# Towards a Multi-dimensional Characterization of Dissemination Control

Roshan K. Thomas
*McAfee Research, Network Associates, Inc.*
*rthomas@nai.com*

Ravi Sandhu
*George Mason University and NSD Security*
*sandhu@gmu.edu*

## Abstract

*Dissemination control (DCON) is emerging as one of the most important and challenging goals for information security. DCON is concerned with controlling information and digital objects even after they have been delivered to a legitimate recipient. The need for DCON arises in many different domains ranging from the dissemination of digital music and movies, eBooks, business proprietary and sensitive electronic documents as well as the propagation of mailing lists in relation to direct marketing. Our goal in this short paper is to present some of the multidimensional technical issues that need to be modeled and understood so as to provide a comprehensive set of DCON capabilities. It represents a first but necessary step in our ongoing work in formulating a family of DCON models.*

## 1. Introduction

Dissemination control (DCON) is among the most challenging goals for information security. DCON seeks to control information and digital objects even after they have been delivered to a legitimate recipient. Control encompasses the usage of the digital object by the recipient (e.g., permission to view a document on a trusted viewer) as well as further dissemination (e.g., permission to distribute a limited number of copies of the document to colleagues but with no further dissemination allowed).

DCON arises in many different forms. A prominent example in recent years is the area of Digital Rights Management (DRM). DRM is concerned with distribution of copyrighted digital content for entertainment, such as music or movies, while ensuring that the revenue stream from this content remains protected. The high stakes in the DRM arena have led to a number of technology, legal and social initiatives that are transforming the entertainment industry. This is reflected in MIT's Technology Review rating of DRM as one of the top 10 emerging technologies that will change the world [4]. Requirements similar to DRM arise in other arenas such as distribution of scientific literature in digital libraries and distribution of high-cost analyst reports. Further, in business proprietary and national security arenas, DCON on sensitive information become mission critical. Intellectual property has been an issue for software of all kinds, and so-called copy protection has been practiced for decades. Other instances of DCON include the need to preserve the privacy of medical information as it is disseminated as well as controls on the exchange of email lists to limit the proliferation of unsolicited email (spam).

The goal of dissemination control is inherently different from the classic security objectives of confidentiality, integrity and availability. Given the diverse contexts mentioned above it is not surprising that the treatment of dissemination control has been strongly driven by the specific context. Our goal in this short paper is to present some of the multidimensional technical issues that need to be modeled and understood so as to provide a comprehensive set of DCON capabilities. It represents a first but necessary step in our ongoing work in formulating a family of DCON models.

Dissemination control has been discussed in the formal literature under the term originator control [1, 3, 5]. However the focus has been rather narrow and the emphasis has been on mechanisms rather than policies. The literature on DRM is also focused on specific technical mechanisms such as watermarking. In our perspective DCON is a vast and policy-rich area. To develop appropriate models we need to understand the components of the dissemination problem and extract common elements and principles. Similar efforts have been successful in areas such as role-based access control [2, 8] and more recently in usage control [9]. Not surprisingly, the dissemination control arena turns out to be much richer than role-based access control.

## 2. High-level decomposition of DCON

Figure 1 shows a high-level decomposition of the DCON space. We distinguish the space along two axes. The vertical axis is related to the value of content being disseminated. This could be driven by the sensitivity and proprietary nature of the contents such as for intelligence reports, medical records, intellectual property etc. Content dissemination could also be driven by revenue generation policies such as in the case of digital entertainment objects like music and video files. There are some cases where the preservation of the sensitivity of contents as well as the driving of content-based revenue are both important.

Proceedings of the Fifth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'04)
0-7695-2141-X/04 $ 20.00 © 2004 IEEE

| | Strength of Enforcement | | |
|---|---|---|---|
| **Content type and value** | Weak | Medium | Strong |
| Sensitive and proprietary | Password-protected documents | Software-based client controls for documents | Hardware based trusted viewers, displays and inputs |
| Revenue driven | IEEE, ACM digital libraries protected by server access controls | DRM-enabled media players such as for digital music and eBooks | Dongle-based copy protection, hardware based trusted viewers, displays and inputs |
| Sensitive and revenue | Analyst and business reports protected by server access controls | Software-based client controls for documents | Hardware based trusted viewers, displays and inputs |

**Figure 1. High-level decomposition of DCON**

The other axis is characterized by strength of enforcement. For the purpose of this paper we consider three categories of strength – weak, medium and strong. Weak enforcement relies on server-side controls only (e.g., IEEE/ACM digital libraries) or weak document controls such as password-based protection of content. These schemes expose unprotected content on the client and the only real recourse in the presence of illegal dissemination is legal enforcement. Medium level enforcement includes DRM[1] schemes on current client-side platforms and digital players such as Windows Media Player and Apple's iPoD platforms. Strong enforcement utilizes trusted hardware to enforce DCON policies and is thus considerably more tamper-resistant and non-bypassable when compared to software based controls. Several trustworthy platform initiatives such as TCPA, NGSCB etc. are moving in this direction [10, 11]. Commercial products in this arena are still to emerge.

## 3. Technical dimensions to DCON

DCON applications demand a wide range of functionality which can be characterized along the multiple technical dimensions shown in Figure 2. The leftmost column shows various functional aspects and requirements that need to be considered when building DCON models (derived from analyzing multiple applications that use some form of DCON). For each functional area, the table indicates a range of simple to complex functionality, as well as strength of enforcement characterized as weak or strong.

**Legally enforceable versus system enforced rights.** One of the first dimensions that came to light in our analysis is the degree of reliance on legal versus system enforced rights. In some domains such as the ACM and IEEE digital libraries, there is very little system enforcement of DCON using DRM and other security technologies. Thus in the presence of any abuse of the contents of these libraries, legal recourse is the only option available to the publishers. Now in the area of payment-based digital music, such as that provided by iTunes, some degree of system enforcement is present. An attempt to play a purchased song on a fourth machine would result in the user being asked to disable one of the three previously authorized machines (maximum number allowed is three).

**Dissemination chains and flexibility.** The simplest form of dissemination involves point-to-point single steps, i.e. the disseminator, such as a server A, disseminates an object to a recipient B, but B is not allowed to disseminate the object any further. A more flexible scheme would allow multi-step and multipoint disseminations. Peer-to-peer sharing (such as in the original Napster model for music dissemination) involved multi-step disseminations where an object released from a server would rapidly be re-disseminated by multiple peers. Incidentally, the rapid spread of spam (junk email) is now attributed to efficient peer-to-peer dissemination by exploited machines.

**Object types supported.** From the standpoint of object models, dissemination of objects such as music, involve read-only objects. However, in many domains, support is needed for modifiable, multi-version, and composite objects. For example, digital libraries (such as that of the ACM/IEEE) distinguish definitive versions from preprints. In the intelligence community, several versions of an intelligence report may be circulated with some versions having undergone sanitizations. Depending on the sensitivity of the contents, each version may be handled differently for the purpose of dissemination.

[1] We use DRM in the sense usually found in the trade press to mean the mechanisms that control entertainment content, and view it as a subset and enabling technology for the broader problem of DCON.

| | Functionality | | Strength of enforcement | |
|---|---|---|---|---|
| | **Simple** | **Complex** | **Weak/Medium** | **Strong** |
| Legally enforceable versus system enforced rights. | | | Reliance on legal enforcement; Limited system enforced controls. | Strong system-enforceable rights, revocable rights. |
| Dissemination chains and flexibility. | Limited to one-step disseminations. | Flexible, multi-step, and multi-point. | Mostly legal enforcement; | System enforceable controls. |
| Object types supported. | Simple, read-only and single-version objects. | Support for complex, multi-version objects. Support for object sensitivity/confidentiality. | Reliance on legally enforceable rights. | System supported and enforceable rights and sanitization on multiple versions. |
| Persistence and modifiability of rights and licenses. | Immutable, persistent and viral on all disseminated copies. | Not viral and modifiable by recipient. | Reliance on legally enforceable rights. | System enforceable. |
| Online versus offline access and persistent client-side copies | No offline access and no client-side copies. | Allows offline access to client-side copies. | Few unprotected copies are tolerated. | No unprotected copies are tolerated. |
| Usage controls | Control of basic dissemination. | Flexible, rule-based usage controls on instances. | Some usage abuse allowed. | No potential for usage abuse. |
| Preservation of attribution. | Recipient has legal obligation to give attribution to disseminator. | System-enabled preservation and trace-back of the attribution chain back to original disseminator. | Attribution can only be legally enforced. | Attribution is system enforced. |
| Revocation | Simple explicit revocations. | Complex policy-based revocation. | No timeliness guarantees. | Guaranteed to take immediate effect. |
| Support for derived and value-added objects. | Not supported. | Supported. | Reliance on legally enforceable rights. | System enforceable rights for derived and valued-added objects. |
| Integrity protection for disseminated objects. | Out of band or non-crypto based validation. | Cryptographic schemes for integrity validation. | Off-line validation. | High-assurance cryptographic validation. |
| Audit | Audit support for basic dissemination operations. | Additional support for the audit of instance usage. | Offline audit analysis. | Real-time audit analysis and alerts. |
| Payment | Simple payment schemes (if any). | Multiple pricing models and payment schemes including resale. | Tolerance of some revenue loss. | No revenue loss; Objective is to maximize revenue. |

**Figure 2. Characterizing the technical dimensions of DCON by functionality and strength of enforcement**

**Persistence and modifiability of rights**. Rights may have to persist along the dissemination chain, as in some models of open software licensing, or they could be modified by the recipient.

**Online versus offline access and persistent client-side copies**. In certain applications, digital objects may be disseminated but clients may not be allowed to make client-side copies. For example, in satellite-based radio services, music is streamed and never stored. In many intelligence community systems, users are allowed to download and view documents but not allowed to save or print. The DCON problem is inherently more complex when client-side copies can be retained.

**Usage controls**. In the simplest case, usage controls prevent redissemination but do not limit the legitimate recipients in frequency or duration of usage. More complex usage controls can enforce such limits on a per instance and per recipient basis.

**Preservation of attribution**. In the simplest case, preservation of attribution (including copyright notices) during redissemination can only be done through procedural and legal controls. More complex functionality would involve system-enabled preservation and trace-back of the attribution chain back to the original disseminator. This is an important requirement in application domains such as that for the intelligence community.

**Revocation**. The ability to revoke rights on previously disseminated objects is an important one, but this is often difficult to enforce on client-side copies. The simplest case would be explicit revocations by the disseminator, but more complex rule-based schemes based on monitoring ongoing conditions are possible.

**Support for derived and value-added objects**. Objects may be derived from or bundled with disseminated objects. The simple cases of DCON would not support this functionality.

Other dimensions of DCON include integrity protection, audit and payment and these can be supported to varying degrees as indicated in the table. It is interesting to note that most revenue-driven services such as retailing of digital music support only a single pricing model. Also, the current pricing and DCON models for digital music don't support the resale of music.

## 4. Summary and conclusions

We have briefly presented a high level decomposition of the DCON space and presented some detailed technical dimensions that exhibit the diversity of requirements that need to be considered in the design of DCON models and schemes. The relevance, priority and level of sophistication of these dimensions vary considerably from one application area to another. Nevertheless, an elaboration and understanding of these individual dimensions and associated dependencies is important to having a unified approach to DCON.

The work presented here is an initial step towards the formulation of a family of DCON models. The richness of the DCON space and associated policies leads us to believe that this effort will inevitably be more complicated than past efforts at building families of models in areas such as role-based, discretionary and lattice-based access controls.


## Acknowledgement

This work was supported by the Advanced Research and Development Activity (ARDA).


## 5. References


[1] Abrams, Marshall, et al., "Generalized Framework for Access Control: Towards Prototyping the ORGCON Policy." Proceedings of the 14th National Computer Security Conference, 1991, pages 257-266.

[2] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn and Ramaswamy Chandramouli. "Proposed NIST Standard for Role-Based Access Control." ACM Transactions on Information and System Security, Volume 4, Number 3, August 2001, pages 224-274.

[3] Graubart, Richard., "On the Need for a Third Form of Access Control." Proceedings of the 12th National Computing Security Conference, 1989 pages. 296-303.

[4] MIT Technology Review Editors. "Ten Emerging Technologies that will Change the World." MIT Technology Review, Jan/Feb 2001.

[5] McCollum, C.J., Messing, J.R. and Notargiacomo, L. "Beyond the pale of MAC and DAC-defining new forms of access control." Proceedings of IEEE Symposium on Security and Privacy, May 1990, pages 190-200.

[6] Jaehong Park, Ravi Sandhu and James Schifalacqua, "Security Architectures for Controlled Digital Information Dissemination." Proc. 16th Annual Computer Security Applications Conference, New Orleans, Louisiana, December 11-15, 2000, pages 224-233.

[7] Jaehong Park and Ravi Sandhu, "Originator Control in Usage Control." Proc. 3rd IEEE International Workshop on Policies for Distributed Systems and Networks, Monterey, California, June 5-7, 2002, pages 60-66.

[8] Ravi Sandhu, Edward Coyne, Hal Feinstein and Charles Youman, "Role-Based Access Control Models." IEEE Computer, Volume 29, Number 2, February 1996, pages 38-47.

[9] Ravi Sandhu and Jaehong Park, "Usage Control: A Vision for Next Generation Access Control." Proc. Mathematical Methods, Models and Architectures for Computer Networks Security, Saint Petersburg, Russia, September 21-23, 2003, Lecture Notes in Computer Science.

[10] The Next-Generation Secure Computing Base: An Overviewhttp://www.microsoft.com/resources/ngscb/ngscb_overview.mspx

[11] The Trusted Computing Group TPM Specification, https://www.trustedcomputinggroup.org/home