Digital Rights Management:
Letting your data out with the lid still on the can

Jeff Baird
GSEC Practical, Version 1.4b
Aug 25, 2004

Abstract

Digital Rights Management (DRM) is an emerging software technology designed to help companies maintain control of their data, on and off the company network. There are many threats to a company's data: theft, tampering, accidental deletion, etc. DRM works with a company’s existing IT infrastructure to protect documents against these threats by utilizing encryption, digital signatures, and other technologies. Of course, implementing a system this complicated requires careful planning and consideration. Information systems and policies/procedures may have to be changed or added in order to insure a successful installation. When it comes to protecting and tracking sensitive information, DRM provides benefits that can be essential to an organization’s success.

1. An Overview

“Get what you can, can what you get, and sit on the lid.” That is how my dad has described some people's attitude towards life. That could seem like a good approach to handling sensitive data too, if it weren't for the fact that doing business efficiently seems to require companies to share confidential information. Outsourcing and other close business relations often make it necessary for internal data to go external. However, once it leaves a company's network, the risk of theft, tampering, unauthorized copying, etc. increases. Data can be at risk even when it is only used internally. How does a company provide information to those who need to have it and keep it away from those who do not? Digital Rights Management.

What is Digital Rights Management?

Digital rights management is the digital management of permissions (who can do what) and auditing (who has done what), of your information regardless of its physical or electronic location. With digital rights management (DRM) a protected file can be on an internal server, your backup tapes, or a competitor's hard drive, and the person attempting to access it must have permission before they can view, edit, print, or perform any other controlled action on it.

Different uses of DRM today

DRM is basically used for two different purposes: a) To keep customers from redistributing digital content (primarily in the music and movie industries), or b) To protect and/or track corporate data. This paper focuses on the protection of corporate data also referred to as Enterprise DRM (or E-DRM).

This protection and tracking has different uses:

Limiting who can do what with a document or email message:

- Protecting the data when it is traveling on laptops. In the event of theft, the laptop user's account can be disabled, rendering the information on the device unreadable.
- Only allow users to do what they need to do. Microsoft explains the reason for this in its technical overview of its Windows Rights Management Service:

> Relying on an individual's discretion to determine to[sic] the manner in which they use and share digital information can introduce an unacceptable degree of risk into an organization's security model. For example, it's easy for users to mistakenly forward sensitive e-mail messages or documents to recipients who have malicious intent.[1]

Auditing/Tracking usage of documents:

- Complying with new government regulations that require more thorough auditing procedures or greater protection of customer information
- Enforcing company policy

Streamlining business processes:
Adobe presented an example of this in one of their whitepapers:

> For example, one U.S. agency is using digitally signed Adobe PDF documents to process grants online for several hundred grantees. The agency drafts a funding agreement and sends the Adobe PDF file to a grantee via the Internet. The grantee opens the Adobe PDF document, digitally signs it, and sends it back via the Internet to the agency's office. The agency then digitally signs and stores the Adobe PDF document for its records. Since deploying this system to manage the grant process online, the state has significantly reduced processing time from weeks to just a few day [sic], providing better service to its citizens and realizing significant cost savings. Additionally, the agency has nearly eliminated paper use, resulting in dramatic cost savings in office supplies as well as reduced expenses for postage and courier services.[2]

This use of DRM could also be used internally to speed a policy change review, or some other business process that requires a record to indicate that several people signed their approval of a document.

The uses of DRM are varied: limiting access, tracking usage, streamlining business process. Each of these are designed to solve today's business problems. The question that still remains is: what problems are companies dealing with and how can DRM help solve them?

[1] Microsoft Corporation. "Technical Overview of Windows Rights Management Services for Windows Server 2003." 3 Dec. 2003. Download from URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/rmenterprisewp.mspx(8 Jun. 2004).

[2] Adobe Systems Incorporated. "Protecting Electronic Documents with Adobe Security Solutions." Sep. 2003. URL: http://www.adobe.com/security/pdfs/acrobat_security_wp.pdf (30 Jun. 2004).

Why do we need it?
Many businesses today are using electronic communications and closer partner relationships with other businesses to drive efficiency and stay competitive. While these methods are often effective in achieving their goal, they have also brought new threats to business information.

One of the major threats is the theft and unauthorized copying of confidential information. This has become expensive and too pervasive to ignore. The 2004 CSI/FBI Computer Crime and Security Survey lists it as the 2nd most costly computer crime[3], and in a survey by CSO magazine 15 percent of the 476 senior security executives who responded, "said that their employer had lost or had critical documents or corporate information copied without authorization in the last year."[3] Almost another quarter said they couldn't be sure.

Though probably not normally classified as a threat, recent legislation could require you to secure your information and track its activity more closely. Sarbanes Oxley requires you to control access to corporate financial data, test those controls, and prove that you have done so. Another example, the Health Insurance Portability and Accountability Act (HIPAA), requires organizations that handle patient information keep that data confidential.[4]

Most security solutions focus on defending the perimeter and lines of communication, and as such, a company has no way of knowing or controlling what happens to their sensitive information after that. Firewalls, VPNs, and encryption can all be worthwhile security measures, but they don't address new questions. What happens when the data is moved or copied? How do we know it was copied and who copied it? DRM is designed to help solve these problems.

Where does DRM fit in a business' information systems?
Evaluating a system such as DRM can easily cause one to ask, "Where does this fit in with the rest of my information systems?" After all, it is not always clear whether this is a business process application that aids security, or a security application that aids business processes.

Actually, the answer to both of those questions is, "Yes." Businesses use identity management, work-flow automation, content management, and numerous other systems to help manage their business processes and direct the way those processes work with the people that run them. DRM helps them do that securely. When a company has this capability, they can expand the use of their information. In other words, who can see it and what they can do with it. This will tend to result in faster and better informed decisions.

[3] Roberts, Paul. "CSI, FBI Survey Finds Hack Attacks Down, Again." csoonline.com.au. 11 Jun. 2004. URL: http://www.csoonline.com.au/index.php/id;225934261;fp;16;fpid;0 (23 Jul. 2004).

[4] Adobe Systems Incorporated. "Protecting Electronic Documents with Adobe Security Solutions." Sep. 2003. URL: http://www.adobe.com/security/pdfs/acrobat_security_wp.pdf (30 Jun. 2004).

One example of this is identity management. “Identity management is the concept of centralizing the control of resource provisioning and system access.”[5] DRM extends identity management by controlling access to documents and email. DRM and authentication/identification systems, such as biometric devices or Microsoft's Active Directory, are often integrated to make sure that changes in any one system are consistent across all systems, which happens to be one of the goals of identity management.[5]

How does DRM work?

Evaluating how a digital rights management system can solve current business problems, requires an understanding of what its capabilities are and are not. To form a basis for that understanding, here is a description of how a DRM system works.

While the processes used by each DRM solution differ, sometimes significantly, they all seem to follow these general steps:

1. The system is setup and connected to a database of users.
2. An authorized user enters some information into a piece of supported client software.
3. The client software either attaches the rights information directly to the file or stores the rights on a server and associates them with the file. The file is then encrypted; it is now protected. In some cases the DRM system assigns the rights automatically according to administrator-defined settings. Other systems or configurations allow/require the user to assign them to the document themselves.
4. The document is put into “circulation” (sent out by email, stored on the LAN, etc) Sometimes the “document” is an email. To handle the special characteristics of this format, some vendors provide solutions that integrate directly into email client or server systems. This allows the DRM software to offer more specific controls, such as limiting to whom a message can be forwarded or if it can be forwarded at all.
5. Using the client software, a recipient attempts to open or manipulate the document in some way (edit, print, take a “screenshot” of it, etc).
6. The client authenticates the user through the server software and checks the rights associated with the document to find out whether to allow or deny the action.

DRM can provide more flexible, transparent security than other technologies, but it is still dependent on current infrastructure. It protects the data no matter where it goes, but the clients and servers must be able to communicate for that information to be useful. This is the basic ability and restriction of DRM.

2. How does DRM improve Security?

As with any new piece of a security infrastructure, it is important to understand how DRM fits into your overall security plan. It is also good to know what aspects of the

[5] Pannell, Paul. “Exploring Identity Management.” 4 Dec. 2002. URL: http://www.sans.org/rr/papers/71/866.pdf (27 May 2004).

system or information DRM can help to protect[6], and how DRM fits in with the other security tools already in place.

CIA-UAP Analysis

Using a framework when analyzing the security of your data, provides a systematic way to evaluate what you need and what a system provides. Confidentiality, integrity, and availability are three common principles used in evaluating the security of a system. In the book *Fighting Computer Crime, A New Framework for Protecting Information*, Donn Parker presents three more aspects to consider: utility, authenticity, and possession[7].

Let's look at how DRM fits in with each of these aspects. Since some of these are very similar or unclear in their meaning, I have followed each term by a short description to help define it in the context of DRM:

Confidentiality – *I can see the information because I'm allowed to, and you can't because you're not.* - Files are encrypted, and "cannot" be viewed without permission. This protects the data even if it is intercepted while in transit or stolen while in storage. For example, in a system that is properly used and configured, copies of secured documents all have this protection whether they are on backup tapes, laptops, and telecommuters' hard drives. Without such a solution files can easily go unprotected whenever they are off the internal file server.

Integrity – *The information is complete, accurate, and free from unauthorized changes.* - Encryption, digital signatures, and controls such as expiration dates help insure that the information stays unaltered and current. Digital signatures work with encryption to identify the signer and to detect changes in a file. If an unauthorized change were to be detected in a document a client could mark it as such or even refuse to open it.

Availability – *You can get it when and where you need it.* - DRM may not increase the reliability of your delivery systems, but it does allow you to make data more freely available to trusted or semi-trusted parties because its safety is no longer restricted by where it goes.

Utility – *"Usefulness of information for a purpose"*[8] Due to its greater availability, the information can now be used by more people for more tasks. For example, a certain user would be able to make better decisions if they could view a weekly report. However, due to the confidentiality of that report, that user should not be able to change, print, or forward it. DRM would allow that information to be provided with the necessary limitations, something encryption or digital signatures cannot do by themselves. Because DRM allows you to limit a user's actions, a given level of trust can be given the appropriate privileges. This allows more people to do more with the information.

[6] Reworded from: Cole, Eric, et al. SANS Courseware, Book 1.2: Defense In-Depth. N/A:The SANS Institute, 2004. 15.

[7] Cole, Eric, et al. SANS Courseware, Book 1.2: Defense In-Depth. The SANS Institute, 2004. 17.

[8] Parker, Donn B. Fighting computer crime: a new framework for protecting information. John Wiley & Sons, Inc., 1998. 240.

Authenticity – *It really is what it says it is, and it really is from whom is it says it is from.* - Digital Signatures help insure that the information is from who it says it is from, and allow the client program to check for unauthorized modifications.

Possession – *Who has it.* While DRM does not help you maintain possession of your document files, it does help make the matter of who else has them irrelevant.

Of the six areas addressed here, DRM directly improves three: confidentiality, integrity, and authenticity; in the other areas it assists or enables other systems in their provision. For example, while information can be more available because a DRM system is protecting its confidentiality, it does not really make that data available itself. This is important to keep in mind when assessing the impact a DRM system would have on data security.

Defense-in-Depth

When looking at the security of a network, the layered or "Defense In-Depth" model can be used to help determine where a new system fits in relation to other security systems, and how well different areas of your information systems are secured. The system can be thought of as a new layer in the network's security map. One such model would be to divide your information systems into Network, Host, Application, and Information layers[9].

From this perspective a DRM system forms a new layer directly over the data by protecting it through encryption anywhere it goes, including backups, copies on remote laptops, etc. It does not prevent an attack on your network, your host computers, or the applications that run the system or display the information. Hence this is the only layer in which it would fit.

3. Security considerations when preparing for and setting up a DRM system

The careful planning required to successfully implement a DRM system should involve at least three checks:

1. Make sure it will work with the other security systems in place,
2. Have the proper policies and procedures in place, and
3. Ensure that the system is properly configured.

Failing to consider these areas will most likely prevent the system from solving the target problem, document security. Not only that, other problems will be caused such as software conflicts, confused and inefficient people, and/or a false sense of security! This is not a step you are going to want to skip!

Infrastructure Considerations

Adding DRM to your security infrastructure can place new requirements on existing sections. These requirements may include reconfiguration, upgrades, or completely new systems. Two of these sections that stand out are the authentication system and network availability.

[9] Cole, Eric, et al. SANS Courseware, Book 1.2: Defense In-Depth. The SANS Institute, 2004. 12 - 14.

Since most DRM applications integrate into current authentication systems, the DRM system relies on them for much of its security. You are going to want to make sure this critical piece of infrastructure can handle the new load. This may mean implementing two-factor authentication, or other more advanced technology than the simple username and password. Moving to a more advanced authentication system can be a large move in and of itself, so some DRM providers have helped ease this transition by building support for smart cards and other authentication technologies into their products. As the gate to a company's information, an authentication system must be strong enough to keep attackers at bay.

There is also an increased dependence placed on your network's availability. Unless they have been previously authorized, DRM clients have to be able to communicate with a DRM server to authorize the actions their users are requesting. Hence, if the external connection to a company's network goes down, any users without a direct connection to the company's internal network lose access to a document, if they have not previously been granted permission to use that document offline. Thus, the cost of an availability compromise greatly increases along with the value of your network's availability. This is especially notable since the 2004 CSI\FBI Security Survey listed Denial-of-Service as the last year's most costly attack;[10]

Deploying a DRM system can be a great money-saver, but it isn't without risks and requirements. Strong authentication systems, multiple points of access, and good policies and procedures to keep it all running smoothly can go a long way towards a successful DRM implementation.

Policy and Procedure Considerations

Defining a set of policies and procedures prior to implementation is a major step towards ensuring that a DRM system runs smoothly and effectively. What is this system supposed to be used for? How is it to be used? Who is in charge of maintaining it? Answering these questions lays out a set of guidelines and rules ahead of time which will help keep users “out of the fog” and information secure.

Since the purpose of a security policy is to define who should do what and why[11], be sure to define the necessary responsibilities when modifying or appending your security policy. These responsibilities basically fall into two categories: system setup/maintenance and system usage. System maintenance would be tasks such as defining user rights and managing document rights categories. System usage policies cover the users' end of the process by defining their role in protecting company information. Both of these work together with procedures to ensure that the users and administrators of the system use DRM effectively as a tool to protect your company's data.

A DRM system should also have a set of procedures to compliment the policies by specifying how, when, and where the policies are to be carried out.[12] Procedures tend to fall into the same two categories as policies: system setup/ maintenance and system

[10] Roberts, Paul. “CSI, FBI Survey Finds Hack Attacks Down, Again.” csoonline.com.au. 11 Jun. 2004. URL: http://www.csoonline.com.au/index.php/id;225934261;fp;16;fpid;0 (23 Jul. 2004).

[11] Cole, Eric, et al. SANS Courseware, Book 1.2: Defense In-Depth. The SANS Institute, 2004. 86.

usage. If a DRM system ties directly into current authentication systems, the process for internal user maintenance probably already has a procedure. However, if there are any external users, they may need to be maintained separately. By clarifying the policies, a good set of procedures will help keep a DRM system effective.

Time Considerations

Everyone has to take time into account when planning a DRM implementation: “How long will it take?”; “When do we see a return on investment?”; among others. One of the potentially less obvious considerations in choosing and setting up a DRM solution is, “How long do your documents need to remain secure?” This decision will help determine the strength of the encryption needed.

DRM provides a large part of its benefit by making the possession of a file irrelevant to its data's confidentiality (in theory). As such the assumption must be made that anyone could get the file and try to extract the information from it by trying every possible key, also known as “brute force” cracking. If a key is too weak (short), the encryption can be broken in an unacceptably-short amount of time and the data exposed.

One example of this is RC4, a popular encryption algorithm also used in securing web site communications. When used with 128-bit keys, data encrypted with this algorithm can be expected to resist brute-force cracking beyond the next decade. The technology to be able to break that size of key in a reasonable amount of time is not estimated to be available until at least the year 2020[12].

On the other hand, a 40-bit RC4 key was broken in 8 days in 1995 with just over a hundred machines working on it. There wasn't a lot of computing power involved in this crack either. In the words of Damien Doligez, one of the first to complete the crack, “You would get roughly the same speed as I did on a network of 40 to 50 high-end Pentium(R) PCs.”[13] (Given that this was in 1995, that would be the original Pentium(R), and not later versions of the Intel processor) Given how far computing power has advanced since then, this clearly is not strong enough to protect even the least sensitive or most rapidly outdated documents.

Some DRM products provide the ability to choose the strength of the encryption used on the documents, others simply use a default strength. Either way, be sure the encryption level is secure enough to protect your critical information for its entire lifetime.

Server Considerations

If the computer on which your DRM server is running were to be compromised, the entire system would be at serious risk. Much of that risk can be limited by properly positioning that computer on your network, appropriately hardening it, and giving it the necessary perimeter defenses. You will have to determine just how much the DRM server is worth, and that will be determined by how valuable your data is.

[12] Ricadela, Aaron. “Quantum's Next Leap.” Information Week May 10, 2004 (2004)

[13] Doligez, Damien. “SSL challenge virtual press conference.” URL: http://pauillac.inria.fr/~doligez/ssl/press-conf.html (29 Jul. 2004).

One of the main considerations is where the server (or servers) should be on the network. Most DRM systems need to be able to connect to your existing authentication and identification system. Many DRM applications also deal with moving data outside the company. If this is the case, the server will also need to be accessible from outside networks. If it is only used internally, of course, that access can be blocked.

“What is depending on this server?” The answer will determine just how much time and money you want to spend to secure it. Do you need a dedicated server? If it is just protecting the salary amounts of the employees in your department from snoopers or accidental exposure, it probably isn't justifiable. Whereas if it is protecting price negotiation data or customer information, the cost of a server and the staff time needed to maintain it could be very small compared to that data's value.

Other considerations when choosing and setting up a DRM system
Because DRM systems encrypt their content, they could interfere with a content or document management system trying to scan or index documents for searching and access. Some DRM vendors provide the ability to integrate with such systems via a Software Development Kit. An integration project of this sort would obviously require extra time and money for a development team whether it is internal or external.

Servers, policies, hardening, encryption, threats! With so many areas to consider, just choosing a DRM system may seem like more trouble than it is worth, let alone implementing one! As with any choice, evaluate the costs if you don't and the costs if you do.

4. What's Next in DRM?

A DRM system can and must solve problems with today's technology, but such an investment can bring even greater returns by taking potential future technologies into account. From expanding where DRM is used to allowing it to interact more closely with other business systems, there are many possibilities for this newly emerging technology.

The proliferation of mobile devices, namely PDAs and PDA/Cell phone combinations, the increase in their document-handling capabilities, and their ever-expanding wireless connectivity would suggest that DRM clients for these devices are not too far away. This would tend to increase the security of such devices, which would allow them to be used for even more purposes.

Standards such as XrML can help the industry grow by allowing DRM systems to interface with other DRM systems and business applications. Should DRM systems become widespread, the cost associated with using DRM to interact with partners outside your organization could drop significantly, since, in theory you would no longer be as directly involved with managing external users' rights. Widely adopted standards could also allow document management systems and collaboration software to also work well with DRM. Some of this is already happening, and as the market continues to mature, I'm guessing that it will expand.

5. Conclusion

By applying protection directly to electronic documents and managing the rights centrally, digital rights management can help companies maintain control of their sensitive data without losing their competitive edge. Implementing such a system takes careful planning and an understanding of where it fits in a business's information security structure and the cost involved. However, for those situations in which DRM fits well, this technology can help a company get the most out of its data and still maintain the necessary control.

Works Cited:

Microsoft Corporation. “Technical Overview of Windows Rights Management Services for Windows Server 2003.” 3 Dec. 2003. Download from URL: http://www.microsoft.com/windowsserver2003/ techinfo/overview/rmenterprisewp.mspx(8 Jun. 2004).

Adobe Systems Incorporated. “Protecting Electronic Documents with Adobe Security Solutions.” Sep. 2003. URL: http://www.adobe.com/security/pdfs/acrobat_security_wp.pdf (30 Jun. 2004).

Roberts, Paul. “CSI, FBI Survey Finds Hack Attacks Down, Again.” csoonline.com.au. 11 Jun. 2004. URL: http://www.csoonline.com.au/index.php/id;225934261;fp;16;fpid;0 (23 Jul. 2004).

Pannell, Paul. “Exploring Identity Management.” 4 Dec. 2002. URL: http://www.sans.org/rr/papers/71/866.pdf (27 May 2004).

Cole, Eric, et al. SANS Courseware, Book 1.2: Defense In-Depth. N/A:The SANS Institute, 2004.

Parker, Donn B. Fighting computer crime: a new framework for protecting information. John Wiley & Sons, Inc., 1998.

Ricadela, Aaron. “Quantum's Next Leap.” Information Week May 10, 2004 (2004).

Doligez, Damien. “SSL challenge virtual press conference.” URL: http://pauillac.inria.fr/~doligez/ssl/ press-conf.html (29 Jul. 2004).

Other resources:

Wheeler, Mark. “Human + Documents = Security Threat.” 26 Nov. 2003. URL: http://www.scmagazine.com/features/index.cfm?fuseaction=FeatureDetails&newsUID=060850c1-c8d7-494f-a230-ff48d4fae01b&newsType=Features (6/30/04).

Becker, David. “Software makers ready desktop lockdown.” 20 Apr 2004. URL: http://zdnet.com.com/2100-1105-5194756.html (8/2/04).

Horwitt, Elisabeth. “Rights of Passage.” Safe House Spring 2004, Vol. 4, No.1 (2004).

Whitepapers from Authentica (www.authentica.com) and Liquid Machines (www.liquidmachines.com) were also consulted to get a feel for the options available. Access to both of these whitepapers required providing the respective websites personal information. There was no charge.