerabilities not initially recognized. Other hindrances including platform specific playback and while the DRM systems limited the ability to copy music, there were still many work methods to circumvent those systems. In the end, the cost of DRM outweighed the results they wished to achieve and thus most Audio CDs today have little or no DRM measures.

Many internet music stores at one point implemented DRM into their music services. These DRM measures normally limited playback to specific software or playback devices.
Services such as iTunes had limited playback of music purchased through their store to Apple certified software or devices (iTunes, QuickTime, iPods, iPhones, etc.). While these measures provided some copy-protection, the main problem is that music purchased from different services was often interoperable (due to specific platform DRM measures). Eventually, many music services recognized that their DRM systems may lower sales shrinking their market share to other services that provide DRM-free music and thus many services begin offering DRM-free music but still discourage sharing of the music.

A successful method to appease customers in the realm of music downloads is to create a service more convenient than other software that infringes upon copyright. Two prominent features are convenience and reasonable pricing. Subscription based services offer a convenient way to access a large catalog of music at a reasonable price and many users opt-in to using a DRM enforced player the tradeoff between song availability. Spotify for example is a very popular service where music can only be streamed not downloaded in a Spotify player, but can be free at the cost of audio ads. The premium service provides a reasonable price and is generally more convenient than buying a library of music. Because of the business model Spotify chooses to use, it has won over the support of a large portion of the market showing that AC through DRM does not equate to intrusive methods.

Fig 7. Spotify Business Model [8]
Software and Computer Games

Software and computer games have implemented various forms of DRM throughout recent decades. Many forms of its modern implementation have been intrusive and frustrating for many users legitimate and otherwise. One of the most common methods is through the use of serial keys. The content can only be accessed if a legitimate serial key is provided by the user normally in the form of an alphanumeric string.

Another approach is to limit the number of times a software or game can be installed. By keeping track of how many times a serial key is used, the software will only work given it is within its approved limit. Many users however (as with other forms of DRM) regularly experience frustration. Software may become unusable even though it has only been used on one computer either by performing unexpected tasks that warrant as a separate install such as upgrading operating systems or reformatting the hard drive.

Persistent online authentication is yet another form of DRM for software and games. By constantly requiring a connection to an authentication server, the software or game access is only granted so long as the user is connected. By creating such a strict trusted environment, it forces the user at their convenience to meet the requirements meaning that the software or game is unusable without an internet connection.

Some games and software’s DRM may be related to its piracy rate. By forcing such an intrusive DRM measure, it may often be easier (and more convenient) to the user to just pirate the game than go through official channels in a legitimate setup though it may not always be the case. While the methods of enforcement advance, the ability of end users to circumvent AC still and will continue to prevail. DRM in this case acts more as a deterrent that is forced on all users with the possibility of problems arising because of its requirement.

However some DRM methods are much less intrusive than others. For example, the PC games platform Steam ties purchases to a personal account. While the user may not be able to sell, trade or give access to other users, it provides many benefits of convenience to the user. Having a centralized location, fast-download speeds, social aspects, availability between multiple devices, low prices as well as other features benefit the end user greatly. Many users aren’t even aware of the DRM enforcement other than providing login credentials and games cannot be traded or sold. Because of the business model of Steam, many users willingly opt-in benefiting the users, publishers and managers of Steam to create a thriving PC gaming ecosystem.
Film and Video

Film and video DRM systems are delivered in 3 main mediums: physical disc based, digital file formats and through internet streams. While generally unobtrusive to playback, the DRM seeks anti-copying measures.

Physical disc based methods are deployed on almost all disc formats. It is a simple and inexpensive measure to deter piracy by having hardware decrypt encrypted video. As long as a user has purchased a legitimate copy, most playback devices are able to access the content without much effort given support by the player.

Digital file formats share more similarities with music DRM-measures where certain playback is affected by the software used and from where the video was purchased.

Streaming video is quickly becoming a popular way to view video content online. Some services do not bother with any form of DRM to protect users from capturing data while it is streaming, however it requires a lot more effort. The main form of AC comes from subscription or pay-per-view services. These are enforced by creating unique sessions for authorized users that cannot be created elsewhere. For example, Netflix as a video subscription service implements Microsoft Silverlight which creates unique viewing sessions every time a video is requested. However it does not come without the occasional hiccup. Netflix requires supported browser and equipment, and while it has a large support matrix, not all equipment is supported. It also introduces limited access and resources are ultimately controlled by Netflix as the user does not have access to a personal copy. Video streaming services are able to add and redact content with little or no notice to the user.
Closing DRM Statements

While DRM provides an important way to protect copyrighted IP, it can also lead to many disservices to both content creator and end users. DRM revolves around the idea of access control in which resource availability is monitored and given only to authorized users. DRM measures are often forced upon the end user thus creating restrictions and limitation for the users. Some methods are unobtrusive while others are problematic to the point of non-usability. DRM enforcement was greatly influenced by the recording industry in the late 80’s and early 90’s as they feared losing monetization from new technologies that allowed distribution of content to be out of their control. Large corporations aimed to regulate control of their distributed content as much as possible through lobbying for new legislation while being backed the forces of the law. While protecting copyrighted IP is important to the copyright holders, many poorly designed systems are implemented at the cost of the end user.

The fear of monetization loss shaped the laws that are in place today. While there was opposition along the way, the corporations who backed mandatory DRM measures often had the financial and political resources to achieve their goals. There was no central way for the public to shift the law in their favor at the time many of the laws were drafted and introduced. In a world connected heavily through social media, the public awareness is much greater than before. As more people share their DRM related experiences, the public opinion and, more importantly,
public voice has a greater presence. The relation between industry and consumers is an interesting one primarily in the fact that they rely upon each other yet are often detrimental with industry imposing DRM and consumers partaking in piracy. While both sides are sometime detrimental, they do not represent either side holistically which is where the disparity comes in on the topic of DRM enforcing it on all users.

While most DRM systems are mostly looked down upon by the public, it is largely necessary to sustain IP protection and income for many copyright holders. While corporations continually look for a way to eliminate piracy through litigation, it is only a temporary solution and only shows the stride of public disinterest in DRM as the users constantly find and provide a growing number of alternate solutions. At the same time, end users continue to hurt content creators through exploiting their systems. A possibility to the problem is that both sides are looking at the extreme end of the spectrums with corporations trying to maximize as much profit through restrictions and users looking to maximize convenience which may entail not paying royalties. A middle ground should be found in order to please both sides. Such a solution that could please the majority of both parties already exists. Looking at existing business models of popular services such as Spotify, Netflix and Steam alleviate much of the tension and problem created by the need for DRM. These solutions create a healthy relationship between creator and consumer and are popular for a reason, because users feel the price and experience is worth opting in for. The popularity of these services only shows that new design methods and business models must be created in order to sustain in today’s internet age rather than holding on to failing practices that have not worked before. Both sides must be informed on what needs to be done rather than resemble a power struggle.

Access control is essential, and while too much may be a bad thing, not enough can be as well. DRM is based on the idea of access control which has shown to be immensely useful yet and its current state is counter-productive because the content of information it controls involve legal issues. While there are two sides, the idea of access control began with good intentions and it is with good intentions how DRM should be carried out, from both sides.

References

[7] Domain Seizure Image

[8] Spotify Business Model Image

[9] FBI Warning Image

[10] Microsoft Silverlight Architecture