Security Requirements for Digital Rights Management

Mayur Kamat
Mays Graduate School of Business, Texas A&M University
College Station, Texas -77840
Tel: (979) 268-6726
TRACK: Leading Edge and Emerging Technologies
Student-Faculty Proposals

ABSTRACT

Recent Gartner survey on IT spending shows that the top priority for budget allocation is security. Huge efforts have been targeted to improve and build upon existing security domains. This paper addresses a topic that adds a new dimension to the realm of security, which can lead to the emergence of a new market for online content. The concept is of *Digital Rights Management* (**DRM**). DRM introduces new business models for content protection, rights managing and secure marketing. It enables the publisher's revenue model by rights enforcement and secure deployment.

The paper attempts to:

- List the reasons favoring adoption of DRM
- Enumerate the security concerns in DRM implementation.
- Discuss tamper-resistant software as a plausible solution.
- Conceptual design of the client-side trusted software component.
- *Super Distribution*, multi-level marketing phenomena to distribute content.

Keywords: Content marketing, rights management, security, superdistribution, trusted software

The paper proposes a technology, which demands academic and industry research before it can be fully implemented and exploited. The paper proposes system that has shown technical and financial feasibility. It opens up a market where the initiative has been taken, only proper co-ordination and support is required. A concept that adds a new dimension to the realm of security. One which can lead to the emergence of a new industry altogether. The concept is of *Digital Rights Management* (**DRM**).

Before delving into the concept of DRM, we start with the need for such a technology. The general consensus is that solutions are plenty and they can be directly applied to any digital domain. But what runs the Information market? Web-portals? Dotcoms? IT professionals? **NO**. Its content that is the lifeline of information technology. And if you are banking your entire business on content, then it becomes invaluable. Till today, no need has been felt to protect this content. **Information Technology**. The industry has long concentrated on the technology part of IT. This is one of the reasons for failure of Dotcoms and antecedent of the recession that we all love to talk about. There is a need today to focus on the Information domain of IT.

Web pages, music, video, E-books are what constitute the majority of the content on the web. And it is just a matter of couple of keystrokes to duplicate this content. The Loss? Site statistics show a decline and so do the finances.

Implementing makeshift solutions has led to the failure online content distribution model. No publishers are willing to spend money publishing their books online just for the fear of losing revenue. The music industry is still reeling from the after-effects of Napster and peer-to-peer music piracy, which is claimed to have generated huge losses. So the users are forced to revert to their normal style of consumption at the expense of convenience and cost.

One of the key challenges in the move from physical to electronic distribution of content is the rapid evolution of a set of common technologies and procedures to identify, or name, pieces of digital content. A widely implemented and well understood approach to naming digital objects is essential if we are to see the development of services that will enable content providers to grow and prosper in an era of increasingly sophisticated computer networking.

One of the key challenges in the move from physical to electronic distribution of content is the rapid evolution of a set of common technologies and procedures to identify, or name, pieces of digital content. A widely implemented and well understood approach to naming digital objects is essential if we are to see the development of services that will enable content providers to grow and prosper in an era of increasingly sophisticated computer networking.

For some companies, the key business decision may be to determine what kind of content will most quickly recover costs if it is migrated to the online medium. This requires editorial and marketing judgments such as:

- Identifying what content the customers actually *want* online.
- Identifying *why* would they want it online

This also requires knowledge about '*who'* the publisher's customers are since the publisher needs to know how the content will impact them, what they will buy and how they will buy. Customers have different needs and will pay different rates depending on whether they are:

- Individuals
- Organizations
- Educational Institutes

Another question that needs to be answered is that which business models are most suitable for content marketing

- Pay-per-piece
- By prior subscription
- By a combination of the two.
- By Super Distribution.

2. DIGITAL RIGHTS MANAGEMENT

DRM can be defined as digital enabling of right holder's revenue model by rights enforcement and secure deployment. It is not management of digital rights but it is Digital management of rights. This is a very important distinction that eventually enlarges the scope of DRM and also widens its horizons as far as applications and marketing goes. DRM means applying technology to provide content online securely and reliable and manage all rights that come a part n parcel of the content. They may be the normal copyrights as defined by the Copyright Law or special rights specific to the content.

The paper concentrates on the security requirements of digital rights management, which is also the most important aspect. Security is a weakest link phenomenon, hence sufficient efforts need to be diverted in this field of DRM.

3. DRM SECURITY REQUIREMENTS

The Internet is a ubiquitous and a capable medium for content distribution and marketing. Using automated tools, content manufacturing, distribution and accountability can be easily implemented at

minimum cost at same time delivering appreciable performance during peak demand. But at the same time, the very ubiquity of the Internet makes it prone to several security vulnerabilities.

Security, though not the favorite topic of any system analyst, is a thriving industry today. Computer security research and development over the last decade has focused on malicious code such as Trojans (SubSeven) and the large family of computer viruses that seem to multiply as days go by. There is anti-virus software available by the tons. The Java sandbox was developed specifically to address the risk of malicious Java applets. You have firewalls for every feasible platform. You also have network scanners like SATAN for network vulnerabilities. In short, there are practical, though not perfect, solutions for network security.

The security model for DRM differs substantially from typical Internet security models, which in general rely on components deployed in trusted environments. For example, companies rely on web servers and applications for Ecommerce because they deploy these in a trusted environment with restricted physical access.

In DRM, the situation is reversed. Content providers must deliver content to legitimate users across a hostile network to a user who has to be assumes hostile as well. This requires the content provider to rely on a trusted entity residing on the user's player device; the trusted entity must represent and enforce the interests of the content owner

The user must be assumed to have complete control and access to the hardware and software that provides access to the content; the user must also be assumed to have an unlimited amount of time and resources to attack and bypass any content protections mechanisms. DRM, hence, requires an entirely different security model, which also requires unique solutions.

In most security solutions requiring protection, we resort to cryptology. Traditional cryptology is A sending B a message, which only B can understand. This model has always assumed that both A and B can be trusted and that they know some secret (key), which C wants.

In the DRM security model, even B can't be trusted. He can't be trusted with any keys or even the unencrypted data. As a matter of fact, B must assumed to be hostile, not naive. Cryptography is an important element of DRM for protecting communications and stored digital content but it is not the complete solution.

Successful deployment of DRM systems requires a trusted software component on the user's computer or device to perform integrity checking, to decrypt the content and to enforce the usage rights associated with digital content. The malicious host security model means that DRM software must preserve its integrity in an extremely hostile environment. This software must be able to perform the integrity checking and hide the decryption keys, in the presence of hostile watchers and attackers.

Trusted Software Component

Trusted end user devices are a foundation component in the delivery of intangible goods. These devices must provide content providers with a high degree of certainty that they are delivering content to authenticated, trusted devices and specific authorized users. But the security mechanisms used on these devices must be cost effective to implement, virtually transparent to the end user and designed to adapt to new security paradigms and transactions that require DRM related security services.

Trusted software is a key requirement for any DRM system. Tamper-resistant solutions must be highly portable to accommodate the heterogeneous environment the future will bring. Finally, tamper-resistant software technology must be considered for the entire chain of trust to provide an end-to-end solution.

Trusted software agents can be downloaded to user's content players and be trusted to enforce the interests of content owners. Since these software agents will be deployed in hostile environments, they must be made tamper-resistant. Tamper resistance software offers the convenience and cost-effectiveness of a software-only solution.

The trusted software agent must satisfy the following requirements:

1. Reverse-engineering-proof
2. Tamper resistance
3. System Portability

At the heart of implementing TSA, is the **tamper resistance software (TRS)** technology. TRS technology is based on mathematical techniques and the application of cryptography to protect the agent against reverse engineering and tampering attacks.

The following abstract is taken from NICKERSON, CHOW, JOHNSON, AND Y. GU, Cloakware Technologies: '*Tamper Resistant Software (TRS) offers a temporal window of protection to software executing on a hostile host. TRS in various implementations has been proposed over the past five years. Despite being a uniquely powerful solution to the survivability of information in this environment, TRS has not seen widespread use on any front. We believe that the lack of a method to transparently and automatically convert source code from a native form*

into a TRS form has been the major impediment to common usage of TRS and the protection it affords.'

What we basically do in TRS is that along with the source code, we also include 'entropy' in the code. This works like the CRC checksum bits used in digital communication. If the TRS code is modified, then the entropy changes which can trigger corresponding events that can foil the hacker attack. TRS can be implemented at source level (unlike other techniques which work at binary level) and hence can offer portable solution to the content protection problem.

To implement TRS, we perform *'Spoof Coding'* which involves:

1. Changing order of instructions (without logical complications)
2. Inserting spoof code
3. Incorporating source-level encryption-decryption program.

Various automated TRS generators are available via individual agencies. The solution they offer varies in features and complexity but the output is generally satisfactory. Though this has to be taken with a pinch of salt because it is not the panacea to all DRM problems. It is an evolutionary technique, which has to be tried and tested before it can get mass following.

What the trusted software component is intended to perform is integrity checking and content decryption at the client side. Assuming the client is hostile and has infinite time and resources to break through the software, what the solution must provide for is that even if the hostile client manages to break through the TSC, what he will be getting is meaningless bytes and not breakpoints. This is achieved using TRS.

TRS ensures that the sensitive elements of the TSC, i.e. the content storage and decryption modules, are now protected against tampering. This gives publisher the guarantee that his content is being distributed only to those people who have made legitimate purchase of the same and that the content remains confided to this realm only and illicit trading or piracy of that content is prevented.

The paper proposes a simple design of the TSC, which is shown in the figures section. The figure is a top-level component diagram. It shows the functional modules of a trusted software component, each catering to particular DRM transaction. Most important aspect of the diagram is that it segregates modules based on their security sensitivity and hence suggests that certain modules need to be isolated and specially designed later so as to satisfy the needs of the problem.

4. SUPERDISTRIBUTION

A fascinating concept assumed to be originated from Japan. It is a radical way of thinking and marketing software products.

Need

Large amount of capital and resources are required for production of goods. Both for tangible good and software products. But it's the ease of duplication the later case that raises concerns of copyright management and protection. Distribution of software or content (or being specific to our case) is a matter of few seconds. This liability makes it difficult to adopt same markets and distribution techniques as that of the hard-copy content. But the concept of Superdistribution changes the way we look at this electronic content and allows us to use this liability as an asset for creating new markets via a new distribution mechanism.

Concept

Superdistribution (Mori and Kawahara 1990) is the idea of free dissemination of content through a network. No restriction whatsoever is imposed on the distribution of content or the intermediary involved. Users are charged based on the use of the content and not its acquisition. However, users cannot use the content until payment is received by its rightful owner. This concept arises from the fact that the current technology allows a piece of software to keep track of its usage but not it's copying and distribution. Superdistribution allows for increased revenue for content owners. The same content holder who previously was presumed to be a potential source of piracy is now a potential sale channel for the content owner. For the consumers it provides easy and anytime access to content at a lower unit price. The lower unit price may be achieved due to the potential for large number of users. Users also will benefit from the flexibility offered in terms of the degree or the type of usage. That is, in a case where the content offers several services, consumers pay only for those services that are used.

The concept of Superdistribution implies *'metered'* billing for products or services. This concept arose from the fact that it is possible for software to keep track of its usage but it's practically impossible for software to track its copying and distribution. So when we remove all restrictions on distribution and charge the user based on the use of the product, we fundamentally nullify the effect of piracy and expand our market way beyond its current horizons.

Superdistribution Requirements

To implement this environment, a stable and trusted architecture must be deployed. An architecture for superdistribution should address the following requirements:

User and Content Identification - Unique content identification is required to track the content throughout the information supply-chain, from the publisher to the end users. This facilitates billing mechanism and usage tracking. User identification is also imperative to uniquely distinguish users, rights, usage monitoring, fiscal transaction tracking, and commission generation and payment.

Rights enforcement - Rights are assigned to users based on the services they are willing to pay for. The users pay only for what they use. It must be assured that the usage rights are enforced. Uniform Rights Description language and enforcement mechanism can be utilized for this purpose. (OMA Approved Specifications: Rights Expression Language Version 1.0, 2002)

Accounting module - The accounting module keeps track of the revenues generated, usage of content, payments received and commissions payments if any. It requires existence of uniform user and content identification.

Security - A trusted defense mechanism is required to ensure the integrity of above three aspects in a hostile environment.

Concerns

As with any new technology or marketing strategy, there exist certain concerns. Superdistribution is not an exception. As the concept is in its rudimentary stage, there are bound to be varied reactions from the market. Producers are not going to go overboard right away and embrace this concept. It'll take time. Questions of efficiency of this system are bound to be raised. Infallible techniques never existed but pragmatic solutions are possible to derive. Superdistribution is a pragmatic solution to the concept of software marketing and enabling content distribution.

CONCLUSION

There is a need today, to explore new markets by seeking a technology that offers potential for growth and substantiation and which is not totally unknown to the user. DRM epitomizes such a technology.

Solutions that offer easy access to content, while maintaining compliance with copyright, will result in the successful adoption of information products. If, through tracking customer preferences and interests, publishers and intermediaries can serve customers with new, targeted and individualized buying opportunities, they will maintain a sustainable customer base.

From this perspective, the widespread adoption of the DRM will enhance the establishment of a vibrant E-commerce marketplace for digital content. This new marketplace will go well beyond simply migrating today's print, music, video, software and other forms of content to the online environment. Instead, it will offer the publishers, the ability to present the content in new and flexible forms tailored specifically to highly targeted audiences. This will allow publishers to capture additional incremental revenue over the same base of digital assets, provided the publisher uses the DRM to actually manage those assets, repackage them in various ways, sell them and control their access rights. In addition to these incremental sales and profits on the revenue side, DRM will certainly reduce costs throughout the entire production and distribution chain, once content producers link their systems more efficiently.

There is enormous publishing industry support for DRM, including the Association of American Publishers, International Publishers Association, the Software & Information Industry Association and many individual publishers. The intention is there. Only consistent efforts are needed-both on the sides of technology (to provide infrastructure) and industry (to adopt the technology). Hitherto sidetracked issues have to be brought to the forefront and given the due that they justly deserve. Security has to be beefed up using combinational technologies (H/W and S/W) but not limiting to only those discussed in this paper. With academic research, consummate with the DRM hype, in the technical and business aspects of DRM, a viable industry solution can be arrived at, which can be the precursor of a new market to immerge.

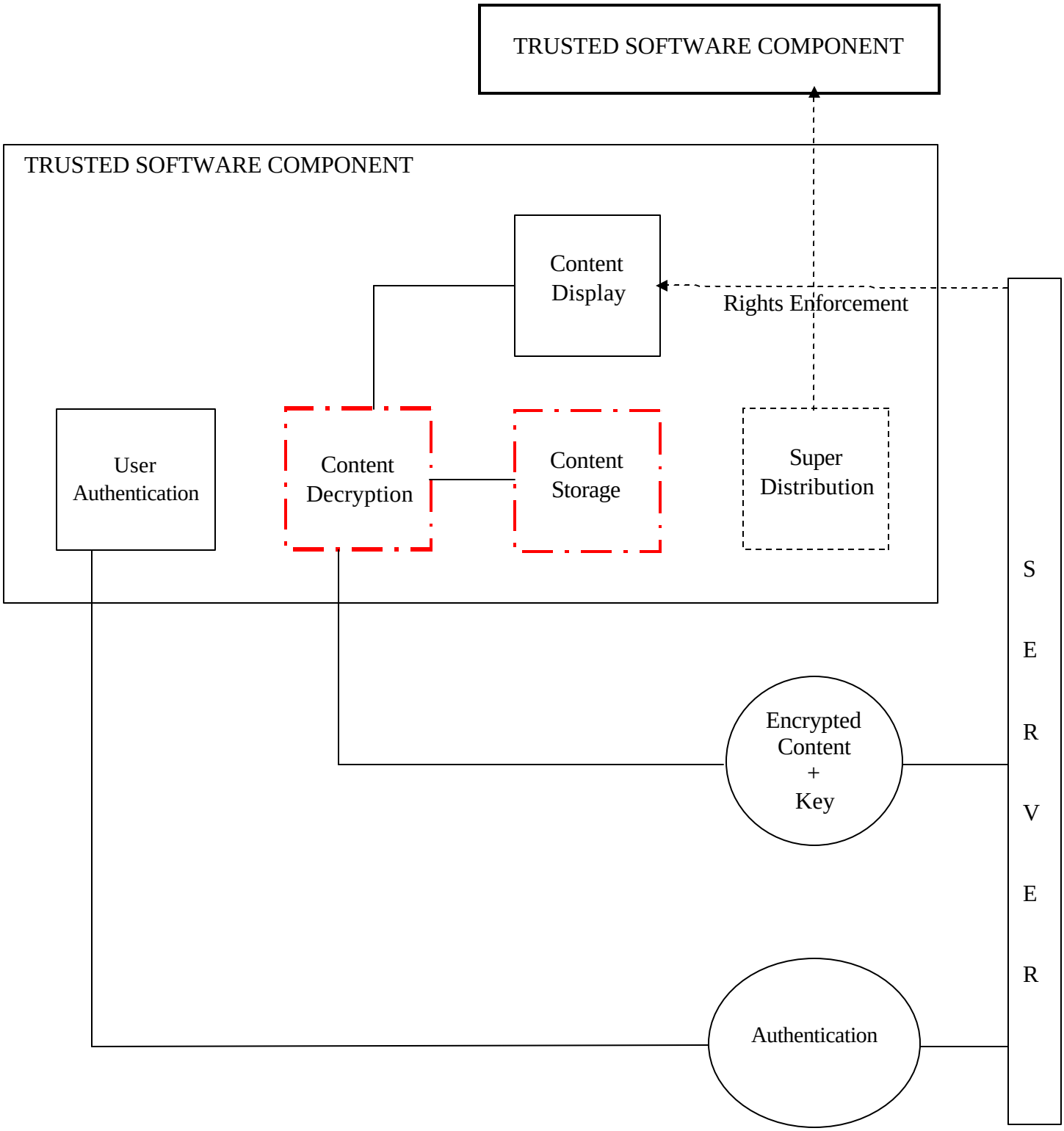

Figure 1: Functional Modules of a client-side trusted software component

References

1. **DOI Handbook (www.doi.org)** - Official site of the International DOI Foundation that offers the digital object identifier services so as to uniquely identify content online, which in turn facilitates content marketing. The site documents all aspects of the universal identifier with detailed documentation regarding system policies, administration and resolution.
2. **Content Guard** (www.contentguard.com / www.xrml.org) - Content Guard is the joint venture of Microsoft and Xerox Inc. The firm tries to address the challenge of lack of common standards of rights management by encouraging the adoption if its eXtensible Rights Markup language (XrML), which extends the range of right-enabled business models applicable to digital content as well as web services
3. **DMD Secure** (www.dmdsecure.com) - DMDsecure, Digital Media Distribution Secure, is a leading independent software vendor of server-side software components and applications embedding Digital Rights Management (DRM) and Conditional Access (CA) technologies.
4. **W3C Consortium on DRM 2000** (http://www.w3.org/2000/12/drm-ws/) - Workshop on DRM conducted by W3C. The workshop had 41 papers reviewed on various aspects of DRM, which make a good reading for a person, new to this field.
5. **Superdistribution – Brad Cox** (www.virtualschool.edu/cox) - Brad Cox is the founder of Coalition for Electronic Market and an ex-faculty member of George Mason University. He is supposed to be the visionary behind the superdistribution phenomena and his works can be perused at this site
6. **The Encoder Solution to Implement Tamper Resistant Software** – Nickerson, Chow, Johnson, and Y. Gu, Cloakware Technologies (http://www.cert.org/research/isw/isw2001/papers/Nickerson-12-09.pdf) - The paper describes the use of TRS and how it can be generated using a automated TRS generator which has been developed by Cloakware.
7. **Duhl, J. and Kevorkian S., Understanding DRM systems**, IDC White paper, www.idc.com, 2001.
8. **Mori, R. and Kawahara, M. Superdistribution Concept and Architecture**, The Transactions Of The IEICE; Vol.E 73, No.7 July 1990.